T.C.
ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

SAFETY

EMNİYET YÖNETİMİ EL KİTABI

(Safety Management Manual - SMM)

Sivil Havacılık Genel Müdürlüğü Yayınları
Havaalanları Daire Başkanlığı

Yayın No: HAD/T-16

T.C.
ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

EMNİYET YÖNETİMİ EL KİTABI

(Safety Management Manual – SMM)

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ YAYINLARI

Yayın No : HAD/T-16
Yayın Türü : Tercüme
Konu : Uluslararası Sivil Havacılık Teşkilatı (ICAO) tarafından yayımlanan Safety Management Manual (SMM) Doc. 9859 AN/474 dokümanının Türkçeye tercüme edilmiş halidir.
İlgili Birim : Havaalanları Daire Başkanlığı
Baskı : 1. Baskı

İlk Yayımlanma tarihi: Aralık 2011

Bu yayın bilgilendirme amacıyla hazırlanmış olup, yapılacak uygulamalarda orijinal dokümandaki bilgilerin esas alınması gereklidir.

www.shgm.gov.tr

Bu yayının basılı hali Sivil Havcılık Genel Müdürlüğü, Havaalanları Daire Başkanlığından temin edilebilir.

E-Posta: HAD@shgm.gov.tr

ISBN: 978-975-493-034-4

Baskı
Pegem Akademi Yayıncılık
Tel: 0 312 430 67 50 Faks: 0 312 435 44 60
pegem@pegem.net

"Her işte olduğu gibi havacılıkta da en yüksek düzeyde,
gökte seni bekleyen yerini az zamanda dolduracaksın.
Buna gerçek dostlarımız sevinecek, Türk Ulusu mutlu olacaktır."

"As in all other fields, in aviation too you are soon going to fill
the high place that is waiting for you in the sky.
Our true friends will rejoice in this, and the Turkish Nation
will be gratified."

M. Atatürk

Globalleşme ve teknolojik gelişmelere paralel olarak bugün dünyada pek çok sektörde olduğu gibi havacılık sektöründe de büyük gelişmeler yaşanmaktadır. Küresel ölçekte yaşanan tüm bu gelişmeler, Türkiye'de de sektörün hızla büyümesini beraberinde getirmiş, sivil havacılık politikaları dünyanın pek çok ülkesinde olduğu gibi, Türkiye'nin de temel politikalarından biri haline gelmiştir.

Bu kapsamda, Bakanlığımız tarafından 2003 yılında başlatılan Bölgesel Havacılık Politikası, Türk Sivil Havacılığı'nda adeta bir dönüm noktası olmuştur. "Her Türk vatandaşı hayatında en az bir kez uçağa binecektir" hedefinin ortaya konduğu bu tarihten itibaren sektör, olanca hızı ile büyüme eğilimine girmiş ve dünyada % 5 olarak gerçekleşen sektörel büyüme hızı, ülkemizde rekor bir gelişme ile % 30'a çıkmıştır.

Sektörde yaşanan tüm bu gelişmeleri etkin bir şekilde karşılamak amacıyla Bakanlığımız, yeni havaalanları yapmak yerine mevcut havalimanlarının standartlarının yükseltilmesi ve altyapılarının iyileştirilmesi yönünde bir çalışma içine girmiştir. Mevcut havaalanlarınızın kapasite ve verimliliklerinin arttırılmasının yanısıra, uzun yıllar atıl durumda bekleyen havaalanlarımız da yenilenerek hizmete açılmıştır. Böylece, hem havayolu işletmelerimizin yurt içinde sefer düzenledikleri şehir sayısı arttırılmış hem de bu havaalanlarının bulundukları bölgenin ekonomik, sosyal ve kültürel gelişimine ve dolayısıyla da ülke ekonomisine katkı sağlamasının yolu açılmıştır.

Ayrıca, üyesi olduğumuz uluslararası sivil havacılık kuruluşları tarafından belirtilen standartlara uyum sağlamak bakımından mevcut havaalanlarının ruhsatlandırılması ve sertifikalandırılması çalışmaları yapılarak, havaalanlarını faaliyetlerinin uluslararası seviyede emniyetli bir şekilde yürütülmesi için gerekli adımlar atılmıştır.

Hızla gelişen sivil havacılık sektöründeki ihtiyaç ve beklentilerin karşılanabilmesi ve sürdürülebilir bir büyümenin gerçekleştirilebilmesi amacıyla; Sivil Havacılık Genel Müdürlüğü, 18 Kasım 2005 tarihinde yürürlüğe giren 5431 sayılı Kanun ile yeniden yapılandırılmıştır. Bakanlığımıza bağlı, kamu tüzel kişiliği haiz, özel bütçeli bir kuruluş haline getirilen SHGM'nin sivil havacılık faaliyetlerinin gerek uluslararası standartlarda yürütülmesi gerekse uçuş emniyeti ve havacılık güvenliğinin en üst düzeyde gerçekleştirilebilmesi için denetim ve kontrol mekanizmalarının etkinliği arttırılmıştır.

Havacılık sektörünü düzenleme ve denetleme görevlerini yerine getiren otorite konumundaki SHGM'nin bu tür yayınlarının; ilgili tüm kişi, kurum ve kuruluşlara büyük katkı sağlayacağı ve böylelikle ülkemizdeki havacılık faaliyetlerinin sağlıklı bir şekilde sürdürülmesi için etkin bir iletişim ortamı oluşturacağı düşünülmektedir.

Binali YILDIRIM
Ulaştırma, Denizcilik ve Haberleşme Bakanı

Sivil Havacılık sektöründe 2002 yılından itibaren ülkemizde yaşanan büyük ilerlemeler bir çok kesimin hayranlığını kazanmıştır. Bu ilerlemeyi oluşturulacak ulusal kaynak yayınlar ile desteklemek sektörün daha sağlıklı büyümesi ve gelişmesine katkı sağlayacaktır.

Ülkemiz sivil havacılık faaliyetlerinin düzenlemesi, denetlenmesi, mevzuat oluşturulması ve yaptırımlarda bulunulması konularında kanunla yetkilendirilen Sivil Havacılık Genel Müdürlüğümüz, bu görevlerinin yanında ulusal kaynak yayınlar ile sektörümüzün gelişimine katkıda bulunmak amacı ile konu kapsamında çeşitli yayınları sektöre kazandırmaktadır.

Bilindiği gibi üyesi bulunduğumuz Uluslararası Sivil Havacılık Teşkilatı (ICAO) başta olmak üzere Avrupa Sivil Havacılık Konferansı (ECAC), Avrupa Hava Seyrüsefer Güvenlik Teşkilatı (EUROCONTROL) ve diğer uluslararası örgütler tarafından belirlenen standartlar ve yayımlanan dokümanlar yol gösterici olmalarından dolayı önemlidir . Bunların Türkçemize kazandırılması bunlardan ilgilenenlerin daha etkin faydalanmasına yardımcı olacaktır.

İlgili kurum ve kuruluşların bilgilendirilmesi, sektörün ihtiyaçlarına çözüm üretilmesi ve vatandaşların bilinçlendirilmesi açısından bu tür uluslararası dokümanların çevrilerinin yaptırılarak yayımlanması takdir edilecek bir yaklaşım olup bu doğrultuda daha önceki dönemlerde yayımlanmış kitaplara ek olarak Genel Müdürlüğümüzce hazırlanmış olan bu çalışmayı yayımlayarak siz değerli paydaşlara sunmaktan büyük mutluluk duyuyor emeği geçen tüm mesai arkadaşlarımı kutluyorum.

Bilal EKŞİ
Genel Müdür

İÇİNDEKİLER

Sayfa

KISALTMALAR

ADREP	Kaza/olay verileri raporlama (ICAO)
AEP	Havaalanı acil durum planı
AIRPROX	Hava araçlarının tehlikeli şekilde birbirine yaklaşması
ALARP	Makul oranda düşük
ALoS	Kabul edilebilir emniyet seviyesi
AMU	Tavsiye edilen malzeme birleşmesi
AMO	Sertifiye edilmiş bakım örgütü
AOC	Hava operatörü sertifikası
ASDE	Havaalanı yüzey araştırma donanımı
ASR	Hava emniyeti raporu
ATC	Hava trafik kontrolü
ATCO	Hava trafik kontrolörü
ATM	Hava trafik yönetimi
ATS	Hava trafik hizmet(ler)i
CAA	Sivil havacılık kurumu
CDA	Sabit alçalmalı inişler
CEO	İcra kurulu başkanı
CFIT	Arazide kontrollü uçuş
CIP	Ticari açıdan önemli kişi
Cir	Dairesel
CMC	Kriz yönetim merkezi
CRDA	Kesişen pist gösterge yardımı
CRM	Ekip beceri yönetimi
CVR	Kokpit ses kayıt cihazı
DME	Mesafe ölçme cihazı
Doc	Belge
ERP	Acil müdahale planı
FDA	Uçuş verileri analizi
FDM	Uçuş verilerinin izlenmesi
FDR	Uçuş veri kayıt cihazı
FOD	Yabancı madde hasarı
ft	Ayak
GPS	Küresel konumlama sistemi
ILS	Aletli iniş sistemi
IMC	Aletli meteorolojik koşullar
ISO	Uluslararası Standartlar Kurumu
kg	Kilogram

LOFT	Hat oryantasyonlu uçuş eğitimi
LOSA	Hat operasyonları emniyet denetimi
m	Metre
MDA	Minimum alçalma irtifası
MEL	Minimum donanım listesi
MOR	Zorunlu olay bildirimi
MRM	Bakım kaynak yönetimi
NM	Deniz mili
OJT	Görev başı eğitimi
PC	Kişisel bilgisayar
QA	Kalite güvencesi
QC	Kalite kontrolü
QMS	Kalite yönetimi sistemi
RVSM	Azaltılmış dikey ayırma minimumu
SA	Emniyetin güvence altına alınması
SAG	Emniyet eylemi grubu
SARPs	Standartlar ve Tavsiye Edilen Uygulamalar (ICAO)
SDCPS	Emniyet verileri toplama ve işleme sistemleri
SHEL	Yazılım/Donanım/Ortam/Personel
SMM	Emniyet yönetimi kılavuzu
SMS	Emniyet yönetimi sistem(ler)i
SMSM	Emniyet yönetimi sistemleri kılavuzu
SOPs	Standart operasyonel prosedürler
SRB	Emniyet denetim kurulu
SRM	Emniyet riski yönetimi
SSP	Devlet emniyet programı
TLH	En üst seviye tehlike
TRM	Takım beceri yönetimi
USOAP	Evrensel Emniyet Denetimi Programı (ICAO)
VIP	Çok önemli kişi
VMC	Görsel meteorolojik koşullar
VOR	Her yöne yayın yapan VHF telsizi

Bölüm 1

EL KİTABINA GENEL BAKIŞ

1.1 GENEL

Bu el kitabının amacı emniyet yönetimi sistemlerinin (SMS) uygulanması için düzenleyici çerçevenin ve destek sağlayan kılavuzluk materyallerinin geliştirilmesi için Devletlere kılavuz bilgiler sağlamaktır. Aynı zamanda, Annex 1 — *Personele Lisans Verilmesi*, Annex 6 — *Uçakların İşletilmesi*, Annex 8 — *Uçakların Uçuşa Elverişliliği*, Annex 11 — *Hava Trafiği Hizmetleri*, Annex 13 — *Uçak Kazaları ve Olaylarının İncelenmesi* ve Annex 14 — *Havalimanları* bölümlerinde bulunan Uluslararası Standartlar ve Tavsiye Edilen Uygulamalara (SARP'ler) uygun olarak bir Devlet emniyet programının (SSP) geliştirilmesi için kılavuz bilgiler de sağlamaktadır.

1.2 HEDEFLER

Bu el kitabının amacı Devletlere aşağıdakileri sağlamaktır:

a) emniyet yönetimi kavramları, Annex 1, 6, 8, 11, 13 ve 14 ve ilgili kılavuz materyallerinden yer alan emniyet yönetimi ile ilgili ICAO Standartları ve Tavsiye Edilen Uygulamaları hakkında bilgi;

b) İlgili ICAO SARP'lerine uygun olarak bir SMS'nin önemli bileşenlerinin uygulanmasının nasıl kabul edileceği ve denetleneceği hakkında kılavuz bilgiler ve

c) İlgili ICAO SARP'lerine uygun olarak bir SSP'nin nasıl geliştirileceği ve uygulanacağı hakkında kılavuz bilgiler.

1.3 KAVRAM

Bu el kitabının temelinde bulunan kavram, bir sürekli döngü kavramıdır (bkz. Şekil 1-1). Bu el kitabı, ilk olarak hem SMS hem de SSP'nin gerekliliğinin anlaşılmasının temelini oluşturan temel emniyet kavramlarını açıklamaktadır. Daha sonra, bu emniyet kavramlarının Annex 1, 6, 8, 11, 13 ve 14'te bulunan ICAO SARP'lerinde nasıl ortaya konduğu açıklanır. Bundan sonra, el kitabında bir SMS'nin hizmet sağlayıcılar tarafından uygulanması ve hizmet sağlayıcıların SMS'yi uygulamasını desteklemede sivil havacılık otoritelerinin oynadığı role vurguda bulunarak, bir SSP'nin kademeli olarak uygulanması ve sürdürülmesi için ilkelere dayalı bir yaklaşım ortaya konur.

1.4 İÇERİK

1.4.1 El kitabı aşağıdaki on bir bölümden oluşur:

a) Bölüm 1 — El kitabına genel bakış;

b) Bölüm 2 — Temel emniyet kavramları;

c) Bölüm 3 – Emniyet yönetimine giriş;

d) Bölüm 4 – Tehlikeler;

e) Bölüm 5 — Emniyet riskleri;

f) Bölüm 6 — ICAO emniyet yönetimi gereklilikleri;

g) Bölüm 7 – Emniyet yönetimi sistemlerine (SMS) giriş;

h) Bölüm 8 – SMS'nin planlanması;

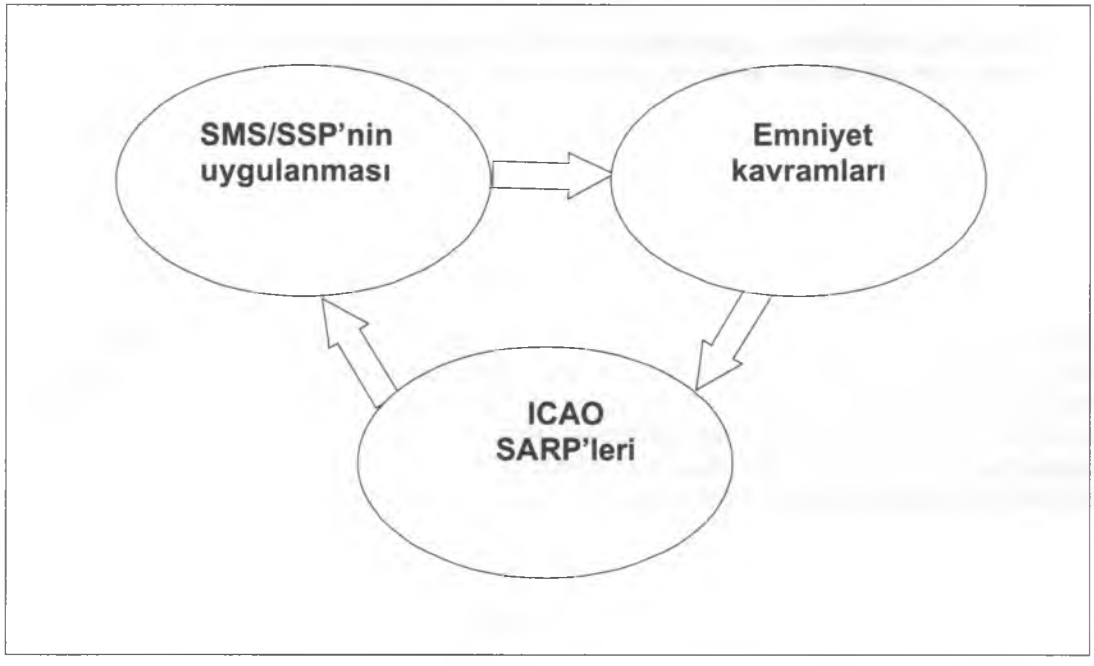
i) Bölüm 9 – SMS'nin işletilmesi;

j) Bölüm 10 – SMS'nin uygulanmasına aşamalı bir yaklaşım ve

k) Bölüm 11 - Devlet emniyet programı (SSP).

1.4.2 Bu el kitabında doğrudan bir SMS'nin ve bir SSP'nin uygulanması ve sürdürülmesi ile bağlantılı pratik örnekler ve bilgiler içeren çeşitli ekler de bulunmaktadır. Bu ekler, desteklediklerı etkinliğin açıklandığı bölümden hemen sonra bulunmaktadır ve "bilinmesi zorunlu" bilgiler olarak kabul edilmelidir.

1.4.3 Bu el kitabında, aynı zamanda doğrudan SMS'nin veya SSP'nin uygulanması ile ilgili olmayan yararlı bilgiler içeren ilaveler de bulunmaktadır. Bu ilaveler, el kitabının sonuna eklenmiştir, "bilinmesi iyi olan" bilgiler şeklinde değerlendirilmelidir.



Şekil 1-1. Bu el kitabında kullanılan sürekli döngü kavramı

1.5 YAPI

1.5.1 El kitabı bir yapı taşı yaklaşımını izler. Bölüm 2'de çağdaş emniyet kavramları açıklanarak temel oluşturulur. Bölüm 3'te, emniyetin neden yönetilmesi gerektiğinin altı çizilerek, emniyet yönetiminin temelleri açıklanır. Bölüm 4 ve 5'te emniyet riski yönetiminin altında yatan çerçeve ortaya konur ve iki temel kavramı, yani tehlikeler ve emniyet riskleri açıklanır. Son olarak, Bölüm 6 ile 11 arasında, sırasıyla Devletler ve örgütler içinde emniyetin yönetilmesini sağlayan sistemler olarak SSP ve SMS'yi kullanarak emniyet yönetimi süreçlerinin tasarlanması, uygulanması ve sürdürülmesine yönelik ilkeli bir yaklaşım sunulur. Bu bölümlerde, emniyet yönetimi kavramı aynı zamanda bir sistematik bir etkinlik olarak da açıklanır.

1.5.2 Devlet emniyet programı hakkındaki Bölüm 11, ICAO ve Devletler tarafından bir SSP'nin geliştirilmesi sırasında deneyimlerin elde edilmesi için bir ara kılavuz materyali olarak sağlanmıştır, daha sonra Devlet emniyet programına ayrılmış bir el kitabı geliştirilecektir. Bir SSP'nin geliştirilmesi ve uygulanması hakkında ayrıntılı kılavuz bilgiler www.icao.int/fsix veya www.icao.int/anb/safetymanagement. adresinden indirilebilecek ICAO SSP Eğitim Kursundan alınabilir.

1.5.3 ICAO *Emniyet Yönetimi El Kitabının (SMM)* (Doc 9859) bu ikinci baskısı, 2006'da yayınlanan ilk baskının tamamen yerine geçer. Artık geçersiz olan ICAO *Kaza Önleme El Kitabının* (Doc 9422) da yerine geçer.

Bölüm 2

TEMEL EMNİYET KAVRAMLARI

2.1 HEDEF VE İÇERİKLER

2.1.1 Bu bölüm emniyete yönelik uzun zaman önce oluşturulmuş yaklaşımların gücünü değerlendirmekte ve emniyete çağdaş bir yaklaşımın altında yatan yeni perspektifleri ve kavramları sunmaktadır.

2.1.2 Bu bölüm aşağıdaki konuları içerir:

a) Emniyet kavramı;

b) Emniyet kavramının gelişmesi;

c) Kazalardaki neden/sonuç ilişkisi – Reason modeli;

d) Örgütlenmeden kaynaklanan kaza;

e) İnsanlar, operasyonel bağlamlar ve emniyet – SHEL modeli;

f) Hatalar ve ihlaller;

g) Örgüt kültürü ve

h) Emniyet incelemesi.

2.2 EMNİYET KAVRAMI

2.2.1 Perspektife bağlı olarak, havacılıktaki emniyet kavramı aşağıdakiler gibi farklı anlamlara sahip olabilir:

a) sıfır kaza veya ciddi olay – yolculuk edenler tarafından geniş oranda kabul gören bir görüş;

b) tehlikelerden, yani kötü bir sonuca neden olan veya olabilecek etkenlerden uzak olma;

c) havacılık örgütlerinin çalışanlarının güvensiz eylem ve koşullara yönelik tavırları;

d) hatalardan kaçınma ve

e) düzenlemelere uyum.

2.2.2 Hangi anlam anlaşılırsa anlaşılsın, hepsinin altında ortak bir anlam bulunmaktadır: mutlak kontrol olasılığı. Sıfır kaza, tehlikelerden uzak olma v.s. tüm bunlar, havacılık operasyonları bağlamında – tasarım veya müdahale ile – kötü veya tehlikeli sonuçlara neden olabilecek tüm değişkenlerin kontrol altına alınmasının mümkün olduğu fikrine dayanmaktadır. Ancak, kazaların ve/veya ciddi olayların ortadan kaldırılması ve mutlak kontrolün elde edilmesi istenen bir şey olsa da, açık ve dinamik operasyonel bağlamlarda ulaşılması mümkün olmayan hedeflerdir. Tehlikeler havacılık operasyonları bağlamında ayrılmaz bileşenlerdir. Önlemek için en iyi şekilde çaba gösterilse de, havacılıkta arızalar ve operasyonel hatalar oluşacaktır. Hiçbir insan etkinliğinin veya insan yapısı sisteminin tamamen tehlikelerden ve operasyonel hatalardan uzak olacağı garanti edilemez.

2.2.3 Bu nedenle, emniyet mutlaktan çok göreli durumları içeren bir kavram olmalıdır, operasyonel bağlamdaki tehlikelerin sonuçlarından kaynaklanan emniyet riskleri yapısı gereği emniyetli bir sistem içinde kabul edilebilir olmalıdır. Temel sorun hala kontroldür, ancak mutlak kontrol yerine göreli kontroldür. Emniyet riskleri ve operasyonel hatalar makul bir kontrol derecesi altında bulunduğu sürece, ticari sivil havacılık gibi açık ve dinamik bir sistem emniyetli olarak kabul edilmelidir. Başka bir deyişle, makul bir dereceye kadar kontrol edilen emniyet riskleri ve operasyonel hatalar yapısal olarak emniyetli bir sistemde kabul edilebilirdir.

2.2.4 Emniyet giderek artan şekilde, operasyonel bağlamlarda bulunan tehlikelerin sonuçlarından doğan emniyet risklerini örgüt kontrolü altında tutma hedefine yönelik belirli örgütlenme süreçlerinin yönetilmesinin sonucu olarak görülmektedir. Bu nedenle, bu el kitabının amaçlarına göre, emniyetin anlamı aşağıdaki şekilde alınmıştır:

> ***Emniyet.*** Kişilerin veya mülkün zarar görme olasılığının, sürekli bir tehlike tanımlama ve emniyet riski yönetimi süreci aracılığıyla kabul edilebilir bir seviyeye indirildiği, bu seviyede veya daha altında tutulduğu durum.

2.3 EMNİYET KAVRAMININ GELİŞMESİ

2.3.1 İlk yıllarında, ticari havacılık gelişmemiş teknoloji, uygun altyapının eksikliği, kısıtlı öngörü, havacılık operasyonlarında bulunan tehlikelerin yetersiz şekilde anlaşılması ve talepleri karşılamak için mevcut olanak ve kaynaklarla orantısız üretim talepleri tarafından belirlenen, sıkı düzenlemelere bağlı olmayan bir etkinlikti.

2.3.2 Sistemlerin emniyeti teorisinde, hedeflere ulaşılması için gerekli araç ve kaynakları oluşturmadan hırslı üretim hedefleri konan üretim sistemlerinde sık sık arızalar oluştuğu bilinen bir gerçektir. Bu nedenle, ticari havacılığın ilk günlerinde sık sık kazalar yaşanması, erken dönem emniyet sürecinin en önemli önceliğinin kazaların önlenmesi olması ve kazaları önlemenin temel yönteminin kaza incelemeleri olması şaşırtıcı değildir. Söz konusu ilk günlerde, temel teknolojik destek dışında başka bir destek olmaması ile kısıtlanan kaza incelemeleri zorlu bir görevdi.

2.3.3 Teknolojik gelişmeler (büyük oranda kaza incelemeleri sayesinde), buna bağlı olarak uygun altyapının da gelişmesi ile birlikte kazaların sıklığında kademeli olarak, ama sürekli bir şekilde azalma olmasına ve bunun yanında giderek artan bir düzenleme gereksinimine yol açmıştır. 1950'lere gelindiğinde, havacılık (kazalar bakımından) en emniyetli endüstrilerden biri olmaya başlamış, ama bunun yanında en sıkı şekilde düzenlenen endüstrilerden biri haline gelmiştir.

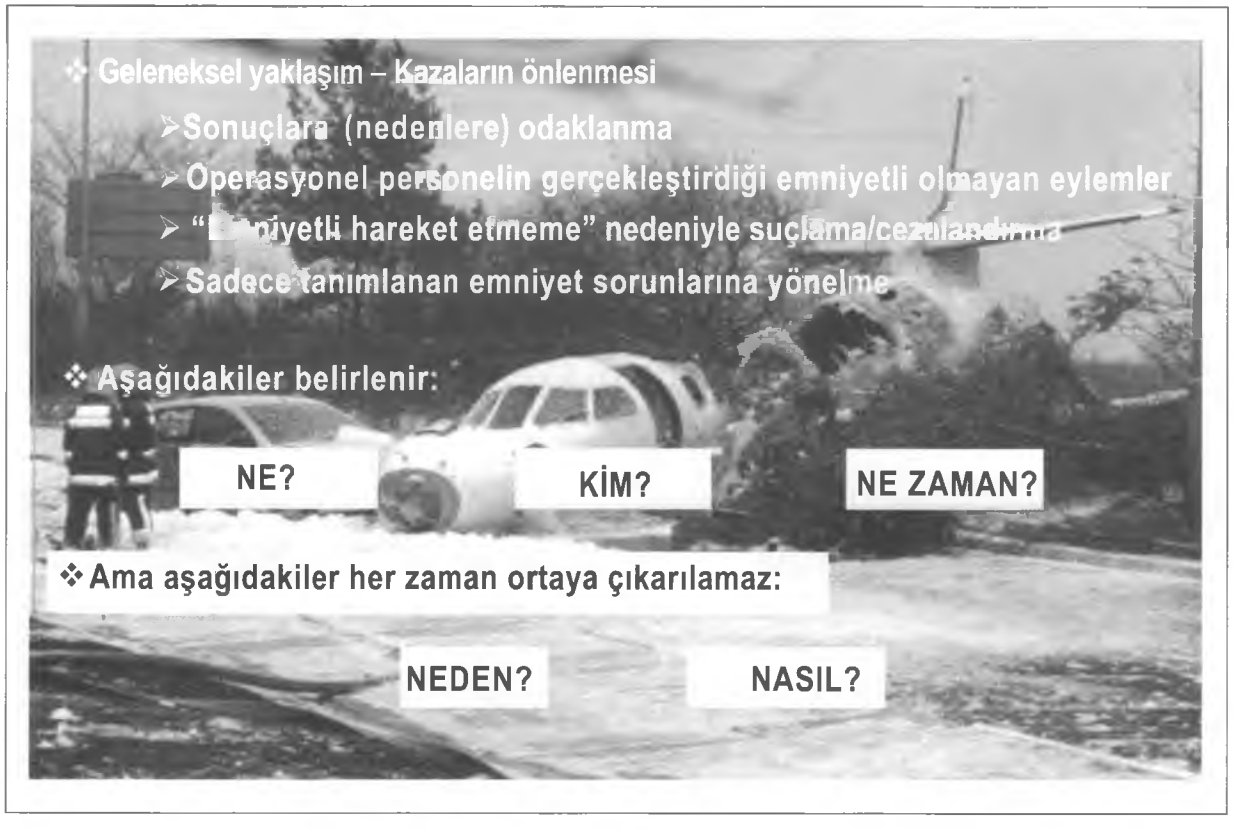
2.3.4 Bu hala geçerliliğini sürdürmekte olan, kurallara uyulduğu sürece emniyetin garanti edilebileceği ve kurallardan sapmanın kesinlikle emniyet sorunlarına neden olacağı kavrayışına neden olmuştur. Düzenlemelere uyulmasının çok önemli olduğunun inkar edilmesi mümkün olmasa da, özellikle havacılık operasyonlarının karmaşıklığı arttıkça, getirdiği sınırlamalar giderek artan şekilde emniyetin dayanak noktası olarak kabul edilmeye başlanmıştır. Havacılık gibi açık ve dinamik bir operasyonel sistemde düşünülebilir tüm operasyonel senaryolar ile ilgili kılavuzluk sağlanması imkansızdır.

2.3.5 Süreçler kanılar tarafından yürütülür. Bu nedenle, düzenlemelere uyulmasının havacılık emniyetinin temeli olduğu kanısına bağlı olarak, erken dönem emniyet süreçleri düzenlemelere uyulmasını ve denetimi kapsayacak şekilde genişletilmişti. Bu yeni emniyet süreci sonuçlara (yani kazalara ve/veya büyük olaylara) odaklanmıştı ve teknolojik hata olasılığı da dahil olmak üzere, nedenleri belirlemek için kaza incelemelerini temel almıştı. Teknolojik hatalar bulunamazsa, dikkatler operasyonel personelin kurallara uymamasına dönüyordu.

2.3.6 Kaza incelemesi, emniyet arızasında doğrudan yer alan kişilerin bir olaylar dizisinde kendilerinden bekleneni yapmadıkları, kendilerinden beklenmeyen bir şeyi yaptıkları veya bunun ikisinin de ortaya çıktığı nokta veya noktaları arayarak geriye doğru ilerliyordu. Teknolojik hatalar olmadığında, incelemeler operasyonel personelin emniyetli olmayan eylemlerine, yani inceleme konusu sonuçla doğrudan bağlantı kurulabilecek eylemlere veya eylemsizliklere yöneliyordu. Bu tür eylemler/eylemsizlikler tanımlandığında ve geriye bakıştan yararlanarak emniyet arızasına bağlandığında, farklı derecelerde ve farklı bahaneler altında suçlamada bulunmak kaçınılmaz sonuç oluyordu ve "emniyetli şekilde davranmamak" nedeniyle cezalar dağıtılıyordu.

2.3.7 Bu yaklaşımın tipik yönü, neredeyse tek başına emniyet arızasına neden olduğu tanımlanan belirli, kesin bir emniyet sorununa yönelik emniyet tavsiyeleri oluşturmasıydı. Farklı koşullarda havacılık operasyonlarında zarar verme potansiyeli bulunan, mevcut olsalar da, inceleme konusu olayda "neden olmayan" tehlikeli koşullara pek az önem veriliyordu.

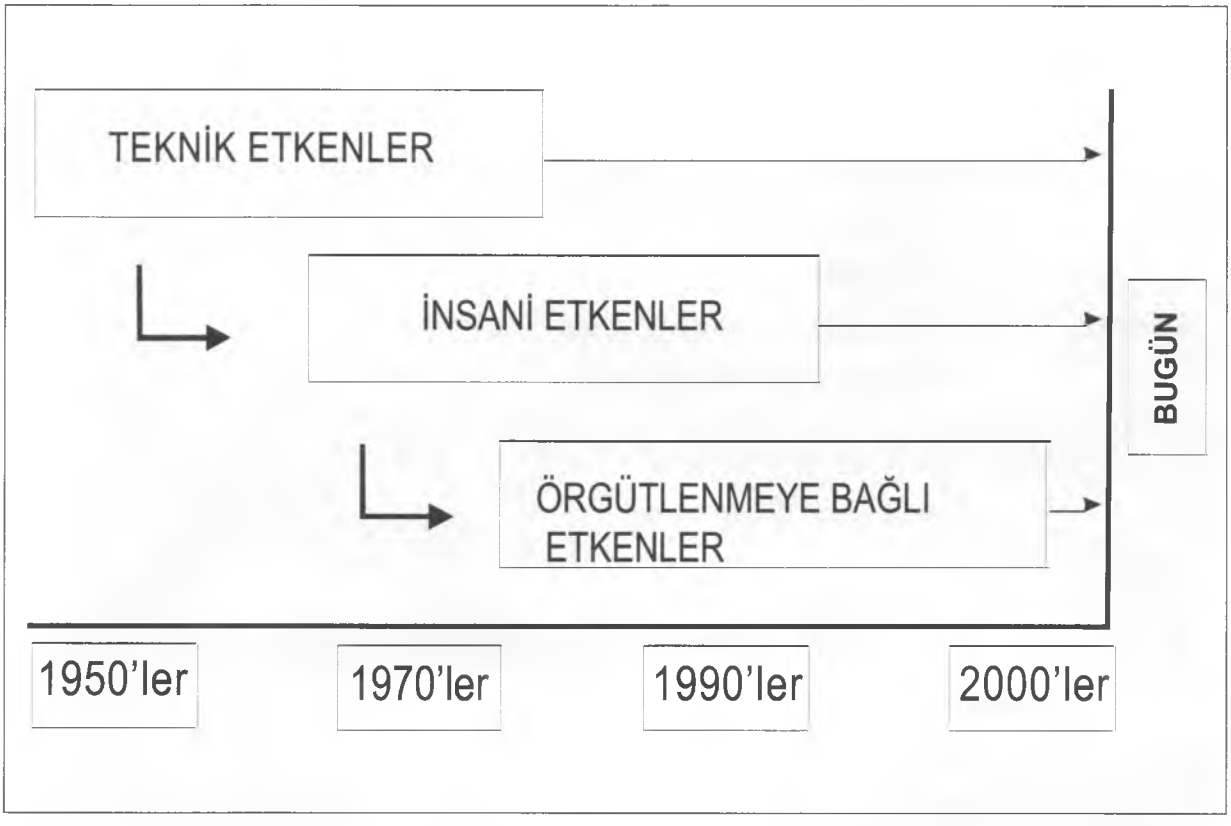
2.3.8 Bu perspektif "ne" olduğunu, "kimin" yaptığını ve "ne zaman" olduğunu belirlemekte son derece etkili olsa da, "neden" ve "nasıl" olduğunu belirlemede önemli ölçüde daha başarısızdı (Şekil 2-1). Bir zamanlar "ne", kim" ve "ne zaman" sorularının yanıtlarını anlamak önemli olsa da, emniyet arızalarını tamamen anlamak için "neden" ve "nasıl" sorularının yanıtlarının anlaşılması giderek daha önemli hale gelmiştir. Geçtiğimiz yıllarda, bu anlayışın elde edilmesi için önemli adımlar atılmıştır. Geçmişe baktığımızda, havacılıktaki emniyet kavramının son elli yılda önemli bir evrim geçirdiği açıktır.



Şekil 2-1. Geleneksel yaklaşım – Kazaların önlenmesi

2.3.9 1970'lere kadar havacılığın ilk yılları, İkinci Dünya Savaşı'ndan önceki ve hemen sonraki yıllar, emniyet sorunlarının genellikle teknik etkenlere bağlandığı "teknik çağ" olarak karakterize edilebilir. Havacılık bir toplu taşıma endüstrisi olarak ortaya çıkıyordu, ancak operasyonlarını destekleyen teknoloji henüz tam olarak gelişmemişti ve teknolojik arızalar emniyet arızalarındaki en sık tekrarlanan etkenlerdi. Emniyetle ilgili çabaların odağı doğru şekilde teknik etkenlerin incelenmesi ve geliştirilmesi olarak belirlenmişti.

2.3.10 1970'lerin ilk yıllarında jet motorlarının, radarın (hem havada hem de yerde), otomatik pilotların, uçuş yönlendiricilerin, gelişmiş navigasyon ve iletişim becerilerinin ve hem havada hem de yerde benzer performans arttırıcı teknolojilerin kullanılmaya başlanması ile önemli teknolojik gelişmeler görülmüştü. Bu "insan çağının" başlangıcını müjdelemiş ve ekip beceri yönetimi (CRM), hat oryantasyonlu uçuş eğitimi (LOFT), insan merkezli otomasyon ve insan performansına yönelik diğer müdahaleler ile emniyetle ilgili çabaların odağı insanların performansına ve İnsani Etkenlere yönelmiştir. 1970'lerin ortası ile 1990'ların ortası arası, havacılığın açıklanması güç ve son derece yaygın insan hatalarını kontrol altına almak için büyük yatırımlarda bulunmasına referansla havacılıkta İnsani Etkenlerin "altın çağı" olarak adlandırılmıştır. Buna karşın, hataların azaltmasına yönelik kaynaklara yapılan büyük yatırıma rağmen, 1990'ların ortasına kadar insan performansı emniyet arızalarında tekrarlayan bir etken olarak ayrılmaya devam etmiştir (Şekil 2-2).



Şekil 2-2. Emniyet kavramının gelişmesi

2.3.11 "Altın çağın" önemli bir kısmında İnsani Etkenlerle ilgili çabaların olumsuz yönü, bireye odaklanma eğiliminde olmaları, bireylerin görevlerini yerine getirdikleri operasyonel bağlama çok az dikkat etmeleri olmuştu. Ancak 1990'ların başında, ilk kez bireylerin bir vakum ortamında çalışmadıkları, tanımlanmış operasyonel bağlamlar içinde çalıştıkları tanınmıştı. Bir operasyonel bağlamın insanların performansını nasıl etkileyebileceği ve olayları veya sonuçları nasıl biçimlendirebileceği hakkında bilimsel yayınlar bulunsa da, havacılığın bu olguyu tanıması ancak 1990'larda gerçekleşmişti. Bu, emniyetin örgütlenmeden kaynaklanan, insani ve teknik etkenleri kapsayacak, sistemli bir perspektiften görülmeye başlandığı "örgüt çağının" başlangıcını gösteriyordu. Aynı zamanda, örgütlenmeden kaynaklanan kaza kavramının havacılık tarafından kabul görmesi de bu dönemdedir.

2.4 KAZALARDAKİ NEDEN/SONUÇ İLİŞKİSİ – REASON MODELİ

2.4.1 Örgütlenmeden kaynaklanan kaza kavramının endüstri çapında kabulü, Profesör James Reason tarafından geliştirilen, havacılığın (veya başka bir üretim sisteminin) nasıl başarılı şekilde çalıştığı veya hataya yöneldiğinin anlaşılması için bir araç sağlayan, basit, ama grafik anlamda güçlü model tarafından mümkün kılınmıştı. Bu modele göre, kazalar ortaya çıkmalarına neden olan bir dizi etkenin bir araya gelmesini gerektiriyordu, bu etkenlerin her biri zorunlu olsa da, kendi başına sistemin savunmasını aşmaya yeterli değildi. Havacılık gibi karmaşık sistemler derinlemesine savunma katmanlarıyla son derece iyi savunulduğundan, havacılık sisteminde tek noktadan kaynaklanan arızalar son derece nadirdir. Donanım arızaları veya operasyonel hatalar hiçbir zaman emniyet savunmalarının ihlalinin nedeni değillerdir, ancak tetikleyicilerdirler. Emniyet savunmalarının ihlalleri, sistemin en yüksek seviyelerinde verilen kararların gecikmeli bir sonucudurlar, etkileri veya zarar verme potansiyelleri belirli operasyonel koşullar tarafından etkinleştirilene kadar etkisiz halde kalmışlardır. Bu türden belirli koşullar altında, insani hatalar veya operasyonel seviyedeki etkin hatalar sistemin yapısında yer alan emniyet savunmalarının ihlal edilmesine olanak sağlayan örtük koşulların tetikleyicisi olurlar. Reason modeli ile geliştirilen kavramda, tüm kazalar hem etkin hem de örtük koşulların bir kombinasyonundan oluşur.

2.4.2 Etkin kusurlar, olumsuz etkileri derhal görülen hatalar ve ihlalleri de içeren eylemler ve eylemsizliklerdir. Genel olarak, geçmişe bakışın yardımıyla, güvensiz eylemler olarak görülürler. Etkin kusurlar genellikle ön saflardaki personelle (pilotlar, hava trafik kontrolörleri, uçak mühendisleri v.s.) ile ilişkilendirilir ve hasar veren bir sonucun ortaya çıkmasına neden olabilirler. Havacılık sistemini korumak için örgütler, düzenleyici kurumlar vs. tarafından konulan savunmaları aşma potansiyeline sahiptirler. Etkin kusurlar normal hataların sonucu olabilir veya önceden belirlenen prosedürlerden ve uygulamalardan sapılmasından kaynaklanabilirler. Reason modeli her bir operasyonel bağlamda bireysel performansı veya takım performansını etkileyebilecek pek çok hata ve ihlal oluşturan koşul olduğunu tanır.

2.4.3 İşletme personeli tarafından gerçekleştirilen etkin kusurlar, örtük koşulları da içeren operasyonel bağlamda gerçekleşir. Örtük koşullar, sistemde zarara neden olan sonuç ortaya çıkmadan çok önce de bulunan ve yerel tetikleyici koşullar nedeniyle görünür hale gelen koşullardır. Örtük koşulların sonuçları uzun süre gizli halde kalır. Tek tek bakıldığında, bu örtük koşullar, başlangıçta hata olarak algılanmadıklarından, genellikle zararlı olarak görülmezler.

2.4.4 Örtük koşullar sistemin savunması aşıldıktan sonra ortaya çıkarlar. Bu koşullar genellikle, olaydan zaman ve mekân bakımından çoktan uzaklaşmış olan kişiler tarafından oluşturulur. Ön saflardaki personel, kötü donanım veya görev tasarımı, çatışan hedefler (örneğin zamanında hizmet karşısında emniyet), sorunlu örgütler (örneğin iç iletişimin kötü olması) veya yönetim kararları (örneğin bir bakım geciktirilmesi) v.s. nedeniyle ortaya çıkan koşullar gibi sistemdeki örtük koşulları devralır. Örgütlenmeden kaynaklanan kazaların altında yer alan perspektifin amacı, bireylerin neden olduğu etkin kusurların en aza indirilmesi için yerel çabalardan çok, bu örtük koşulları sistem çapında tanımlamak ve azaltmaktır. Etkin kusurlar, emniyet sorunlarının nedeni değil, sadece belirtisidir.

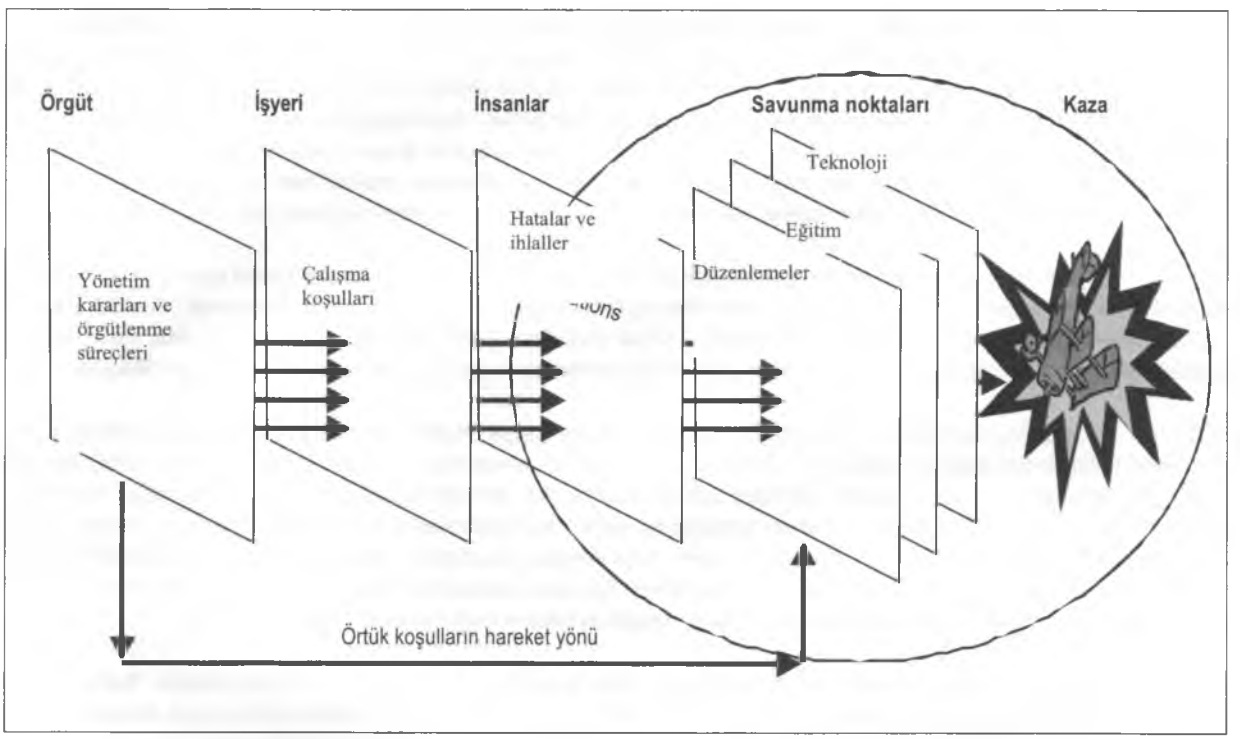
2.4.5 En iyi şekilde yönetilen örgütlerde bile, örtük koşulların çoğu karar vericilerden başlar. Karar vericiler normal insani eğilimlere ve sınırlamalara tabidir, bunun yanında zaman, bütçe ve politika gibi gerçek kısıtlamalara da tabidirler. Yönetim kararlarındaki başarısızlıkları her zaman önlenmesi mümkün olmadığından, bu başarısızlıkları belirlemek ve kötü sonuçlarını azaltmak için adımlar atılmalıdır.

2.4.6 Bölüm yönetimi tarafından verilene kararlar yetersiz eğitime, programlama çakışmalarına veya işyeri önlemlerinin ihmal edilmesine neden olabilir. Yetersiz bilgi ve beceriye veya uygun olmayan operasyonel prosedürlerine neden olabilirler. Bölüm yönetiminin ve bir bütün olarak örgütün işlevlerini ne kadar başarılı şekilde yerine getirdikleri, hata veya ihlale neden olan koşulların ortaya çıktıkları ortamı belirler. Örneğin: Yönetimin ulaşılabilir hedefleri koymada, görev ve kaynakları organize etmede, günlük işleri yönetmede ve iç ve dış iletişimde ne kadar etkili olduğu. Şirket yönetimi ve düzenleyici otoriteler tarafından verilen kararlar genellikle yetersiz kaynakların sonucudur. Ancak, sistemin emniyetinin arttırılmasının başlangıçtaki maliyetinden kaçınılması örgütlenmeden kaynaklanan kazalara giden yolu açabilir.

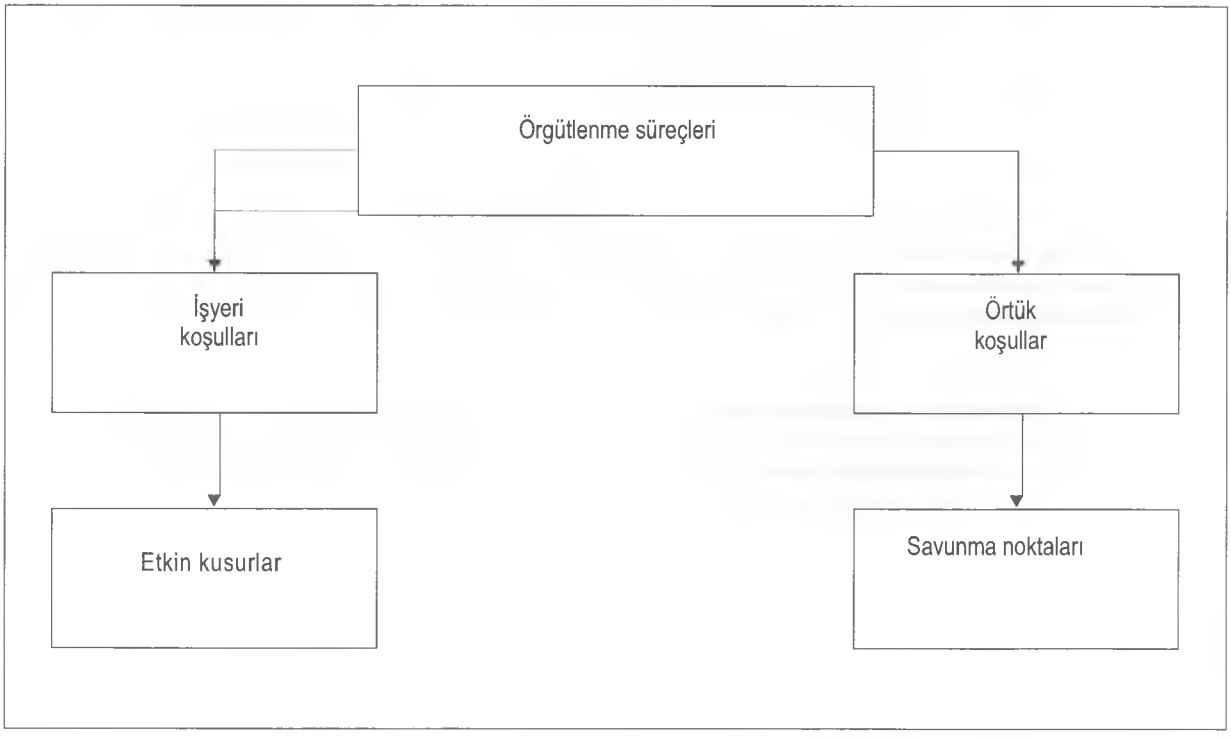
2.4.7 Şekil 2-3'de Reason modeli örgütten ve yönetimden kaynaklanan etkenlerin (yani sistem etkenlerinin) kaza neden/sonuç ilişkisindeki etkileşimlerinin anlaşılmasını sağlayacak şekilde gösterilmiştir. Havacılık sisteminde insan performanslarında dalgalanmalara veya sistemin tüm seviyelerinde (yani ön saflarda iş alanlarında, denetim seviyelerinde ve üst yönetimde) olumsuz bir sonuca neden kararlara karşı korumak için çeşitli savunma noktaları oluşturulmuştur. Savunmalar, sistem tarafından üretim etkinliklerinde bulunan örgütlerin oluşturdukları ve kontrol etmeleri gereken emniyet risklerine karşı korunmak için sağlanan kaynaklardır. Bu model, yönetim kararları dahil olmak üzere örgütlenmeden kaynaklanan etkenlerin sistemin savunma noktalarında ihlallere neden olan örtük koşullara yol açabilmelerine karşın, aynı zamanda sistemin savunmasının sağlamlığına da katkıda bulunabileceklerini gösterir.

2.5 ORGANİZASYONDAN KAYNAKLANAN KAZA

2.5.1 Reason modelinin altında yatan örgütlenmeden kaynaklanan kaza kavramı, beş yapıtaşından oluşan bir yapıtaşı yaklaşımı ile anlaşılabilir (Şekil 2-4).



Şekil 2-3. Kazalardaki neden/sonuç ilişkisi kavramı



Şekil 2-4. Örgütlenmeden kaynaklanan kaza

2.5.2 Üst blok örgütlenme süreçlerini gösterir. Bunlar, herhangi bir örgütün üzerinde makul bir derecede doğrudan kontrole sahip olduğu etkinliklerdir. Tipik örnekleri şunlardır: politika oluşturma, planlama, iletişim, kaynakların ayrılması, denetim vs. Açıktır ki, emniyet söz konusu olduğunda iki temel örgüt süreci kaynakların ayrılması ve iletişimdir. Bu örgütlenme süreçlerindeki olumsuzluklar veya bozulmalar, arızaya giden çift taraflı yolda artışın kaynaklarıdır.

2.5.3 Yollardan biri örtük koşulların oluşturduğu yoldur. Örtük koşulların örnekleri şunlardır: donanım tasarımındaki bozukluklar, eksik/yanlış standart operasyonel prosedürler ve eğitimdeki eksiklikler. Genel olarak, örtük koşullar iki büyük kümede gruplanabilir. Bir küme yetersiz tehlike tanımlaması ve emniyet riski yönetimidir, burada tehlikelerin sonuçlarından kaynaklanan emniyet riskleri kontrol altında tutulmaz, ama operasyonel tetikleyiciler aracılığıyla nihayetinde etkinleşmek üzere sistem içinde serbestçe hareket edilirler.

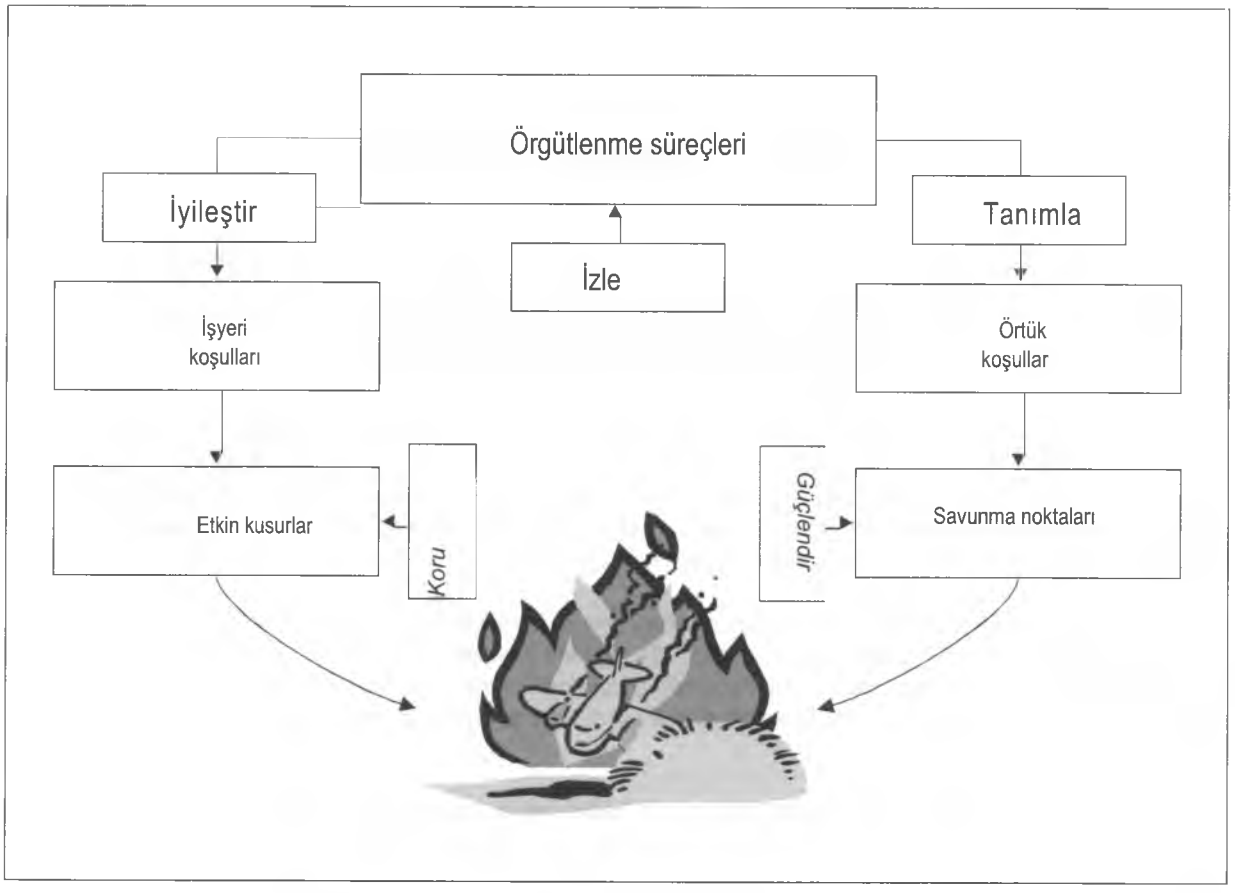
2.5.4 İkinci küme sapmanın normalize edilmesi olarak bilinir, bu kavram basitçe ifade edilirse istisnaların kural haline geldiği operasyonel bağlamları gösterir. Bu örnekte kaynakların ayrılması, aşırı derecede sorunludur. Kaynak eksikliğine bağlı olarak, üretim etkinliklerinin gerçekleştirilmesinden doğrudan sorumlu olan operasyonel personel, bu etkinlikleri kuralların ve prosedürlerin sürekli olarak ihlal edilmesini içeren kısa yollar oluşturarak başarılı bir şekilde yerine getirebilirler.

2.5.5 Örtük koşullar havacılık sisteminin savunmasını aşma potansiyeline tamamen sahiptir. Tipik olarak, havacılıktaki savunmalar üç büyük başlık altında gruplanabilir: teknoloji, eğitim ve düzenlemeler. Savunmalar genellikle, insan performansındaki kusurların sonuçlarının yanında, örtük koşulların da engellenmeleri için son emniyet ağlarıdır. Tehlikelerin sonuçlarından kaynaklanan emniyet risklerinin azaltılması stratejilerinin hepsi olmasa da, çoğu mevcut savunmaların güçlendirilmesini veya yeni savunmaların geliştirilmesini temel alır.

2.5.6 Örgütlenme süreçlerinden kaynaklanan diğer yol ise işyeri koşullarından kaynaklanan yoldur. İşyeri koşulları, havacılık alanında çalışanların etkinliğini doğrudan etkileyen etkenlerdir. İşyeri koşulları, operasyonel deneyimi olanların tümü bu koşulları çeşitli derecelerde yaşamış olduklarından büyük oranda kolayca anlaşılabilir ve şunlardan oluşur: işgücünün istikrarı, kalifikasyonları ve deneyimi, morali, yönetimin güvenilirliği ve aydınlatma, ısıtma ve soğutma gibi klasik ergonomik etkenler.

2.5.7 Optimum seviyenin altındaki işyeri koşulları operasyonel personelin etkin hatalarda bulunmasına neden olur. Etkin kusurlar, hatalar veya ihlaller olabilir. Hatalar ve ihlaller arasındaki fark motivasyon unsurudur. Bir görevi yerine getirmek için elinden gelenin en iyisini yapan, aldığı eğitime göre kuralları ve prosedürleri uygulayan, ama görevde tanımlanan hedefe ulaşamayan bir kişi bir hata yapmış olur. Bir görevi yerine getirirken kurallardan, prosedürlerden veya alınan eğitimden isteyerek ayrılan bir kişi bir ihlal gerçekleştirir. Dolayısıyla, hatalar ve ihlaller arasındaki temel fark niyettir.

2.5.8 Örgütlenmeden kaynaklanan kaza perspektifinden, emniyetle ilgili çalışmalar sırasında örtük koşulları belirlemek ve böylece savunma noktalarını güçlendirmek için örgütlenme süreçleri izlenmelidir. Emniyetle ilgili çalışmalar sırasında aynı zamanda, etkin kusurları içeren işyeri koşullarını da iyileştirmelidir, çünkü emniyet ihlallerine neden olan tüm bu etkenlerin birbiri üzerine gelmesidir (Şekil 2-5).



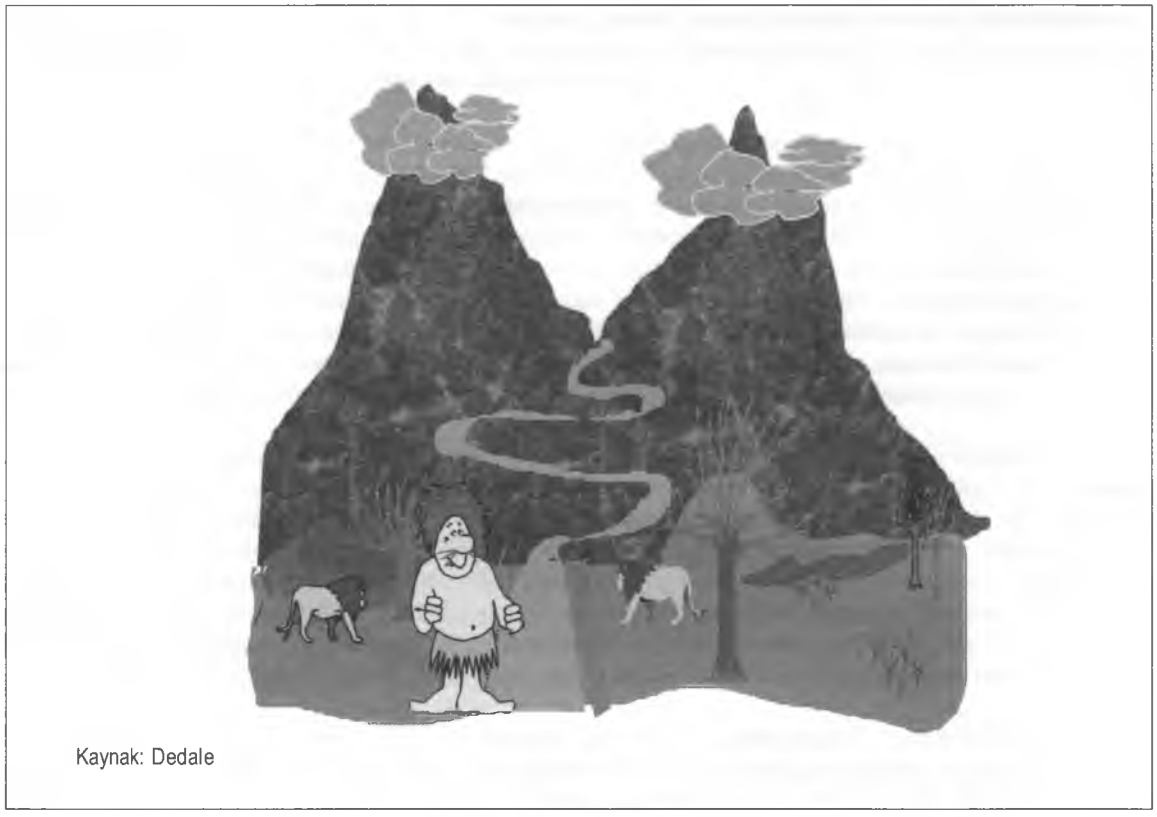
Şekil 2-5. Örgütlenmeden kaynaklanan kaza perspektifi

2.6 İNSANLAR, BAĞLAM VE EMNİYET – SHEL MODELİ

2.6.1 Havacılık işyerleri çok bileşenli, çok özellikli, karmaşık operasyonel bağlamlardır. Sistemin üretim hedeflerine ulaşabilmesi için, bu işyerlerinin işlevleri ve performansları pek çok bileşenlerinin arasındaki karmaşık ilişkileri de içerir.

2.6.2 Emniyete insan katkısını anlayabilmek ve sistemin üretim hedeflerine erişmek için gereken kişisel operasyonel performansı desteklemek için, kişisel operasyonel performansın operasyonel bağlamın çeşitli bileşenleri ve özelliklerinden nasıl etkilenebileceğini ve bileşenler, özellikler ve insanlar arasındaki ilişkileri anlamak gerekir.

2.6.3 Çok basit bir örnek Şekil 2-6'da sunulmuştur. Mağara adamı operasyonel personeli temsil etmektedir ve görev (ya da sistemin üretim hedefi) paketlerin dağların diğer tarafına ulaştırılmasıdır. İşletme bağlamının farklı bileşenleri ve özellikleri ve bunların mağara adamıyla ve kendileri arasındaki etkileşimleri, paketlerin teslimatının emniyetini ve etkinliğini etkileyecektir. Dolayısıyla, mağara adamının aslanlarla etkileşimi, mağara adamı aslanlarla başa çıkmak için yeterli donanıma sahip olmadığında, bu tür bir teslimat üzerinde olumsuz etkilere sahip olacaktır.



Kaynak: Dedale

Şekil 2-6. İnsanlar ve emniyet

2.6.4 Muhtemelen dolambaçlı ve toprak bir araç yolundan ayakkabılar olmadan dağlar üzerinden geçiş, etkin bir performans elde edilmesini önleyecek (paketlerin teslimatında gecikmeler) ve yaralanmalara neden olabilecektir, dolayısıyla emniyet sorunlarına neden olacaktır. Yağmurluk olmadan olası hava koşullarına aldırmaksızın yola koyulmak da emniyet ve etkinlikte olası sorunlara neden olacaktır.

2.6.5 Dolayısıyla operasyonel bağlamın uygun bir şekilde değerlendirilmesi ve analiz edilmesinin, desteklenmesi ve geliştirilmesi için operasyonel performansın anlaşılmasını sağlamada kullanılabilecek değerli bilgilerin bir kaynağı olduğu açıktır.

2.6.6 İşletme performansının içinde yer aldığı operasyonel bağlam içinde anlaşılması gerekliliği Şekil 2-7A'daki diğer bir örnekle de gösterilmiştir.

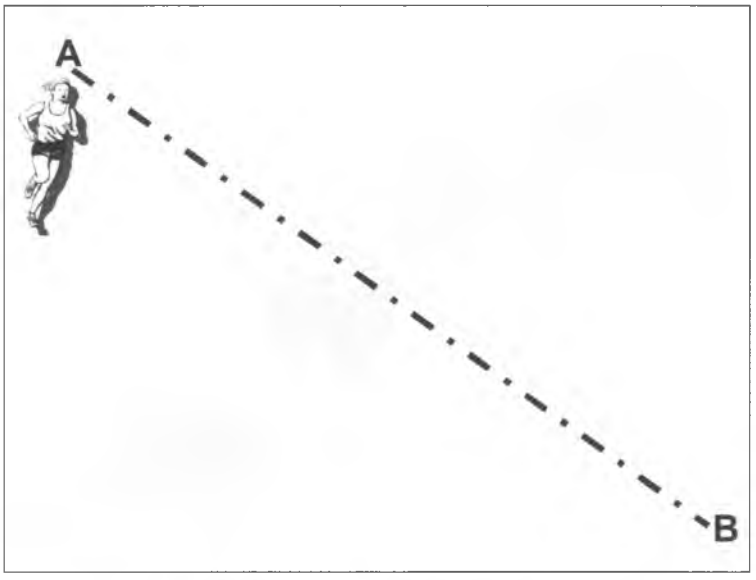
2.6.7 Bu örnekte, sistemin üretim hedefi paketlerin koşucular tarafından A ve B noktaları arasında taşınmasıdır. Sistemin tasarımında, koşucuların düz çizgi ile gösterilen en kısa yolu izleyecekleri temel bir varsayımdır.

2.6.8 Sistem kaynaklarını en uygun şekilde belirlemek için yatırım yapılmamıştır. Mevcut en iyi insan kaynakları (bu örnekte koşucular) seçilmiş, eğitilmiş, işin esasları öğretilmiş ve en iyi koşu malzemeleri (teknoloji) ile donatılmıştır. Sistem tasarımının bir parçası olarak, operasyonların gerçek zamanda izlenmesi de eklenmiştir. Tasarım adımları tamamlandığında, operasyonlar başlatılmıştır. Sistemin işletilmeye başlamasından kısa süre sonra, operasyonların gerçek zamanda izlenmesi başlar. Sistem yöneticilerini sıkıntıya sokacak şekilde, gerçek zamanlı izleme sonucunda çoğu koşucunun düz çizgi üzerindeki amaçlanan yolu kullanarak değil, zikzak çizerek ilerledikleri ortaya çıkmıştır. Sonuç olarak, teslimatta gecikmeler ve aynı zamanda kazalar oluşmaktadır (Şekil 2-7B).

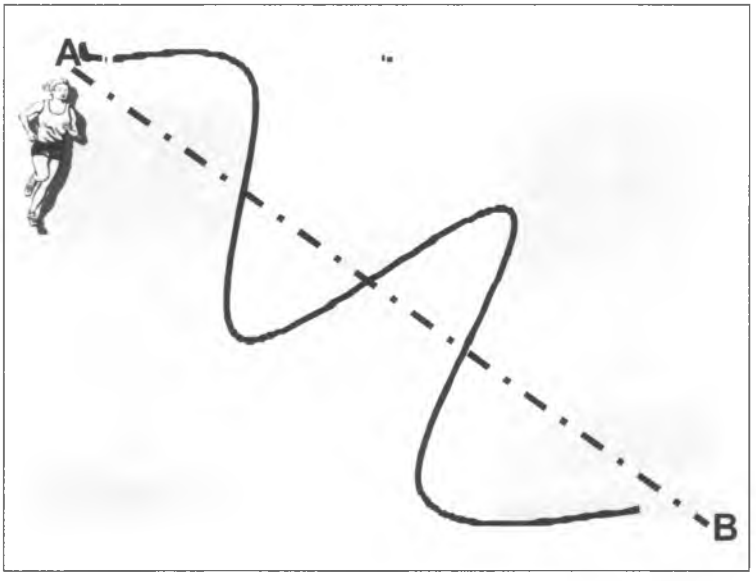
2.6.9 Bu noktada, sistem yöneticileri iki seçeneğe sahiptir. Seçeneklerden biri 2.3.6'da açıklanan klasik perspektifi izlemektir: koşuculara bildiklerini ve yapmak için eğitim gördüklerini yapmaları için boş hatırlatma notları hazırlamak ve koşucuları kendilerinden beklenen şekilde performans göstermedikleri için suçlamada bulunmak ve cezalandırmak. Diğer seçenek, koşucularla olumsuz etkileşimlerin kaynağı olabilecek bağlam bileşenleri ve özellikleri olup olmadığını görmek için operasyonel bağlamı analiz etmektir. İkinci seçenekte, bağlamdaki belirli bileşenler ve özellikler hakkında değerli bilgiler elde edilecektir (Şekil 2-7C), bu bilgiler tasarım varsayımlarının yeniden ayarlanmasını ve bağlamdaki öngörülmeyen bileşenler ve özelliklerin sonuçların kaynaklanan emniyet riskleri için risk azaltma stratejilerinin geliştirilmesini sağlayacaktır. Başka bir deyişle, operasyonel bağlamdaki tehlikeler hakkında bilgi edinerek (Bölüm 4'te açıklanmıştır) ve bunların insanlarla etkileşimlerini anlayarak, sistem yöneticileri sistemi tekrar örgüt kontrolü altına alabilirler.

2.6.10 Böylece, operasyonel performans ve operasyonel hataların doğru şekilde anlaşılmasının, operasyonel performans ve hatalarının ortaya çıktığı operasyonel bağlamı doğru şekilde anlamadan mümkün olmayacağı öne sürülmektedir. Bu anlayış, süreçler ve sonuçları arasında açık bir ayrım yapılmadıkça elde edilemez. İşletme hatalarının nedenlerine ve sonuçlarına bir simetri tanımak gibi bir eğilim vardır, oysa gerçek hayatta böyle bir simetri yoktur. Aynı hata, operasyonel hatanın ortaya çıktığı bağlama bağlı olarak önemli derecede farklı sonuçlara sahip olabilir. İşletme hatalarının sonuçları kişiye değil, bağlama bağlıdır (Şekil 2-8). Bu kavram, hata azaltma stratejileri üzerinde önemli bir etkiye sahiptir: etkin ve etkili hata azaltma stratejileri, insanları değiştirmeye çalışmak yerine, operasyonel bağlamın hataların sonuçlarının büyümesine neden olan özelliklerini ve bileşenlerini değiştirmeyi hedefler.

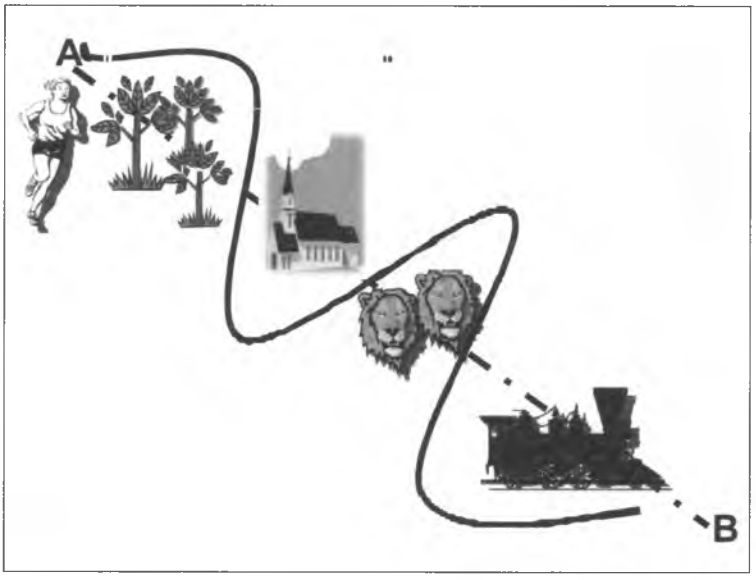
2.6.11 Şekil 2-8'de de, 2.3.6'da açıklanan iki yönetim seçeneğinin uygulanabileceği bir senaryoyu göstermektedir. Klasik yaklaşımı izlemek, pencere eşiğinde eğilirken dikkatli olunması (veya eğilinmemesi) ve saksıların pencereden dışarı itilmesi hakkında hatırlatma notları oluşturulmasına, ardından, önceki etkiler için prosedürlerin yeniden yazılmasına veya saksıların pencereden dışarı itilmesinin (beklenen veya emniyetli şekilde performans gösterememe) cezalandırılmasına neden olacaktır. Diğer yandan, örgüte bağlı yaklaşım, pencerenin altına bir ağ yerleştirme, pencere eşiğini genişletme, kolay kırılır tipte saksılar kullanma, pencerenin altındaki trafiği yeniden yönlendirme veya aşırı durumlarda pencerenin perdeyle örülmesi sonuçlarına neden olacaktır. Sonuç olarak, operasyonel bağlamın hataya yol açan özelliklerini ortadan kaldırarak veya değiştirerek, operasyonel hataların sonuçlarının olasılığında ve ciddiyetinde üssel bir azalma elde edilebilir.



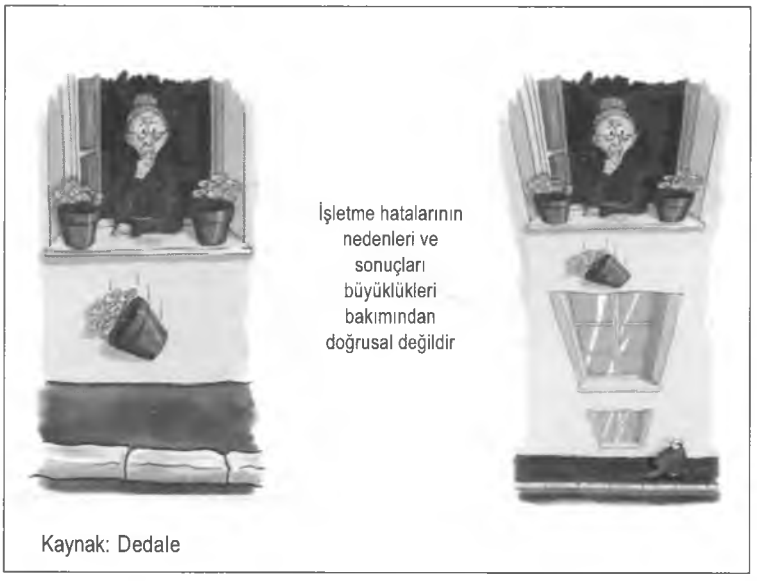
Şekil 2-7A. İnsan performansının anlaşılması



Şekil 2-7B. İnsan performansının anlaşılması



Şekil 2-7C. İnsan performansının anlaşılması



Şekil 2-8. Süreçler ve sonuçlar

2.6.12 İşletme bağlamlarının bileşenlerinin ve özelliklerinin ve bunların insanlarla olası etkileşimlerinin analizi için basit, ama görsel açıdan güçlü, kavramsal bir araç SHEL modelidir. SHEL modeli (bazen SHEL(L) modeli olarak da adlandırılır) havacılık sisteminin çeşitli bileşenleri ve özellikleri arasındaki ilişkilerin görselleştirilmesi için kullanılabilir. Bu model bireye ve insanların havacılık sisteminin diğer bileşenleri ve özellikleri ile iletişim arayüzlerine vurgu yapar. SHEL modelinin ismi, dört bileşeninin ilk harflerinden oluşturulmuştur:

a) Yazılım (Software, S) (prosedürler, eğitim, destek v.s.);

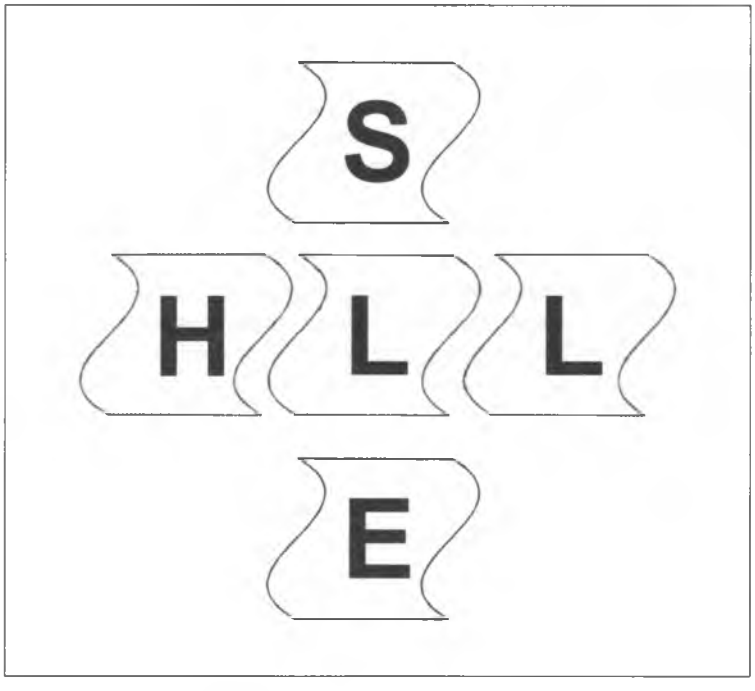
b) Donanım (Hardware, H) (makineler ve donanım);

c) Ortam (Environment, E) (L-H-S sisteminin geri kalanının çalışması gereken çalışma ortamları); ve

d) Personel (Liveware, L) (işyerindeki insanlar).

2.6.13 Şekil 2-9'da SHEL modeli gösterilmektedir. Bu yapıtaşı şeması, bireylerin işyerindeki bileşenler ve özelliklerle ilişkisi hakkında temel bir anlayış sağlamayı amaçlamaktadır.

2.6.14 ***Personel.*** SHEL modelinin merkezinde, operasyonların ön saflarında bulunan insanlar yer alır. İnsanlar önemli ölçüde uyumlu olsalar da, performanslarında önemli değişmeler görülebilir. İnsanlar donanımla aynı derecede standardize edilemez, dolayısıyla bu bloğun kenarları basit ve düz değildir. İnsanlar, çalıştıkları dünyanın çeşitli bileşenleri ile mükemmel şekilde arayüze sahip değildir. İnsan performansını etkileyebilen gerilimlerden kaçınmak için, çeşitli SHEL blokları ile merkezi Personel bloğu arasındaki arayüzlerdeki düzensizliklerin etkileri anlaşılmalıdır. Sistemdeki gerilimlerden kaçınılması gerekiyorsa, sistemin diğer bileşenleri dikkatli bir şekilde insanlara uyarlanmalıdır.



Şekil 2-9. SHEL modeli

2.6.15 Personel bloğuna düzgün olmayan kenarlar farklı etkenler tarafından eklenir. Bireysel performansı etkileyen en önemli etkenlerden bazıları şunlardır:

a) ***Fiziksel etkenler.*** Bunlar kişinin istenen görevleri yerine getirmesi için gereken fiziksel özelliklerini, örneğin gücünü, boyunu, uzanma mesafesini, görme ve duyma yetilerini içerir.

b) ***Fizyolojik etkenler.*** Bunlar, bireyin fiziksel ve bilişsel performansını olumsuz etkileyebilen dahili fiziksel süreçlerini etkileyen etkenleri, örneğin oksijen mevcudiyetini, genel sağlık ve form durumunu, hastalık veya rahatsızlıkları, tütün, ilaç veya alkol kullanımını, stres, yorgunluk ve hamilelik durumlarını içerir.

c) ***Psikolojik etkenler.*** Bunlar, bireyin ortaya çıkabilecek tüm koşullara karşı fizyolojik olarak hazırlık derecesini etkileyen etkenleri, örneğin eğitiminin, bilgi ve deneyiminin yeterliliğini ve iş yükünü içerir.

d) ***Psiko-sosyal etkenler.*** Bunlar, bireylerin iş ortamlarında ve iş dışındaki ortamlarında taşımaları gereken baskılara neden olan, sosyal sistemdeki dış etkenleri, örneğin üstleri ile tartışmayı, işçi-yönetim tartışmalarını, ailedeki bir ölümü, kişisel maddi sorunları veya ev yaşamındaki diğer sorunları içerir.

2.6.16 SHEL modeli, özellikle havacılık sisteminin çeşitli bileşenleri arasındaki arayüzlerin görselleştirilmesinde yararlıdır.

Bu etkenler aşağıdakiler içerir:

a) ***Personel-Donanım (L-H).*** İnsan ve teknoloji arasındaki arayüz, insan performansından konuşurken en sık ele alınandır. İnsanın fiziksel iş ortamı ile nasıl ilişki kurduğunu belirler, örneğin koltukların tasarımının insanın bedeninin oturma karakteristiklerine uygun olup olmadığı, ekranların kullanıcının algılarına ve bilgi işleme karakteristiklerine uyup uymadığı ve kontrollerin kullanıcıya uygun şekilde hareket edip etmediği, kodlanıp kodlanmadığı ve konumları ele alınır. Ancak, insanlarda L-H uyumsuzluklarına uyum sağlama yönünde doğal bir eğilim vardır. Bu eğilim, sadece ortaya çıktıktan sonra görülebilir hale gelen ciddi sorunları gizleyebilir.

b) ***Personel-Yazılım (L-S).*** L-S arayüzü insanla işyerinde bulunan destek sistemleri, örneğin düzenlemeler, el kitapları, kontrol sistemleri, yayınlar, standart operasyonel prosedürler (SOP'ler) ve bilgisayar yazılım arasındaki ilişkidir. Güncellik, doğruluk, biçim ve sunum, kelime haznesi, açıklık ve sembol kullanımı gibi "kullanıcı dostu" olma sorunlarını içerir.

c) ***Personel-Personel (L-L).*** L-L arayüzü insan ve işyerindeki diğer kişiler arasındaki ilişkidir. Uçuş ekipleri, hava trafik kontrolörleri, uçak mühendisleri ve diğer operasyonel personel gruplar halinde çalışır ve grup etkileri insan performansının belirlenmesinde rol oynar. Ekip beceri yönetiminin (CRM) ortaya çıkması bu arayüze dikkatlerin önemli oranda bu arayüzde toplanmasına neden olmuştu. CRM eğitimi ve hava trafik hizmetlerindeki (ATS) (takım beceri yönetimi (TRM)) ve bakımdaki (bakım kaynak yönetimi (MRM)) uzantıları operasyonel hataların yönetilmesine odaklanmıştır. Personel/yönetim ilişkileri de, tıpkı tümü insan performansını önemli şekilde etkileyebilen kurumsal kültür, kurumsal ortam ve şirket çalışma baskıları gibi, bu arayüz kapsamında yer alır.

d) ***Personel-Ortam (L-E).*** Bu arayüz, insan ile hem dahili hem de harici ortamlar arasındaki ilişkileri içerir. Dahili işyeri ortamı sıcaklık, aydınlatma, gürültü, titreşim ve hava kalitesi gibi fiziksel koşulları içerir. Harici ortam ise görüş mesafesi, türbülans ve arazi gibi konuları içerir. 7 gün 24 saat boyunca havacılıktaki iş ortamı, örneğin uyku düzenleri gibi normal biyolojik ritimlere müdahaleleri içerir. Ek olarak, havacılık sistemi geniş bir politik ve ekonomik kısıtlamalar bağlamında yer alır, bu da genel olarak kurumsal ortamı etkiler. Burada, fiziksel tesislerin ve destek altyapısının yeterliliği, yerel finansman durumu ve düzenlemelerin etkililiği gibi etkenler de yer alır. Yakın çalışma ortamının kısa yollar kullanmak için baskı yaratması gibi, yetersiz altyapı desteği de karar verme kalitesini olumsuz etkileyebilir.

2.6.17 İşletme hatalarının arayüzlerdeki "çatlaklardan geçmemesi" için dikkatli olunmalıdır. Çoğunlukla, bu arayüzlerin bozuk kenarlarının yönetilmesi mümkündür, örneğin:

a) Tasarımcı belirtilen çalışma koşulları altında donanımın performansının güvenilirliğini sağlayabilir.

b) Sertifikasyon süreci sırasında, düzenleyici otorite donanımın kullanılabileceği gerçekçi koşullar tanımlayabilir.

c) Örgüt yönetimi, standart operasyonel prosedürler (SOP'lar) geliştirebilir ve donanımın emniyetli şekilde kullanılması için ilk eğitimleri ve tekrarlayan eğitimleri sunabilir.

d) Bireysel donanım operatörleri, donanımın istenen tüm çalışma koşulları altında emniyetli bir şekilde kullanılması için donanımı tanıdığından ve kendine güvendiğinden emin olabilir.

2.7 HATALAR VE İHLALLER

İşletme hataları

2.7.1 Havacılık endüstrisinin son yirmi yılda yaşadığı büyüme, artan hizmet talebini desteklemek için gelişmiş teknoloji olmasaydı mümkün olmayabilirdi. Modern havacılık gibi üretim yoğunluğuna sahip endüstrilerde, hizmetlerin sunulması ile ilgili gerekliliklerin karşılanması için teknoloji zorunludur. Bu, emniyet analizlerinde genellikle atlanan temel bir noktadır. Teknolojinin kullanılmaya başlaması ilk olarak emniyetin iyileştirilmesini hedef almaz; teknolojinin kullanılmaya başlaması ilk olarak, mevcut emniyet marjlarını korurken, hizmetlerin sunulmasındaki artışa yönelik talebi karşılamayı hedefler.

2.7.2 Dolayısıyla, teknoloji büyük ölçekte üretim taleplerini karşılamak için kullanılmaya başlar. Teknolojinin büyük ölçekte kullanılmaya başlamasının hedefinin hizmet sunumunun iyileştirilmesi olmasının bir sonucu, SHEL modelindeki Personel-Donanım arayüzünün dikkate alınmaması veya olması gerektiği kadar dikkate alınmamasıdır. Sonuç olarak, yeterince geliştirilmemiş bir teknoloji erken dönemde kullanılmaya başlayabilir, bu da beklenmeyen kusurlara neden olabilir.

2.7.3 Yeterince gelişmemiş teknolojinin kullanılmaya başlamasının, herhangi bir seri üretim endüstrisinin gereksinimlerinin kaçınılmaz bir sonucu olmasına karşın, emniyetin yönetimi ile ilgisi ihmal edilmesi mümkün değildir. İşletme personeli gibi ön saflardaki insanlar, hizmetleri sunmak için operasyonel görevlerini yerine getirirken her gün teknoloji ile etkileşime girmek zorundadırlar. Donanım-Personel arayüzü teknolojinin tasarımı sırasında doğru şekilde hesaba katılmamışsa ve insanlar ile teknoloji arasındaki etkileşimlerin operasyonla ilgili sonuçları dikkate alınmamışsa, sonuç açıktır: operasyonel hatalar ortaya çıkar.

2.7.4 İnsan/teknoloji sistemlerinin yeni ortaya çıkmakta olan bir özelliği olarak operasyonel hatalar perspektifi, operasyonel hatalar ile ilgili klasik, psikoloji temelli perspektifle kıyaslandığında, emniyetin yönetilmesinde son derece farklı bir perspektif sunmaktadır. Psikoloji temelli perspektife göre, hatanın kaynağı kişide "bulunur" ve farklı araştırmacı ve uygulamalı psikoloji dalları tarafından araştırılan ve açıklanan belirli psiko-sosyal mekanizmaların bir sonucudur.

2.7.5 Psikoloji temelinde bir perspektifi izleyerek operasyonel hataları tahmin etmeye ve azaltmaya çalışmak, tamamen imkansız değilse bile, son derece zordur. Seçim yaparak eldeki iş için yeterli niteliklere sahip olmayan bireyler elenebilir ve davranışlar eğitim ve düzenlemelerle etkilenebilir. Yine de, tamamen operasyonel bir bakış açısından bakıldığında, bu perspektifin eksik yönü açıktır: dikkat dağılması, yorgunluk ve unutkanlık gibi tipik insani zayıflıkların ve bunların belirli operasyonel koşullar altında bir operasyonel bağlamdaki bileşenler ve özelliklerle nasıl etkileşime girdiklerinin sistematik bir şekilde tahmin edilmesi imkansızdır. Bireyi temel alan kusur azaltma stratejileri "yumuşak" kusur azaltma girişimleri olarak değerlendirilir, çünkü insan performansındaki bozuklukların zorlu koşullarda ortaya çıkmaları gerekmez, en beklenmedik anda ortaya çıkabilir ve hasar verme potansiyellerini ortaya çıkarabilirler.

2.7.6 İnsan/teknoloji sistemlerinin yeni ortaya çıkmakta olan bir özelliği olarak operasyonel hatalar perspektifi, operasyonel hatanın kaynağını insandan alır ve fiziksel dünyada olması gereken yere, L/H arayüzüne koyar. Bu ara yüzdeki bir uyumsuzluk, operasyonel hatanın kaynağıdır. Böylece, operasyonel hata fiziksel dünyanın bir parçası olarak görülür hale gelir ve bilimsel terimler (algısal sınırlamalar) yerine operasyonel terimler (bir kolun arkasında kısmen gizli kalan bir anahtar gece operasyonları sırasında doğru konumunun görülmesini zorlaştırıyor) ile ifade edilebilir. Dolayısıyla, operasyonel hatanın kaynağı tahmin edilebilir ve operasyonel bağlamdaki müdahalelerle azaltılabilir. Emniyet yönetiminin insanın algı kısıtlamaları hakkında yapabileceği pek bir şey yoktur, ama emniyet yönetiminin kısmen gizlenmiş bir anahtarı içeren bir tasarımın sonuçları ile başa çıkmak için uygulayabileceği bir dizi seçenek vardır.

2.7.7 Havacılıktaki emniyet geleneğinde, operasyonel hataların hep çok havacılık olayında katkıda bulunan bir etken düşünülür. Yukarıdaki psikoloji temelli perspektifi temel alan bu görüşte, sanki operasyonel personelin bir operasyonel hatayı yapmak ve yapmak gibi bir seçeneği varmış ve isteyerek ilk seçeneği seçiyormuş gibi, operasyonel hatalar operasyonel personelin isteyerek yaptığı bir davranış biçimi olarak görülür. Dahası, bir operasyonel hata standartların altında performansın, karakter eksikliklerinin, profesyonellik eksikliğinin, disiplinsizliğin ve yıllarca insan performansının kısmi bir şekilde anlaşılmasının getirdiği benzer özelliklerin göstergesi olarak kabul edilir. Olayları açıklamada ve insanları suçlamada kullanışlı olsalar da, bu nitelemeler operasyonel hataların anlaşılması ve açıklanmasında yetersiz kalır.

2.7.8 İşletme hatalarını açıklayan alternatif perspektif izlendiğinde, operasyonel hataların insan/teknoloji sistemlerinde ortaya çıkan bir özellik olarak kabul edildiğinde ve hataların kaynağı L/H arayüzündeki uyumsuzluğa bağlandığında, en yeterli personelin bile operasyonel hatalar yapabileceği açıkça anlaşılır. Bu durumda, operasyonel hatalar insan ve teknoloji etkileşimi bulunan herhangi bir sistemin normal bir bileşeni olarak görülür ve bir tür hatalı davranış olarak görülmez. Hatalar, herhangi bir üretim sisteminde hizmetlerin sunulmasına yönelik operasyonel etkinlikler sırasında insan-teknoloji etkileşimlerinin doğal bir yan ürünü olarak görülebilir. İşletme hataları insan ve teknoloji etkileşimi bulunan herhangi bir sistemin normal bir bileşeni olarak görülür ve operasyonel hataları kontrol etmek için operasyonel emniyet stratejileri uygulamaya konur.

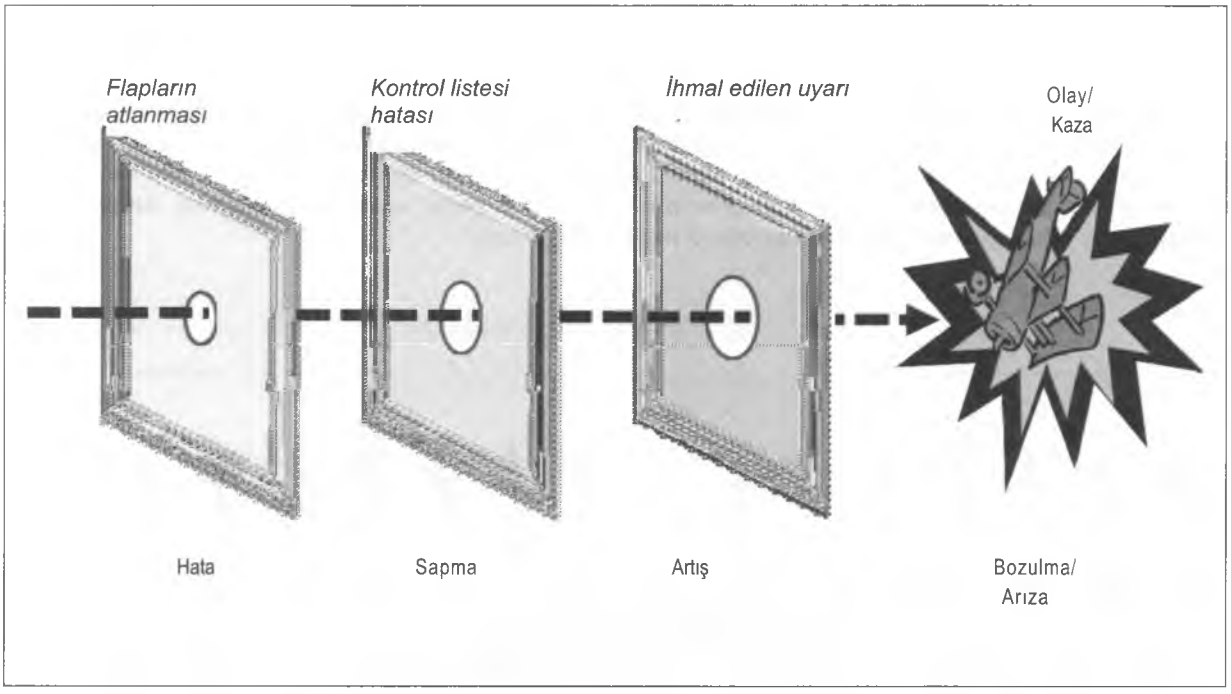
2.7.9 Havacılık operasyonlarında SHEL arayüzlerinde uyumsuzluk bulunmasının kaçınılmaz olduğu düşünüldüğünde, havacılıktaki operasyonel hataların kapsamı çok büyüktür. Bu uyumsuzlukların, işyerindeki ortalama bir insanı nasıl etkileyebileceğinin anlaşılması emniyet yönetimi için temel önemdedir. Ancak bundan sonra operasyonel hataların emniyet üzerindeki etkilerini kontrol etmek için etkili önlemler alınabilir.

2.7.10 İşletme hataları ve sonuçlarının dolaysızlığı ve büyüklüğü arasında doğrusal bir ilişki kurulması sık yapılan bir algı yanlışıdır. Bu yanlış algı 2.6.10 ve 2.6.11'de operasyonel hatalar ve sonuçlarının büyüklüğü bakımından ele alınmıştır. Burada, operasyonel hatalar ile potansiyel sonuçlarının büyüklüğü arasında bir simetri olmadığı öne sürülmektedir. Ayrıca, operasyonel hataların sonuçlarının büyüklüğünün, hatalarının kendilerinin bir sonucu olmaktan çok, hataların ortaya çıktığı operasyonel bağlamın bir fonksiyonu olduğu da öne sürülmektedir. Burada konu operasyonel hatalar ve sonuçlarının dolaysızlığı bakımından ele alınmaktadır.

2.7.11 Havacılıkta, önemli bir arıza oluşmadan önce her gün milyonlarca operasyonel hatanın yapıldığı istatistiksel bir olgudur (Şekil 2-10). Küçük yıllık dalgalanmalar bir tarafa bırakıldığında, endüstri istatistiklerinde son on yılda milyon kalkış başına birden az ölümlü kaza görülmektedir. Başka bir deyişle, dünya çapındaki ticari havayolu operasyonlarında, bir milyon üretim çevriminde bir sistem savunmalarını aşacak ve büyük bir emniyet hatasına neden olacak kadar güçlü hasar verme potansiyeline sahip bir operasyonel hata ortaya çıkar. Yine de, SHEL modelinin arayüzlerindeki uyumsuzluklar, normal havacılık operasyonları sırasında günde binlerce operasyonel hataya neden olur. Ancak, bu operasyonel hatalar, havacılık sistemine tümleşik savunma noktalarında yakalanır ve hasar verme potansiyelleri azaltılarak, olumsuz sonuçlar önlenir. Başka bir deyişle, havacılık sistemi savunmalarının her gün etkili bir şekilde yerine getirilmesiyle operasyonel hataların kontrolü sağlanır.

2.7.12 İşletme hataları ile sonuçlarının dolaysızlığı arasındaki asimetriyi açıklamak için basit bir operasyonel senaryo verilmiştir (Şekil 2-11A). Motorun çalıştırılmasından sonra, bir uçuş ekibi motor çalışması sonrası tarama akışı sırasında flapları standart çalıştırma prosedürlerinde gösterilen şekilde uygun kalkış ayarına getirmeyi atlar. Böylece bir operasyonel hata yapılmış olur, ama dolaysız sonuçları olmaz. İşletme hatası ilk savunma katmanını (SOP'ler, motorun çalıştırılmasından sonra uçuş ekibi tarama akışı sırası) aşmıştır, ama hasar verme potansiyeli hala gizli durumdadır. Dolaysız sonuç yoktur; operasyonel hata sadece örtük halde sistemde kalır.

Şekil 2-10. İşletme hataları ve emniyet – Doğrusal olmayan bir ilişki

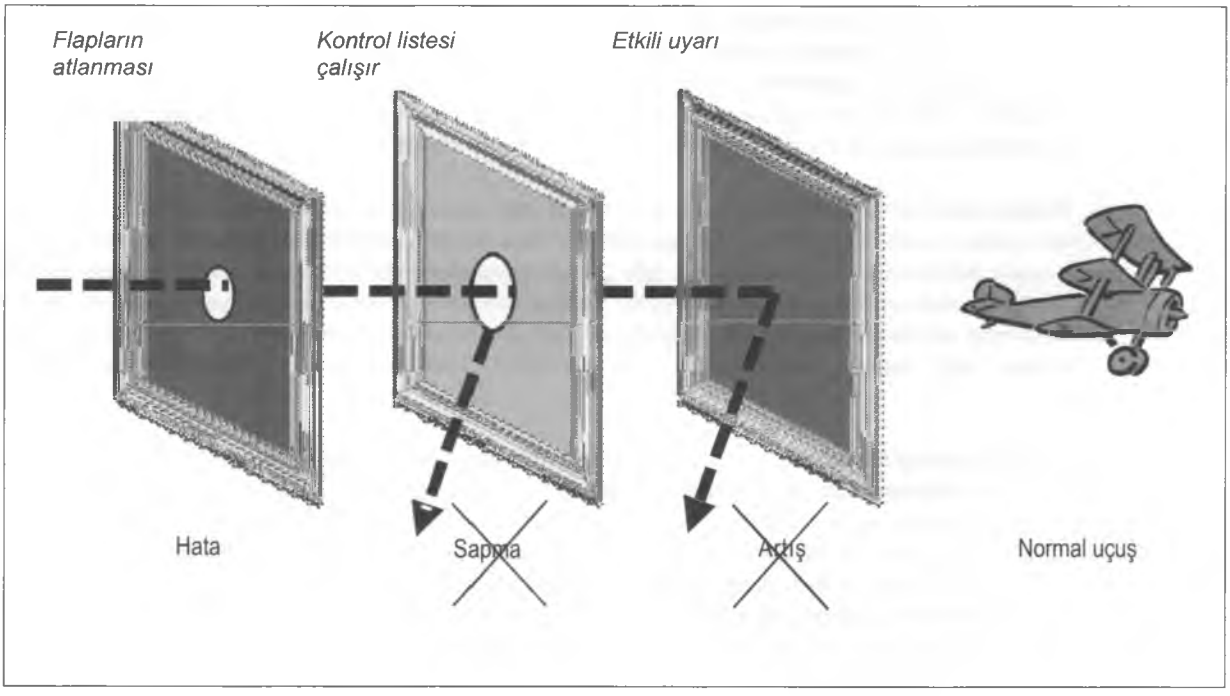


Şekil 2-11A. Önemli arızaların incelenmesi — Bir milyon uçuşta bir

2.7.13 Uçuş ekibi motor çalışması sonrası kontrol listesini yerine getirir, ama yanlış flap ayarını tespit edemez ve uçak kalkış için taksi yapmaya başlar. Böylece, hala zararsız şekilde sistemde kalmaya devam eden operasyonel hatandan kurtulmak için ikinci bir fırsat da kaçırılır. Yine de, sistem şimdi bir sapma durumunda veya istenmeyen bir durumdadır (yani uçak yanlış bir flap ayarı ile kalkış için taksi yapmaktadır). Uçuş ekibi, taksi yapma kontrol listesini ve kalkış öncesi kontrol listesini yerine getirir. Her iki durumda da, yanlış flap ayarı gözden kaçırılır. İşletme hatasının sonuçlarından kurtulmak için diğer olanaklar da kaçırılmıştır. İşletme hatası hala bir sonuca neden olmamıştır, ama sistemin sapma durumu veya istenmeyen durumu büyümektedir.

2.7.14 Uçuş ekibi kalkış işlemlerini başlatır ve kalkış uyarı yapılandırması uyarısı çalar. Uçuş ekibi uyarının nedenini belirleyemez ve kalkış işlemlerine devam eder. İşletme hatası hala bir sonuca yol açmamıştır, ama sistemin istenmeyen durumu şimdi bir artış durumuna ulaşmıştır. Uçak, yanlış flap yapılandırmasında kalkar. Sistem şimdi bir bozulma durumuna geçmiştir, ama istenmeyen durumun hala uçuş ekibi tarafından düzeltilmesi mümkündür. Uçak yanlış flap ayarı yüzünden uçmayı sürdüremez ve çakılır. Sadece bu noktada, önemli sayıda tümleşik sistem savunmasının aşılmasından sonra, operasyonel hata tam zarar verme potansiyeline ulaşmış ve bir sonuca neden olmuştur. Sistem yıkıcı bir arıza geçirir.

2.7.15 İşletme hatasının uçuş ekibi tarafından yapılması ile hasar potansiyelinin geri dönülemez şekilde gerçekleşmesi arasında göreli olarak önemli bir zaman aralığı olduğuna dikkat ediniz. Ayrıca, sisteme tümleşik savunma noktalarında operasyonel hatanın sonuçlarından kurtulmak için mevcut olanak sayısına da dikkat ediniz. Bu zaman aralığı, bir sistemin operasyonel hataların sonuçlarını kontrol etmek için sağladığı zamandır ve sistem savunmalarının derinliği ve etkinliği ile orantılıdır. Bu, emniyet yönetiminin önemli bir başarı potansiyeli ile çalışmasını sağlayan zaman aralığıdır.



Şekil 2-11B. Emniyet yönetimi — Neredeyse her uçuşta

2.7.16 Sistem ne kadar çok tümleşik savunma noktası ve önleme katmanı içerirse, performansı o kadar etkin ve operasyonel hataların sonuçlarının kontrol edilmesi olasılığı o kadar yüksek olur. Tersi de doğrudur.

2.7.17 Bu tartışmanın bakış açısından, bir sonuç açıktır: 2.7.12 ile 2.7.14 arasında tartışılan senaryo – kaçınılmaz olarak – pek çok kaza incelemesinin ulaşacağı bulgudur: yıkıcı sistem arızalarına neden olan, yönetilmeyen operasyonel hatalar. Bu, insan ve sistem kusurları hakkında değerli bir bilgidir; neyin başarısız olduğunu, neyin çalışmadığını, hangi savunma noktalarının amaçlanan şekilde çalışmadığını gösteren bilgidir. Bir temel bilgi olarak değerli olsa da, bu bilgi emniyet arızalarının tamamen anlaşılması için yeterli değildir ve alternatif kaynaklardan gelen bilgilerle tamamlanmalıdır.

2.7.18 2.7.12 ile 2.7.14 arasında verilen senaryonun değiştirilmiş bir versiyonunu düşünelim (Şekil 2-11B). İlk operasyonel hatanın (motor çalışması sonrası tarama akışı sırasında kalkış flaplarını seçmeyi atlama) hasar verme potansiyelini engellemek için savunmaların tetiklenebileceği en az dört nokta olduğuna dikkat ediniz:

a) kalkış sonrası kontrol listesi;

b) taksi yapma kontrol listesi;

c) kalkış öncesi kontrol listesi ve

d) kalkış yapılandırma uyarısı.

2.7.19 Açık olmasa da, savunmaların tetiklenmiş olabileceği başka noktalar da vardır: apron personelinin uyarıları, benzer bir uçaktaki uçuş ekibinin uyarıları, ATC personelinin uyarıları v.s. Bu durumların her birinde savunma işlemlerinin etkili bir şekilde yerine getirilmesi, ilk operasyonel hatanın sonuçlarını kontrol edebilir ve sistemi normal duruma geri getirebilirdi. Her bir durumda operasyonel hatanın hasar verme potansiyeli ortadan kaldırılabilir ve böylece pratik bakımdan operasyonel hatanın ortadan kalkmasına neden olabilirdi.

2.7.20 Burada geliştirilen argüman, yıkıcı arızalara neden olan operasyonel hataların senaryoların nadir olduğu, ancak operasyonel hataların sistemi istenmeyen duruma getirdiği senaryolarla (sapma/bozulma) sık karşılaşıldığıdır. Bu senaryolar başta neyin çalışmadığı, ama tasarlandığı gibi çalışan savunmalar da sahil olmak üzere sonrasında neyin çalıştığı hakkında bilgilerin elde edilmesini sağlar. Bu bilgiler, kazaların incelenmesine alternatif veya tamamlayıcı emniyet bilgileri kaynaklarının elde edilmesini sağladığı türden bilgilerdir. Bir kaza incelemesinden elde edilen bilgiler, savunmanın tetiklenmesi gereken dört durumu belirleyecektir, ancak büyük olasılıkla sadece neden tetiklenmediklerini açıklayabilecektir.

2.7.21 Söz konusu ek bilgi kaynakları, savunmaların tetiklenmiş olabileceği durumları belirleyecek ve neden ve nasıl tetiklemiş olabileceklerini açıklayacaktır. Bu kaynaklar başarıları karakterize ederler, böylece kazalardan elde edilen bilgileri bu alternatif kaynaklardan alınan bilgilerle bütünleştirerek, belirli emniyet sorunları hakkında daha eksiksiz bir resim sağlarlar. Ayrıca, yukarıda açıklanana benzer senaryolarla sık karşılaşıldığında, bu alternatif emniyet bilgileri kaynakları kullanıldıklarında, kazalardan elde edilen daha seyrek bilgileri tamamlamak üzere, önemli bir sürekli bilgi hacmi sağlayabilirler, böylece emniyet arızalarının daha eksiksiz bir şekilde anlaşılmasını sağlarlar. Öyleyse, bu ikinci senaryo ile ulaşılabilecek sonuç, emniyetin sağlamlığının hata barındırmayan bir operasyonel performans değil, etkili bir operasyonel hata yönetimi elde etmeye bağlı olduğudur.

İşletme hatalarını kontrol etmek için üç strateji

2.7.22 İşletme hatalarının kontrol edilmesine yönelik üç temel strateji, havacılık sisteminin üç temel savunma noktasını temel almaktadır: teknoloji, eğitim ve düzenlemeler (süreçler dahil olmak üzere).

2.7.23 ***Azaltma stratejileri*** operasyonel hataya katkıda bulunan etkenleri azaltarak veya ortadan kaldırarak, doğrudan operasyonel hatanın kaynağına müdahale eder. Azaltma stratejisi örnekleri arasında bakım için uçak parçalarına erişimin iyileştirilmesi, yapılacak görevdeki aydınlatmanın iyileştirilmesi ve ortamda dikkat dağıtan unsurların azaltılması bulunur, örneğin:

a) insan merkezli tasarım;

b) ergonomik etkenler ve

c) eğitim.

2.7.24 ***Yakalama stratejileri*** operasyonel hatanın zaten yapılmış olduğunu kabul eder. Amaç, operasyonel hatayı, herhangi bir olumsuz etkisi hissedilmeden "yakalamaktır". Yakalama stratejileri, doğrudan hatayı ortadan kaldırmaya hizmet etmemeleri bakımından azaltma stratejilerinden farklıdır, örneğin:

a) kontrol listeleri;

b) görev kartları ve

c) uçuş koridorları.

2.7.25 ***Tolerans stratejileri*** bir sistemin ciddi sonuçlara yol açmadan bir operasyonel hatayı kabul etme becerisine atıfta bulunur. İşletme hatalarına karşı bir sistemin toleransını arttırmak alınabilecek önlemlerin örneklerinden biri yedekleme sağlamak için bir uçakta çoklu hidrolik veya elektrik sistemleri bulundurmak veya bir yorgunluk çatlağını kritik uzunluğa erişmeden tespit etmek için çok sayıda olanak sağlayan bir yapısal denetim programı oluşturmaktır, örneğin:

a) sistem yedeklemeleri

b) yapısal denetimler.

2.7.26 İşletme hatalarının yönetimi sadece ön saflardaki personelle sınırlanmamalıdır. SHEL modelinde de gösterildiği gibi, ön saflardaki personelin performansı örgütle, düzenlemelerle ilgili ve çevresel etkenlerden etkilenir. Örneğin, yetersiz iletişim, muğlak prosedürler, makul olmayan programlamalar, yetersiz kaynaklar ve gerçekçi olmayan bütçelendirme gibi örgütlenme süreçleri operasyonel hataların çoğalma ortamını oluştururlar. Daha önce açıklandığı gibi, tüm bu süreçler bir örgütün üzerinde makul bir derecede doğrudan kontrole sahip olduğu etkinliklerdir.

Hatalar karşısında ihlaller

2.7.27 Buraya kadar, bu bölümde ele alınanlar, sistem üretim hedeflerine ulaşılması için insan ve teknoloji arasında etkileşimin bulunduğu herhangi bir sistemin normal bir parçası olarak tanımlanan operasyonel hatalarına odaklanıyordu. Bundan sonra ise, operasyonel hatalardan oldukça farklı olan ihlaller ele alınacaktır. Her ikisi de sistemde arıza oluşmasına neden olabilir ve yüksek miktarda sonuç içeren durumlara yol açabilir. İşletme hataları ve ihlalleri arasında açık bir ayrım yapılması ve bu kavramların anlaşılması emniyet yönetimi için zorunludur.

2.7.28 İşletme hataları ve ihlalleri arasındaki temel fark kasıttadır. Hata kasıtsızken, ihlal kasıtlı bir eylemdir. İşletme hataları yapan kişiler doğru olanı yapmaya çalışmaktadır, ama operasyonel hatalar hakkındaki önceki paragraflarda açıklanan pek çok nedenle, beklentileri karşılayamamaktadırlar. Diğer taraftan ihlalde bulunan kişiler, oluşturulmuş prosedürler, protokoller, normlar veya uygulamalardan sapma içeren bir davranışa girdiklerinde ne yaptıklarını bilmektedirler, ancak kasıtlı bir şekilde davranmaktadırlar.

2.7.29 Örneğin, bir kontrolör iki uçak arasındaki DME mesafesi 18 NM iken bir uçağın seyir halindeki bir uçağın seviyesinden geçerek izin vermektedir ve bu durum doğru mesafenin en az 20 NM olduğu koşullarda gerçekleşmiştir. Kontrolör pilotlar tarafından önerilen DME mesafelerdeki farkı yanlış hesaplamışsa, bu bir operasyonel hata olacaktır. Kontrolör mesafeyi doğru hesaplamış ve minimum ayrım mesafesinin mevcut olmadığını bilerek alçalan uçağın seyir halindeki uçağın seviyesinden geçmesine izin vermişse, bu bir ihlal olacaktır.

2.7.30 Havacılıkta, çoğu ihlal insanların görevlerini yerine getirmek için ara çözümler geliştirdikleri sorunlu veya gerçekçi olmayan prosedürlerin sonucudur. Çoğu, işi iyi yapma isteğinden doğar. Nadiren ihmalkarlık sonucudurlar. İki genel ihlal tipi vardır: durumsal ihlaller ve rutin ihlaller.

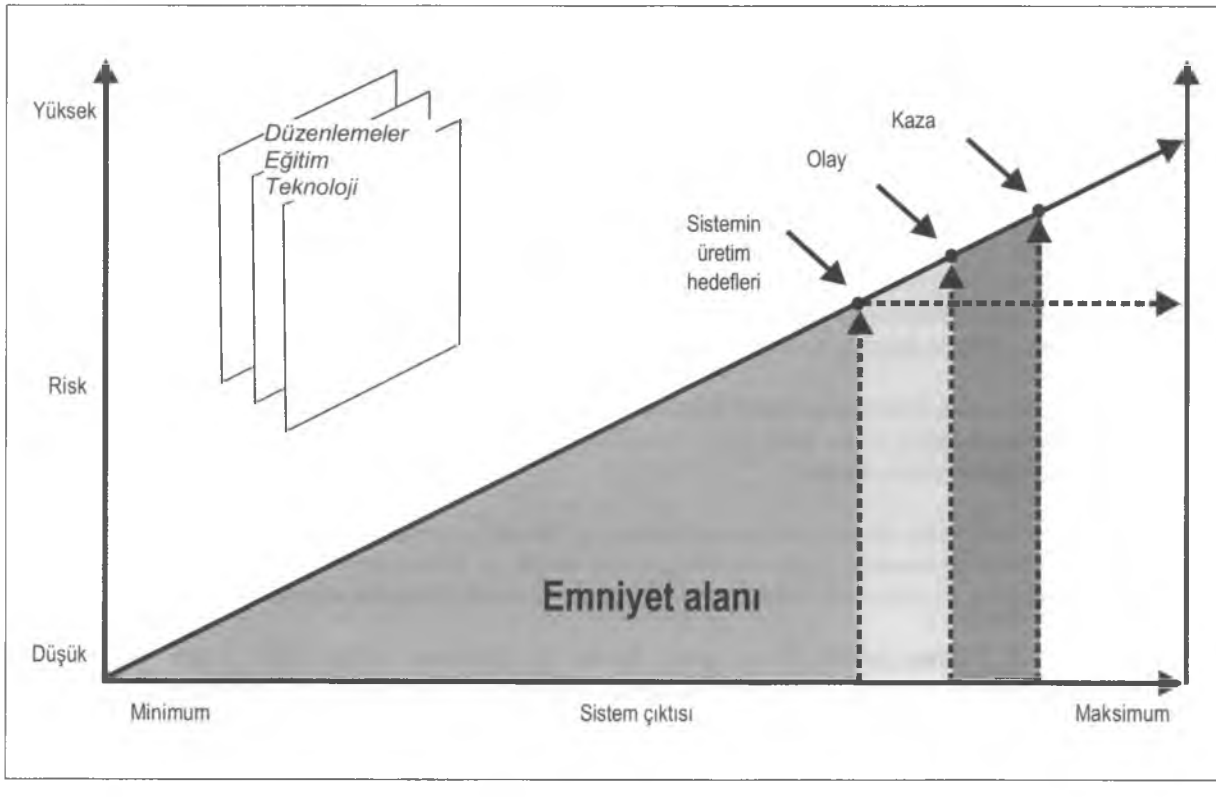
2.7.31 ***Durumsal ihlaller*** zaman baskısı veya yüksek iş yükü gibi, o anda mevcut belirli etkenlerden kaynaklanır. Bir ihlale yol açacağının bilinmesine karşın, hedefe yönelmiş olmak ve görevi yerine getirmek istemek insanların, bu sapmanın olumsuz sonuçlara neden olmayacağı inancıyla normlardan sapmasına neden olur.

2.7.32 ***Rutin ihlaller*** bir iş grubu içinde "işi yapmanın normal yolu" haline gelen ihlallerdir. Uygulanabilirlik/işletilebilirlik sorunları, insan-teknoloji arayüz tasarımındaki bozukluklar v.s. nedeniyle iş grubu yerleşik prosedürleri izleyerek işi yapmada zorlandığında ve resmi olmayan şekilde, daha sonra rutin haline gelen "daha iyi" prosedürler geliştirdiklerinde ve uyguladıklarında ortaya çıkarlar. Bu, 2.5.4'te ele alınan şekilde sapma durumunun normalleştirilmesidir. Rutin ihlaller iş grubu tarafından nadiren ihlal olarak değerlendirilir, çünkü amaçları işin yapılmasını sağlamaktır. Bir görevi basitleştirerek (köşelerin yontulmasını içerse de) zaman ve çaba tasarrufu sağlamayı hedeflediklerinden, cihazların "optimize edilmesi" olarak değerlendirilirler.

2.7.33 Genellikle görmezden gerilen üçüncü bir ihlal tipi, rutin ihlallerin genişletilmesi olarak da görülebilecek olan **örgütlenmeden kaynaklanan ihlallerdir**. İhlallerin taşıyabileceği emniyet mesajının tam potansiyeli sadece, örgütün vermek için oluşturulduğu hizmetlerin sunulması ile ilgili olarak örgüt tarafından yüklenen taleplere karşı ele alındığında anlaşılabilir. Şekil 2-12'de bir örgütün hizmetlerinin sunulması ile ilgili olarak ve örgütlenme süreçlerinin tanımlanması sırasında dengelemesi gereken iki temel düşünce, yani sistem çıktısı ve ilgili emniyet riskleri arasındaki ilişkiyi göstermektedir.

2.7.34 Hizmet sunmaya yönelik her örgütte, sistem çıktıları ve emniyet riskleri iç içe geçmiştir. Sistem çıktısına (yani hizmetlerin sunulmasına) talepler arttıkça, risklere maruz kalma oranı da artacağından, hizmetlerin sunulması ile ilgili emniyet riskleri de artar. Bu nedenle, Şekil 2-12'de gösterildiği gibi, minimum sistem çıktısı en düşük emniyet riskine karşılık gelirken, maksimum sistem çıktısı da en yüksek emniyet riskine karşılık gelir. En yüksek emniyet riskine maruz kalarak sürekli çalışma, sadece emniyet açısından değil, mali açıdan da istenen bir şey değildir. Dolayısıyla, örgütler istenen çıktı ve tolere edilebilir emniyet riskini dengelerler ve sistem çıktısını mümkün olan maksimum değerden az, ama tolere edilebilir bir emniyet riskine karşılık gelecek bir değerde tanımlarlar. Böylece, örgüt üretim hedeflerini kabul edilebilir çıktıyı kabul edilebilir emniyet riski ile dengeleyecek bir fonksiyon olarak tanımlar.

2.7.35 Üretim hedeflerini tanımlama süreci ile ilgili temel bir karar (sistem çıktısı ile emniyet riskleri arasındaki bir denge temelinde uzlaşılan) örgütün üretimde bulunduğu sırada kendini emniyet risklerinden korumak için geliştirmesi gereken savunma noktalarının oluşturulmasıdır. Daha önce açıklandığı gibi, havacılık sistemindeki üç temel savunma noktası teknoloji, eğitim ve düzenlemelerdir (prosedürler dahil olmak üzere). Bu nedenle, üretim hedeflerini tanımlarken, örgütün aynı zamanda hizmetin emniyetli ve etkin bir şekilde sunulması için gereken araçları (teknolojiyi), işgücünün araçları emniyetli ve etkin bir şekilde kullanması için gereken davranışlarının nasıl oluşturulacağını (eğitimi) ve işgücü performansını belirleyen normlar ve prosedürler kümesini (düzenlemeleri) tanımlaması gerekir.



Şekil 2-12. İhlallerin anlaşılması

2.7.36 Dolayısıyla, sistem çıktısı, emniyet riski seviyesi ve savunma noktaları, örgütün üretim hedeflerini tanımlayan noktaya yakınsar. Aynı zamanda "örgütün emniyet alanı" olarak adlandırılabilecek sınırları gösterirler. Emniyet alanı korumalı bir alanı, örgütün oluşturduğu savunma noktalarının, üretim hedefleri bakımından sistem çıktısını sağlarken örgütün karşılaşacağı emniyet risklerine karşı maksimum dayanma oranını sağladığı bir alanı temsil eder.

2.7.37 Maksimum dayanma oranının bu emniyet alanı tarafından sağlanmasının nedeni, örgüt tarafından oluşturulan savunma noktalarının planlanan sistem çıktısı ile orantılı olmasıdır, yine bu sistem çıktısı da tolere edilebilen emniyet riski ile orantılıdır. Başka bir deyişle, örgüt tarafından korumaya ayrılan kaynaklar hizmetlerin sunulması ile ilgili etkinliklere uygundur ve bu etkinliklerle orantılıdır. Bu, örgütün bir kaza yaşamayacağı anlamına gelmez, çünkü kazalar öngörülemeyen koşulların bir araya gelmesinden kaynaklanan rasgele olaylardır. Örgütün emniyet yönetimi için, öngörülebilir koşullar altında hizmetlerin sunulması sırasında emniyet risklerinin kabul edilebilir bir seviyede kontrolünü sağlayan düzenlemelere sahip olduğu anlamına gelir. Basitçe dile getirmek gerekirse, örgüt emniyet bakımından elinden gelenin en iyisini yapmış demektir.

2.7.38 Havacılığın dinamik doğası düşünüldüğünde, havacılık örgütleri kısa süreler boyunca artan çıktıya (yani artan hizmet sunumuna) yönelik geçici, kısa vadeli taleplerle karşı karşıya kalabilirler, örneğin koltuk taleplerinde sezona bağlı değişimler, dünya çapında bir spor etkinliği gibi özel durumlar v.s. yaşanabilir. Emniyet alanının korunabilmesi için, örgüt mevcut kaynak dağılımını gözden geçirmeli ve yeniden düzenlemeli veya değiştirmelidir ve artan çıktı ve buna bağlı olarak artan emniyet riski seviyesi ile başa çıkmak için mevcut savunma noktalarını güçlendirmelidir.

2.7.39 Ne yazık ki, havacılık endüstrisi aksini gösterir. Emniyet arızalarının sonrasında görüldüğü gibi, havacılık örgütleri sıklıkla kısa süreli sistem çıktısı artışlarıyla savunma noktalarını "esneterek" başa çıkmaya çalışırlar: ek personel alımı yerine fazla mesaiye başvurmak, dolayısıyla artan iş yüküne ve yorgunluğa neden olmak; yeni teknoloji kullanmak yerine teknolojiyi "daha etkin" şekillerde kullanmak; standart operasyonel prosedürleri ve normlarını gözden geçirmeden prosedürleri ve kaynakları "optimize etmek" v.s. gibi.

2.7.40 Savunma noktalarının bu şekilde esnetilmesi aslında örgütü emniyet alanının dışına, önce ihlal alanına ve nihayetinde, istisnai ihlal alanına taşır. Başka bir deyişle, artan çıktıyı aynı miktarda kaynakla sunmak için, operasyonel personel yerleşik süreçlerden örgüt tarafından izin verilmiş kısa yollara veya ara çözümlere sapmak zorunda kalır. Bu tür kısa yollara veya ara çözümlere başvurmayı seçen operasyonel personel değildir, örgüttür. "Şirkete omuz vermek" deyimi aslında insanların sağlanan kaynaklarla oransız bir sistem çıktısı sağlamak için örgüt tarafından onay verilen sapmalara nasıl zorlandığını gösteren anlamlı bir ifadedir.

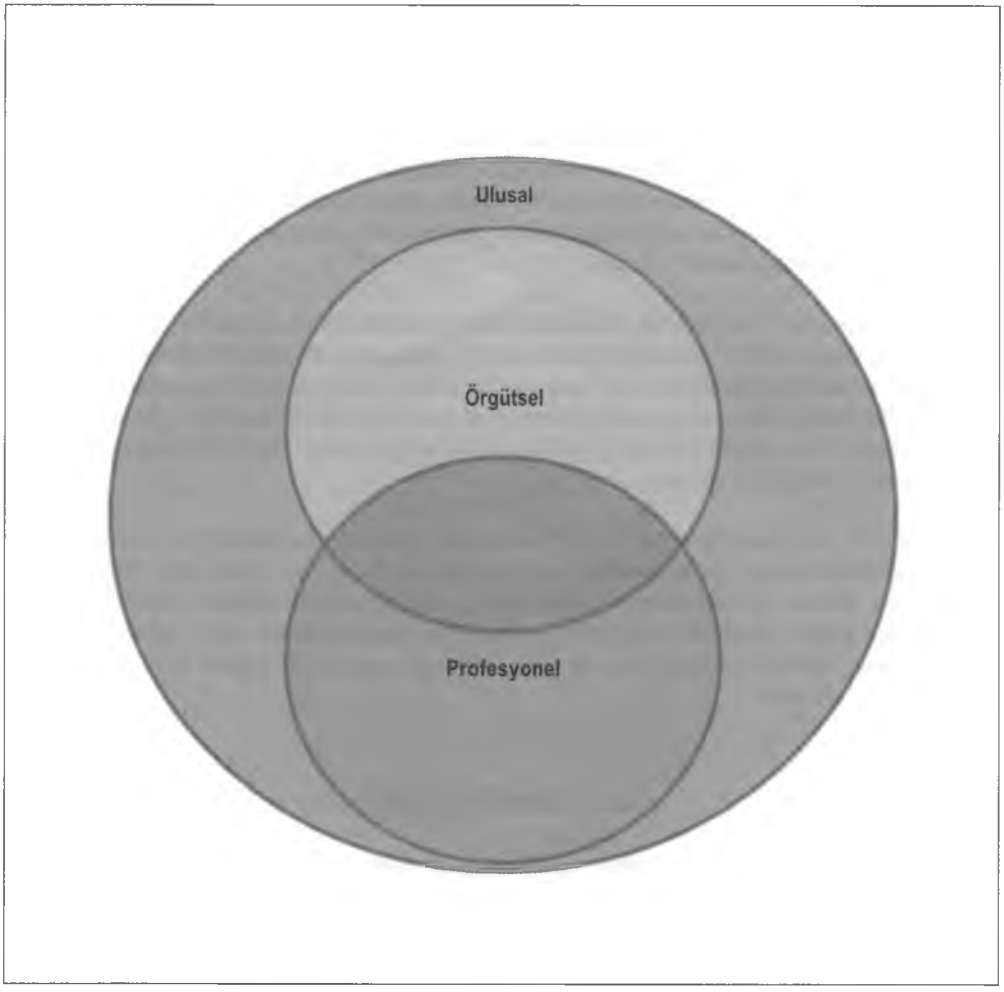
2.7.41 Örgütün ihlal alanına sürüklendiğinin somut kanıtları genellikle olaylar tarafından sağlanır. Öğrenmeyi bilen bir örgüt bu durumda, sistem çıktısı, tolere edilebilir emniyet riski ve savunma riskleri arasındaki uyumu korumak için kaynaklarının dağıtılma şeklini emniyet alanını genişletecek şekilde yeniden değerlendirecek veya emniyet alanını genişletemiyorsa, sistem çıktısını azaltarak yerleşik emniyet alanına geri dönecektir. Bazı örgütler ise olayların sağladığı uyarıları görmezden gelir, hareket şekillerinde ısrar eder ve kaçınılmaz olarak istisnai ihlal alanına sürüklenirler. Bu durumda bir kaza olası bir sonuçtur.

2.8 ÖRGÜT KÜLTÜRÜ

2.8.1 Kültür en basit şekliyle "zihnin ortaklaşa programlanması" olarak tanımlanabilir. Kültürün en grafik tanımlarından biri, kültürü "zihnin yazılımı" olarak tasvir eder. Kültür çeşitli sosyal grupların diğer üyeleri ile paylaştığımız değerleri, inançları ve davranışları etkiler. Kültür, grupların üyeleri olarak bizi birbirimize bağlar ve hem normal hem de olağan dışı durumlarda nasıl davranmamız gerektiğinin ipuçlarını sağlar. Kültür oyunun kurallarını belirler veya insanlar arasındaki tüm etkileşimlerimizin çerçevesini tanımlar. İnsanların belirli bir sosyal ortamda ilişkilerini yürütme şeklinin toplamından oluşur ve olayların gerçekleştiği bağlamı sağlar. Emniyet yönetimi bakımından, kültür insan performansının önemli bir belirleyicisi olduğundan, kültürün anlaşılması bağlamın anlaşılması kadar önemlidir.

2.8.2 Kültürü ve özellikle de havacılık emniyetini etkileyebileceklerinden kültürler arası sorunları incelerken düşülen ortak bir hata, kasıtsız olarak yargıda bulunmak ve belirli bir kültürü diğerinden "daha iyi" veya "daha uygun" veya belirli bir kültürü belirli emniyet önerileri için "kötü" veya "uygunsuz" olarak sunmaktır. Kültürler arası sorunların araştırılması – emniyet bakımından – yargılar değil, farkların araştırılmasını içerdiğinden bu uygunsuz ve yarar getirmeyen bir durumdur. Kültürler birbirinden farklıdır ve her bir kültürün önemli güçlü yönleri olabileceği gibi, tanımlanabilir zayıflıkları da vardır. Emniyet yönetime uygulandığında, ciddi kültürlerarası çalışmaların amacı, bir araya gelen kültürel zayıflıkların olumsuz yönlerini en aza indirirken, bir araya gelen kültürel güçlü yönleri, emniyet uygulamaları ile ilgili oldukları noktalarda daha da güçlendirmektir.

2.8.3 İnsanlardan oluşan gruplar olarak, örgütler kültürel etkenlerden bağımsız değildirler. Örgüt performansı her seviyede kültürel etkilere açıktır. Aşağıdaki üç kültür seviyesi (Şekil 2-13), bu üç seviye örgüt performansının belirleyicileri olduğundan, emniyet yönetimi girişimleri ile ilgilidir:



Şekil 2-13. Üç farklı kültür

a) ***Ulusal kültür*** ulusların ulusal karakteristikleri ve değer sistemlerinin farklarını ortaya koyar. Farklı uluslardan insanlar, örneğin, otoriteye tepkileri, belirsizlik ve muğlaklıkla nasıl başa çıktıkları ve bireyselliklerini nasıl ifade ettikleri bakımından birbirinden farklıdırlar. İnsanlar grubun (takım veya örgüt) ortak gereksinimlerine aynı şekilde uyum sağlamazlar. Örneğin, kolektivist kültürlerde eşitsiz durumda olmak kabul edilebilir ve liderlere saygı gösterilir. Bu, yaşlıların kararlarının veya eylemlerinin sorgulanması olasılığını etkileyebilir; bu örneğin takım çalışmasında önemli bir sorun olabilir. Dolayısıyla ulusal kültürlerin bir araya getirildikleri görevlendirmelerde, yanlış anlaşılmalar nedeniyle takım performansı etkilenebilir.

b) ***Profesyonel kültür*** belirli profesyonel grupların karakteristikleri ve değer sistemlerinin farklarını ortaya koyar (pilotların tipik davranışlarının karşısında hava trafik kontrolörlerinin veya bakım mühendislerinin davranışları). Personel seçimi, eğitim, iş deneyimi, meslektaşların baskısı v.s. nedeniyle profesyoneller (doktorlar, avukatlar, pilotlar, kontrolörler) meslektaşları ile uyumlu değer sistemlerini kabul etme ve benzer davranış şekilleri geliştirme eğilimi gösterirler; benzer şekilde "yürümeyi ve konuşmayı" öğrenirler. Genellikle mesleklerin gurur duyarlar ve mesleklerinde öne çıkmaya çalışırlar. Diğer yandan, kişisel dokunulmazlıklarına, kişisel sorunlarının performanslarını etkileyemeyeceğine veya stresli durumlarda hata yapmayacaklarına dair bir his geliştirmelerine neden değer sistemlerini de kabul edebilirler.

c) ***Örgüt kültürü*** belirli örgütlerin karakteristikleri ve değer sistemlerinin farklarını ortaya koyar (bir şirketin üyelerinin davranışına karşı diğer şirketin üyelerinin davranışları veya devlet sektörü karşısında özel sektör davranışı). Örgütler ulusal ve profesyonel kültürler için bir çatı oluşturur. Örneğin, bir havayolunda, pilotlar farklı profesyonel arka planlardan gelebilirler (askeri veya sivil, küçük havalimanlarına uçuşlar veya günlük hatlardaki uçuşların karşısında büyük uçaklarla uçuşlar). Kurumsal birleşmeler veya işten çıkarmalar nedeniyle farklı örgüt kültürlerinden de gelebilirler.

2.8.4 Yukarıda açıklanan üç kültürel grup operasyonel bağlamlarda etkileşime girer. Bu etkileşimler, örneğin aşağıdaki durumları belirler:

a) astların üstleriyle ilişkileri;

b) bilginin nasıl paylaşıldığı;

c) personelin zorlu operasyonel koşullarda nasıl tepki verdiği;

d) belirli teknolojilerin nasıl karşılanacağı;

e) otoritenin nasıl kurulacağı ve örgütlerin operasyonel hatalarına nasıl tepki gösterecekleri (karşı gelenlerin cezalandırılması veya deneyime dayalı öğrenme);

f) otomasyonun nasıl kullanılacağı;

g) prosedürlerin (SOP'lar) nasıl geliştirileceği;

h) dokümantasyonun nasıl hazırlanacağı, sunulacağı ve alınacağı;

i) eğitimin nasıl geliştirileceği ve sunulacağı;

j) görev atamalarının nasıl yapılacağı;

k) farklı çalışma gruplarının (pilotlar, ATC, bakım personeli, kabin ekibinin) ilişkileri ve

l) yönetim ve sendika ilişkileri.

Başka bir deyişle, kültür neredeyse tüm kişiler arası ve örgütler arası etkileşimler üzerinde etkiye sahiptir. Ek olarak, kültürel hususlar donanım ve araçların tasarımına da etkide bulunur. Teknoloji kültür bakımından nötr görünebilir, ama üreticisinin eğilimlerini de yansıtır (dünyadaki bilgisayar yazılımların çoğunda örtük olarak bulunan İngilizce eğilimini düşününüz). Yine de, yukarıdaki tüm açıklamalara karşın, doğru veya yanlış kültür yoktur; kültürler ne ise odur ve her birinin çeşitli güçlü yönleri ve zayıflıkları vardır.

2.8.5 Emniyet yönetimi için etkili, üretken bir kültür oluşturmanın ve yeşertmenin en genel kapsamı örgüt seviyesidir. Havacılıktaki operasyonel personel örgütlerindeki değer sisteminin getirdiği günlük davranışlardan etkilenir. Örgüt emniyetle ilgili liyakati tanıyor mu, bireysel inisiyatifleri destekliyor mu, emniyet riski toleransını teşvik ediyor mu, engelliyor mu, katı SOP uyumu zorunluluğu uyguluyor mu, SOP'ların ihlal edilmesini tolere ediyor mu veya iki taraflı açık iletişimleri destekliyor mu? Dolayısıyla, örgüt çalışanların örgütün iş alanındaki hizmetlerin sunulmasını destekleyen operasyonel etkinlikleri gerçekleştirirken yapacakları davranışların en önemli belirleyicisidir. Örgüt kültürü normları ve limitleri koyarak işyerindeki kabul edilen operasyonel performansın sınırlarını çizer. Dolayısıyla, örgüt kültürü yönetimin ve çalışanların karar verme sürecinde bir yapıtaşı oluşturur: "Burada işleri böyle yaparız ve burada işleri yapma şeklimiz hakkında böyle konuşuruz".

2.8.6 Öyleyse, örgüt kültürü paylaşılan inançlar, uygulamalar ve tavırlardan oluşur. Etkili, üretken bir örgüt kültürünün biçimi, üst yönetiminin sözleri ve eylemleri ile oluşturulur ve geliştirilir. Örgüt kültürü, çalışanların diğer uygulamaların yanında, emniyet uygulamalarına yönelik tavırlarını da belirleyen üst yönetim tarafından oluşturulan atmosferdir. Örgüt kültürü aşağıdakiler gibi etkenlerden etkilenir:

a) politikalar ve prosedürler;

b) denetim uygulamaları;

c) emniyet planlaması ve hedefleri;

d) güvensiz davranışa verilen tepki;

e) çalışan eğitimi ve motivasyonu ve

f) çalışanların ortak olması ve "satın alma".

2.8.7
Sağlam emniyet uygulamalarının oluşturulması ve bu uygulamalara uyulmasında en büyük sorumluluk, ister havayolu, ister havaalanı, ATS veya bir AMO olsun, örgütün yöneticilerinde ve yönetimindedir. Bir örgütün emniyetle ilgili değerler sistemi, en baştan üst yönetimin emniyetli operasyonların ve ortaya çıkan emniyet sorunları ile başa çıkmanın sorumluluğunu kabul etmesi ile oluşturulur.

2.8.8 Bölüm yönetiminin günlük etkinliklerle nasıl ilgilendiği, emniyet yönetimi için üretken bir örgüt kültürü oluşturulmasında temel önem taşır. Bölümdeki gerçek deneyimlerden doğru dersler çıkarılıyor mu ve uygun eylemler gerçekleştiriliyor mu? Etkilenen personel yapıcı şekilde bu süreç içinde yer alıyor mu, yoksa kendilerini yönetimin tek taraflı eylemlerinin kurbanı olarak mı görüyorlar?

2.8.9 Bölüm yönetiminin düzenleyici otoritenin temsilcileri ile ilişkisi de, üretken bir örgüt kültürünün göstergesidir. Bu ilişki profesyonel nezaket içermelidir, ama hesap verme sorumluluğuna zarar vermeyecek bir mesafe korunmalıdır. Açıklık, düzenlemelerin katı bir şekilde uygulamasından daha iyi emniyet iletişimi sağlayacaktır. İlk yaklaşım yapıcı diyalogları desteklerken, ikincisi gerçek emniyet sorunlarının gizlenmesine veya görmezden gelinmesine yol açar.

2.8.10 Emniyet düzenlemelerine uyulması sağlam emniyet uygulamalarının geliştirilmesinde temel önemde olsa da, çağdaş düşünceye göre çok daha fazlası gerekir. Sadece düzenlemelerin getirdiği minimum standartlara uyan örgütler ortaya çıkan emniyet sorunlarını belirlemek için doğru şekilde konumlanmamıştır.

2.8.11 Emniyetli operasyonları desteklemenin etkili bir yöntemi, bir operatörün tüm personelin kendilerini sorumlu hissettiği ve yaptıkları her şeyin emniyet üzerindeki etkisini düşündüğü bir operasyonel ortamı yaratmaktır. Bu düşünme şekli etkinliklerinde o kadar köklü hale gelir ki, gerçekten "burada işlerin bu şekilde yapıldığı" düşüncesi haline gelir. Yönetim kurulu, aprondaki bir sürücü veya bir mühendise ait olsun, tüm kararlarda, kararın emniyet üzerindeki etkileri dikkate alınmalıdır.

2.8.12 Bu tür bir operasyonel ortam "üstten alta" doğru oluşturulmalıdır ve işçiler ile yönetim arasında yüksek seviyede güven ve saygı olmasına dayanır. Çalışanlar emniyetle ilgili tüm kararlarda desteklenecek lerine inanmalıdır. İşletmeyi tehlikeye atan kasıtlı emniyet ihlallerine tolerasyon gösterilmeyeceğini de anlamalıdırlar.

Etkili emniyet raporlaması

2.8.13 Emniyet yönetimi bakımından bir örgüt kültürünün en etkili yönlerinden biri, emniyetle ilgili raporlama prosedürlerini ve operasyonel personelin uygulamalarını biçimlendirmesidir. Tehlikelerin tanımlanması emniyet yönetiminin altında yatan temel bir etkinliktir. Kimse tehlikelerinin varlığının bildirilmesinde ve neyin olması gerektiği gibi olduğunun ve neyin olmadığının bildirilmesinde, her gün tehlikelerle birlikte yaşamak ve tehlikelerle karşı karşıya gelmek zorunda olan operasyonel personelden daha iyi konumda değildir. Dolayısıyla, tehlikelerin operasyonel personel tarafından etkili bir şekilde raporlanması, emniyet yönetiminin yapıtaşlarından biridir. Bu nedenle, operasyonel personelin tehlikeleri raporlamak için eğitildiği ve sürekli olarak cesaretlendirildiği bir operasyonel ortam, etkili emniyet raporlamasının ön koşuludur.

2.8.14 Etkili emniyet raporlaması, aşağıdaki gibi belirli temel özellikler üzerine inşa edilir:

a) üst yönetim emniyet yönetimi stratejisinin bir parçası olarak tehlikelerin tanımlanmasına özel önem verir ve sonuç olarak örgütün her seviyesinde tehlike bilgilerinin iletilmesinin önemi hakkında farkındalık oluşur;

b) üst yönetim ve operasyonel personel örgütün hizmet sunma etkinliklerinde karşılaşılan tehlikeler hakkında gerçekçi bir görüş sahibi olurlar, bunun sonucunda tehlikeler ve potansiyel hasar kaynakları ile ilgili daha gerçekçi kurallar konur;

c) üst yönetim etkin tehlike raporlamasını desteklemek için gereken operasyonel gereklilikleri tanımlar, önemli emniyet verilerinin doğru şekilde kaydedilmesini sağlar, operasyonel personel tarafından tehlikelerin raporlanmasına açık bir tavır sergiler ve tehlikelerin sonuçlarının ele alınması için önlemler alır;

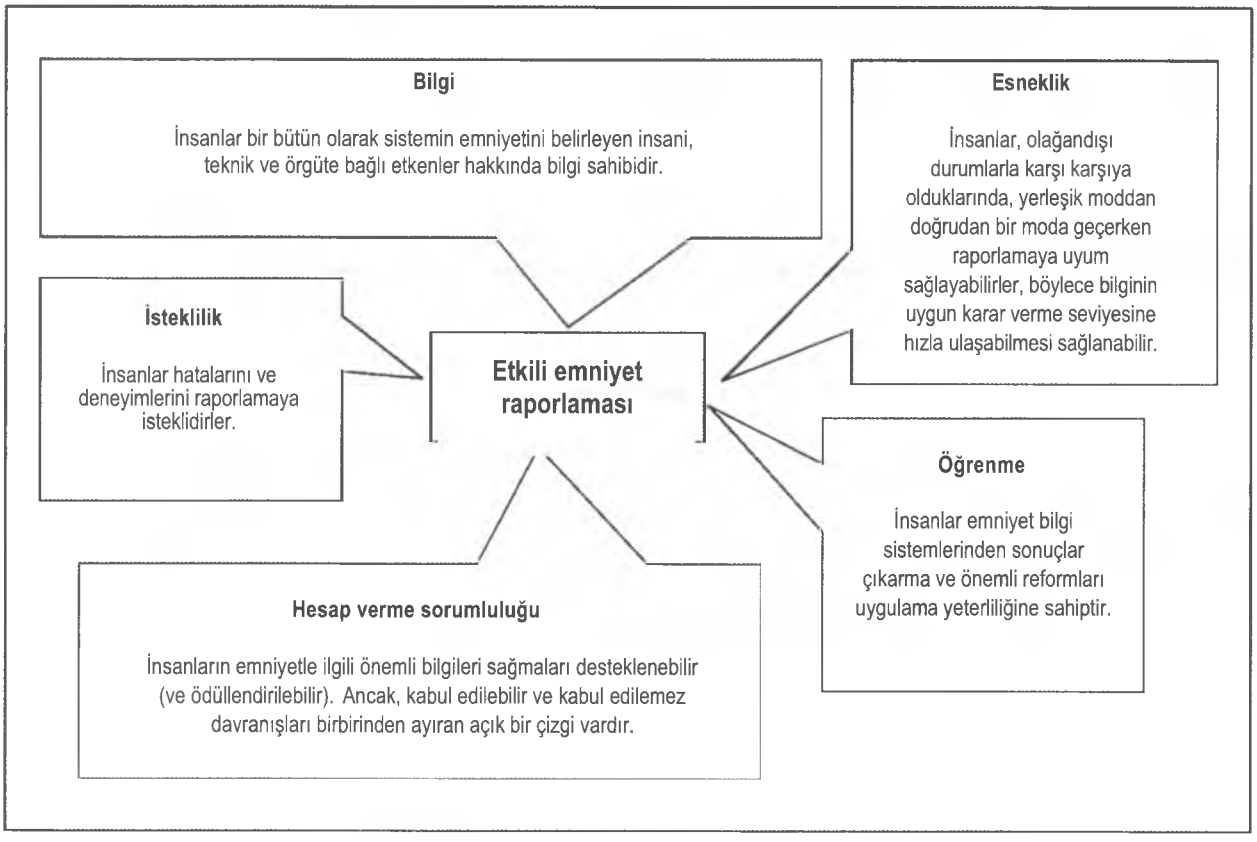
d) üst yönetim önemli emniyet verilerinin uygun şekilde korunmasını sağlar ve tehlikeleri bildirenlerin tehlike raporlamasının başka bir amaçla (emniyet yönetimi dışında) kullanılmayacağından emin olmaları için kontrollü ve dengeli bir sistem oluşturulmasını destekler;

e) personel tehlikelerin farkına varılması ve raporlanması ve tehlikelerin hizmetlerin sunulmasındaki etkinlikler üzerindeki etkilerinin anlaşılması için eğitilir;

f) tehlikeli davranışlar daha az sıklıkta ortaya çıkar ve bu tür davranışları engelleyen bir emniyet etiği vardır.

Etkili emniyet raporlaması – Beş temel unsur

2.8.15 Evrensel olarak, etkili emniyet raporlaması sistemleri ile ilişkilendirilen beş temel unsur vardır. (Şekil 2-14). Bu beş temel unsur etkili emniyet raporlamasının 2.8.14'te açıklanan temel özellikleri ile ilgilidir:



Şekil 2-14. Etkili emniyet raporlaması – Beş temel unsur

a) ***İsteklilik.*** Üst yönetimin etkin tehlike raporlamasını desteklemek ve önemli emniyet verilerinin doğru şekilde kaydedilmesini sağlamak için gereken operasyonel gereklilikleri tanımlamak için gösterdiği bilinçli çabaların sonucu olarak, operasyonel personel tehlikeleri, tehlikelere maruz kalmaktan kaynaklanabilecek operasyonel hataları ve uygun olduğunda kişisel deneyimlerini raporlamak için isteklidirler.

b) ***Bilgi.*** Tehlikeleri tanımak ve raporlamak ve hizmetlerin sunulmasını destekleyen etkinliklerdeki tehlikelerin ortaya çıkma sıklıklarını ve sonuçlarını anlamak için verilen formel eğitimin sonucu olarak, operasyonel personel bir bütün olarak sistemin emniyetini belirleyen insani, teknik ve örgütlenmeden kaynaklanan etkenler hakkında bilgi sahibidir.

c) ***Esneklik.*** Örgütün hizmet sunduğu etkinliklerin altında yatan tehlikeler hakkında gerçekçi görüşler sahibi olmanın ve tehlikeler ve potansiyel hasar kaynakları ile ilgili gerçekçi kurallar geliştirmenin sonucu olarak, olağandışı durumlarla karşı karşıya olduklarında operasyonel personel yerleşik moddan doğrudan bir moda geçerek tehlike raporlamasına uyum sağlayabilirler, böylece bilgilerin uygun karar verme seviyesine hızla ulaşmasını sağlayabilirler.

d) ***Öğrenme.*** Örgütün tüm seviyelerinde tehlike bilgilerinin iletilmesinin önemi hakkında farkındalık sağlanmasının sonucunda, operasyonel personel emniyet bilgi sistemlerinden sonuçlar çıkarma yeterliliğine ve örgüt önemli reformları uygulama isteğine sahiptir.

e) ***Hesap verme sorumluluğu.*** Önemli emniyet verilerinin uygun şekilde korunmasının ve tehlikeleri bildirenlerin tehlike raporlamasının başka bir amaçla (emniyet yönetimi dışında) kullanılmayacağından emin olmaları için kontrollü ve dengeli bir sistem oluşturulmasının desteklenmesinin sonucu olarak, operasyonel personel tehlikelerle ilgili önemli emniyet verilerinin sağlamaları için cesaretlendirilir (ve ödüllendirilir). Ancak, kabul edilebilir ve kabul edilemez operasyonel performansı birbirinden ayıran açık bir çizgi vardır.

2.8.16 Etkili emniyet raporlaması emniyet yönetiminin bir yapıtaşıdır. Raporlandıklarında, tehlikelerle ilgili veriler emniyet bilgilerine dönüşür. Bu nedenle, etkili emniyet raporlaması emniyet verilerinin elde edilmesinin yoludur. Elde edildiğinde, emniyet verilerinin yönetilmesi gerekir. Emniyet verileri yönetimi açıkça tanımlanmış üç adım üzerinde inşa edilir. Emniyet verileri yönetiminin ilk iki adımı tehlikelerle ilgili emniyet verilerinin toplanması ve verilerin bilgiye dönüştürülmesi için emniyet verilerinin analiz edilmesidir. Üçüncü ve genellikle gözden kaçırılan adım, geliştirilen emniyet bilgilerinin sonucunda örgüt tarafından tehlikelerin azaltılması veya tehlikelere yönelik etkinliklerin uygulanmasıdır. Bir örgütün tehlikelerle ilgili emniyet bilgilerine tepkisi, tehlikelerin etkin şekilde azaltılmasından açık bir şekilde görmezden gelinmesine kadar değişebilir.

2.8.17 Örgütlerle ilgili yayınlarda, tehlikelerle ilgili bilgilere verdikleri tepkilere emniyet bilgilerinin yönetilmesine bağlı olarak, üç örgüt karakteri ortaya konur:

a) patolojik — bilgilerin saklanması;

b) bürokratik — bilgilerin kısıtlanması ve

c) üretken – bilgilerin değerlendirilmesi.

2.8.18 Tablo 2-1'de 2.8.17'de açıklanan üç örgüt karakteri bakımından emniyet bilgilerinin yönetiminin temel yönlerini içeren bir matris sunulmuştur.

	Zayıf	*Bürokratik*	*Olumlu*
Bilgi	Gizli	Dikkate alınmaz	Aranır
Bilgi getirenler	Bağırılır	Tolere edilir	Eğitilir
Sorumluluklar	Yerine getirilmez	Sınırlanır	Paylaşılır
Raporlar	Desteklenmez	İzin verilir	Ödüllendirilir
Başarısızlıklar	Üstü örtülür	Şefkat gösterilir	Dikkatle incelenir
Yeni fikirler	Ezilir	Sorunlu	Hoş karşılanır
Sonuçta ortaya çıkan örgüt	Çatışma içeren örgüt	Bürokratik örgüt	Güvenilir örgüt
Kaynak: Ron Westrum			

Tablo 2-1. Üç olası örgüt kültürü

Etkili emniyet raporlaması ve kültür

2.8.19 İlk kez 1970'lerin sonunda geliştirilen gönüllü raporlama sistemleri mevcut koşullar veya ortamdan kaynaklanan operasyonel hataların raporlanmasına odaklanmıştı. Bu el kitabında açıklanan şekilde etkili emniyet raporlaması ise ortaya çıkmadan ortadan kaldırılmaları veya azaltılmaları için bu operasyonel hataların nedenlerinin aranması ve tanımı ile daha ileri gider. Bu, aynı zamanda tehlikelerin raporlanmasını da içeren gönüllü raporlama sistemlerini doğurmuştur. Genel bir kural olarak, asıl yönetilmesi gereken tehlikedir ve insanları daha emniyetli hale getirmektense, operasyonu daha emniyetli hale getirmek daha pratik, kolay ve önemli ölçüde daha etkilidir. Bu nedenle, tehlikelerin ve diğer emniyet sorunlarının sistematik olarak tanımlanması, emniyet yönetimi için sadece hata raporlamasından daha fazla yarar sağlar. Ancak, hata raporlama ile tehlike raporlama arasındaki fark temel önemdedir ve tanınması ve ele alınması gereken uygulama sorunlarına neden olabilir. Önemli bir fark, tehlike raporlamasının tahmine dayalı olmasına ve nesnel ve nötr olmasının gerekmesine karşın, hata raporlamasının tepkisel olması ve suçlama ve cezaya neden olabilecek şekilde raporlayan ve rapor edilenin itham edilmesine neden olabilmesidir.

2.8.20 Etkili emniyet raporlaması, insanların gönüllü şekilde hata ve tehlikeleri raporlamasına dayanır. Bunlar, genellikle tehlikelerle birlikte yaşayan veya tehlikelerle karşılaşan operasyonel personeldir. Ancak, bir tehlikenin operasyonu (ve yürütüldüğü koşulları) tanımayan veya ilgisi olmayan bir kişi için daha açık olabileceği durumlar olduğundan, kimin neyi rapor edeceği konusunda sınırlama olmamalıdır. Raporlama hiçbir şekilde caydırılmamalıdır; bu nedenle raporlayanların ve emniyet bilgilerinin kaynaklarının korunması her iki raporlama sisteminin oluşturulmasında da her zaman tartışmalı bir sorun olmuştur ve emniyet yönetiminin ilerlemesinde ve başarısında önemli bir engel oluşturabilir.

2.8.21 Emniyet bilgilerini ve rapor edeni cezadan koruma çabaları *kültür* terimini kullanarak geliştirilmişti; örneğin "cezalandırmama kültürü", "suçlama yapmama kültürü" ve son dönemlerde "emniyet kültürü" veya "adil kültür". *Kültür* kelimesinin özel anlamları vardır ve bu durumda kullanıldığı bağlam yanlış algılama ve yanlış anlamaya neden olabilir. Yine de, emniyet kültürü veya adil kültür, bir örgütteki emniyet uygulamalarının geliştirildiği bağlamı açıklamak için evrensek olarak tanımlanmış olmasalar da, yaygın kabul görmüş terimler haline gelmiştir. Emniyet uygulamaları belirli bir sonuca, yani tehlikelerin tanımlanmasına yönelik bir dizi örgüt süreci, prosedürü ve politikasını içerir. Süreçler (etkili emniyet raporlaması), prosedürler (tehlike raporlama sistemi) ve politikalar (emniyet politikası, raporlayanlara adil davranma v.s.) büyük bir topluluk tarafından kolayca anlaşılabilmeleri ve buna bağlı olarak büyük ölçekte daha kolay uygulanabilmelerini sağlayacak şekilde paketlenebilecek karmaşık, belirli fikirler ve davranışlardır. Ancak, mevcudiyetleri veya uygulanma şekilleri, geliştirildikleri Devlet veya örgütünün kültürünü (kelimenin gerçek anlamıyla) yansıtacaktır. Bu nedenle, yerel kültür aynı değilse, küresel olarak tek bir emniyet kültürü veya adil kültürün kabul edilmesi ayrımcı, hatta yargılayıcı olabilir.

2.8.22 Emniyet politikası etkili emniyet raporlamasını aktif bir şekilde desteklemelidir ve kabul edilebilir performans (genellikle kasıtlı olmayan hatalar) ve kabul edilemez performans (ihmalkarlık, umursamazlık, ihlaller veya sabotaj gibi) arasındaki çizgiyi tanımlayarak, raporlayanlara adil bir koruma sağlamalıdır. Ancak, emniyet kültürü veya adil kültür, yerleşik uluslararası anlaşmalara uyulduğu sürece, yasal, etik ve moral olarak bir Devletin egemenlik hakları içinde yer alan "hatanın suç olarak tanımlanmasını" engelleyemez. Herhangi bir ihmalkarlık veya olumsuz niyet olmamasına karşın, özellikle bir sistem arızasının can kaybına veya mülkün hasar görmesine neden olduğu bir kazadan veya ciddi bir olaydan sonra hukuki bir inceleme veya buna benzer sonuçlar beklenebilir. Dolayısıyla, bir sistemdeki veya uygulanmasındaki örtük bozukluklarla ilgili gönüllü tehlike raporlarının, kaza ve ciddi olay incelemelerini ilgilendiren raporlarla aynı şekilde ele alınması durumunda potansiyel bir sorun ortaya çıkabilir. Tehlike raporlarının korunmasının amaçlanması hukuki bir incelemenin meşruiyetini sorgulamaya yönelmemeli veya uygunsuz muafiyetler talebinde bulunmamalıdır. Ancak, yasal argümanlar genellikle herhangi bir teknik argümandan veya emniyetle ilgili argümandan önce gelir.

2.8.23 Devletler ve örgütler emniyet kültürünün ve adil kültürün kabul edilmesinin ve bunun kültürel ve yasal sonuçlarının avantajlarını ve dezavantajlarını dikkate almalıdır. Emniyet yönetimi ile ilgili amaçlar bakımında, desteklenmesi, beslenmesi ve savunulması gereken süreç etkili emniyet raporlamasıdır; "hatanın suç olarak tanımlanmasının" önemi daha azdır. Etkili emniyet raporlaması pek çok farklı şekilde ve pek çok farklı stratejiyi izleyerek elde edilebilir. Nasıl elde edildiği, yerel kültürle çakışma potansiyeline sahip raftan inme çözümler önermek yerine, belirli operasyonel bağlamlardaki tercihlere, olasılıklara ve kısıtlamalara bırakılmalıdır.

2.9 EMNİYET İNCELEMESİ

2.9.1 Emniyetle ilgili olayların incelenmesi emniyet yönetiminin önemli bir parçasıdır. Bölüm 7'de sistem emniyetinin en önemli koruyucusu olarak kaza inceleme süreci tanımlanmaktadır. Ancak, emniyet incelemesinin değeri, incelemenin hangi yaklaşımla gerçekleştirildiğine bağlıdır.

2.9.2 2.3.8'de ele alınan klasik yaklaşım "cenazenin kaldırılması" amaçlarına yönelik bir emniyet incelemesini açıklamaktadır:

a) kayıpları arkada bırakmak;

b) sisteme güveni ve inancı yeniden oluşturmak;

c) normal etkinliklere göre dönmek ve

d) politik amaçları yerine getirmek.

2.9.3 Bölüm 2.4'te açıklanan neden/sonuç ilişkisi kavramı ve Bölüm 2.5'te ele alınan örgütlenmeden kaynaklanan kaza kavramı gelişmiş sistem güvenilirliği olarak adlandırılan amaçla bağlantılıdır:

a) sistemin hasar görebilme olasılığının öğrenilmesi;

b) değişime yönelik stratejilerin geliştirilmesi ve

c) emniyet kaynaklarına yatırıma öncelik verilmesi.

2.9.4 Bu bölümü kapatırken, emniyet incelemesi yaklaşımlarına birer örnek şematik olarak sunulmuştur. Her iki örnek de kazaların incelenmesi ile ilgilidir.

"Cenazenin kaldırılması" amacına yönelik emniyet incelemesi

2.9.5 ***Olgular***

- Sadece iki kişilik bir uçuş ekibini taşıyan eski nesil, dört motorlu bir turboprop yük uçağı, iç hatlardaki bir gece uçuşu sırasında ciddi buzlanma koşullarına girer.

- Buz birikiminin sonucunda, 2 ve 3 numaralı motorlar durur, yedi dakika sonra 4 numaralı motor bozulur. Uçuş ekibi 2 numaralı motoru yeniden çalıştırmayı başarır.

- Uçak şimdi önemli bir miktarda asimetrik güç durumundadır, sol taraftaki iki motor güç sağlamakta, ama sağ taraftaki iki motor çalıştırılamaz durumdadır. Uçuş ekibi, uçağı kontrol etmede ciddi bir şekilde zorlanmaktadır.

- Uçağın kalan elektrik gücü kaynakları üzerindeki yüksek talep nedeniyle, elektrik yükünün atılması mümkün değildir ve elektrik sistemi akü gücüne döner. Şimdi uçuş ekini uçağın kontrolünü sürdürmek için sınırlı acil durum göstergeleri, sınırlı telsiz iletişimi ve sınırlı navigasyon kapasitesi ile karşı karşıya kalmıştır.

- Acil durum inişi yapmaya çalışırken, akü gücü boşalmış ve tüm elektrik gücü kaybedilmiştir.

- Uçuş ekibinin elinde sadece kendi gücünü sağlayan bekleme jiroskopu, bir flaşör ve kendi gücünü sağlayan motor göstergeleri bulunmaktadır.
- Uçuş ekini kontrollü uçuşu sürdüremez ve uçak kontrolden çıkarak çakılır.

2.9.6 ***Emniyet incelemesindeki bulgular***

- Uçuş ekibi buzlanma koşullarından kaçınmak için hava durumu radarını kullanmamıştır.
- Uçuş ekibi, güç kaynağı ve elektrik sistemi arızalarını çözmek için acil durum kontrol listesine başvurmamıştır.
- Uçuş ekibi, kararlı düşünüş ve net eylemlerde bulunmayı gerektiren zorlu bir durumla karşılaşmıştır.
- Uçak, motorlar için sertifikasyon koşullarını aşan buzlanma koşullarına girmiştir.
- Uçuş ekibi yakın bir havaalanına yönelme isteğinde bulunmamıştır.
- Uçuş ekibi bir acil durum bildiriminde bulunmak için doğru sözcükleri kullanmamıştır.
- Uçuş ekibi kötü ekip beceri yönetimi (CRM) göstermiştir.
- Uçak sistemleri yanlış yönetilmiştir.
- Acil durum kontrol listesinde görsel bilgilerin sunumu yetersizdir.
- Uçuş operasyonları için dahili kalite güvencesi prosedürlerinde sorun vardır.

2.9.7 ***Nedenler***

- Çok sayıda motor arızası;
- Acil durum tatbikatlarının eksik şekilde yerine getirilmesi;
- Motorların korunması ve yeniden çalıştırılmasında uçuş ekibinin eylemleri;
- Çalışmayan pervanelerin neden olduğu sürüklenme;
- Buzun ağırlığı;
- Zayıf CRM;
- Beklenmedik durum planlarının bulunmaması ve
- Durum farkındalığının kaybolması.

2.9.8 ***Emniyetle ilgili tavsiyeler***

- Otorite pilotları doğru sözcükleri kullanmalarını hatırlatmalıdır.
- Otorite acil durum referans materyalinin sunulması için en etkili biçimi araştırmalıdır.

Gelişmiş sistem güvenilirliğine yönelik emniyet incelemesi

2.9.9 ***Olgular***

- Düzenli yolcu taşımacılığında kullanılan eski nesil, iki motorlu bir turboprop kısa mesafeli uçak, marjinal hava koşullarında kontrolsüz, radar bulunmayan, uzak bir havaalanına hassas olmayan bir yaklaşma gerçekleştirmektedir.
- Uçuş ekibi, tamamen yayınlanmış yaklaşma prosedürü yerine bir doğrudan yaklaşma gerçekleştirir.
- MDA'ya ulaşıldığında, uçuş ekibi görsel referansları alamaz.
- Uçuş ekibi, inişi sürdürmek için gereken görsel referansları almadan MDA'dan çıkar.
- Uçak, pistten önce araziye çakılır.

2.9.10 ***Emniyet incelemesindeki bulgular***

- Uçuş ekibi sayısız hata ve ihlal yapmıştır.

Ama:

- Uçuş ekibi, yasal olsa da, zorlu uçuş koşulları bakımından uygun olmayan bir şekilde oluşturulmuştur.
- Şirket uygulamalarına göre, uçuş ekibindeki pilot doğrudan yaklaşma yapmıştır, bu da düzenlemelere aykırıdır.
- Devlette kısa mesafeli uçuş operasyonları için standartlar eksiktir.
- Devlette hava trafiği tesislerinin denetimi eksiktir.
- Otoriteler, operatörün önceki emniyet ihlallerini dikkate almamıştır.
- Devletin yönetmelikleri güncel değildir.
- Otorite, endüstrinin gelişmesine karşı emniyet denetimi gereksinimleri bakımından çakışan hedeflere sahiptir.
- Otoritenin sorumluluklarını yerine getirmek için kaynakları yetersizdir.
- Otoriteye destek olması için Devlet havacılık politikası bulunmamaktadır.
- Devletteki eğitim sisteminde sorunlar vardır.

2.9.11 ***Nedenler***

- Uçuş ekibinin görsel temas olmadan MDA'nın altında yaklaşmaya devam etme kararı;
- Kararın performans baskısı altında alınmış olması ve
- Kararın havayolunun zayıf emniyet kültüründen etkilenmesi.

2.9.12 ***Emniyetle ilgili tavsiyeler***

- Rapor uçuş ekibinin performansı ile ilgili olarak ön saflardaki personele yönelik çok sayıda tavsiye içermektedir.

- Rapor aynı zamanda aşağıdakilerle ilgili tavsiyeler de içermektedir:

  — otorite tarafından bir AOC verilmesi sürecinin gözden geçirilmesi;
  — Devletteki eğitim sisteminin gözden geçirilmesi;
  — havacılık yönetiminin desteklenmesini sağlayan bir havacılık politikası tanımı;
  — mevcut havacılık mevzuatında reformlar yapılması;
  — bir ara önlem olarak mevcut mevzuatın güçlendirilmesi ve
  — hem kaza inceleme hem de uçak ve havayolu denetim süreçlerinin iyileştirilmesi.

Bölüm 3

EMNİYET YÖNETİMİNE GİRİŞ

3.1 HEDEF VE İÇERİKLER

3.1.1 Bu bölüm emniyet yönetimi gereksinimini, buna yönelik stratejileri ve temel özelliklerini ele almaktadır. Bölümde bir örgüt süreci olarak emniyet yönetimi ve çözüm bulmaya yönelik bir etkinlik olarak kazaların önlenmesi arasındaki farklar ele alınmaktadır.

3.1.2 Bu bölüm aşağıdaki konuları içerir:

a) Emniyet klişesi;

b) Yönetim ikilemi;

c) Emniyet yönetimi gereksinimi;

d) Emniyet yönetimi için stratejiler;

e) Değişim zorunluluğu;

f) Emniyet yönetimi — Sekiz temel ilke ve

g) Emniyet yönetiminin sağlanması için dört sorumluluk.

3.2 EMNİYET KLİŞESİ

3.2.1 Havacılıkta, öncelik bakımından emniyetin havacılık örgütlerinin, sunabilecekleri hizmetlerin doğasından bağımsız olarak, peşinde oldukları hedefler yelpazesi içinde nereye oturduğu konusunda yaygın bir yanlış algı vardır. Bu yanlış algı, evrensel olarak kabul edilen bir klişeye dönüşmüştür: havacılıkta, emniyet ilk önceliktir. İnsan yaşamının en üstte yer alan değerinin içkin olarak tanınması nedeniyle toplumsal, etik ve ahlaksal olarak bu klişeden kuşku duymak mümkün olmasa da, emniyet yönetiminin bir örgüt süreci olduğu perspektifinden bakıldığında, bu klişe ve taşıdığı perspektif sağlam görünmemektedir.

3.2.2 Doğalarından bağımsız olarak, tüm havacılık örgütleri, az ya da çok, bir ticari bileşene sahiptir. Dolayısıyla, tüm havacılık örgütleri ticari örgütler olarak kabul edilebilir. Bu durumda, emniyet klişesinin doğruluğu veya doğru olmaması üzerine ışık tutmak için basit bir soru sorulabilir: bir ticari örgütün temel hedefi nedir? Bu sorunun yanıtı açıktır: en başta örgütün yerine getirmek için kurulduğu hizmeti sunmak, üretim hedeflerine ulaşmak ve nihayetinde hissedarlara kar payı sunmak.

3.2.3 Sadece emniyet sunmak için kurulmuş bir havacılık örgütü yoktur. Havacılık emniyetini korumak için çalışan örgütler, hissedarları tarafından belirlenen, dahili veya harici etkinlik kısıtlamalarına tabidirler. Buna, Uluslararası Sivil Havacılık Teşkilatı, ulusal veya ulusal üstü sivil havacılık kurumları, uluslararası ticaret örgütleri ve emniyeti savunan uluslararası örgütler da dahildir.

3.2.4 Bölüm 2'de emniyetin nasıl giderek artan şekilde, operasyonel bağlamlarda bulunan tehlikelerin sonuçlarından doğan emniyet risklerini örgüt kontrolü altında tutma hedefine yönelik belirli örgütlenme süreçlerinin yönetilmesinin sonucu olarak görüldüğü açıklanmaktadır. Örgütlerin hizmet sunarak üretim hedeflerine ulaşabilmeleri için, çoğu işle ilgili, belirli örgütlenme süreçlerinin yönetilmesi zorunlu bir koşuldur. İletişim, kaynakların ayrılması, planlama ve denetimi de içeren bu örgütlenme süreçleri yine Bölüm 2'de açıklanmıştır. Bu süreçlerin yönetimi mali yönetim, insan kaynakları yönetimi ve hukuki yönetim gibi temel operasyonel işlevler ve yönetim sistemleri aracılığıyla sağlanır.

3.2.5 Bu el kitabında geliştirilen perspektif, emniyetin havacılık örgütlerinin ilk önceliği olmadığıdır. Aksine, emniyet yönetimi sadece örgütlerin hizmetlerini sunarak iş hedeflerine ulaşmasını sağlayan örgütlenme süreçlerinden biridir. Bu nedenle, emniyet yönetimi diğer temel operasyonel işlevler aynı seviyede ve aynı öneme sahip olarak görülmesi gereken bir başka operasyonel işlevdir ve bu amaca ayrılmış bir yönetim sistemi ile (emniyet yönetimi sistemi, SMS, Bölüm 7'de açıklanmaktadır) sağlanır.

3.3 YÖNETİM İKİLEMİ

3.3.1 Örgütsel bir süreç olarak emniyetin yönetimi ve bir temel operasyonel işlev olarak emniyet yönetimi perspektifi, bu tür bir işlev için nihai emniyet sorumluluğunu ve hesap verebilirliğini açıkça havacılık örgütlerinin en yüksek seviyesine yerleştirmektedir (hizmetlerin sunulmasındaki bireysel sorumluluğun önemini reddetmeden). Bu türden bir sorumluluk ve hesap verebilirliğin en açık olduğu yer, kaynakların ayrılması ile ilgili kararların verilmesidir.

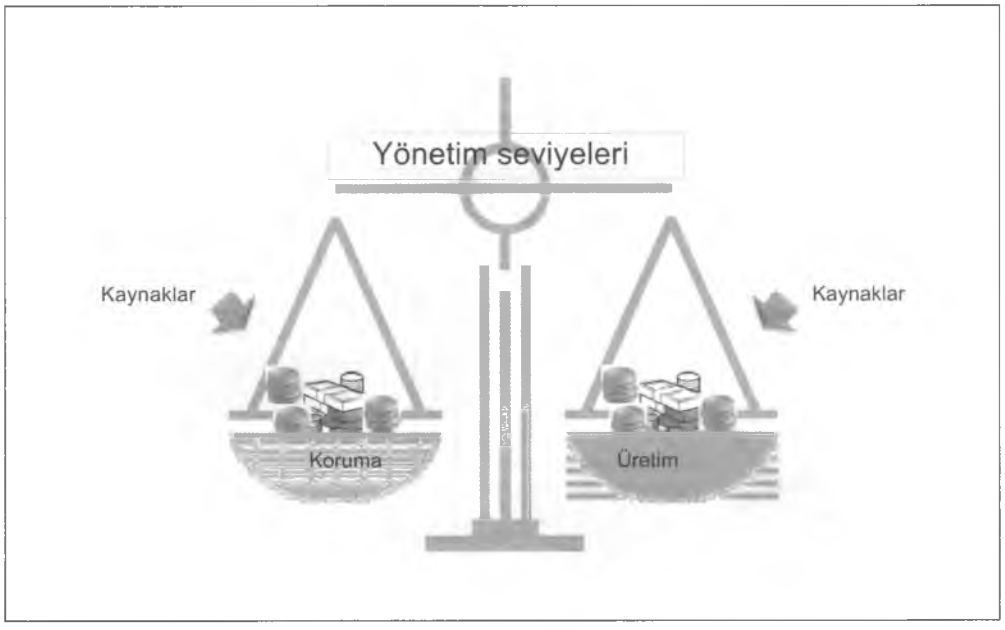
3.3.2 Havacılık örgütlerinin sahip olduğu kaynaklar sınırlıdır. Sonsuz kaynaklara sahip bir havacılık örgütü yoktur. Kaynaklar, hizmetlerin sunulmasını doğrudan ve dolaylı olarak destekleyen bir örgütün temel operasyonel işlevlerin yerine getirilmesinde temel önemdedir. Bu nedenle, kaynakların dağıtılması üst yönetimin hesaba katması gereken örgütlenme süreçlerinin en önemlilerinden biri (eğer en önemlisi değilse) haline gelir.

3.3.3 Örgüt bir temel operasyonel işlev olarak emniyet yönetimi perspektifine bağlı kalmazsa, hizmetlerin sunulmasını doğrudan veya dolaylı olarak destekleyen temel operasyonel işlevlerin yerine getirilmesi için kaynakların dağıtılmasındaki rekabeti ortadan kaldırma potansiyeli vardır. Bu tür bir rekabet, "İki P ikilemi" olarak adlandırılan yönetim ikilemine neden olabilir.

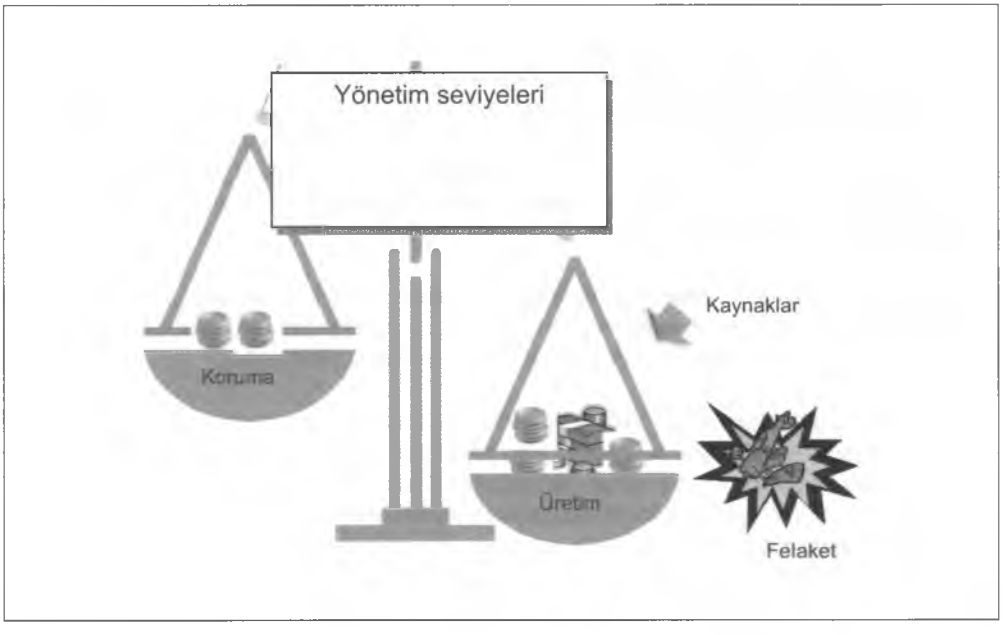
3.3.4 Basitçe dile getirildiğinde, "iki P ikilemi" örgütün üst yönetim kademesinde kaynakların birbiri ile çakışan hedefler oldukları düşünülen aşağıdaki hedeflere ya/ya da bağlamında dağıtılması gerektiği yönünde bir algı gelişmesine neden olan çatışma olarak açıklanabilir: üretim (production) hedefleri (hizmetlerin sunulması) veya koruma (protection) hedefleri (emniyet).

3.3.5 Şekil 3-1A, kaynakların temel bir operasyonel işlev (yani temel operasyonel işlevlerden herhangi biri) olarak emniyet yönetimi temelinde örgüt karar verme süreçlerinden kaynaklanan üretim ve koruma hedeflerine dengeli bir şekilde dağıtılmasını göstermektedir. Emniyetin yönetimi herhangi bir örgüt süreci olarak ve emniyet yönetimi herhangi bir temel operasyonel işlev olarak görüldüğünden, etkinlik ve emniyet rekabet halinde değildir, iç içe geçmiş haldedir. Bunun sonucunda, örgütün üretirken korunmasını sağlayacak şekilde dengeli bir kaynak dağılımı ortaya çıkmaktadır. Bu durumda, "iki P ikilemi" ile etkili bir şekilde başa çıkılmış olur. Aslında, bu durumda bu ikilemin var olup olmadığı tartışılabilir.

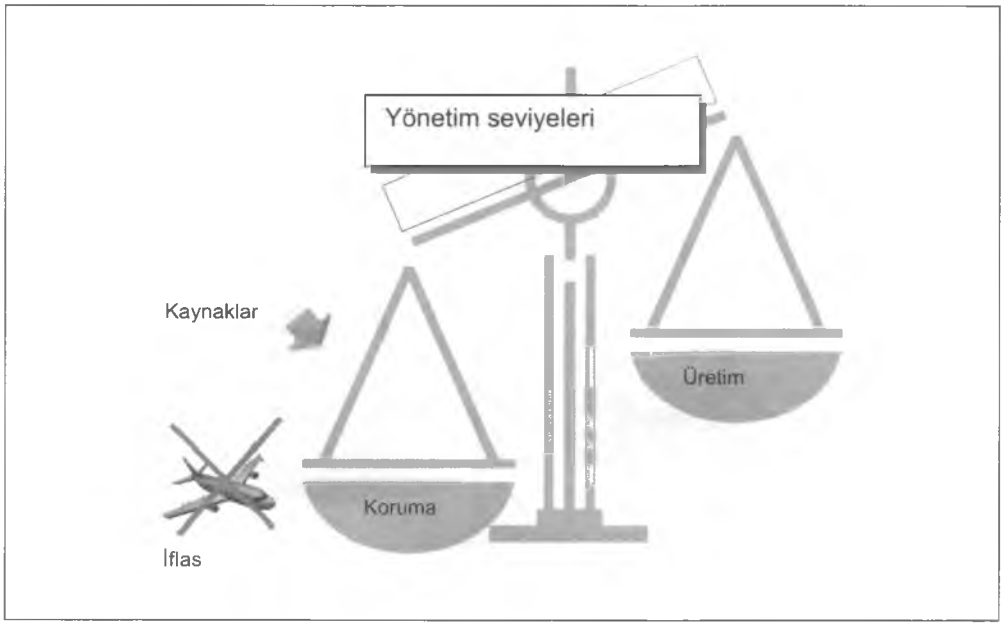
3.3.6 Yazık ki, havacılık tarihi bu ikilemin etkili bir şekilde çözülmesinin pek yaygın olmadığını göstermektedir. Tarihin gösterdiği, üretim ve koruma arasındaki rekabet algısı nedeniyle örgütlerin kaynakların dağıtılmasında dengesizliğe savrulduklarıdır. Bu tür bir rekabet oluştuğunda, genellikle kaybeden koruma olur, örgütler üretim hedeflerine öncelik tanır (aksi yönde çok sayıda uyarıya rağmen). Şekil 3-1B'de gösterildiği gibi, bu tür bir kısmi örgütsel karar verme etkinliği kaçınılmaz olarak bir felakete dönüşür. Bunun gerçekleşmesi sadece zaman meselesidir.



Şekil 3-1A. Yönetim ikilemi



Şekil 3-1B. Yönetim ikilemi



Şekil 3-1C. Yönetim ikilemi

3.3.7 Şekil 3-1C'de önceki iki paragrafta açıklanan kısmi kaynak dağıtımına bir alternatif gösterilmektedir. Bu durumda, kaynakların dağıtılmasındaki eğilim dengenin koruma tarafındadır, dolayısıyla iflasa gitmektedir. Havacılık tarihi yıllıklarında bu alternatifi bulmak zor olsa da, kaynakların dağıtımı ile ilgili olarak makul şekilde karar verilmesinin önemi hakkında uyarıda bulunmaktadır. Son çözümlemede, emniyet yönetimine diğer temel operasyonel süreçler ile aynı seviyede ve aynı öneme sahip, temel bir operasyonel işlev olarak odaklanan bir örgüt perspektifinin "iki P ikileminin" gelişmesini önlediği açıktır. Bu şekilde, emniyet yönetimi örgütün dokusunun bir parçası haline gelir ve kaynakların örgütün sahip olduğu toplam kaynaklarla orantılı şekilde dağıtılması sağlanır.

3.3.8 Emniyet yönetiminin temel bir operasyonel işlev olmasının mantığı, emniyet yönetimi ile ilgili operasyonel etkinlikler ve işlevler olarak tehlikenin tanımlanmasını ve emniyet riski yönetimini vurgulayan süreçlerle önemli bir bağı olan son bir argümana dönüştürülebilir (Bölüm 4 ve 5'te açıklanmıştır).

3.3.9 Havacılık örgütlerinin temel hedefi hizmetlerin sunulması olduğundan, bazı durumlarda hizmetlerin zamanında ve etkin bir şekilde sunulması operasyonel emniyet ile ilgili konularla çatışabilir. Örneğin, bir programa uyma gereksinimi nedeniyle, bir havayolunun tamamen hizmetlerin sunulması ile ilgili olan hava koşulları, trafik hacmi, havaalanı sınırlamaları ve benzer kısıtlamalardan bağımsız olarak belirli bir havaalanına belirli bir zamanda inmesi gerekmektedir. Hizmetin sunulması ile ilgili etkinlik sorunları (bir programa uyma) ortadan kaldırılsaydı, operasyonel emniyeti (olumsuz hava koşulları, yüksek trafik hacmi, havaalanı sınırlamaları) bir etken olmaktan çıkacaktı. İşletme sadece kısıtlamalar ortadan kalktığında gerçekleştirilecekti. Ancak, havacılık endüstrisinin yaşama olanağını ortadan kaldıracağı için bu mümkün değildir. Bu nedenle, havacılık operasyonları, operasyonel emniyet ile ilgili konular tarafından değil, hizmet sunumu ile ilgili konular tarafından belirlenen koşullar altında gerçekleştirilmek zorundadır.

3.3.10 Sonuç ortadadır: havacılık emniyeti ile ilgili konular havacılık operasyonlarının yapısında bulunan veya doğal koşulları değildir, aksine üretim veya hizmetlerin sunulması ile ilgili etkinliklerin getirdiği gereksinimlerin ve bu etkinliklerde bulunmanın bir yan ürünüdür.

Bu, bir örgütün kaynaklarının ve hedeflerinin analizini sağlayan ve örgütün genel hizmet sunumu gereksinimlerini destekleyecek şekilde, kaynakların üretim ve koruma hedefleri arasında dengeli ve gerçekçi bir şekilde dağıtılmasını sağlayan bir temel operasyonel işlev olarak emniyet yönetimine duyulan ihtiyacı güçlendirmektedir.

3.4 EMNİYET YÖNETİMİ GEREKSİNİMİ

3.4.1 Geleneksel olarak, emniyet yönetimi gereksinimi tahmin edilen bir endüstri büyümesi ve bu tür bir büyümenin sonucunda kazalardaki artış potansiyeli temelinde gerekçelendirilir. Kazaların azaltılmasının daima havacılığın önceliklerinden biri olarak kalacak olmasına rağmen, dünya çapındaki uluslararası sivil havacılıkta emniyet yönetimi ortamına geçişin altında yatan, istatistiksel projeksiyonlardan daha zorlayıcı nedenler vardır.

3.4.2 Havacılık muhtemelen en emniyetli toplu taşımacılık şeklidir ve insanoğlunun tarihindeki en emniyetli sosyo-teknik üretim sistemlerinden biridir. Bu başarı, özellikle geçmişi on yıllarla ölçülen havacılık endüstrisinin, yüzyıllara uzanan geçmişlere sahip diğer endüstrilerin karşısında ne kadar genç olduğu düşünüldüğünde önemlidir. Sadece yüz yıl içinde, emniyet açısından bakıldığında, kırılgan bir sistemden taşımacılık tarihindeki ilk son derece emniyetli sisteme ulaşan havacılığın ilerlemiş olması havacılık emniyet topluluğunun ve durmak bilmeyen çabalarının övgüyü hak ettiğini göstermektedir. Geçmişe bakıldığında, havacılık emniyetindeki güvenilirliğin gelişmesinin tarihi (Bölüm 2'de açıklanan emniyet düşüncesinin gelişimi gibi) her biri farklı özelliklere sahip üç ayrı çağa ayrılabilir.

3.4.3 1900'lerin başındaki öncülerin günlerinden 1960'ların sonlarına uzanan ilk çağda (Bölüm 2'de ele alınan teknik çağ) emniyet konusundaki güvenirlik bağlamında havacılık kırılgan bir sistem olarak tanımlanabilir. Günlük olarak ortaya çıkmasa da, emniyet arızaları ile sık karşılaşılmadığı söylenemezdi. Bu nedenle, emniyet anlayışının ve önleme stratejilerinin genel olarak kaza incelemelerinden elde edilmesi mantıklı bir durumdu. Üzerinde konuşulacak gerçek bir sistem yoktu, ancak endüstri işlemeye devam ediyordu, çünkü bireyler endüstriyi ileri taşımayı kendileri üstlenmişlerdi. Emniyet bireylere ve emniyet risklerinin bireysel olarak yönetilmesine odaklanmıştı, bu da kapsamlı eğitim programları tarafından sağlanan temeller üzerinde yükseliyordu.

3.4.4 1970'lerin başından 1990'ların ortasına uzanan ikinci çağ (insan çağı) boyunca, havacılık sadece bir sistem haline değil, emniyetli bir sistem haline gelmişti. Emniyet arızalarının sıklığı önemli ölçüde azalmıştı ve bireylerin ötesine geçerek daha geniş sisteme uzanan daha kapsamlı bir emniyet anlayışı kademeli olarak gelişmişti. Doğal olarak, bu kaza incelemesinden elde edilenlerin ötesinde emniyet derslerinin alınması için araştırmalara yol açmıştı, dolayısıyla önem verilen nokta olayların incelenmesi haline gelmişti. Daha geniş bir emniyet ve olay incelemesi perspektifine yönelen bu geçişe teknolojinin seri halde kullanılmaya başlanması (artan sistem üretim taleplerini karşılamanın tek yolu olarak) ve buna bağlı olarak emniyet düzenlemelerinde çok katmanlı artış eşlik etmişti.

3.4.5 1990'ların ortalarından günümüze kadar (örgüt çağı) havacılık üçüncü emniyet güvenilirliği çağına girmiş, son derece emniyetli bir sistem (yani milyon üretim çevriminde bir yıkıcı emniyet arızası yaşayan bir sistem) haline gelmiştir. Küresel bir perspektiften bakıldığında, bölgesel ani artışlara karşın, kazaların sıklığı istisnai olaylar veya sistemdeki anomaliler haline gelmelerini sağlayacak kadar azalmıştır. Ciddi olaylar da azalmış ve uzaklaşmışlardır. Olayların ortaya çıkma sıklığındaki bu azalmaya uygun olarak, önceki çağda ortaya çıkmaya başlayan daha geniş bir sistemli emniyet perspektifine geçiş daha belirgin hale gelmiştir. Bu belirgin hale gelişin temelinde, günlük operasyon verilerinin rutin olarak toplanması ve analiz edilmesine dayanan, emniyet yönetimine iş benzeri yaklaşımın kabul edilmesi yatıyordu. Emniyete iş benzeri yaklaşım, Bölüm 7'de ele alınan emniyet yönetimi sistemlerinin (SMS) mantığını oluşturur. En basit şekilde ifade edildiğinde, SMS iş yönetimi uygulamalarının emniyet yönetimine uygulanmasıdır. Şekil 3-2'de yukarıda ele alınan şekilde emniyetin gelişimi gösterilmektedir.

3.4.6 İşletme verilerinin rutin olarak toplanması ve analizi ile birlikte, iş yönetimi uygulamalarının havacılıktaki emniyete uygulanmasının amacı Bölüm 2'de ele alınan emniyet alanının geliştirilmesidir. Bu emniyet alanında, örgüt hizmetlerini sunmayı sürdürürken, hizmetlerini sunmak için içinde çalışmak zorunda olduğu bağlamda bulunan tehlikelerin sonuçlarından kaynaklanan emniyet risklerine maksimum direnç gösterebileceği bir alanda bulunmasının güvencesi ile çalışmaya devam edebilir.

3.4.7 Kaynakların dengeli dağıtılmasının koruma ve üretim hedeflerine ulaşılmasındaki, dolayısıyla "iki P ikileminin" gelişmesi potansiyelinin ortadan kaldırılmasındaki önemi önceden ele alınmıştır. Bu tartışmaya ek olarak, üretim ve koruma kavramları Şekil 3-3'te gösterilen şekilde bir örgütün emniyet alanının sınırlarının tanımı ile ilgilidir.

3.4.8 Korumaya yönelik olarak aşırı miktarda kaynak ayrılmasına neden olan bir karar verme tercihinin, örgütün finansal durumunda etkili olabileceği ve en azından teoride nihai olarak iflasa neden olabileceği hatırlatılmalıdır. Bu nedenle, örgüt tarafından emniyet alanı içinde ilerlerken yaklaşıldığında, kaynakların dengesiz dağıtımının ortaya çıkmakta olduğu veya ortaya çıkmış olduğu bir durum konusunda erken uyarı sağlayan sınırların tanımı önemlidir. Emniyet alanının iki yönü veya iki sınırı vardır: finansal sınır ve emniyet sınır.

3.4.9 Finansal sınır örgütün finansal yönetimi tarafından tanımlanır. Örgütün finansal sınıra yaklaştığı konusunda uyarıda bulunan bir erken uyarı geliştirmek için, finansal yönetiminin en kötü sonucu (iflas) dikkate alması gerekmez. Finansal yönetim uygulamaları belirli finansal göstergelerin günlük olarak toplanması ve analizini temel alır: pazar eğilimleri, örgütün hizmetlerin sunulmasında ihtiyaç duyduğu malların ve harici kaynakların fiyatlarındaki değişim. Böylece, finansal yönetim sadece emniyet alanının finansal sınırını tanımlamakla kalmaz, ama konumunu sürekli olarak yeniden ayarlar.

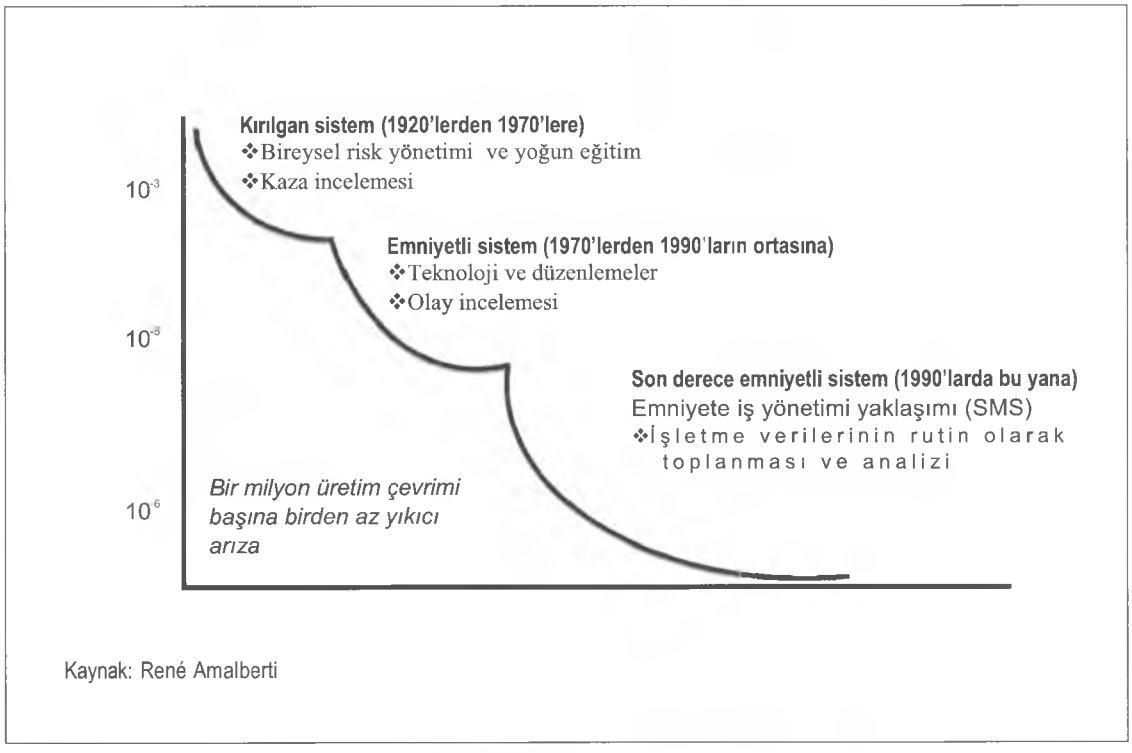
3.4.10 Korumaya yönelik olarak aşırı miktarda kaynak ayrılmasına neden olan bir karar verme tercihinin, örgütün emniyet performansında etkili olabileceği ve nihai olarak felakete neden olabileceği hatırlatılmalıdır. Bu nedenle, bu kez koruma ile ilgili olarak, kaynakların dengesiz dağıtımının ortaya çıkmakta olduğu veya ortaya çıkmış olduğu bir durum konusunda erken uyarı sağlayan bir emniyet sınırının tanımı önemlidir. Emniyet alanının "emniyet sınırı" örgütün emniyet yönetimi tarafından tanımlanmalıdır.

3.4.11 Bu sınır, örgütün üretim hedeflerine öncelik verecek şekilde kaynakların dengesiz bir biçimde dağıtılmasının ortaya çıkmakta olduğu ve ortaya çıktığı ve bunun da nihayetinde bir yıkıma neden olabileceği konusunda uyarılması için önemlidir. Ne yazık ki, finansal yönetimle emniyet yönetimi tarafından kullanılan uygulamalar arasında bir paralellik yoktur. Kazaların veya ciddi olayların olmaması şeklinde yerleşmiş emniyet kavramı nedeniyle, havacılık örgütlerinde emniyet alanının emniyet sınırı nadiren mevcuttur. Aslında, çok az sayıda (o da varsa) havacılık örgütünün emniyet alanını gerçekten gerçekleştirmiş oldukları öne sürülebilir.

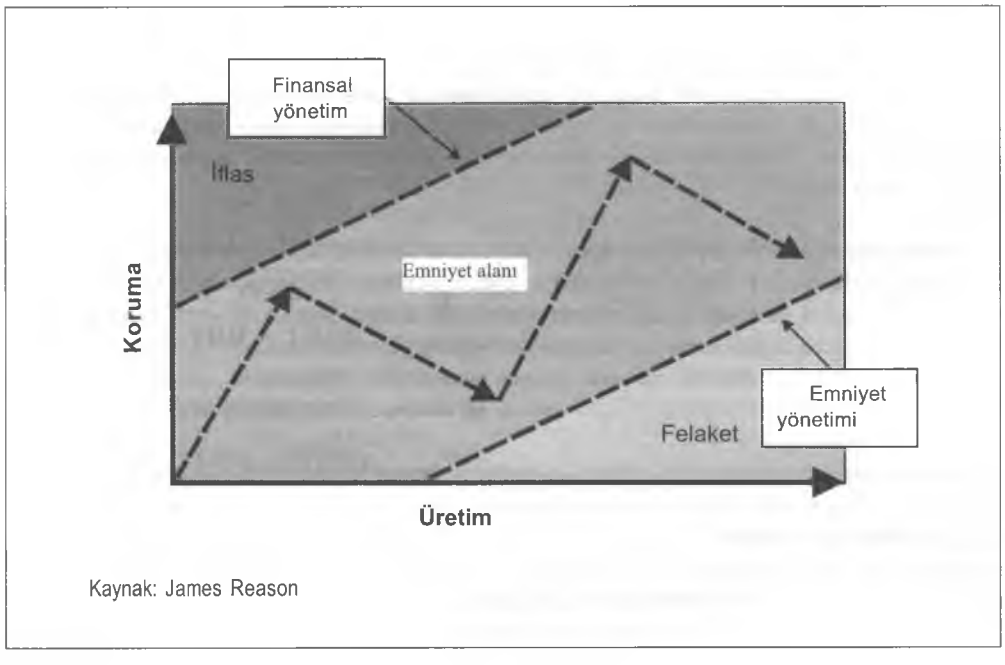
3.4.12 Emniyet bağlamında, erken uyarılar ve bildirimler mevcut olsa da, bunlar genellikle görmezden gelinmekte veya doğrulanmamaktadır ve örgütler kaynaklarının dağıtımında dengesiz davrandıklarını bir kaza veya ciddi olayla karşılaştıklarında öğrenmektedirler. Dolayısıyla, finansal yönetimden farklı olarak, kazaların veya ciddi olayların olmaması bakımından emniyet perspektifine bağlı olarak, örgüt başarılı emniyet yönetiminin göstergesi olarak en kötü sonuçları (veya bunların ortaya çıkmamasını) almaktadır. Bu yaklaşım, pek emniyet yönetimi değil, hasar kontrolüdür. Havacılık örgütleri, "finansal sınır" ile döngüyü kapatmak ve böylece örgütün emniyet alanını tanımlamak için, emniyet sınırının tanımlanmasını sağlayacak bir emniyet yönetimine geçmek zorundadır.

3.4.13 3.4.3 ile 3.4.5 arasında ele alınan emniyetle ilgili güvenilirliğin gelişiminde, kaza ve olay raporlarının ötesinde emniyet verilerinin toplanması için ek, alternatif yöntemler geliştirilmesi gereksiniminden söz edilmektedir. 1970'lerin sonuna kadar, emniyet verilerinin toplanması çoğunlukla kaza ve olay incelemeleri ile sağlanıyordu ve emniyetteki iyileştirmelerin kaza sayılarının azalmasını sağlaması sonucunda giderek azalmıştı. Ayrıca, emniyet verilerinin elde edilmesi bakımından, kaza ve ciddi olay inceleme süreci tepkiseldir: veri toplama sürecinin başlatılması için bir tetikleyici (bir emniyet arızası) gerekir.

3.4.14 Emniyet verilerinin sabit bir hacimde kalması gereksiniminin sonucunda, kazalardan ve ciddi olaylardan elde edilen emniyet verileri genişletilmiş veri toplama sistemlerinden elde edilen emniyet verileri ile tamamlanmıştı. Genişletilmiş sistemlerde, düşük ciddiyetteki olaylardan elde edilen emniyet verileri zorunlu ve gönüllü raporlama programları aracılığıyla alınmıştı. Emniyet verilerinin elde edilmesi bağlamında, bu yeni sistemler proaktiftir, çünkü emniyet verilerinin toplanması sürecinin başlatılması için gereken tetikleyici olaylar, kaza ve ciddi olaylardan emniyet verisi toplama sürecinin tetikleyen olaylara göre çok daha az sonuca yol açmaktadırlar. Yine de, raporlama programlarından elde edilen emniyet verilerinin ancak emniyet sorunlarının daha az sonuca neden olan bir olayı tetiklemesi sonucunda elde edilebildikleri gerçeği değişmemektedir.



Şekil 3-2. İlk son derece emniyetli endüstriyel sistem



Şekil 3-3. Emniyet alanı

3.4.15 1990'ların başlarına kadar, son derece emniyetli sistem emniyeti sürdürebilmek için, SMS'nin altında yatan emniyete işletme benzeri yaklaşımı desteklemek için, tetikleyicilere ihtiyaç duyulmadan elde edilen çok büyük miktarda emniyet verilerine gereksinim olduğu anlaşılmıştı. Bu, mevcut proaktif ve reaktif emniyet verileri toplama sistemlerini tamamlamak için, tahmine dayalı emniyet verileri toplama sistemlerinin gelişmesine neden olmuştu. Bu bakımdan, emniyet verilerinin toplanması sürecini başlatmak için tetikleyici olaylara gerek kalmadan normal işletmelerden emniyet verilerinin toplanması için elektronik veri toplama sistemleri ve risk almadan kendiliğinden raporlama programları kullanılmaya başlanmıştı. Tahmine dayalı emniyet verileri toplama sistemlerine en çok eklenen, normal işletmeler sırasında operasyonel personelin doğrudan gözlenmesini temel alan veri elde etme sistemleri olmuştur.

3.4.16 Normal havacılık işletmelerinden emniyet verileri toplanmasında sağlam bir mantık vardır. Emniyette öne çıkmasına karşın, havacılık sistemi de, diğer insan yapısı sistemler gibi, mükemmel olmaktan uzaktır. Havacılık açık bir sistemdir; kontrol edilemeyen bir doğal ortamda çalışır ve çevreden kaynaklanan sorunlara açıktır. Başka hiçbir nedenle olmasa bile, insanlar, teknoloji ve havacılık operasyonlarının gerçekleştiği bağlam arasındaki olası tüm işletmeler etkileşimleri tahmin etmek mümkün olmadığından, tamamen taslaktan başlayarak mükemmel bir açık sistem tasarlamak imkansızdır. Normal işletmelerin gerçek zamanlı olarak izlenmesi, sistemin tasarımı sırasında tahmin edilemeyen hatalar ve eksikliklerin tanımlamasını ve düzeltilmesini sağlar. Bu argüman 3.4.17 ile 3.4.19 arasında geliştirilmektedir.

Pratik sapma

3.4.17 Sistem tasarımının erken aşamalarında, sistemin belirtilen üretim hedeflerini düşünerek, sistem tasarımcılarının zihnini en çok meşgul eden iki soru şunlardır:

a) bu üretim hedeflerine ulaşmak için gereken kaynaklar nelerdir? ve

b) üretim hedeflerine ulaşmak için gereken işletmeler sırasında sistem tehlikelerden nasıl korunabilir?

Sistem tasarımcılar bu sorulara yanıt vermek için farklı yöntemler kullanırlar. Bu yöntemlerden biri, operasyonel etkileşimlerdeki potansiyel tehlikeleri belirlemek için insanlar, teknoloji ve operasyonel bağlam arasındaki operasyonel etkileşimlerden makul senaryolar (mümkün olduğunca çok) tanımlamaktır.

3.4.18 Sürecin sonucunda, üç temel varsayıma dayanan bir ilk sistem tasarımı olur: sistem üretim hedeflerine ulaşmak için gereken teknoloji, insanların teknolojiyi doğru şekilde kullanabilmesi için gereken eğitim ve sistem ve insanların davranışını belirleyen düzenlemeler ve prosedürler. Bu varsayımlar temel (veya ideal) sistem performansını gösterir. Bu açıklamaya göre, ideal veya temel sistem performansı (yani sistemin nasıl çalışması gerektiği) düz bir çizgiyle gösterilebilir (Şekil 3-4).

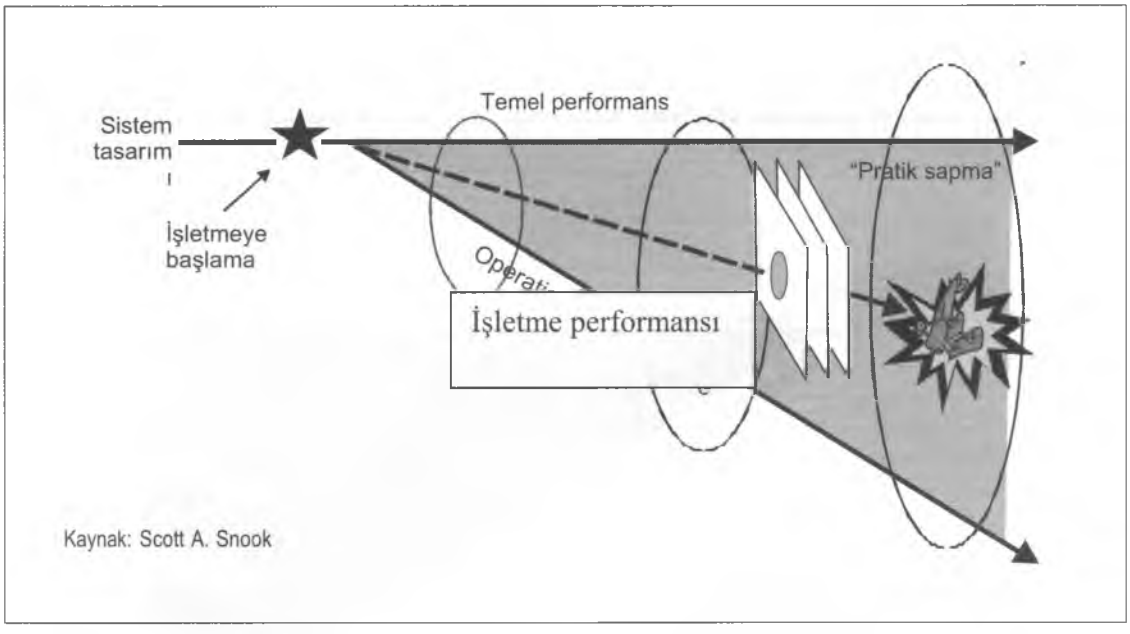
3.4.19 Varsayımlar test edilir, temel performans doğrulanır ve sonunda sistem çalışmaya başlar. Çalıştırılmaya başlandığında, sistem çoğu zaman temel performansa uygun şekilde, tasarlandığı gibi çalışır. Yine de, çoğu kez operasyonel performans temel performanstan farklıdır. Başka bir deyişle, sistem çalıştırılmaya başlandığında, sistem tasarım varsayımlarına göre beklenen temel performanstan kademeli olarak sapma gerçekleşir ve sistemin operasyonel performans kademeli olarak, kaçınılmaz şekilde gerçek yaşamdaki işletmelerin sonucunda belirlenen biçimde gerçekleşir. Sapma günlük pratiğin bir sonucu olduğunda, "pratik sapma" olarak adlandırılır.

3.4.20 Temel performanstan operasyonel performansa doğru pratik bir sapma, sistemin tasarım planlaması ne kadar dikkatli ve iyi yapılırsa yapılsın, tüm sistemlerde kaçınılmazdır. Pratik sapmanın nedenleri çok katmanlıdır: her zaman tahmin edildiği gibi çalışmayan teknoloji; dinamik çalışma koşulları altında planlandığı gibi yürütülemeyen prosedürler; bağlamsal sınırlaması dikkate almayan düzenlemeler; tasarımından sonra sistemde temel tasarım varsayımları üzerindeki etkileri yeniden değerlendirilmeden yapılan değişiklikler; bileşenlerin getirebileceği tehlikeler hakkında uygun bir emniyet değerlendirmesi yapılmadan sisteme yeni bileşenlerin eklenmesi; diğer sistemlerle etkileşim, v.s. Yani, herhangi bir sistemde, insanların hizmetlerin sunulmasına yönelik etkinlikleri bu sapma içinde yerine getirdiklerini söylemek doğrudur. Ancak, sistemdeki sapmaya neden olan tüm eksikliklere rağmen, pratik sapma içinde çalışan insanların sistemin günlük temelde çalışmasını sağladığı da unutulmamalıdır. İnsanlar, (havacılık profesyonellerinin ortak alan uzmanlarını bir arada toplayan) yerel uyarlamalar ve kişiler stratejiler geliştirirler, böylece sistemdeki eksikliklerin üstesinden gelirler. Bu uyarlama süreci "kitapta yazanın ötesinde, biz işleri burada böyle yaparız" ifadesi ile dile getirilendir.

3.4.21 Pratik sapma içinde gerçekleşenlerin formel araçlarla tespit edilmesi (örneğin ortak alan uzmanlığının formel şekilde tespit edilmesi) başarılı emniyet uyarlamalarının öğrenilmesi, dolayısıyla emniyet risklerinin kontrolü için önemli bir potansiyel barındırır. Ortak alan uzmanlığının formel şekilde tespit edilmesi, öğrenme potansiyeli ilkeli bir şekilde uygulanırsa sistemin yeniden tasarlanması veya iyileştirmeler için formel müdahalelere dönüştürülebilir. Olumsuz yönde ise, yerel uyarlamaların ve kişisel stratejilerin kontrolsüz şekilde yaygınlaşması, pratik sapmanın beklenen temel performanstan, bir olay veya kazanın olası hale gelmesini sağlayacak kadar uzaklaşmaya neden olmasına yol açabilir. Şekil 3-4'te bu paragrafta ele alınan pratik sapma kavramı gösterilmektedir.

3.5 EMNİYET YÖNETİMİ İÇİN STRATEJİLER

3.5.1 Pratik sapmanın ortaya çıkması kaçınılmazdır. En sağlam, dayanıklı organizasyonlar da dahil olmak üzere, tüm havacılık organizasyonları günlük işletmeleri pratik sapma içinde gerçekleştirirler. Pratik sapma, havacılığın önemli örneklerinden biri olduğu dinamik ve açık sosyo-teknik üretim sistemlerinin doğasında yer alan bir durumdur. Günlük olarak, hizmetlerini sunmanın peşindeyken, organizasyonlar pratik sapma içinde kendilerini sapmanın en yüksek olduğu yerlerden mümkün olduğunca uzakta ve pratik sapmanın başlangıç noktasına mümkün olduğunca yakın tutmaya çalışarak hareket ederler. Bu günlük hareket içinde, organizasyonlar karşılarına çıkabilecek "akışların" veya engellerin üstesinden gelmelidirler: bunlar organizasyonun gereksinimlerini desteklemek için gereken kaynakların dengesiz şekilde dağıtılmasının ve "iki P ikileminin" çözülmesinin sonucunda ortaya çıkan tehlikelerdir.



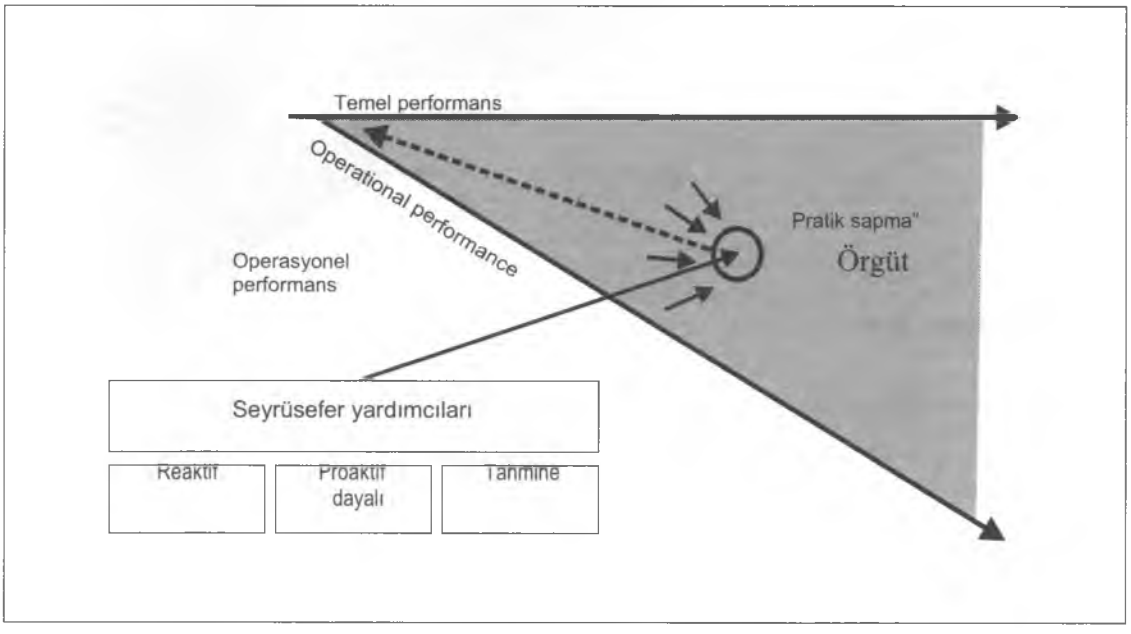
Şekil 3-4. Pratik sapma

3.5.2 Pratik sapmayı başarılı bir şekilde yönlendirebilmek için, organizasyonlar akışları ve engelleri atlatmalarını sağlayacak bilgileri oluşturan seyrüsefer yardımcılarına ihtiyaç duyarlar (bkz. Şekil 3-5). Bu seyrüsefer yardımcıları analiz edildiğinde organizasyonları akış ve engeller arasından en iyi geçitler konusunda bilgilendirecek operasyonel verilerin elde edilmesini sağlar. Havacılık organizasyonlarının sahip olabileceği çeşitli seyrüsefer yardımcıları vardır, bunlar emniyet verileri elde etme sürecini başlatan tetikleyici olayın sonuçlarının ciddiliğine göre üç tipe ayrılabilir: reaktif, proaktif ve tahmine dayalı.

3.5.3 ***Reaktif*** seyrüsefer yardımcıları, emniyet verileri toplama sürecinin başlatılması için, çoğu kez önemli hasarlara yol açan sonuçları olan, çok ciddi bir tetikleyici olayın gerçekleşmesine ihtiyaç duyar. Reaktif seyrüsefer yardımcıları "onarmak için bir şeyin bozulmasını" bekleme kavramına dayanır. Teknoloji arızaları ve/veya olağandışı olayları içeren durumlar için daha uygundurlar. Reaktif seyrüsefer yardımcıları olgun bir emniyet yönetiminin ayrılmaz bir parçasıdır. Yine de, reaktif seyrüsefer yardımcılarının emniyet yönetimine katkısı, üretilmesini sağladıkları bilginin olayın tetikleyici neden(ler)inin ve kimlerin suçlanacağının belirlenmesin ne kadar ötesine gittiğine ve emniyet riskleri ile ilgili katkı sağlayan etkenler ve bulgular içerip içermediğine bağlıdır. Kazaların ve ciddi olayların incelenmesi reaktif seyrüsefer yardımcılarının örnekleridir.

3.5.3 ***Proaktif*** seyrüsefer yardımcıları, emniyet verileri toplama sürecinin başlatılması için, az hasara veya daha önemsiz hasarlara yol açan sonuçları olan, daha az ciddi bir tetikleyici olayın gerçekleşmesine ihtiyaç duyar. Proaktif seyrüsefer yardımcıları, sistem arızalarının arızalanmadan önce sistemin içindeki emniyet risklerinin tanımlanması ve bu türden emniyet risklerinin azaltılması için gereken önlemlerin alınması ile en aza indirilebileceği kavramına bağlıdır. Zorunlu ve gönüllü raporlama sistemleri, emniyet denetimleri ve emniyet anketleri proaktif seyrüsefer yardımcılarının örnekleridir.

3.5.3 ***Tahmine dayalı*** seyrüsefer yardımcıları, emniyet verileri toplama sürecinin başlatılması için bir tetikleyici olayın gerçekleşmesine ihtiyaç duymaz. Rutin operasyon verileri gerçek zamanlı olarak, sürekli toplanır. Tahmine dayalı seyrüsefer yardımcıları, emniyet yönetiminin en iyi şekilde sorunun ortaya çıkmasını bekleyerek değil, sorunu arayarak gerçekleştirilebileceği kavramına dayanır. Bu nedenle, tahmine dayalı emniyet verileri toplama sistemleri, ortaya çıkabilecek emniyet risklerinin göstergesi olabilecek emniyet verilerini çeşitli kaynaklardan agresif olarak elde etmeye çalışır.



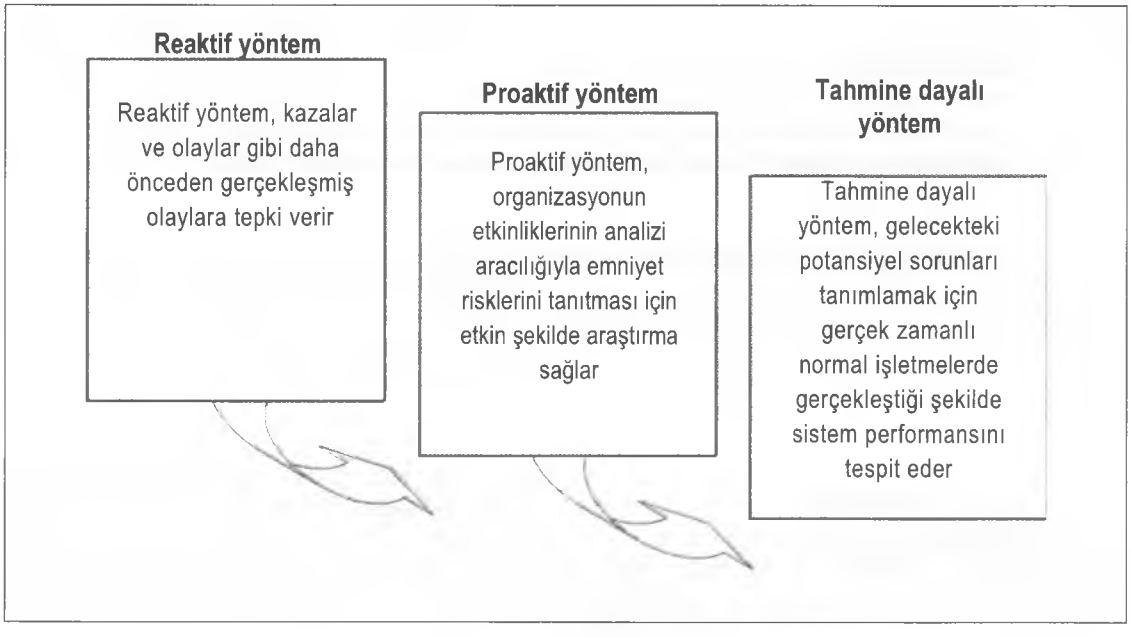
Şekil 3-5. Pratik sapma içinde yönlendirme

3.5.6 Tahmine dayalı emniyet verileri toplama sistemleri temelde istatistiksel sistemlerdir, bu sistemlerde tek başına olduğunda büyük oranda önemsiz olan, çok miktarda operasyon veri toplanır ve analiz edilir ve reaktif ve proaktif veri toplama sistemlerinden alınan verilerle birleştirilir. Böylece, verilerin birleştirilmesi organizasyonların engeller ve akışlar arasında yönlerini bulmalarını sağlayacak ve kendilerini sapma içinde optimum şekilde konumlarına yardımcı olacak en eksiksiz bilgi birikiminin geliştirilmesini sağlar. Tehlike raporlama sistemleri, uçuş verileri analizi ve normal işletmelerin izlenmesi tahmine dayalı seyrüsefer yardımcılarının örnekleridir.

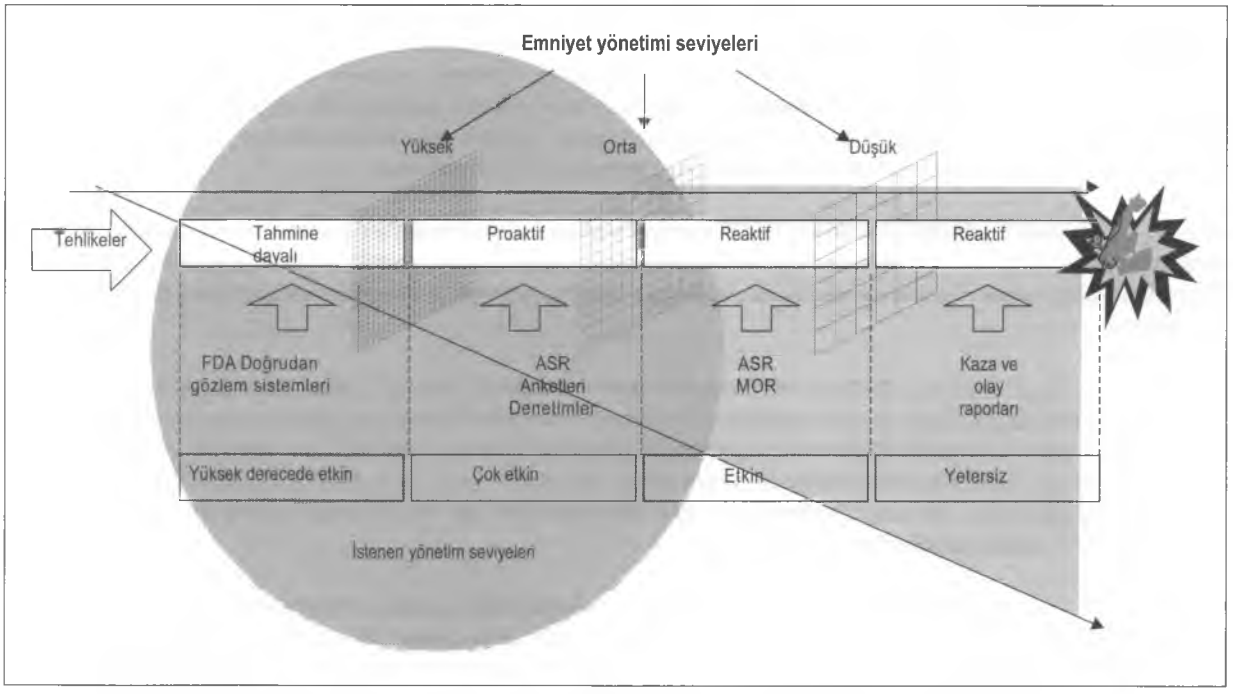
3.5.7 Reaktif, proaktif ve tahmine dayalı emniyet verileri toplama sistemleri benzeri reaktif, proaktif ve tahmine dayalı emniyet yönetimi stratejilerine emniyet verileri sağlarlar, bu stratejiler ise reaktif, proaktif ve tahmine dayalı azaltma yöntemlerine bilgi sağlar. Önceki paragraflarda açıklanan şekilde, emniyet yönetimi stratejilerinin bir özeti Şekil 3-6'da sunulmuştur.

3.5.7 Olgun emniyet yönetimi reaktif, proaktif ve tahmine dayalı emniyet verileri toplama sistemlerinin, reaktif, proaktif ve tahmine dayalı sorun azaltma stratejilerinin makul bir kombinasyonunun entegrasyonunu ve reaktif, proaktif ve tahmine dayalı sorun azaltma stratejilerinin geliştirilmesini gerektirir. Yine de, sorun azaltma stratejilerini geliştirirken, ele alınan üç emniyet verisi toplama sisteminin operasyonel sapmanın farklı seviyelerinde emniyet verisi topladığının unutulmaması önemlidir. Üç sorun azaltma stratejisi ve yönteminin her birinin pratik sapmanın farklı seviyelerinde devreye girdiğinin unutulmaması da önemlidir.

3.5.9 Bunu göstermek için, Şekil 3-7'de gösterilen şekilde pratik sapmaya dönülmelidir. Tehlikeler pratik sapma boyunca bir süreklilik halinde bulunmaktadır. Sınırlanmazlarsa, hasar potansiyelleri artarak sapma boyunca aşağı hareket ederler. Pratik sapmanın başlangıç veya çıkış noktasının yakınlarında, hasar verme potansiyellerine ulaşma olanağını bulamadıklarından tehlikeler göreli olarak zararsızdırlar. Tehlikeler engellenmeden pratik sapma boyunca ilerlediklerinde, daha fazla momentum kazanırlar ve hasar verme potansiyelleri artar. Tehlikeler pratik sapmanın en geniş olduğu noktaya yaklaştıkça, hasar için maksimum potansiyel gelişmiş olur, buna ciddi arıza potansiyelleri de dahildir. Bu nedenle, emniyet yönetimi için tehlikelerin pratik sapmanın başlangıç noktasına mümkün olduğunca yakında tespit edilmesi önemlidir.



Şekil 3-6. Emniyet yönetimi stratejileri



Şekil 3-7. Stratejiler — Müdahale seviyeleri ve araçlar

3.5.10 Tahmine dayalı emniyet verileri toplama sistemleri, stratejileri ve yöntemleri, pratik sapmanın başlangıç veya çıkış noktasının çok yakınında çalışır. Bu, son derece yüksek seviyeli ve etkin bir müdahaledir. Tahmine dayalı emniyet verileri toplama sistemleri, stratejileri ve yöntemlerinin yüksek etkinliğinin nedeni iki katmanlıdır: bir yandan, tehlikelerle henüz emekleme döneminde, henüz hasar verme potansiyellerini geliştirme fırsatını bulamadan, bu nedenle engellenmeleri henüz kolayken başa çıkarlar. Bu nedenle, tahmine dayalı emniyet verilerinden geliştirilen azaltmalar, neredeyse ortaya çıkmakta olan tehlikelerin pratik sapmanın sürekliliği içinde daha aşağı inmelerine izin vermeyen sıkılığa sahip ağlar veya filtrelere dönüşürler.

3.5.11 Proaktif dayalı emniyet verileri toplama sistemleri, stratejileri ve yöntemleri de pratik sapmanın ve tehlike sürekliliğinin öncesinde çalışırlar, ama tahmine dayalı emniyet verileri toplama sistemleri, stratejileri ve yöntemleri kadar pratik sapmanın başlangıç veya çıkış noktasının yakınında değillerdir. Bu da yüksek seviyeli ve çok etkin bir müdahaledir. Yine de, tehlikeler hasar verme potansiyellerini geliştirmeye başlamışlardır. Bu nedenle, proaktif dayalı emniyet verilerinden geliştirilen azaltmalar, sıkı olsalar da, ortaya çıkmakta olan tehlikelerin pratik sapmanın sürekliliği içinde daha aşağı inmelerine izin veren ağlar veya filtrelere dönüşürler.

3.5.10 Reaktif emniyet verileri toplama sistemleri, stratejileri ve yöntemleri, pratik sapmanın iki seviyesinde çalışır. Zorunlu olay raporlama sistemleri gibi bazıları orta müdahale seviyesinde çalışır. Bu etkin bir seviyedir, ama tehlikelerin hasar verme potansiyelleri artmaya devam eder. Dolayısıyla, reaktif emniyet verilerinin bu birinci seviyesinden geliştirilen azaltmalar, tehlikelerin sıklıkla arasından geçebildiği gevşek yapılı bir ağ veya filtreye dönüşür. Reaktif emniyet verileri toplama sistemleri, stratejileri ve yöntemlerinin en düşük seviyesinde, kaza ve ciddi olay incelemeleri hasar onarım modunda çalışır. Tamamen reaktif emniyet verilerinden elde edilen bilgiler emniyet yönetimi için yeterli değildir.

3.6 DEĞİŞİM ZORUNLULUĞU

3.6.1 Küresel havacılığın etkinliği ve karmaşıklığı artmaya devam ettikçe yeni zorluklarla büyük ölçüde değişen operasyonel bağlamlar kabul edilebilir seviyedeki klasik emniyet yönetimi yöntemlerini daha az etkin ve etkili bir hale getirmiştir. Emniyet yönetiminin anlaşılması ve yönetilmesi için farklı, gelişmiş yöntemler gerekir. Uluslararası sivil havacılıkta şu anda, geçmişin emniyetle ilgili çalışmaları tarafından getirilen paradigmadan önemli bir sapmayı yansıtan bir geçiş gerçekleşmektedir.

3.6.2 Daha önce açıklandığı gibi, klasik emniyet paradigması ana emniyet müdahalesi ve yöntemi olarak kaza/ciddi olay incelemelerine dayanıyordu ve üç temel varsayım üzerine kurulmuştu:

a) Havacılık sistemi çoğu kez tasarım özelliklerine (yani temel performansa) uygun şekilde çalışır;

b) Düzenlemelere uyulması sistemin temel performansını garanti eder ve böylece emniyeti (uyum temelinde) sağlar ve

c) Düzenlemelere uyum sistem temel performansını garanti eder, rutin işletmeler (yani süreçler) sırasında küçük, pek sonuç yaratmayan sapmalar önemli değildir, sadece kötü sonuçlara (yani neticelere) neden olan önemli sapmalar önemlidir.

3.6.3 Buna karşı, bu el kitabında da olumlu görülen, çağdaş bir emniyet paradigması ortaya çıkmaktadır. Bu paradigma, ortaya çıkan olayların incelenmesinin ötesinde, süreç kontrolü ile emniyet yönetimi kavramını temel almaktadır ve yine üç temel varsayıma dayanmaktadır:

a) Havacılık sistemi çoğu kez tasarım özelliklerine uygun şekilde çalışmaz (yani operasyonel performans pratik sapmaya yol açar);

b) Sadece düzenlemelere uyuma dayanmak yerine, sistemin gerçek zamanlı performansı izlenir (performans temelinde) ve

c) Rutin işletmeler sırasında küçük, pek sonuca yol açmayan sapmalar sürekli olarak izlenir ve analiz edilir (sürece yönelik).

3.7 EMNİYET YÖNETİMİ — SEKİZ TEMEL İLKE

3.7.1 Emniyetin yönetilmesi süreci aşağıdaki sekiz temel ve ayrı ilkeye dayanır.

a) ***Üst yönetimin emniyet yönetimine bağlılığı.*** Emniyetin yönetimi, diğer yönetim etkinlikleri gibi, kaynakların dağıtılmasını gerektirir. Kaynakların dağıtımı, tüm organizasyonlarda, üst yönetimin bir işlevidir, dolayısıyla üst yönetimin emniyetin yönetimine bağlı kalması gerekir. Düz bir ifadeyle: para olmazsa, emniyet de olmaz.

b) ***Etkili emniyet raporlaması.*** "Ölçemediğini yönetemezsin" bilinen bir deyiştir. Emniyeti yönetmek için, organizasyonlar ölçümün yapılabilmesini sağlayan tehlikelerle ilgili emniyet verilerini elde edebilmelidir. Bu verilerin çoğu gönüllü ve kendiliğinden raporlar sunan operasyonel personelinden elde edilir. Bu nedenle, organizasyonların operasyonel personel tarafından etkili emniyet raporlaması yapılan çalışma ortamları geliştirmeleri önemlidir.

c) Normal işletmeler sırasında tehlikelerle ilgili emniyet verilerini toplayan sistemler aracılığıyla ***sürekli izleme***. Emniyet verilerinin toplanması sadece ilk adımdır. Toplamanın ötesinde, organizasyonlar

verilerden emniyet bilgilerini ve emniyet istihbaratını çıkarmalı ve analiz etmelidir, çünkü toplanan ve bir çekmeceye kaldırılan verilerin hiç veri olmamasından bir farkı yoktur. Ayrıca, elde edilen emniyet bilgileri ve istihbaratını günlük olarak sistemi çalıştıran kişilerle paylaşmak da önemlidir, çünkü etkili emniyet raporlamasının sonuçlarını azaltmaya çalıştığı tehlikelerle sürekli temas halinde olan bu kişilerdir.

d) Suçlama yapmak yerine sistemli emniyet sorunlarının belirlenmesi hedefiyle ***emniyetle ilgili sorunların incelenmesi.*** "Kimin yaptığını" belirlemek "neden gerçekleştiğini" öğrenmek kadar önemli değildir. Sistemin dayanıklılığı "uygun olmadığı" düşünülen bireylerin çıkarılması yerine sistemli sorunların ortadan kaldırılması ile daha etkili bir şekilde güçlendirilebilir.

e) Emniyet bilgilerinin etkin bir şekilde aktarılması ile ***öğrenilen emniyet derslerinin ve en iyi pratiklerin paylaşılması.*** Başka bir bildik deyim de, verilerin paylaşılmasının ve emniyet bilgilerinin aktarılmasının gerekliliğini göstermektedir: "başkalarının hatalarından ders almalısın, hepsini kendin yapmaya ömrün yetmeyecektir". Havacılık endüstrisinin emniyet verilerini paylaşmaya yönelik mükemmel geleneği korunmalı ve mümkünse güçlendirilmelidir.

f) ***İşletme personeline yönelik emniyet eğitiminin entegrasyonu.*** İşletme personelinin eğitim müfredatı nadiren özel emniyet eğitimini içerir. "Emniyet herkesin sorumluluğu olduğundan", operasyonel personelin kendiliğinden emniyet uzmanları olduğuna dair bir kabul vardır. Bu akıl yürütmenin yanlışlığı açıktır ve Bölüm 7'de ele alınmıştır. İşletme personeli eğitiminin tüm seviyelerinde emniyet yönetiminin temellerine yönelik ayrı bir eğitim eklenmesi acil bir gereksinimdir.

g) Kontrol listeleri ve brifinglerin kullanılmasını da içerecek şekilde, ***standart operasyonel prosedürlerin (SOP'lar) etkili bir şekilde uygulanması***. İster bir uçuş güvertesinde, ister bir hava trafiği kontrol odasında, bir bakım atölyesinde, bir apronda olsun, SOP'lar, kontrol listeleri ve brifingler operasyonel personelin günlük sorumluluklarını yerine getirmesinde en etkili emniyet araçları arasındadır. Organizasyonun getirdiği güçlü bir zorunlulukturlar ve üst yönetimin işletmelerin nasıl gerçekleştirilmesini istediğini gösterirler. Gerçekçi, doğru şekilde yazılmış ve sürekli olarak uygulanan SOP'lar, kontrol listeleri ve brifinglerin emniyet değeri hafife alınmamalıdır.

h) **Genel emniyet seviyesinin sürekli olarak iyileştirilmesi** Emniyet yönetimi bir günlük bir iş değildir. Sadece sürekli iyileştirme yapılması ile başarılı olunabilen sürekli bir etkinliktir.

3.7.2 Bu sekiz temel ilkenin uygulanmasının sonucu, emniyetli uygulamaları ortaya çıkaran, etkili emniyet iletişimini destekleyen ve emniyeti etkin bir şekilde yöneten bir örgüt kültürü olacaktır.

3.8 EMNİYET YÖNETİMİNİN SAĞLANMASI İÇİN DÖRT SORUMLULUK

3.8.1 Emniyet yönetimi için sorumluluklar, aşağıdaki gibi dört genel ve temel alana ayrılabilir:

a) ***Emniyetle ilgili politikalar ve prosedürlerin tanımlanması.*** Politika ve prosedürler, üst yönetimin işletmelerin nasıl gerçekleştirilmesini istediğini gösteren organizasyonel zorunluluklardır. Bu nedenle, operasyonel personele organizasyonun günlük işletmelerde operasyonel personelden beklediği operasyonel davranış hakkında açık bir kılavuz sağlamak için politikaların ve prosedürlerin açık bir şekilde tanımlanması zorunludur.

b) ***Kaynakların emniyet yönetimi etkinlikleri için dağıtılması.*** Emniyetin yönetilmesi için kaynaklara ihtiyaç duyulur.Kaynakların dağıtılması bir yönetim işlevidir. Yönetim, organizasyonun kapasitelerini tehdit eden tehlikelerin sonuçlarından doğacak emniyet risklerini azaltmak için kaynakların dağıtılması yetkisine ve dolayısıyla sorumluluğuna sahiptir.

c) ***En iyi endüstri uygulamalarının kabul edilmesi.*** Havacılığın emniyetin mükemmelleştirilmesi geleneği, sağlam emniyet uygulamalarının sürekli olarak geliştirilmesine yol açmıştır. Ayrıca, havacılık hem kurumsal hem de resmi olmayan kanallarla emniyet bilgisi alışverişi geleneğine sahiptir. En iyi endüstri uygulamalarının kabul edilmesi için bu iki olumlu özellik güçlendirilmeli ve uygulanmalıdır.

d) ***Sivil havacılık emniyeti ile ilgili düzenlemelerin birleştirilmesi.*** Emniyet yönetiminin önceki düzenleme çerçevelerini gereksiz veya fazlalık durumunda bırakacağı gibi bir yanlış algılama olabilir. Bu en güçlü şekilde ortadan kaldırılması gereken bir yanlış algılamadır. Emniyet yönetimi çabalarının oturduğu temel olarak, düzenleyici çerçevelere daima ihtiyaç olacaktır. Aslında, makul bir emniyet yönetimi sadece makul düzenlemelerden yola çıkarak geliştirilebilir.

3.8.2 Özet olarak, emniyet yönetimi:

a) tüm işletmeyi içerir;

b) süreçler ve sonuçlar arasında açık bir ayrım yaparak, süreçlere odaklanır;

c) verileri temel alır;

d) sürekli izlemeyi içerir;

e) kesin bir şekilde belgelenir;

f) dramatik değişimlerden çok kademeli olarak iyileştirmeyi hedefler ve

g) parça parça inisiyatifler yerine stratejik planlamayı temel alır.

Bölüm 4

TEHLİKELER

4.1 HEDEF VE İÇERİKLER

Bu bölüm tehlikenin tanımlanması ve analizinin temellerini açıklamaktadır ve aşağıdaki konuları içerir:

a) Tehlikeler ve sonuçları;

b) İlk temel bilgi – Tehlikelerin anlaşılması;

c) İkinci temel bilgi – Tehlikelerin tanımlanması;

d) Üçüncü temel bilgi – Tehlikelerin analizi ve

e) Dördüncü temel bilgi – Tehlikelerin dokümantasyonu.

4.2 TEHLİKELER VE SONUÇLARI

4.2.1 Tehlikenin tanımlanması ve emniyet riski yönetimi emniyetin yönetiminde yer alan temel süreçlerdir. Ne yenidirler ne de emniyet yönetimine ve özellikle de emniyet yönetimi sistemlerine (SMS) son zamanlarda gösterilen ilginin sonucu olarak geliştirilmişlerdir. Tehlikenin tanımı ve emniyet riski yönetimi, çatıyı oluşturan sistem emniyeti kavramının altında yatan dogmatik bileşenlerdir. Bu, sistem tasarımına katkıda bulunan ve kırk yıldan uzun süre önce geliştirilmiş kapsayıcı, mühendislik temelli bir yaklaşımdır. Geleneksel sistem emniyeti ile günümüzdeki emniyet yönetimi arasındaki fark, mühendislik kökenleri nedeniyle sistem emniyetinin çoğunlukla belki de insani bileşeni devre dışı bırakarak, ilgili sisteminin teknik yönlerinin ve bileşenlerinin emniyetle ilgili çıkarımlarına odaklanmış olmasıdır. Diğer yandan, emniyet yönetimi sistem emniyeti (tehlikenin tanımlanması ve emniyet riski yönetimi) dogması üzerine inşa edilir ve perspektifi sistem tasarımı ve işletilmesi sırasında İnsani Etkenleri ve insan performansını önemli emniyet konuları olarak içerecek şekilde genişletir.

4.2.2 Tehlikeler ve emniyet riskleri arasındaki fark sıklıkla zorluk ve kafa karışıklığı nedenidir. Anlamlı ve etkili emniyet yönetimi uygulamaları geliştirmek için, tehlikenin ne olduğunun ve bir emniyet riskinin ne olduğunun açıkça anlaşılması önemlidir. Bu bölümde özel olarak tehlikeler ele alınmaktadır, Bölüm 5'te ise emniyet riskleri ele alınacaktır. Tehlikeleri ele alırken, tehlikeler ve emniyet riskleri arasındaki farkın anlaşılmasına katkıda bulunmak için, genel tehlike kavramı iki bileşene ayrılmaktadır: tehlikenin kendisi ve sonuçları. Bu iki bileşen arasındaki farkın açıkça anlaşılması da, emniyet yönetimi uygulamasının önemli noktalarından biridir.

4.2.3 Bir tehlike, personelin yaralanması, donanım veya yapıların hasar görmesi, malzeme kaybı veya belirli bir işlevin gerçekleştirilmesi becerisinin azalmasına neden olma potansiyeline sahip bir koşul veya nesne olarak tanımlanır. İnsanların, hizmetleri sunarak üretim hedeflerine ulaşmak için teknoloji ile etkin ve yakın etkileşime girmesi gereken sistemler aynı zamanda sosyo-teknik sistemler olarak da adlandırılır. Dolayısıyla, tüm havacılık organizasyonları sosyo-teknik sistemlerdir. Tehlikeler sosyo-teknik sistemlerin normal bileşenleri veya unsurlarıdır. Sosyo-teknik sistemler tarafından hizmetlerin sunulduğu bağlamların ayrılmaz parçalarıdır. Kendiliklerinde, tehlikeler "kötü şeyler" değildir. Tehlikeler zorunlu olarak bir sistemin hasara neden olan veya olumsuz bileşenleri değildir. Ancak tehlikeler hizmet sunumuna yönelik sistemin işletmeleri ile etkileşime girdiklerinde, hasar verme potansiyelleri bir emniyet sorunu haline gelir.

4.2.4 Örneğin, doğal ortamın normal bir bileşeni olan rüzgarı ele alalım. Rüzgar bir tehlikedir: personelin yaralanması, donanım veya yapıların hasar görmesi, malzeme kaybı veya belirli bir işlevin gerçekleştirilmesi becerisinin azalmasına neden olma potansiyeline sahip bir koşuldur. On beş deniz mili hızındaki bir rüzgarın, kendiliğinde, havacılık işletmeleri sırasında hasar verme potansiyeli taşıması gerekmez. Aslında, doğrudan pist üzerinde esen on beş deniz mili hızındaki bir rüzgar kalkış sırasında uçağın performansına katkıda bulunacaktır. Ancak, on beş deniz mili hızındaki bir rüzgar kalkış veya iniş yapılmak istenen bir piste doksan derece açıyla estiğinde, bir yan rüzgar haline gelir. Ancak bu durumda, tehlike hizmet sunumuna (bir programa uyarak yolcuları veya kargoyu belirli bir havaalanından diğerine taşıma) yönelik sistemin işletmeleri (bir uçağın kalkışı veya inişi) ile etkileşime girdiğinde, hasar potansiyeli bir emniyet sorunu (yan rüzgar nedeniyle pilot uçağı kontrol edemeyebileceğinden bir pistten yana doğru çıkış) haline gelir. Bu örnek 4.2.32'teki konuyu açıklamaktadır: bir tehlike zorunlu olarak "kötü bir şey" veya olumsuz içeriği olan bir şey olarak alınmamalıdır. Tehlikeler operasyonel bağlamların ayrılmaz parçasıdır ve sonuçları bu el kitabında daha sonra ele alınacak olan tehlikenin hasar verme potansiyelini sınırlamak için çeşitli azaltma stratejileri aracılığıyla ele alınabilir.

4.2.5 Bir sonuç, bir tehlikenin potansiyel neticesi (veya neticeleri) olarak tanımlanabilir. Bir tehlikenin hasar verme potansiyeli bir veya daha fazla sayıda sonuç aracılığıyla ortaya çıkabilir. Yukarıdaki yan rüzgar örneğinde, "yan rüzgar" tehlikesinin sonuçlarından biri "yan kontrolün kaybedilmesi" olabilir. Daha ciddi bir sonuç ise "pistten yana doğru çıkış" olabilir. Çok daha ciddi bir sonuç ise "iniş takımlarında hasar" olabilir. Bu nedenle, tehlike analizi sırasında, sadece en açık veya yakın sonuçların değil, tüm olası sonuçların açıklanması önemlidir.

4.2.6 Tehlikelerin sonuçlarının ele alınması, unutulmaması gereken iki önemli noktayı getirir. İlki, tehlike şu ana aittir. Çoğunlukla, operasyonel bağlamın parçasıdırlar ve bu nedenle operasyonel personel "işe gelmeden" önce de işyerinde mevcut durumdadırlar. İşletme bağlamının veya işyerinin fiziksel bileşenleri olarak, çoğu tehlike denetimler sırasında tespit edilebilir veya edilmelidir. Diğer taraftan, sonuçlar gelecekte yer alır. Tehlikeler hizmet sunumuna yönelik sistemin belirli işletmeleri ile etkileşime girene kadar ortaya çıkmazlar. Tehlikelerin hasar verme potansiyellerini göstermeleri bu etkileşimin sonucudur. Bu, emniyet yönetiminin önemli ilkelerinden birini ortaya çıkarır: azaltma stratejileri proaktif olarak tehlikelerin hasar verme potansiyellerini sınırlamaya yönelik olmalıdır ve tehlikelerin sonuçları ortaya çıkana ve sonrasında bu sonuçları reaktif olarak ele almaya yönelmemelidir.

4.2.7 İkincisi, emniyet yönetimi amacıyla, tehlikelerin sonuçları operasyonel terimler ile ifade edilmelidir. Pek çok tehlikede, nihai ve son derece uç sonucun potansiyeli bulunur: insan kaybı. Pek çok tehlike mal kaybı, ekolojik hasar ve benzeri yüksek seviyeli sonuçların potansiyelini taşır. Ancak, tehlikelerin sonuçlarının aşırı şekilde ifade edilmesi, işletmenin iptali dışındaki azaltma stratejilerinin tasarlanmasını zorlaştırır. Tehlikenin aşırı olmayan, düşük seviyeli operasyonel sonuçların (örneğin yan rüzgarın) altında yatan emniyet sonuçlarını ele almak üzere azaltma stratejilerini tasarlamak için, bu tehlikeler aşırı terimler (can kaybı) yerine operasyonel terimler (yana doğru pistten çıkış) açıklanmalıdır.

4.2.8 Bölüm 2'de emniyet kontrollü emniyet riskinin bir koşulu olarak ele alınmaktadır. Belirli bir işletmeyi etkileyebilecek tehlikelerin sonuçlarının tanımlanması, tehlikelerin sonuçlarına ait emniyet risklerinin değerlendirilmesinin bir parçasıdır (bölüm 5'te ele alınmıştır). Tehlikelerin sonuçlarına ait emniyet risklerinin değerlendirilmesi, bir işletmenin emniyet risklerinin kontrolünü elde edip edemeyeceği ve dolayısıyla operasyona devam edip edemeyeceği konusunda bilgiye dayanan bir karar vermesini sağlar. Tehlikenin (rüzgar) sonuçları, operasyonel terimler (yana doğru pistten çıkış) yerine aşırı terimlerle (can kaybı) ifade edilirse, zorlu masraflara göğüs germedikçe ve riskin azaltılmasının olası yöntemi işletmenin iptali olduğu için, emniyet risklerinin kontrol edilmesi koşuluna ulaşılamayacağı için, emniyet riski değerlendirmesi büyük oranda atlanır.

4.3 İLK TEMEL BİLGİ – TEHLİKELERİN ANLAŞILMASI

4.3.1 Daha önce açıklandığı gibi, tehlikelerin sonuçları ile karıştırılması gibi bir eğilim vardır. Bu olduğunda, operasyonel terimler ile tehlikenin tanımı tehlikenin kendisi yerine sonuçlarını yansıtır. Başka bir deyişle, tehlikelerin sonuçları şeklinde tanımlanması alışılmadık bir durum değildir.

4.3.2 Bir tehlikenin sonuçların biri olarak ifade edilmesi ve adlandırılması, sadece söz konusu tehlikenin gerçek doğası ve hasar verme potansiyelinin gizlenmesi potansiyeline sahip değildir, aynı zamanda tehlikenin diğer önemli sonuçlarının tanıtmasını da engelleyebilir.

4.3.3 Diğer yandan, tehlikelerin doğru şekilde ifade edilmesi ve adlandırılması tehlikenin gerçek doğası ve hasar verme potansiyelinin belirlenmesini, tehlikenin kaynaklarının veya mekanizmalarının doğru şekilde anlaşılması ve en önemlisi (aşırı sonuçlar yerine) potansiyel kayıplar bakımından sonuçların değerlendirilmesini sağlar, bu da Bölüm 5'te ele alınan emniyet riski yönetiminin nihai hedeflerinden biridir.

4.3.4 Tehlikeler ve sonuçları arasındaki farkı göstermek için başka bir örnek daha verilebilir. Bir havaalanı, yön işaretleri onarılmamış olarak çalışmaktadır. Bu hem uçak hem de yer araçlarından oluşan havaalanı kullanıcılarının yerdeki navigasyonlarını karışık hale getirmektedir. Bu durumda, tehlikenin doğru şekilde adlandırılması "havaalanındaki işaretlerin açık olmaması" (yani personelin yaralanması, donanım veya yapıların hasar görmesi, malzeme kaybı veya belirli bir işlevin gerçekleştirilmesi becerisinin azalmasına neden olma potansiyeline sahip bir koşul) olmalıdır. Bu tehlikeye bağlı olarak, pek çok sonuç ortaya çıkabilir. "Havaalanındaki işaretlerin açık olmaması" tehlikesinin sonuçlarından biri (yani potansiyel sonuçlardan biri) "piste giriş" olabilir. Ama başka sonuçlar da olabilir: yer araçlarının kısıtlı alanlara girmesi, uçakların yanlış taksi yollarına taksi yapması, uçakların çarpışması, yer araçlarının çarpışması, yer araçları ve uçakların çarpışması v.s. Dolayısıyla, tehlikenin "havaalanındaki işaretlerin açık olmaması" yerine "piste giriş" olarak adlandırılması tehlikenin doğasını gizler ve diğer önemli sonuçların tanıtmasını engeller. Bu, kısmi veya yetersiz azaltma stratejilerine neden olacaktır.

4.3.5 Tehlikeler üç genel gruba ayrılabilir: doğal tehlikeler, teknik tehlikeler ve ekonomik tehlikeler.

4.3.6 ***Doğal tehlikeler*** hizmetlerin verilmesi ile ilgili işletmelerin içinde yer aldığı ortam veya habitatın sonucudur. Doğal tehlikelerin örnekleri şunlardır:

a) ciddi hava veya iklim olayları (örneğin kasırgalar, fırtınalar, kuraklıklar, tornadolar, gök gürültülü fırtınalar, ışık ve rüzgar değişimi);

b) olumsuz hava koşulları (örneğin buzlanma, donma başlangıcı, şiddetli yağmur, kar, rüzgar ve görüş mesafesinin azalması);

c) jeofizik olaylar (örneğin depremler, yanardağ patlamaları, tsunamiler, seller ve toprak sapmaları);

d) coğrafi koşullar (örneğin olumsuz yer koşulları veya büyük su birikintileri);

e) çevre olayları (örneğin orman yangınları, vahşi yaşam etkinlikleri veya böcek veya zararlı istilası) ve/veya

f) kamu sağlığı olayları (örneğin grip salgını veya diğer hastalıklar).

4.3.7 ***Teknik tehlikeler*** enerji kaynaklarının (elektrik, yakıt, hidrolik basınç, pnömatik basınç v.s.) veya hizmetlerin yerine getirilmesi ile ilgili işletmeler için gerekeli emniyet bakımından kritik işlevlerin (donanım arızası potansiyeli, yazılım sorunu, uyarılar v.s.) sonucudur. Teknik tehlikelerin örnekleri aşağıdakilerle ilgili sorunları içerir:

a) uçaklar ve uçak parçaları, sistemleri, alt sistemleri ve ilgili donanım;

b) bir organizasyonun tesisleri, araçları ve ilgili donanımı ve/veya

c) organizasyonun dışındaki tesisler, sistemler, alt sistemler ve ilgili donanım.

4.3.8 ***Ekonomik tehlikeler*** hizmetlerin verilmesi ile ilgili işletmelerin içinde yer aldığı sosyo-politik ortamın sonucudur. Ekonomik tehlikelerin örnekleri şunlardır:

a) büyüme;

b) resesyon ve

c) malzeme veya donanım maliyeti.

4.3.9 Emniyet risklerinin kontrol edilmesine yönelik emniyet yönetimi etkinlikleri, sadece bunlarla sınırlı olmasa da, büyük oranda teknik ve doğal tehlikeleri ele almalıdır.

4.4 İKİNCİ TEMEL BİLGİ – TEHLİKELERİN TANIMLANMASI

4.4.1 Tehlikelerin tüm sosyo-teknik üretim sistemlerinin dokusunun bir parçası olduğu daha önce ele alınmıştı. Bu nedenle, havacılıktaki tehlikelerin kapsamı geniştir. Tehlikelerin tanımlanması sırasında araştırılması gereken etkenlerin ve süreçlerin kapsamı aşağıdaki örneklerden oluşur:

a) donanım ve görev tasarım dahil olmak üzere, tasarım faktörleri;

b) Dokümantasyonları ve kontrol listeleri ve gerçek çalışma koşulları altında doğrulanmaları dahil olmak üzere, prosedürler ve çalışma pratikleri;

c) araçlar, terminoloji ve dil dahil olmak üzere iletişim;

d) işe alma, eğitim, ücret ve kaynak dağıtımı ile ilgili şirket politikaları gibi personel faktörleri;

e) üretim ve emniyet hedeflerinin uygunluğu, kaynakların dağıtımı, çalışma baskıları ve kurumsal emniyet kültürü gibi örgüt faktörleri;

f) ortam gürültüsü ve titreşim, sıcaklık, aydınlatma ve koruyucu donanım ve giysiler gibi iş ortamı faktörleri;

g) düzenlemelerin uygulanabilirliği ve yürütülebilirliği, donanım, personel ve prosedürlerin sertifikasyonu ve denetimin yeterliliği gibi düzenleyici denetim faktörleri;

h) yeterli tespit ve uyarı sistemlerinin tedariki, donanımın hata toleransı ve donanımın hata ve arızalara dayanıklılığı gibi faktörler de dahil olacak şekilde savunmalar ve

i) tıbbi koşullar ve fiziksel sınırlamalarla kısıtlı kalacak şekilde insan performansı.

4.4.2 Bölüm 3'te ele alındığı gibi, tehlikeler emniyetle ilgili gerçek olayların (kazalar veya olaylar) sonrasında belirlenebilir veya emniyet olaylarına yol açmadan önce tehlikelerin belirlenmesine yönelik proaktif ve tahmine dayalı süreçler aracılığıyla belirlenebilir. Tehlikenin tanımlanması için çeşitli kaynaklar vardır. Bazı kaynaklar organizasyonun içinde, bazıları ise dışında bulunur.

4.4.3 Bir organizasyondaki tehlikelerin tanımlanması için iç kaynakların örnekleri aşağıdakilerdir:

a) uçuş verileri analizi;

b) şirket gönüllü raporlama sistemi;

c) emniyet araştırmaları;

d) emniyet denetimleri;

e) normal operasyon izleme programları;

f) trend analizi;

g) eğitimden alınan geri bildirim ve

h) olayların incelenmesi ve izlenmesi.

4.4.4 Bir organizasyondaki tehlikelerin tanımlanması için dış kaynakların örnekleri aşağıdakilerdir:

a) kaza raporları;

b) Devlet zorunlu olay raporlama sistemi;

c) Devlet gönüllü raporlama sistemi;

d) Devlet denetimleri ve

e) bilgi alışverişi sistemleri.

4.4.5 Bu konudaki temel nokta, hiçbir kaynak veya programın tamamen diğerlerinin yerine geçemeyeceği veya diğer kaynakları veya programları gereksiz hale getirmeyeceğidir. Olgun emniyet yönetimi pratikleri altında gerçekleştirilen tehlike tanımlanması işlemi, iç ve dış kaynakların, reaktif, proaktif ve tahmine dayalı süreçlerin ve bunların altında yatan programların makul bir kombinasyonuna yönelir.

4.4.6 Havacılık organizasyonlarında tüm personel sorumlulukları ile orantılı bir seviyede, uygun emniyet yönetimi eğitimini almalıdır, böylece organizasyondaki herkes tehlikeleri tanımlamaya ve raporlamaya hazır olabilir ve bunu yerine getirebilir. Bu perspektiften bakıldığında, tehlikenin tanımlanması ve raporlanması herkesin sorumluluğundadır. Ancak, organizasyonlar tehlikenin tanımlanması ve analizi için ayrıca sorumlu personel bulundurmalıdır. Bu, normal olarak Bölüm 8'de ele alındığı şekilde emniyet hizmetleri ofisine atanan personel olmalıdır. Dolayısıyla, önceki perspektif genişletildiğinde, havacılık organizasyonlarında, tehlikenin tanımlanması herkesin sorumluluğundadır, ama tehlikenin tanımlanması ile ilgili hesap verme sorumluluğu bu işe ayrılmış emniyet personeline aittir.

4.4.7 Tehlikelerin nasıl tanımlanacağı her bir organizasyonun kaynaklarına ve kısıtlamalarına bağlıdır. Bazı organizasyonlar kapsamlı, yoğun teknoloji içeren tehlike tanımlama programları oluşturacaklardır. Diğer organizasyonlar, kendi ölçülerine ve işletmelerinin karmaşıklığına daha uygun orta seviyede tehlike tanımlama programları oluşturacaklardır. Yine de, uygulanması, karmaşıklığı ve ölçüsünden bağımsız olarak, tehlikenin tanımlanması organizasyonun emniyet dokümantasyonunda açıkça tanıtılan resmi bir süreç olmalıdır. Geçici tehlike tanımlama, emniyet yönetimi uygulamalarında kabul edilemez.

4.4.8 Olgun emniyet yönetim pratikleri uygulandığında, tehlikenin tanımlanması sürekli devam eden, günlük bir etkinliktir. Asla durmaz ve ara verilemez. Organizasyonun iş alanındaki hizmetlerin sunulmasına yönelik örgütlenme süreçlerinin ayrılmaz bir parçasıdır. Yine de, tehlikenin tanımlanmasına özel önem gösterilmesi gereken üç özel koşul vardır. Bu üç koşul daha derinlemesine ve uzun vadeli tehlike tanımlama etkinliklerini tetiklemelidir ve aşağıdakilerden oluşurlar:

a) emniyetle ilgili olaylar veya düzenleme ihlallerinde organizasyonda açıklanamayan bir artış yaşandığında;

b) kritik personel veya diğer önemli donanım veya sistemlerdeki değişiklikler dahil olmak üzere önemli operasyonel değişiklikler öngörüldüğünde;

c) hızlı büyüme veya küçülme, şirket birleşmeleri, alımları veya personel çıkarımları dahil olmak üzere önemli örgütlenme değişiklik dönemleri sırasında veya öncesinde.

4.5 ÜÇÜNCÜ TEMEL BİLGİ – TEHLİKELERİN ANALİZİ

4.5.1 Tehlikenin tanımlanması, toplanan verilerden emniyet bilgileri çıkarılmadığında boşuna bir tatbikattır. Emniyet bilgilerinin geliştirilmesinde ilk adım tehlike analizidir.

4.5.2 Tehlike analizi, özünde üç adımdan oluşan bir süreçtir:

a) ***İlk adım.*** Genel tehlikeyi (en üst seviye tehlike veya TLH olarak da adlandırılır) belirleyiniz. Bu el kitabının bağlamında genel tehlike, genel tehlikeden kaynaklanan pek çok ayrı tehlikenin izlenmesi ve sınıflandırılmasını basitleştirmeye yardımcı olmanın yanında, bir emniyet sorunu ile ilgili odaklanma ve perspektif sağlamayı amaçlayan bir terimdir.

b) ***İkinci adım.*** Genel tehlikeyi, belirli tehlikelere veya genel tehlikenin bileşenlerine ayırınız. Her bir özel tehlikenin muhtemelen farklı ve benzersiz bir nedensel etkenler kümesi olacaktır, böylece her bir tehlikenin doğası farklı ve benzersiz olacaktır.

c) ***Üçüncü adım.*** Özel tehlikeleri potansiyel olarak özel sonuçlara, yani özel olaylara veya sonuçlara bağlayınız.

4.5.3 Genel tehlike, özel tehlike ve sonuçları kavramlarını göstermek için bir örnek verilmiştir. Yılda 100.000 hareketin gerçekleştiği bir uluslararası havaalanında kesişen iki pistin genişletilmesi ve yeniden asfalt döşenmesi için bir inşaat projesi başlatılmıştır. Aşağıdaki üç adımlı tehlike analizi süreci geçerli olacaktır:

a) Adım A. Genel tehlikeyi (tehlike ifadesi veya TLH) belirtiniz.

— havaalanı inşaatı

b) Adım B. Özel tehlikeleri veya genel tehlikenin bileşenlerini belirleyiniz

— inşaat donanımı
— kapalı taksi yolları v.s.

c) Adım C. Belirli tehlikeleri belirli sonuçlara bağlayınız.

— inşaat donanımına çarpan uçak (inşaat donanımı)
— yanlış taksi yolundan kalkan uçak (kapalı taksi yolları) v.s.

4.5.4 4.5.3'te ele alınan pist inşaatı örneği Bölüm 3'teki "iki P ikilemi" hakkındaki konunun tehlike analizini kapsayacak şekilde genişletilmesi için de kullanılabilir: hizmetin etkin ve emniyetli bir şekilde verilmesi üretim hedefleri ve emniyet hedefleri arasında sürekli bir denge bulunmasını gerektirir. Pist inşaatı örneğinde, açık bir etkinlik (üretim) hedefi vardır: pist inşaatı sırasında normal havaalanı operasyonlarının sürdürülmesi. Aynı şekilde açık bir emniyet (koruma) hedefi vardır: pist inşaatı projesi sırasında havaalanı operasyonlarının mevcut emniyet marjlarının sürdürülmesi. Tehlike analizi yapılırken, emniyet yönetiminin iki temel öncülü analizlerin önünde yer almalıdır:

a) tehlikeler sosyo-teknik üretim sistemlerinin yapısında bulunan potansiyel açıklardır. Sağladıkları özelliklerin sonucu olarak sistemin zorunlu bir parçasıdırlar veya potansiyel olarak sistemin hizmetlerini sunmasını sağlayabilirler. Bu nedenle, havacılık işyerleri işletmelerin sürmesi gerektiğinde ele alınmaları maliyet faydası sağlamayacak tehlikeler barındırabilirler ve

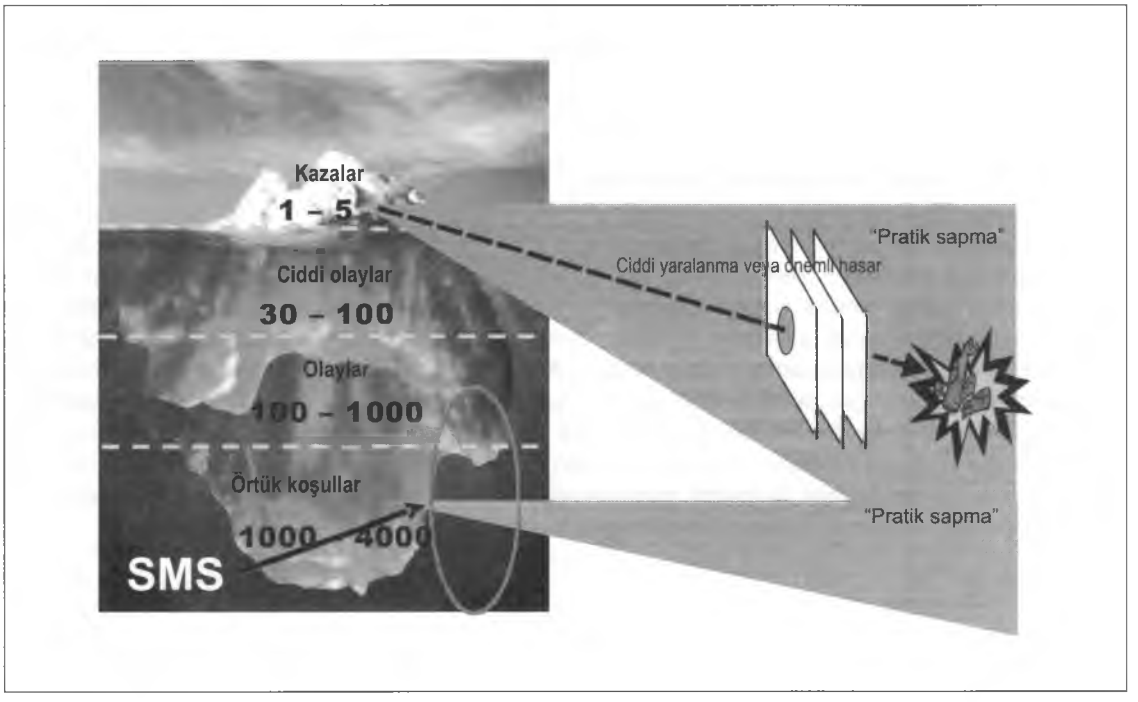
b) ciddi yaralanma veya önemli hasar içeren nadir olayların sonrası ile sınırlandığında tehlikelerin tanımlanması boşuna bir çaba olabilir. Bu durum, tehlike tanımlamasını Bölüm 3'te ele alınan pratik sapma ile bağlantılandırarak Şekil 4-1'de gösterilmiştir.

4.6 DÖRDÜNCÜ TEMEL BİLGİ – TEHLİKELERİN DOKÜMANTASYONU

4.6.1 Tehlikeler tipik olarak bir sistem içinde sürekli olarak bulunurlar ve hasar verme potansiyellerine genel olarak tehlike tanımlamasının bulunmaması veya etkisizliği nedeniyle ulaşırlar. Tehlikenin tanımlanmasının eksikliği sıklıkla aşağıdaklerin sonucudur:

a) tehlikelerin hasar verme potansiyelini açığa çıkaracak potansiyele sahip operasyonel koşulların düşünülmemesi;

b) tehlikelerin hasar verme potansiyelini açığa çıkaracak potansiyele sahip operasyonel koşulların bilinmemesi;



Şekil 4-1. Tehlike Tanımlamasının odağı

c) tehlikelerin hasar verme potansiyelini açığa çıkaracak potansiyele sahip operasyonel koşulların ele alınması veya incelenmesi ile ilgili isteksizlik;

d) tehlikelerin hasar verme potansiyelini açığa çıkaracak potansiyele sahip operasyonel koşulların incelenmesi için harcama yapmaya isteksizlik;

4.6.2 Farkında olmama veya isteksiz olma durumunun üstesinden sadece bilgi ile gelinebilir. Bu nedenle, tehlikelerin formel şekilde dokümantasyonu tehlike tanımlanmasının gerekli bir koşulu olduğu gibi olgun emniyet yönetiminin de bir özelliğidir. Emniyet bilgileri (yani analiz edilen ham veriler) ve emniyet istihbaratı (yani bağlam katarak analiz edilen ve güçlendirilen emniyet bilgileri) birleşerek, organizasyonun bireysel üyelerinin kafalarında değil, organizasyonun kendisi içinde yer alması gereken emniyet bilgisini oluştururlar. Emniyet bilgilerinin formel bir şekilde saklanması, bilgilerin uçuculuğuna karşı bir güvencedir. Ek olarak, geçmişe dayanan emniyet bilgilerine sahip bir örgüt kararlarını fikirler değil, olgulara dayalı olarak vermelidir.

4.6.3 Tehlike tanımlanması ile ilgili olarak dokümantasyonun uygun bir şekilde yönetilmesi, ham operasyonel emniyet verilerinin tehlike ile ilgili bilgiye çevrilmesi için kullanılan formel bir prosedür kadar önemlidir. Tehlike ile ilgili bu bilgilerin sürekli olarak derlenmesi ve formel bir şekilde yönetilmesi, organizasyonun "emniyet kütüphanesi" haline gelecektir. Tehlikeler hakkında bilgi sahibi olmak ve "emniyet kütüphanesini" inşa etmek için, tehlikelerin izlenmesi ve analizinin standartlaştırma ile kolaylaştığı unutulmamalıdır:

a) kullanılan terimlerin tanımları;

b) kullanılan terimlerin anlaşılması;

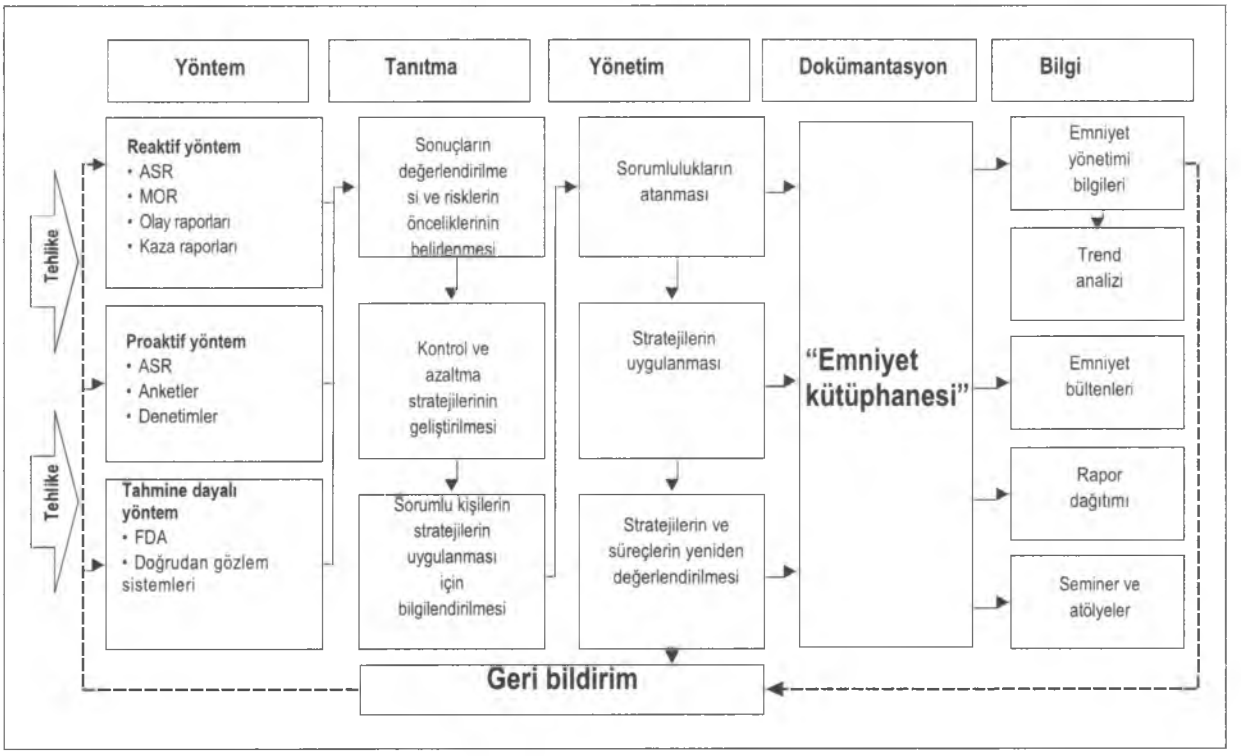
c) toplanan emniyet bilgilerinin doğrulanması;

d) raporlama (yani organizasyonun bekledikleri);

e) toplanan emniyet bilgilerinin ölçümü ve

f) toplanan emniyet bilgilerinin yönetilmesi;

4.6.7 Şekil 4-2'de tehlike dokümantasyonu süreci gösterilmiştir. Tehlikeler reaktif, proaktif ve tahmine dayalı kaynaklara ve emniyet bilgilerinin toplanmasında uygulanan yöntemlere göre sürekli olarak tanımlanır. Toplama ve tanıtılma işleminden sonra, tehlike bilgileri sonuçlar ve azaltma müdahaleleri ve stratejileri ile ilgili öncelik ve sorumluluklara göre değerlendirilir. Tehlikeler, sonuçlar, öncelikler, sorumluluklar ve stratejileri içeren bütün bu bilgiler organizasyonun "emniyet kütüphanesinde" toplanmalıdır. "Emniyet kütüphanesinin" ürünü sadece kurumsal emniyet belleğinin korunması değildir, aynı zamanda emniyet kütüphanesi organizasyonda emniyet kararlarının verilmesi için bir referans olarak kullanılabilecek bir emniyet bilgisi kaynağı haline gelir. "Emniyet kütüphanesinde" bulunan emniyet bilgileri tehlike analizi ve sonuç yönetiminin ve aynı zamanda emniyet bilgilerinin toplanma kaynaklarının ve yöntemlerini etkinliğinin ölçülmesi için geri bildirim ve kontrol referansı sağlar. Ayrıca, emniyet trend analizleri ve emniyet eğitimi için malzeme sağlar (emniyet bültenleri, raporlar, seminerler v.s.).



Şekil 4-2. Tehlikelerin dokümantasyonu

Bölüm 4 Ek 1

EMNİYET BİLGİLERİ ANALİZİ

1. Tehlike tanımlanmasının çeşitli kaynakları aracılığıyla emniyet bilgileri toplandıktan ve kaydedildikten sonra, anlamlı çıkarımlara ancak bu bilgilerin analizi sonrasında ulaşılabilir. Bu bilgilerin basit istatistik verilere indirilmesi, bu istatistiklerin çözülebilecek bir sorunu tanımlamadaki pratik önemi değerlendirilmediği sürece pek az işe yarayacaktır.

2. Emniyet veritabanları ve raporlama sistemleri oluşturulduktan sonra, herhangi bir emniyet eyleminin gerekip gerekmediğini belirlemek için organizasyonlar raporlarında ve veritabanlarında bulunan bilgileri analiz etmelidir.

EMNİYET BİLGİLERİ ANALİZİ – NEDİR?

3. Analiz olguların belirli yöntemler, araçlar veya teknikler kullanılarak düzenlenmesidir. Diğer amaçların yanında, aşağıdaki amaçlarla kullanılabilir:

a) başka hangi olguların gerektiğine karar vermeye

yardımcı olmak;

b) emniyet sorunlarının altında yatan faktörleri belirlemek ve

c) geçerli çıkarımlara ulaşmaya yardımcı olmak.

4. Emniyet analizi çeşitli kaynaklardan gelen olgulara dayalı bilgileri temel alır. İlgili veriler toplanmalı, düzenlenmeli ve saklanmalıdır. Bundan sonra analiz için uygun analitik yöntemler ve araçlar seçilir ve uygulanır. Emniyet analizi genellikle tekrarlara dayalıdır, çok sayıda çevrim gerektirir. Nicel veya nitel olabilir. Nicel temel verilerin eksikliği, daha nitel analiz yöntemlerine dayanmayı gerektirebilir.

NESNELLİK VE YANLILIK

5. İlgili tüm bilgilerin ele alınması gerekir, ancak tüm emniyet verilerinin güvenilir olması mümkün değildir. Zaman kısıtları her zaman nesnellik için yeterli bilgi toplanmasına ve değerlendirilmesine izin vermeyebilir. Bazen, güvenilir emniyet analizi için gereken nesnellikle tutarlı olmayan sezgisel çıkarımlara ulaşılabilir.

6. İnsanlar yargıda bulunurken belirli seviyede yanlılık gösterirler. Geçmiş deneyimler sıklıkla yargı üzerinde etkide bulunacaktır, yine yaratıcılık da hipotezlerin oluşturulmasını etkileyecektir. Yargı hatalarının en sık karşılaşılan biçimlerinden biri "onaylama yanlılığıdır". Bu, kişinin doğru olduğuna inandığı şeyi onaylayan bilgileri arama ve bulma eğilimini ifade eder.

ANALİTİK YÖNTEMLER VE ARAÇLAR

7. Emniyet analizinde kullanılan farklı yöntemler vardır. Bazıları otomatikleştirilmiştir, bazıları değildir. Ek olarak, bazı yazılım temelli araçlar (geçerli uygulama için farklı seviyelerde uzmanlık gerektiren) mevcuttur. Aşağıda bazı analitik yöntemler ve araçlar listelenmiştir:

a) ***İstatistiksel analiz.*** Emniyet analizinde kullanılan analitik yöntemlerin çoğu istatistiksel prosedür ve konseptlere dayanır; örneğin risk analizi istatistiksel olasılık konseptlerini kullanır. İstatistik durumların nicelleştirilmesine yardımcı olarak, böylece sayılar aracılığıyla öngörü sağlayarak emniyet analizinde önemli bir rol oynar. Bu ikna edici bir emniyet argümanı için daha güvenilir sonuçlar sağlar.

Organizasyonun emniyet yönetimi etkinlikleri seviyesinde gerçekleştirilen emniyet analizi tipi, sayısal verilerin analiz edilmesi, trendlerin belirlenmesi ve aritmetik ortalama, yüzde ve medyanlar gibi temel istatistik hesaplamaların yapılması için temel becerileri gerektirir. İstatistiksel yöntemler analizlerin grafik sunumlar için de yararlıdır.

Bilgisayarlar büyük hacimlerde verilerin işlenmesini gerçekleştirebilirler. Çoğu istatistiksel analiz prosedürü ticari yazılım paketlerinde (örneğin Microsoft Excel) sunulmuştur. Bu tür uygulamalar kullanılarak, veri önceden programlanmış bir prosedüre doğrudan girilebilir. Tekniğin altında yatan istatistik teorisinin ayrıntılı olarak anlaşılması gerekmese de, analist prosedürün ne yaptığını ve hangi sonuçların araştırıldığını anlamalıdır.

İstatistik emniyet analizi için güçlü bir araç olsa da, yanlış kullanılabilir ve dolayısıyla, hatalı çıkarımlara neden olabilir. İstatistiksel analizdeki verilerin seçimi ve kullanımında özen gösterilmelidir. Daha karmaşık yöntemlerin uygun şekilde uygulanmasını sağlamak için, istatistiksel analizde uzmanların yardımı gerekir.

b) ***Trend analizi.*** Emniyet verilerindeki trendler izlenerek, gelecekteki olaylar hakkında tahminlerde bulunulabilir. Ortaya çıkmakta olan trendler, henüz oluşum halindeki tehlikelerin göstergesi olabilir. İstatistiksel yöntemler algılanan trendlerin öneminin değerlendirilmesi için kullanılabilir. Mevcut performansla karşılaştırmak için kabul edilebilir performansın alt ve üst sınırları tanımlanabilir. Trend analizi, performansın kabul edilebilir sınırların dışına çıkmak üzere olduğu durumlarda "alarmları" tetiklemek için kullanılabilir.

c) ***Normatif karşılaştırmalar.*** Günlük deneyimlerle incelenen olay veya durumun ortaya çıktığı ortamı karşılaştırmak amacıyla olgulara dayanan bir temel oluşturmak için yeterli veri bulunmayabilir. Güvenilir normatif verinin eksikliği çoğunlukla emniyet analizlerinin kullanılmasını tehlikeye sokar. Bu tür durumlarda, gerçek dünyadaki deneyimin benzer operasyonel koşullarda örneklenmesi gerekir. Normal işletmeleri izleme programları, havacılık işletmelerinin analizi için yararlı normatif verileri sağlar.

d) ***Simülasyon ve test.*** Bazı durumlarda, tehlikeler test aracılığıyla açığa çıkarılabilir; örneğin malzeme bozukluklarını analiz etmek için laboratuar testleri gerekebilir. Kuşkulu operasyonel prosedürler için, gerçek operasyonel koşullar altında alanda veya bir simülatördeki simülasyon sağlanabilir.

e) ***Uzman paneli.*** Tehlikelerin farklı doğaları ve herhangi bir güvensiz koşulun değerlendirilmesindeki farklı perspektifler düşünüldüğünde, meslektaşlar ve uzmanlar dahil olmak üzere, diğer kişilerin görüşleri de alınmalıdır. Güvensiz bir koşulun ortaya çıkışının kanıtını değerlendirmek üzere oluşturulmuş çok disiplinli bir takım, düzeltmeye yönelik en iyi eylemin belirlenmesi ve değerlendirilmesine de yardımcı olabilir.

f) ***Maliyet-yarar analizi.*** Tavsiye edilen emniyet risk kontrolü önlemlerinin kabulü makul maliyet-yarar analizlerine bağlı olabilir. Önerilen önlemlerin maliyeti zaman içinde beklenen yararlarla kıyaslanabilir. Bazen, maliyet-yarar analizi emniyet riskinin sonuçlarını kabul etmenin düzeltme eyleminin uygulanması için harcanacak zaman, çaba ve maliyete tercih edilebilir olduğunu gösterebilir.

— — — — — — — — — —

Bölüm 4 Ek 2

EMNİYET BİLGİLERİNİN YÖNETİMİ

1. GENEL

1.1 Kaliteli emniyet verileri emniyet yönetiminin yaşam damarıdır. Etkili emniyet yönetimi "verilerle yürütülür". İşletme ve bakım raporlarından, emniyet raporlarından, denetimlerden, iş pratiklerinin değerlendirilmesinden v.s. toplanan bilgiler, hepsi emniyet yönetimi ile ilgili olmasa da çok sayıda veri üretir. Çok fazla emniyetle ilgili veri toplandığında ve saklandığında, sorumlu müdürlerin iş yükü altında boğulması, dolayısıyla verilerin kullanışlılığının ortadan kaldırılması riski vardır. Organizasyonun veritabanlarının sağlam bir şekilde yönetilmesi, (trend izleme, risk değerlendirme, maliyet-yarar analizleri ve olay incelemeleri gibi) etkili emniyet yönetimi işlevleri için temel önemdedir.

1.2 Emniyet değişimi için gereken argüman toplanan verilerin ve emniyet verilerinin analizini temel almalıdır. Emniyet veritabanının oluşturulması ve sürdürülmesi kurumsal yöneticiler, emniyet yöneticileri ve sistem emniyet sorunlarını izleyen düzenleyici otoriteler için önemli bir araçtır. Ne yazık ki, pek çok veritabanında, emniyet önceliklerinin ayarlanması, risk azaltma önlemlerinin etkinliğinin değerlendirilmesi ve emniyetle ilgili araştırmaların başlatılması için güvenilir bir temel oluşturacak veri kalitesi bulunmamaktadır. Zamanında ve geçerli kararlar vermek için verilerin, veritabanlarının anlaşılması ve uygun araçların kullanılması gerekir.

1.3 Giderek artan şekilde, emniyet bilgilerinin kaydedilmesi, saklanması, analizi ve sunumunu kolaylaştırmak için bilgisayar yazılımları kullanılmaktadır. Şimdi veritabanlarındaki bilgilerin karmaşık analizlerinin kolayca yapılması mümkün olmaktadır. Masaüstü bilgisayarlarda, organizasyonun veri yönetimi gerekliliklerini destekleyebilecek, geniş bir yelpazedeki görece ucuz elektronik veritabanları ticari olarak mevcuttur. Bu bağımsız sistemlerin avantajı organizasyonun ana bilgisayar sisteminin kullanılmaması, böylece verilerin emniyetinin iyileştirilmesidir.

2. BİLGİ SİSTEMİ GEREKLİLİKLERİ

Organizasyonlarının ölçüsüne bağlı olarak, kullanıcılar emniyet verilerini yönetebilmek için geniş bir kapasite ve çıkış yelpazesine sahip bir sisteme ihtiyaç duyarlar. Genel olarak, kullanıcıların aşağıdakilere ihtiyacı vardır:

a) büyük miktarda veriyi karar vermeyi destekleyen kullanışlı bilgilere dönüştürme kapasitesine sahip bir sistem;

b) yöneticiler ve emniyet personeli için iş yükünü azaltacak bir sistem;

c) kendi kültürlerine göre özelleştirilebilecek bir otomatikleştirilmiş sistem;

d) görece düşük maliyetle çalışabilecek bir sistem.

3. VERİTABANLARININ ANLAŞILMASI

3.1 Emniyet veritabanlarının potansiyel faydalarının avantajını kullanabilmek için, işletmeleri hakkında temel bir anlayış gereklidir. Bir veritabanı nedir? Düzenli bir şekilde gruplanan herhangi bir bilgi kümesi, bir veritabanı olarak kabul edilebilir.

Kağıt üzerindeki kayıtlar, basit bir dosyalama sistemi (yani manüel bir "veritabanı") ile yürütülebilir, ama bu tür bir sistem sadece küçük işletmeler için yeterli olacaktır. Verinin saklanması, kaydedilmesi, geri çağrılması ve alınması zorlu işlerdir. Hangi kaynaktan gelirse gelsin emniyet verileri, bu bilgilerin çeşitli formatlarda alınmasını kolaylaştıran bir elektronik veritabanında saklanmalıdır.

3.2 Bilgilerin çeşitli şekillerde değiştirilmesi, analizi ve alınması kapasitesine veritabanı yönetimi adı verilir. Çoğu veritabanı yönetimi yazılımı paketleri, bir veritabanının tanımlanması için aşağıdaki örgütlenme unsurlarını içerir:

a) ***Kayıt.*** Bir birim halinde bir araya gelen bir bilgi unsurları grubu (bir olayla ilgili tüm veriler gibi);

b) ***Alan.*** Bir kayıttaki her bir bilgi unsuru (bir olayın tarihi ve yeri gibi) ve

c) ***Dosya.*** Aynı yapıya ve aralarında bir ilişkiye sahip kayıtlardan oluşan bir grup (örneğin belirli bir yıldaki motorla ilgili tüm olaylar).

3.3 Her bir veri alanı sabit bir uzunluğa sahip olduğunda ve format tipi bir sayı, "evet/hayır" yanıtı, karakter veya metin tarafından açıkça tanımlanmış olduğunda veritabanlarının "yapılandırılmış" olduğu kabul edilir. Çoğunlukla, kullanıcı için sabit sayıda değer seçeneği mevcuttur. Bu değerler, genellikle baz tablolar veya liste değeri tabloları (örneğin önceden belirlenmiş bir listeden uçak markaları ve modelleri arasından seçim) olarak adlandırılan referans dosyalarında kaydedilir. Nicel analizleri ve sistematik aramaları kolaylaştırmak için, yapılandırılmış veritabanlarında serbest biçimli metin girişi sabit bir baz uzunluğu ile sınırlandırılarak en aza indirilir. Genellikle, bu tür bilgiler bir anahtar kelime sistemi tarafından kategorize edilir.

3.4 Bilginin tutulma şekli genellikle yazılı belgeler olduğunda veritabanları "metin tabanlı" olarak kabul edilir. Veriler serbest biçimli metin alanlarında sıralanır ve saklanır. Bazı veritabanları büyük miktarda metin ve yapılandırılmış veri içerir; ancak modern veritabanları elektronik dosyalama dolaplarının çok daha ötesindedir.

4.VERİTABANI SINIRLAMALARI

Veritabanlarını geliştirir, sürdürür veya kullanırken dikkate alınması gereken sınırlamalar vardır. Bu sınırlamaların bazıları doğrudan veritabanı sistemi ile ilgiliyken, diğerleri verinin kullanımı ile ilgilidir. Desteklenmesi mümkün olmayan çıkarımlar ve kararlardan kaçınılması için, veritabanı kullanıcılarının bu sınırlamaları anlaması gerekir. Veritabanı kullanıcıları aynı zamanda veritabanının oluşturulma amacını ve oluşturan ve sürdüren örgüt tarafından girilen bilgilerin güvenilirliğini de bilmelidirler.

5.VERİTABANI BÜTÜNLÜĞÜ

5.1 Emniyet veritabanları organizasyonun emniyet yönetimi etkinliklerinin stratejik bir unsurudur. Veriler pek çok kaynak nedeniyle bozulabilir ve verilerin bütünlüğünün korunması için özen gösterilmelidir. Veri girişi için veritabanına pek çok çalışanın erişimi olabilir. Diğer çalışanlar, emniyet görevlerini yerine getirmek için verilere erişim sağlamalıdırlar. Ağa bağlı bir sistemin çok sayıda noktasından erişim veritabanının hasar görebilme olasılığını arttıracaktır.

5.2 Bir veritabanının kullanılabilirliği, verilerin bakımına yeterince özen gösterilmediğinde zarar görebilir. Eksik veriler, geçerli verilerin girilmesinde gecikmeler, yanlış veri girişi v.s. veritabanının bozulmasına neden olabilir. En iyi analitik araçların uygulanması bile, kötü verileri telafi edemez.

6.VERİTABANI YÖNETİMİ

Emniyet verilerinin korunması

Sadece havacılık emniyetinin geliştirilmesi için amacıyla derlenen emniyet verilerinin yanlış amaçla kullanılması potansiyeli düşünüldüğünde, veritabanı yönetimi verilerin korunması ile başlamalıdır. Veritabanı yöneticileri verilerin korunması gereksinimini, verilerin havacılık emniyetini geliştirebilecek kişilerin erişimine açılması ile dengelemelidir. Koruma sırasında aşağıdakiler dikkate alınmalıdır:

a) "bilgilere erişim" yasalarının emniyet yönetimi gereklilikleri karşısındaki yeterliliği;

b) emniyet verilerinin korunması hakkında örgüt politikaları;

c) bireylerin kimliklerinin üçüncü taraflar tarafından öğrenilmesine neden olabilecek tüm ayrıntıların çıkarılması ile kimliksizleştirme (örneğin uçuş numaraları, tarih/saat, yer ve uçak tipi bilgileri);

d) bilgi sistemlerinin, veri saklama ve iletişim ağlarının emniyeti;

e) Veritabanlarına erişiminin "bilmesi gerekenlerle" sınırlandırılması

ve

f) verilerin yetkisiz kişilerce kullanılmasını yasaklanması.

7.EMNİYET VERİTABANININ ÖZELLİKLERİ

Farklı veritabanı yönetimi sistemlerinin işlevsel özellikleri ve nitelikleri değişebilir ve operatörün gereksinimlerine en uygun sisteme karar vermeden önce her biri dikkate alınmalıdır. Deneyimler, emniyetle ilgili olayların en iyi şekilde PC tabanlı veritabanları kullanılarak kaydedildiğini ve izlendiğini göstermektedir. Mevcut özellik sayısı seçilen sistem tipine bağlıdır. Temel özellikler kullanıcının aşağıdaki gibi görevlerini gerçekleştirmesini sağlamalıdır:

a) emniyet olaylarının çeşitli kategoriler altında günlüğünün tutulması;

b) olayların ilgili dokümanlarla (örneğin raporlar ve fotoğraflar) bağlantılandırılması;

c) trendlerin izlenmesi;

d) analiz, çizelge ve raporların derlenmesi;

e) geçmiş kayıtların kontrol edilmesi;

f) verilerin diğer organizasyonlarla paylaşılması;

g) olay incelemelerinin izlenmesi ve

h) zamanı gelen eylem müdahalelerinin işaretlenmesi.

8. VERİTABANI SEÇİMİNDE DİKKATE ALINACAKLAR

8.1 Ticari olarak sunulan veritabanı sistemlerinin seçimi kullanıcının beklentilerine, istenen verilere, bilgisayarın işletim sistemine ve yapılacak sorgulamaların karmaşıklığına bağlıdır. Farklı kapasiteler ve beceriler gerektiren çeşitli programlar mevcuttur. Hangi tipin kullanılacağının seçimi aşağıdaki listede bulunan dikkate alınacak noktaların dengelenmesini gerektirir:

a) ***Kullanıcı dostu olma.*** Sistem kolay anlaşılabilir ve kolay kullanılabilir olmalıdır. Bazı programlar geniş bir özellik yelpazesi sunar, ama önemli miktarda eğitim gerektirir. Ne yazık ki, kullanıcı dostu olmakla arama gücü arasında sıklıkla takas yapılması gerekir; araç ne kadar kullanıcı dostu olursa, karmaşık sorgulamaları yapma olasılığı da o kadar az olacaktır.

b) ***Erişim.*** Veritabanında saklanan tüm ayrıntılara erişim ideal bir durum olsa da, tüm kullanıcıların bu tür erişime ihtiyacı yoktur. Veritabanının yapısı ve karmaşıklığı, herhangi bir belirli sorgulama aracının seçilmesini etkileyecektir.

c) ***Performans.*** Performans sistemin ne kadar etkin işlediğinin ölçüsüdür. Aşağıdakiler gibi noktalara dayanır:

1) verinin ne kadar iyi toplandığı, sürdürüldüğü ve izlendiği;

2) verilerin trend analizini veya diğer analizleri kolaylaştıran formatlarda saklanıp saklanmadığı;

3) veritabanı yapısının karmaşıklığı ve

4) ana bilgisayar sisteminin (veya ağın) tasarımı.

d) ***Esneklik.*** Esneklik sistemin aşağıdaki becerilerine bağlıdır:

1) çeşitli sorgulamaları işleme;

2) verileri filtreleme ve düzenleme;

3) ikili mantık kullanma (yani sistem "kaptan olan ve 15.000 saat deneyime sahip tüm pilotlar" veya "kaptan olan veya 15.000 saat deneyime sahip tüm pilotlar" gibi "VE/VEYA" koşullarını işleyebilmelidir);

4) temel analiz (sayımlar ve çapraz listelemeler) yapabilme;

5) kullanıcı tanım çıktılar üretebilme ve

6) veri almak veya vermek için diğer veritabanlarına bağlanabilme.

8.2 Maliyetler organizasyonun gerekliliklerine göre değişebilir. Bazı sistem tedarikçileri tarafından yapılan ücretlendirme, tek bir lisans üzerinde çok sayıda kullanıcıya izin veren düz bir ücretlendirmedir. Alternatif olarak, diğer sistem tedarikçilerinde, ücret izin verilen kullanıcı sayısına bağlı olarak artar. Satın alma sırasında aşağıdakiler gibi ilgili maliyet faktörleri de dikkate alınmalıdır:

a) kurulum maliyetleri;

b) eğitim maliyetleri;

c) yazılım yükseltme maliyetleri;

d) bakım ve destek ücretleri ve

e) gerekebilecek diğer yazılım lisansı ücretleri.

Bölüm 5

EMNİYET RİSKLERİ

5.1 HEDEF VE İÇERİKLER

Bu bölümde emniyet riski yönetiminin temelleri açıklanmaktadır. Bu bölüm aşağıdaki konuları içerir:

a) Emniyet riskinin tanımı;

b) İlk temel bilgi - Emniyet riski yönetimi;

c) İkinci temel bilgi - Emniyet riskinin olasılığı;

d) Üçüncü temel bilgi - Emniyet riskinin ciddiyeti;

e) Dördüncü temel bilgi - Emniyet riskinin tahammül edilebilme oranı;

f) Beşinci temel bilgi - Emniyet riskinin kontrolü/azaltılması ve

g) Emniyet riski yönetiminin beş temel bileşeni – Özet.

5.2 EMNİYET RİSKİNİN TANIMI

5.2.1 Bu el kitabının 2. Bölümünde, emniyet bir dizi örgütlenme sürecinin sonucu olarak tanımlanmaktadır. Bu örgütlenme süreçlerinin yönetimi, emniyet risklerinin organizasyonun kontrolü altında tutulmasını hedeflemektedir. Bu perspektifteki anahtar nokta, emniyetin bir sonuç ve emniyet riski yönetiminin bir süreç olmasıdır.

5.2.2 Bu el kitabının 4. Bölümünde, tehlikenin tanımlanması emniyet yönetimini destekleyen iki temel etkinlikten biri olarak ele alınmaktadır. Tehlikenin tanımlanmasının aynı zamanda, emniyet yönetimi ile dolaylı şekilde ilgili diğer örgütlenme süreçlerinin sağlamlığına katkıda bulunur. Tehlikelerin doğru şekilde tanımlanması ve analiz edilmesi için, 4. Bölümde potansiyel yaralanma veya hasar kaynağı olarak tehlikeler ve emniyetle ilgili olarak operasyonel terimler ile ifade edilen sonuçları arasında açık bir ayrım yapılmıştır.

5.2.3 Emniyet riski yönetimi, emniyet yönetimini destekleyen diğer temel etkinliktir ve dolaylı şekilde ilgili olan diğer örgütlenme süreçlerine katkıda bulunur. Daha genel olan risk yönetimi terimine karşılık, emniyet riski yönetimi terimi, emniyetin yönetilmesinin – doğrudan – mali risk, hukuki risk, ekonomik risk vs. risklerin yönetilmesini hedeflemediğini, temel olarak emniyet risklerinin yönetimi ile sınırlandığını göstermek için kullanılmaktadır.

5.2.4 Emniyet yönetimi etkinliklerinin çoğu zaman tehlike tanımlanması veya analizinin ötesine geçmemesi veya başka durumlarda, tehlikelerin sonuçlarından kaynaklanan emniyet risklerinin değerlendirilmesi ve önceliklerinin belirlenmesini atlayarak, tehlikenin tanımlanmasından doğrudan risk azaltmanın gerçekleştirilmesine atlanması sık karşılaşılan bir hatadır. Her şeye rağmen, tehlike veya hasar kaynakları tanımlandığında ve sonuçları analiz edilip üzerlerinde uzlaşıldığında, sonuçlardan korunmak için risk azaltma stratejileri uygulanmaya başlayabilir.

Bu görüş, "ilk öncelik olarak emniyet" kavrayışına bağlı kalınsa ve kötü sonuçların önlenmesine odaklanılsa doğru olabilirdi. Ancak, emniyet yönetimi kavrayışına göre, belirlenen tehlikelerin sonuçları üzerinde uzlaşılması ve bunların operasyonel terimler ile açıklanması risk azaltmanın uygulanması için yeterli değildir. Risk azaltma stratejileri önerirken, kaynakların dağıtılması için öncelikleri tanımlamak üzere, sonuçların ciddiyetinin değerlendirilmesi gerekir.

5.2.5 Ölçülemeyenin yönetilemeyeceğlnin temel yönetim kurallarından biri olduğu daha önce ifade edilmişti. Bu nedenle, tehlikelerin sonuçlarının ciddiyetinin bir şekilde ölçülmesi önemlidir. Emniyet riski yönetiminin emniyet yönetimi sürecine en önemli katkısı budur. Tehlikelerin sonuçlarına "bir sayı vererek", emniyet yönetimi süreci organizasyona emniyet riski kararları ve buna bağlı olarak tehlikelerin hasar verme potansiyellerinin sınırlanması için örgüt kaynaklarının dağıtılması için ilkelere dayalı bir temel sağlar. Bu şekilde, emniyet riski yönetimi tehlikeler-sonuçlar-emniyet risklerinden oluşan temel emniyet yönetimi üçlemesini tamamlamakta ve Bölüm 3'te ele alınan "iki P ikileminin" çözümünü doğrudan desteklemektedir.

5.2.6 En genel ve geniş anlamıyla risk pek çok tartışmaya konu olmuştur ve bu konu üzerinde pek çok yayın bulunmaktadır. Kısmen terimin, çok sık, son derece geniş ve genel olarak boş şekilde kullanılan, genel kullanımına bağlı olarak bir karışıklık olasılığı bulunmaktadır. Karışıklığı ele alınmasının ilk adımı, genel terimin kullanımını son derece belirli bir terim olan emniyet riski ile sınırlamaktır. Bunun ötesinde, en baştan açık bir emniyet riski tanımı oluşturmak ve bu tanımı operasyonel terimler ile ifade edilen tehlike ve sonuç kavramları ile bağlantılandırmak önemlidir.

5.2.7 Genel terimin kullanılmasını son derece belirli bir terim olan emniyet riski ile sınırlandırdıktan sonra bile, hala karışıklıklar olabilir. Bunun nedeni, risk kavramının yapay bir kavram olmasıdır. Emniyet riskleri herhangi bir fiziksel veya doğal ortamın elle tutulur veya görülür bileşenleri değildir; anlamak veya bir imgelerini oluşturmak için emniyet riskleri hakkında düşünülmesi gerekir. Diğer yandan, tehlikeler ve sonuçları fiziksel veya doğal bir ortamın elle tutulur veya görülür bileşenleridir, dolayısıyla, anlaşılmaları ve görselleştirilmeleri daha kolaydır. Emniyet riski kavramı bir kurgudur, yani insanlar tarafından oluşturulmuş yapay bir uzlaşıdır. Basit bir ifadeyle, tehlikeler ve sonuçlar doğal dünyanın fiziksel bileşenleri iken, emniyet riskleri doğal dünyada bulunmaz. Emniyet riski, tehlikelerin sonuçlarının ciddiyetini ölçmek veya "bir sayı vermek" için insan zihninin bir ürünüdür.

5.2.8 Emniyet riski, öngörülebilir en kötü durumu referans alarak, bir tehlikenin sonuçlarının tahmin edilen olasılık ve ciddiyeti bakımından ifade edilen değerlendirilmesi olarak tanımlanır. Tipik olarak, emniyet riskleri, ölçümlerine izin veren bir alfanümerik bir uzlaşma ile belirlenir. Bölüm 4'te ele alınan yan rüzgar örneğini kullanarak, önerilen emniyet riski tanımının emniyet risklerinin tehlikeler ve sonuçları ile bağlantılandırılmasını, böylece tehlike-sonuç-emniyet riski üçlemesindeki döngüyü tamamlanmasını sağladığı görülebilir:

a) pist üzerinde doğrudan yandan esen 15 deniz mili hızındaki bir rüzgar bir tehlikedir;

b) pilotun kalkış veya iniş sırasında uçağı kontrol edememesi nedeniyle pistten yana doğru çıkış potansiyeli, tehlikenin sonuçlarından biridir ve

c) pistten yana doğru çıkışın sonuçlarının, alfanümerik bir uzlaşmaya dayalı olarak ciddiyet ve olasılık terimleri ile ifade edilen değerlendirilmesi, emniyet riskidir.

5.3 İLK TEMEL BİLGİ – EMNİYET RİSKİ YÖNETİMİ

5.3.1 Emniyet riski yönetimi, bir organizasyonun kapasitelerini tehdit eden tehlikelerin sonuçlarına ait emniyet risklerinin değerlendirilmesini ve azaltılmasını, makul oranda düşük (ALARP) seviyeye kadar kapsayan genel bir terimdir. Emniyet riski yönetiminin amacı, değerlendirilen tüm emniyet riskleri ve kontrolü ve azaltılması mümkün olan emniyet riskleri arasında kaynakların dengeli bir şekilde dağıtılması için bir temel oluşturmaktır.

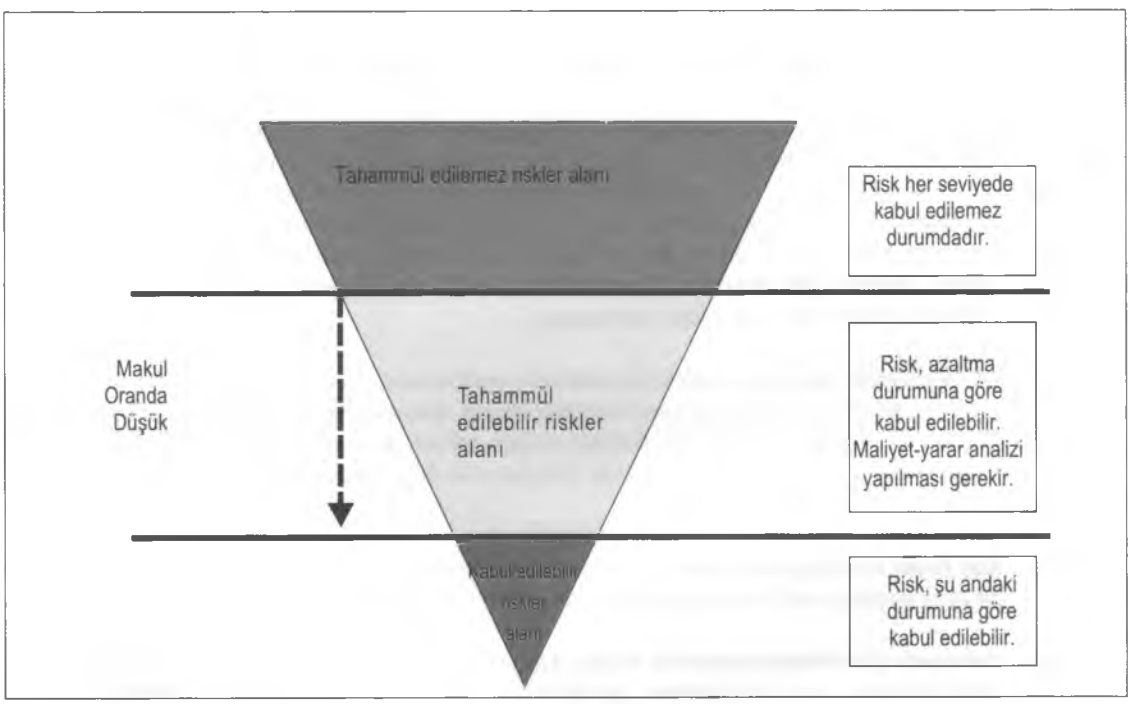
Başka bir deyişle, emniyet riski yönetimi "iki P ikileminin" çözülmesine yardımcı olur. Dolayısıyla, emniyet riski yönetimi emniyet yönetimi sürecinin önemli bir bileşenidir. Ancak, katma değeri kaynak dağıtımına veriler üzerinden bir yaklaşım olması, bu nedenle savunulabilir ve daha kolay açıklanabilir olmasından kaynaklanır.

5.3.2 Şekil 5-1'de emniyet riski yönetimi sürecinin yaygın bir şekilde benimsenmiş, genel bir görsel sunumu verilmektedir. Üçgen ters konumdadır, böylece havacılığın (diğer tüm sosyo-teknik üretim sistemleri gibi) emniyet riski perspektifiyle bakıldığında "üst kısmı ağır" bir sistem olduğunu göstermektedir: tehlikelerin sonuçlarına ait çoğu emniyet riski başlangıçta tahammül edilemez riskler alanına ait olarak değerlendirilecektir. Tehlikelerin sonuçlarına ait daha az sayıda emniyet riski, değerlendirme doğrudan tahammül edilebilir riskler alanında olacak şekilde değerlendirilecek ve çok daha azı ise değerlendirme doğrudan kabul edilebilir riskler alanında olacak şekilde değerlendirilecektir.

5.3.3 Başlangıçta tahammül edilemez riskler alanına ait olarak değerlendirilen emniyet riskleri, hiçbir koşulda kabul edilemez . Tehlikelerin sonuçlarının olasılığı ve/veya ciddiyeti o kadar yüksektir ve tehlikenin hasar verme potansiyeli organizasyonun yaşaması için o kadar önemli bir tehlike arz ediyordur ki, derhal risk azaltma eylemi yapılması gerekir. Genel olarak, organizasyonun önünde emniyet risklerini tahammül edilebilir veya kabul edilebilir alanlara getirmek için iki alternatif vardır:

a) tehlikenin sonuçlarının hasar verme potansiyeline daha az maruz kalınması ve/veya bu potansiyelin büyüklüğünün azaltılması için kaynakların dağıtılması veya

b) riskin azaltılması mümkün değilse, işletmesinin iptal edilmesi.



Şekil 5-1. Emniyet riski yönetimi

5.3.4 Başlangıçta tahammül edilebilir alanda olarak değerlendirilen emniyet riskleri, tehlikelerin olasılığı ve/veya ciddiyetinin, ön görülebilir oranda, örgüt kontrolü altında tutulmasını sağlayan risk azaltma stratejilerinin bulunması koşuluyla kabul edilebilir olarak değerlendirilir. Aynı kontrol ölçütü, tahammül edilemez alanda yer alan yer alan ve tahammül edilebilir alana girecek şekilde azaltılan emniyet riskleri için de geçerlidir. Başlangıçta tahammül edilemez alanda olarak değerlendirilen ve ardından azaltılarak tahammül edilebilir alana indirilen bir emniyet riski, kontrol edilmesini garanti eden azaltma stratejileri ile "korunmalıdır." Her iki durumda, bir maliyet-yarar analizi yapılması gerekir:

a) Tehlikelerin sonuçlarının olasılığı ve/veya ciddiyetini örgüt kontrolü altına almak için kaynakların dağıtılmasının sonucunda bir yatırım geri dönüşü var mıdır? veya

b) Kaynakların dağıtılmasının, tehlikelerin sonuçlarının olasılığının ve/veya ciddiyetinin örgüt kontrolü altına alınmasından çok organizasyonun yaşama gücü için bir tehlike oluşturacak büyüklükte olması mı gerekmektedir?

5.3.5 ALARP kısaltması makul derecede az bir seviyeye indirilen bir emniyet riskini açıklamak için kullanılmaktadır. Emniyet riski yönetimi yönetiminde neyin "makul oranda" olduğunu belirlemek için, hem emniyet riskini hem de maliyeti daha da azaltmanın teknik fizibilitesine dikkat edilmelidir. Bunun için bir maliyet-yarar analizi yapılmalıdır. Bir sistemdeki emniyet riskinin ALARP olduğunun gösterilmesi, riskin daha fazla azaltılmasının pratik olmadığını ve maliyet nedeniyle büyük oranda devre dışı bırakıldığını gösterir. Ancak, bir örgüt bir emniyet riskini "kabul ettiğinde", bunun emniyet riskinin ortadan kaldırıldığı anlamına gelmediği unutulmamalıdır. Emniyet riskinin bir kısmı kalacaktır; ancak örgüt kalan emniyet riskinin yararlar tarafından fazlasıyla karşılanacak derecede düşük olduğunu kabul etmiştir.

5.3.4 Başlangıçta kabul edilebilir alanda olarak değerlendirilen emniyet riskleri, tehlikelerin olasılığı ve/veya ciddiyetinin örgüt kontrolü altında tutulmasını sağlayan risk azaltma stratejileri geliştirmek ve sürdürmek için bir eylem gerektirmedikleri oranda kabul edilebilir durumdadır.

5.3.7 Maliyet-yarar analizleri emniyet riski yönetiminin merkezinde yer alır. Maliyet-yarar analizinde dikkate alınması gereken iki ayrı maliyet vardır: doğrudan maliyetler ve dolaylı maliyetler.

5.3.8 ***Doğrudan maliyetler*** açık maliyetlerdir ve belirlenmeleri kolaydır. Çoğunlukla fiziksel hasarla ilgilidirler ve yaralanmalar, uçak/donanım ve mülk hasarları için düzeltme, değiştirme ve karşılama masraflarını içerirler. Örneğin kazalarda olduğu gibi, tehlikelerin belirli aşırı sonuçlarında organizasyonun kontrolünün kaybının altında yatan yüksek maliyetler, sigorta kapsamına alınarak azaltılabilir. Ancak, bir sigorta yaptırmanın, tehlikelerin sonuçlarının olasılığını ve/veya ciddiyetini örgüt kontrolü altına almak için bir katkıda bulunmadığı unutulmamalıdır; bu sadece maddi riski organizasyondan sigorta şirketine aktarmaktadır. Emniyet riski henüz ele alınmamıştır. Parasal riski aktarmak için sigorta almak, bir emniyet yönetimi stratejisi olarak görülemez.

5.3.9 ***Dolaylı maliyetler*** doğrudan sigorta kapsamında bulunmayan tüm maliyetleri içerir. Dolaylı maliyetler, tehlikelerin belirli aşırı sonuçlarının organizasyonun kontrolü dışına çıkmasından kaynaklanan dolaylı maliyetlerden daha fazla tutabilirler. Bu tür maliyetler bazen açık değildir ve çoğu zaman gecikmeli olarak ortaya çıkarlar. Tehlikelerin belirli aşırı sonuçlarının organizasyonun kontrolü dışına çıkmasından kaynaklanabilen, sigorta kapsamında olmayan maliyetlerin bazı örnekleri aşağıda verilmiştir:

a) ***İşin kaybı ve organizasyonun itibarının zarar görmesi.*** Pek çok örgüt, personelinin sorgulanabilir bir uçuş geçmişi olan bir havayolu uçmasına izin vermez.

b) ***Donanım kullanılamamasından doğan kayıplar.*** Bu, kar kaybına eşittir. Değiştirilen donanımın satın alınması veya kiralanması gerekebilir. Tek bir tip uçak çalıştıran şirketler yedek parça envanterlerinin ve özellikle bu uçak için eğitilmiş personelinin fazla olduğunu görebilirler.

c) ***Personel üretkenliği kaybı.*** Bir olayda yaralananlar olursa ve çalışamaz duruma gelirlerse, iş mevzuatı bir tür tazminat almaya devam etmelerini gerektirebilir.

Ayrıca, bu personelin yerine en azından kısa vadede yenileri alınmalıdır, bu organizasyonun ücret, eğitim, fazla mesai maliyetlerini ödemesini gerektirir ve deneyimli işçilerin iş yükünün artmasına neden olabilir.

d) ***İnceleme ve temizlik.*** Bunlar genellikle sigorta kapsamında yer almayan maliyetlerdir. Operatörler, personellerinin incelemeye katılması ve testlerin ve analizlerin maliyeti, enkazın toplanması ve olay yerinin düzeltilmesi dahil olmak üzere inceleme maliyetleri ile karşı karşıya kalabilirler.

e) ***Sigortadan düşülebilir maliyetler.*** Sigortalının herhangi bir olayın maliyetinin ilk kısmını karşılama yükümlülüğü yerine getirilmelidir. Bir talep, şirketi sigorta için daha yüksek risk kategorisine taşıyabilir, dolayısıyla primlerin artmasına neden olabilir. (Diğer yandan, emniyetle ilgili risk azaltma müdahalelerinin uygulanması bir şirketin daha düşük bir prim için pazarlık etmesini sağlayabilir).

f) ***Yasal işlemler ve hasar talepleri.*** Yasal maliyetler hızla artabilir. Mali sorumluluklar ve hasarlar için sigorta yaptırılması mümkün olsa da, yasal işlem ve hasar taleplerinin yerine getirilmesi sırasında kaybedilen zamanın maliyetinin karşılanması mümkün değildir.

g) ***Cezalar ve tebligatlar.*** Devlet kurumları ceza kesebilir veya tebligatta bulunabilir ve güvensiz işletmeleri kapatabilirler.

5.3.10 Maliyet-yarar analizleri sayısal açıdan doğru ve analitik bakımından kesin sonuçlar üretebilirler. Yine de, bir maliyet-yarar analizinde yer tutan daha az kesinlikte sayısal etkenler vardır. Bu etkenler aşağıdakilerden oluşur:

a) ***Yönetimsel.*** Emniyet riski organizasyonun emniyet politikasına ve hedeflerine uygun mu?

b) ***Hukuki.*** Emniyet riski geçerli mevzuata ve uygulama kapasitelerine uygun mu?

c) ***Kültürel.*** Organizasyonun personeli ve diğer hissedarlar emniyet riskini nasıl görmektedirler?

d) ***Pazar.*** Organizasyonun rekabet gücü ve diğer organizasyonlar karşısında sağlam durumda olması emniyet riski nedeniyle tehlikeye girer mi?

e) ***Politik.*** Emniyet riskinin ele alınmamasının getireceği politik bir maliyet var mı?

f) ***Halkla ilişkiler.*** Medya veya kamunun fikri üzerinde etkide bulunan özel çıkar grupları emniyet riski ile ne kadar etkili olabilirler?

5.4 İKİNCİ TEMEL BİLGİ - EMNİYET RİSKİNİN OLASILIĞI

5.4.1 Tehlikelerin sonuçlarından kaynaklanan emniyet risklerinin örgüt kontrolü altına alınması süreci, hizmetlerin sunulmasına yönelik işletmeler sırasında tehlikelerin sonuçlarının ortaya çıkmasının olasılığının değerlendirilmesi ile başlar. Bu emniyet riskinin olasılığının değerlendirilmesi olarak adlandırılır.

5.4.2 Emniyet riskinin olasılığı, güvensiz bir olay veya koşulun ortaya çıkması ihtimalidir. Bir olasılığın gerçekleşme ihtimalinin tanımı aşağıdaki sonuçlarla daha kolay gösterilebilir:

a) Söz konusu olayla benzer olaylar geçmişte de ortaya çıkmış mı veya bu olay tamamen ayrı mı?

b) Benzer tipte başka hangi donanım veya bileşenler benzer arızalara sahip olabilir?

c) Söz konusu prosedür kaç personel tarafından yerine getiriliyor veya kaç personele bu prosedür uygulanıyor?

d) Kuşkulanılan donanım veya sorgulanan prosedürün kullanılma süresi yüzde kaç?

e) Kamu emniyetine daha fazla tehdit oluşturabilecek, örgütlenme, yönetim ve mevzuat ile ilgili çıkarımlar ne dereceye etkili?

5.4.3 Örnek olarak verilen bu soruların altında yatan etkenlerin herhangi biri veya tümü geçerli olabilir, bu durum da çok nedenliliğin dikkate alınmasının önemini vurgulamaktadır. Güvensiz bir eylem veya koşulun ortaya çıkma olasılığının değerlendirilmesinde, potansiyel olarak geçerli tüm perspektifler değerlendirilmelidir.

5.4.4 Güvensiz bir eylem veya koşulun ortaya çıkma olasılığının değerlendirilmesinde, bilgiye dayalı kararlar vermek için organizasyonun "emniyet kütüphanesinde" bulunan geçmişe ait verilere başvurulması çok önemlidir. Bunun anlamı, bir "emniyet kütüphanesine" sahip olmayan bir organizasyonun, olasılık değerlendirmelerini sadece en iyi durumda endüstri trendlerine ve en kötü durumda bir kanıya göre yapabileceğidir.

5.4.5 5.4.2'de listelenen sorular gibi sorulara verilen yanıtlardan doğan konular temelinde, güvensiz bir eylem veya koşulun ortaya çıkma olasılığı ortaya konabilir ve bu olasılığın önemi emniyet riski olasılığı tablosuna göre değerlendirilebilir.

5.4.6 Şekil 5-2'de tipik bir emniyet riski olasılığı tablosu gösterilmektedir, bu örnekte beş noktalı bir tablo bulunmaktadır. Tablo, güvensiz bir eylem veya koşulun ortaya çıkma olasılığını gösteren beş kategoriyi, her bir kategorinin anlamını ve her bir kategoriye bir değer atanmasını içermektedir. Bunun sadece eğitim amacıyla sunulan bir örnek olduğu vurgulanmalıdır. Bu tablo ve aşağıdaki paragraflarda ele alınan ciddiyet tablosu ve risk değerlendirme ve tahammül edilebilirlik matrisleri, kavramsal olarak düşünüldüğünde endüstri standartları olsa da, tabloların ve matrislerin ayrıntı ve karmaşıklık düzeyi farklı organizasyonların belirli gereksinimlerine ve karmaşıklıklarına uyarlanmalı ve uygun hale getirilmelidir. Hem nicel hem de nitel tanımlar içeren organizasyonlar bulunmaktadır. Benzer şekilde, bazı tablolar on beş noktaya kadar ulaşır. Beş noktalı tablolar ve beşe beş matrisler asla bir standart değildir. Sadece eğitim amacına ve bu el kitabının gereksinimlerine uygun bir karmaşıklığa sahip olarak düşünülmelidirler.

5.5 ÜÇÜNCÜ TEMEL BİLGİ - EMNİYET RİSKİNİN CİDDİYETİ

5.5.1 Güvensiz bir eylem veya koşulun emniyet riski olasılık bakımından değerlendirildiğinde, tehlikelerin sonuçlarından kaynaklanan emniyet risklerinin örgüt kontrolü altına alınması sürecindeki ikinci adım, hasar verme potansiyeli hizmetlerin verilmesine yönelik işletmeler sırasında ortaya çıkıyorsa, bir tehlikenin sonuçlarının ciddiyetinin değerlendirilmesidir. Bu emniyet riskinin ciddiyetinin değerlendirilmesi olarak adlandırılır.

	Anlam	Değer
Sık	Pek çok kez ortaya çıkabilir (sıklıkla ortaya çıkmıştır)	5
Arada bir	Arada bir ortaya çıkabilir (sık olmayan şekilde ortaya çıkmıştır)	4
Uzak olasılık	Ortaya çıkması olası değildir, ama mümkündür (nadiren ortaya çıkmıştır)	3
Olası değil	Ortaya çıkma olasılığı çok düşüktür (daha önce ortaya çıktığı bilinmemektedir)	2
Son derece düşük olasılık	Olayı ortaya çıkma olasılığı kavranamayacak derecede düşüktür	1

Şekil 5-2. Emniyet riski olasılık tablosu

5.5.2 Emniyet riskinin ciddiyeti, öngörülebilir en kötü durum referans olarak alındığında, güvensiz bir olay veya koşulun olası sonuçları olarak tanımlanır. hasar verme potansiyeli hizmetlerin verilmesine yönelik işletmeler sırasında ortaya çıkıyorsa, bir tehlikenin sonuçlarının ciddiyetinin değerlendirilmesine aşağıdakiler gibi sorular yardımcı olabilir:

a) Kaç can kaybı olabilir (personel, yolcular, olay yerinde bulunanlar ve genel kamu)?

b) Maddi veya mali hasarın olası kapsamı nedir (operatörün doğrudan mülk kaybı, havacılık altyapısında hasar, üçüncü tarafların görebileceği ikincil zararlar, Devlet üzerinde mali ve ekonomik etki)?

c) Çevre üzerindeki etkilerin olasılığı nedir (yakıt veya diğer tehlikeli ürünlerin saçılması ve doğal ortamın fiziksel olarak hasar görmesi)?

d) Olası politik sonuçlar ve/veya medyanın ilgi gösterme olasılığı nedir?

5.5.3 5.5.2'de listelenen sorular gibi sorulara verilen yanıtlardan doğan konular temelinde, güvensiz bir eylem veya koşulun olası sonuçlarının ciddiyeti ortaya konabilir ve öngörülebilir en kötü durumu referans alarak, bu ciddiyetin önemi emniyet riski ciddiyeti tablosuna göre değerlendirilebilir.

5.5.4 Şekil 5-3'de tipik bir emniyet riski ciddiyeti tablosu gösterilmektedir, bu örnekte yine beş noktalı bir tablo bulunmaktadır. Tablo, güvensiz bir eylem veya koşulun ortaya çıkmasının ciddiyet seviyesini gösteren beş kategoriyi, her bir kategorinin anlamını ve her bir kategoriye bir değer atanmasını içermektedir. Emniyet riski olasılığı tablosunda olduğu gibi, bu tablo da sadece eğitim amaçlarıyla verilen bir örnektir ve 5.4.6'de dile getirilen uyarılar geçerlidir.

Riskin ortaya çıkmasının ciddiyeti	Anlam	Değer
Yıkıcı düzeyde	— Donanım kullanılamaz hale gelir — Çok sayıda ölüm	**A**
Tehlikeli	— Operatörlerin görevlerini doğru şekilde veya tamamen yerine getirmelerinden emin olunamayacak şekilde emniyet marjlarında büyük bir azalma, fiziksel sıkıntı veya iş yükü — Ciddi yaralanma — Önemli donanım hasarı	**B**
Önemli	— Emniyet marjlarında önemli bir azalma, iş yükünde artış veya etkinliklerini etkileyen koşulların sonucunda operatörlerin olumsuz çalışma koşulları ile başa çıkabilme becerisinde azalma — Ciddi olaylar — Kişisel yaralanmalar	**C**
Önemsiz	— Rahatsızlık — Çalışmanın sınırlanması — Acil durum prosedürlerinin kullanılması — Önemsiz olaylar	**D**
İhmal edilebilir	— Küçük sonuçlar	**E**

Şekil 5-3. Emniyet riski ciddiyet tablosu

5.6 DÖRDÜNCÜ TEMEL BİLGİ - EMNİYET RİSKİNİN TAHAMMÜL EDİLEBİLME ORANI

5.6.1 Güvensiz bir eylem veya koşulun sonuçlarının emniyet riski olasılık ve ciddiyet bakımından değerlendirildiğinde, güvensiz bir eylem veya koşulun sonuçlarından kaynaklanan emniyet risklerinin örgüt kontrolü altına alınması sürecindeki üçüncü adım, hasar verme potansiyeli hizmetlerin verilmesine yönelik işletmeler sırasında ortaya çıkıyorsa, tehlikenin sonuçlarının tahammül edilebilme oranının değerlendirilmesidir. Bu emniyet riskinin tahammül edilebilirliğinin değerlendirilmesi olarak adlandırılır. İki adımdan oluşan bir süreçtir.

5.6.2 Öncelikle, emniyet riskinin genel bir değerlendirmesinin elde edilmesi gerekir. Bu, emniyet riski olasılık ve emniyet riski ciddiyet tablolarının bir emniyet riski değerlendirme matrisinde bir araya getirilmesiyle gerçekleştirilir, bu matrisin bir örneği Şekil 5-4'te verilmiştir. Örneğin, bir emniyet riski olasılığı arada bir (4) olarak değerlendirilmiştir. Emniyet riski ciddiyeti tehlikeli (B) olarak değerlendirilmiştir. Olasılık ve ciddiyetin birleşimi (4B), söz konusu tehlikenin sonuçlarının emniyet riskidir. 5.2'deki tartışma genişletildiğinde, bu örnek üzerinden, emniyet riskinin sadece bir sayı veya alfanümerik bir kombinasyon olduğu ve doğal dünyanın görülür veya elle tutulur bir bileşeni olmadığı görülebilir. Şekil 5-4'teki matrisin renk kodlaması, Şekil 5-1'ye yer alan ters üçgendeki tahammül edilebilirlik alanlarını göstermektedir.

5.6.3 İkinci olarak, emniyet riski değerlendirme matrisinden elde edilen emniyet riski indeksi, tahammül edilebilirlik ölçütlerini açıklayan bir emniyet riski tahammül edilebilirlik matrisine aktarılmalıdır. 4B olarak değerlendirilen bir emniyet riskinin ölçütü, Şekil 5-5'teki tahammül edilebilirlik tablosuna göre, "mevcut koşullarda kabul edilemezdir". Bu durumda, emniyet riski ters üçgenin tahammül edilemez risk alanında yer alır. Tehlikenin sonuçlarının emniyet riski kabul edilemezdir. Örgüt aşağıdakileri yapmalıdır:

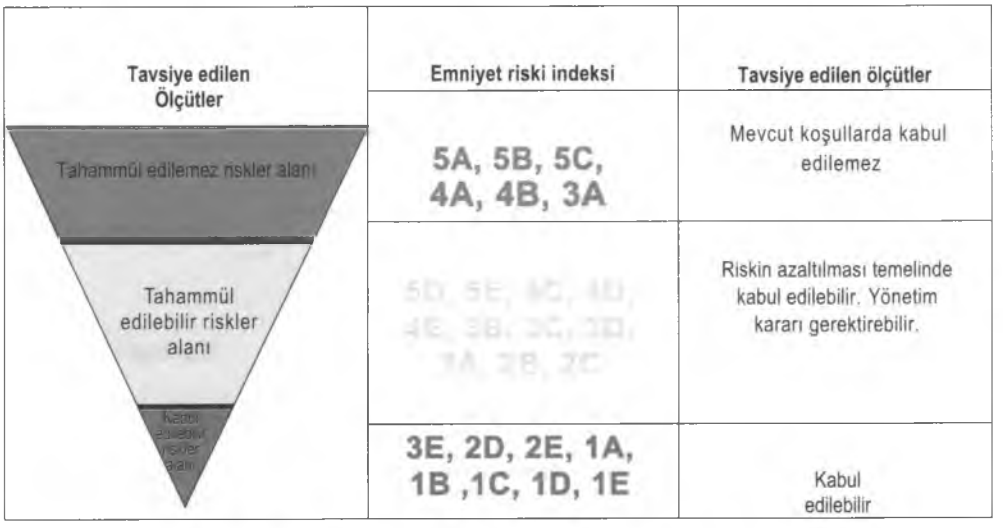
a) tehlikelerin sonuçlarına maruz kalma oranını azaltmak için kaynak ayırmak;

b) tehlikenin sonuçlarının büyüklüğünün veya hasar verme potansiyelinin azaltılması için kaynakların dağıtılması veya

c) riskin azaltılması mümkün değilse, işletmesinin iptal edilmesi.

Risk olasılığı	Risk ciddiyeti				
	Yıkıcı düzeyde A	Tehlikeli B	Önemli C	Önemsiz D	İhmal edilebilir E
Sık 5	5A	5B	5C		
Arada bir 4	4A	4B			
Uzak olasılık 3	3A				3E
Olası değil 2				2D	2E
Son derece düşük olasılık 1	1A	1B	1C	1D	1E

Şekil 5-4. Emniyet riski değerlendirme matrisi



Şekil 5-5. Emniyet riski tahammül edilebilirlik matrisi

5.7 BEŞİNCİ TEMEL BİLGİ - EMNİYET RİSKİNİN KONTROLÜ/AZALTILMASI

5.7.1 Güvensiz bir eylem veya koşulun sonuçlarından kaynaklanan emniyet risklerinin örgüt kontrolü altına alınması sürecindeki dördüncü ve sonuncu adımda, kontrol/azaltma stratejileri uygulanmalıdır. Genel olarak, kontrol ve risk azaltma birbirinin yerine kullanılabilen terimlerdir. Her ikisi de tehlikenin ele alınması için gerekli önlemlerin belirlenmesi ve tehlikenin sonuçlarına ait emniyet riskinin olasılığı ve ciddiyetinin organizasyonun kontrolünün altına alınmasını amaçlamaktadır.

5.7.2 5.6'da sunulan örnekle devam edildiğinde, analiz edilen tehlikenin sonuçlarının emniyet riski 4B ("mevcut koşullarda kabul edilemez") olarak değerlendirilmiştir. Bundan sonra kaynaklar, üçgenin aşağısına doğru, emniyet risklerinin ALARP olduğu alana doğru kayacak şekilde dağıtılmalıdır. Bunun elde edilmesi mümkün olmazsa, organizasyonu söz konusu tehlike sonuçlarına maruz bırakan hizmetlerin sunulmasına yönelik operasyon iptal edilmelidir. Şekil 5-6'da emniyet riski yönetimi süreci grafik olarak sunulmaktadır.

5.7.3 Emniyet riskinin kontrolü/azaltılması için üç genel strateji vardır:

a) ***Kaçınma.*** Emniyet riskleri işletmenin veya etkinliğinin sürdürülmesinin yararlarını aştığından operasyon veya etkinlik iptal edilir. Kaçınma stratejilerinin örnekleri şunlardır:

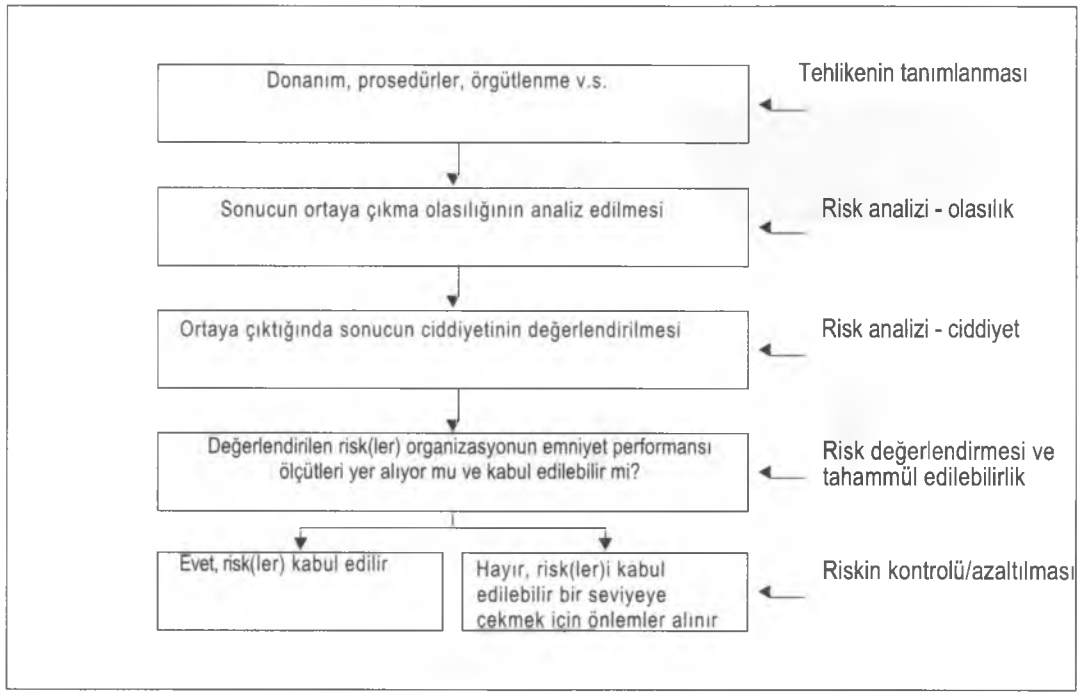
1) karmaşık bir coğrafyada yer alan ve gereken desteklerin bulunmadığı bir havaalanına yönelik işletmeler iptal edilir;

2) RVSM donanımı bulunmayan bir uçakla bir RVSM hava alanındaki işletmeler iptal edilir.

b) ***Azaltma.*** İşletme veya etkinliğin sıklığı azaltılır veya kabul edilen risklerin sonuçlarının büyüklüğünün azaltılması için önlem alınır. Azaltma stratejilerinin örnekleri şunlardır:

1) karmaşık bir coğrafyada yer alan ve gereken desteklerin bulunmadığı bir havaalanına yönelik işletmeler gündüz saatleri ve uygun görsel koşullarla sınırlanır;

2) RVSM donanımı bulunmayan bir uçakla işletmeler RVSM hava alanının üstü veya altında yapılır.



Şekil 5-6. Emniyet riski yönetimi süreci

c) ***Risk alanından ayırma.*** Tehlikelerin sonuçlarının etkilerini izole etmek veya tehlikelerden korunmak için yedekleme oluşturmak için önlem alınır. Risk alanından ayırmaya dayanan stratejilerin örnekleri aşağıda verilmiştir.

1) karmaşık bir coğrafyada yer alan ve gereken desteklerin bulunmadığı bir havaalanına yönelik işletmeler belirli performansta navigasyon özelliklerine sahip uçaklarla sınırlanır;

2) RVSM donanımlı olmayan uçakların RVSM hava alanında çalışmasına izin verilmez.

5.7.4 Emniyet riskinin azaltılmasına yönelik belirli alternatiflerin değerlendirilmesinde, her bir alternatifin emniyet risklerinin azaltılmasında aynı potansiyele sahip olmadığı unutulmamalıdır. Bir karar vermeden önce her bir alternatifin etkili olma oranı değerlendirilmelidir. Olası kontrol önlemlerinin tümünün dikkate alınması ve optimum bir çözüm elde etmek için önlemlerin getirdikleri ve götürdüklerinin ele alınması önemlidir. Önerilen her bir emniyet riski azaltma seçeneği aşağıdakiler gibi perspektiflerden incelenmelidir:

a) ***Etkililik.*** Güvensiz eylem veya koşulun sonuçlarına ait emniyet risklerinin azaltılmasını veya ortadan kaldırılmasını sağlıyor mu? Alternatifler bu emniyet risklerini ne dereceye kadar azaltıyor? Etkililik, aşağıdaki şekilde bir süreklilik içinde olarak görülebilir:

1) ***Mühendisliğe dayalı azaltmalar.*** Bu risk azaltma şekli, güvensiz eylem veya koşulun sonuçlarına ait emniyet riskini, örneğin uçuş sırasında yön değiştirme mekanizmasını korumak için emniyet tertibatları sağlayarak ortadan kaldırabilir.

2) ***Kontrole dayalı azaltmalar.*** Bu risk azaltma şekli güvensiz eylem veya koşulun sonuçlarına ait emniyet riskini kabul eder, ama örneğin daha kısıtlayıcı çalışma koşulları getirerek, bu emniyet riskini yönetilebilir seviyeye indirerek sistemi ayarlar. Hem mühendislik hem de kontrole dayalı azaltmalar, insanların kusursuz performansına dayalı olmadığından "sert" azaltma biçimleri olarak kabul edilirler.

3) ***Personele dayalı azaltmalar.*** Bu azaltma şekli, mühendislik ve/veya kontrole dayalı azaltmaların etkili ve etkin olmadığını kabul eder, bu yüzden örneğin uyarlar, gözden geçirilmiş kontrol listeleri, SOP'lar ve/veya fazladan eğitim gibi özellikler ekleyerek, personele tehlikenin sonuçlarına ait emniyet riski ile nasıl başa çıkacaklarının öğretilmesi gerekir. Personele dayalı azaltmalar, insanların kusursuz performansına dayalı olduğundan "yumuşak" azaltma biçimleri olarak kabul edilirler.

b) ***Maliyet-yarar.*** Azaltma işleminde görülen yararlar maliyetlerden daha fazla mı? Potansiyel kazançlar, gereken değişimin etkisi ile orantılı olacak mı?

c) ***Pratiklik.*** Azaltma işlemi mevcut teknoloji, mali fizibilite, yönetimsel fizibilite, geçerli mevzuat ve yönetmelikler, politik irade v.s. bakımından pratik ve uygun mu?

d) ***Karşı gelme.*** Azaltma işlemi tüm ilgili tarafların (personel, yöneticiler, hissedarlar/Devlet yönetimi v.s.) eleştirel incelemelerine karşı gelebilir mi?

e) ***Her bir ilgi taraf tarafından kabul edilebilme.*** İlgili taraflardan ne kadar destek (veya direnç) beklenebilir? (Emniyet riski değerlendirmesi aşaması sırasında ilgili taraflarla görüşmeler, tercih ettikleri risk azaltma seçeneğini gösterebilir.)

f) ***Uygulanabilirlik.*** Yeni kurallar (SOP'lar, yönetmelikler v.s.) getirilirse, uygulanmaları mümkün mü?

g) ***Dayanıklılık.*** Azaltma işlemi zamana karşı dayanaklı mı? Geçici bir yarar mı sağlayacak, yoksa uzun vadeli bir araç mı olacak?

h) ***Artık emniyet riskleri.*** Azaltma işlemi uygulandıktan sonra, orijinal tehlikeye göre kalan emniyet risklerinin oranı ne olacaktır? Artık emniyet risklerinin azaltılması olanağı nedir?

i) ***Yeni sorunlar.*** Önerilen azaltma işlemi ile hangi yeni sorunlar veya yeni (belki de daha kötü) emniyet riskleri ortaya çıkacaktır?

5.7.5 En etkili azaltma biçimi, sert azaltmalardır. Sert azaltmalar genellikle pahalı olduğundan, organizasyonlar sıklıkla yumuşak azaltmalara (eğitim gibi) yönelirler. Bu tür durumlarda, örgüt çoğunlukla emniyet riski yönetiminin astların sorumluluğuna güvenmekten başka bir şey yapmamaktadır.

5.7.6 Özet olarak, emniyet riski kontrol/azaltma stratejileri çoğunlukla ek emniyet savunmalarının getirilmesine veya mevcut savunmaların güçlendirilmesine dayanmaktadır. Savunmalar Bölüm 2'de ele alınmıştır ve havacılık sistemindeki savunmaların üç genel kategori altında toplanabileceği hatırlanacaktır:

a) teknoloji;

b) eğitim ve

c) düzenlemeler.

5.7.7 Emniyet riskinin kontrolü/azaltılmasının bir parçası olarak, yeni savunmaların neden gerekli olduğu veya mevcut savunmaların neden güçlendirilmesi gerektiğinin belirlenmesi gerekir. Aşağıdaki sorular bu türden bir belirleme işlemi ile ilgili olabilir:

a) Tehlikenin sonuçlarına ait emniyet risklerine karşı koruma sağlayacak savunmalar var mı?

b) Savunmalar amaçlanan şekilde çalışıyor mu?

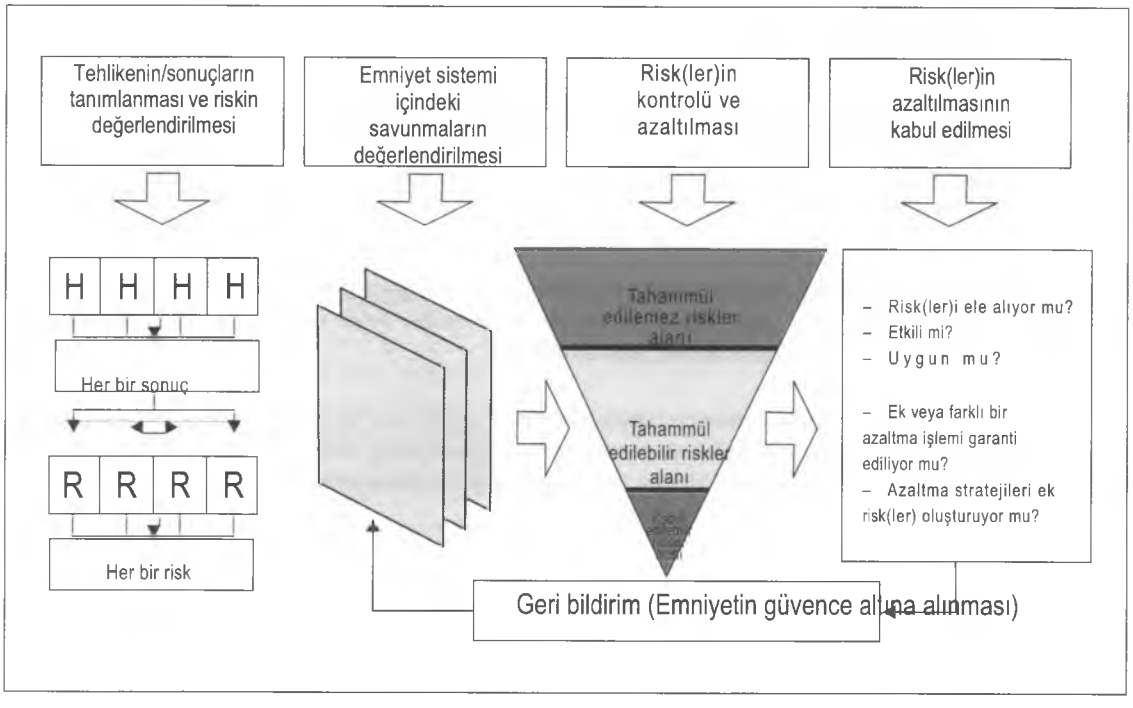
c) Savunmalar gerçek çalışma koşulları altında kullanılmaya uygun mu?

d) İlgili personel tehlikenin sonuçlarına ait emniyet risklerinin farkında mı ve savunmalar yerinde mi?

e) Ek emniyet riskli azaltma/kontrol önlemleri gerekiyor mu?

5.7.8 Şekil 5-7'de emniyet riski azaltma sürecinin tümü grafik olarak sunulmaktadır. Tehlikeler, havacılık sisteminin yapısında yer alan potansiyel emniyet açıklarıdır. Bu açıklar, bir dizi sonuç halinde ortaya çıkarlar. Emniyetin yönetilebilmesi için, her bir emniyet riskine bir indeks atayarak tehlikenin sonuçlarına ait emniyet risklerinin değerlendirilmesi gerekir. Her bir tehlike bir veya daha fazla sayıda sonuç ortaya çıkarabilir ve her bir sonuç bir veya daha fazla sayıda emniyet riski ile değerlendirilebilir. Bu nedenle, emniyet riski azaltma/kontrol sürecindeki ilk adım, tehlikenin/sonucun tanımlanması ve emniyet riskinin değerlendirilmesidir.

5.7.9 Tehlikeler ve sonuçların tanımlandıktan ve emniyet riskleri değerlendirildikten sonra, ilgili tehlikeler ve sonuçlara göre mevcut havacılık sistemi savunmalarının (teknoloji, eğitim ve yönetmelikler) etkili ve etkin olup olmadıkları değerlendirilmelidir. Bu değerlendirmenin sonucunda, mevcut savunmalar güçlendirilecek, yeni savunmalar getirilecektir veya her ikisi de yapılacaktır. Bu nedenle, emniyet riski azaltma/kontrol sürecindeki ikinci adım, havacılık sistemindeki mevcut savunmaların etkili olup olmadığının değerlendirilmesidir.



Şekil 5-7. Emniyet riski azaltma süreci

5.7.10 Mevcut savunmaların güçlendirilmesi ve/veya yeni savunmaların getirilmesine dayanarak, başlangıçtaki emniyet risklerinin ALARP olup olmadıklarının belirlenmesi için bu riskler yeniden değerlendirilir. Bu nedenle, emniyet riski azaltma/kontrol sürecindeki üçüncü adım, kontrol ve/veya azaltma eylemidir.

5.7.11 Emniyet risklerinin yeniden değerlendirilmesinden sonra, azaltma/kontrol stratejilerinin etkin ve etkili olup olmadıkları onaylanmalıdır. Emniyet riski azaltma/kontrol sürecindeki dördüncü adım, emniyet riskinin azaltılmasının kabul edilmesidir. Aşağıdaki sorular sorulmalıdır:

a) Azaltma işlemi emniyet risklerini ele alıyor mu?

b) Azaltma işlemi etkili mi?

c) Azaltma işlemi uygun mu?

d) Ek veya farklı bir azaltma işlemi garanti ediliyor mu?

e) Azaltma stratejileri ek riskler oluşturuyor mu?

5.7.12 Azaltma işlemi kabul edildikten sonra, emniyetin güvence altına alınması sürecinin bir parçası olarak, yeni operasyonel koşullar altında savunmaların bütünlüğünü, etkinliğini ve etkililiğini sağlamak için, geliştirilen ve uygulanmasına başlanan stratejiler, organizasyonun (azaltma stratejilerinin temelini oluşturan) savunmalarına geri beslenmelidir.

5.8 EMNİYET RİSKİ YÖNETİMİNİN BEŞ TEMEL BİLEŞENİ - ÖZET

5.8.1 Bu bölümde ele alınan, emniyet riski yönetimi ile ilgili önemli konseptler aşağıdaki gibi özetlenebilir:

a) Mutlak emniyet diye bir şey yoktur, havacılıkta tüm emniyet risklerinin ortadan kaldırılması mümkün değildir.

b) Emniyet riskleri "makul derecede düşük" (ALARP) seviyesine inecek şekilde yönetilmelidir.

c) Emniyet riskinin azaltılması aşağıdakilere göre dengelenmelidir:

1) zaman;

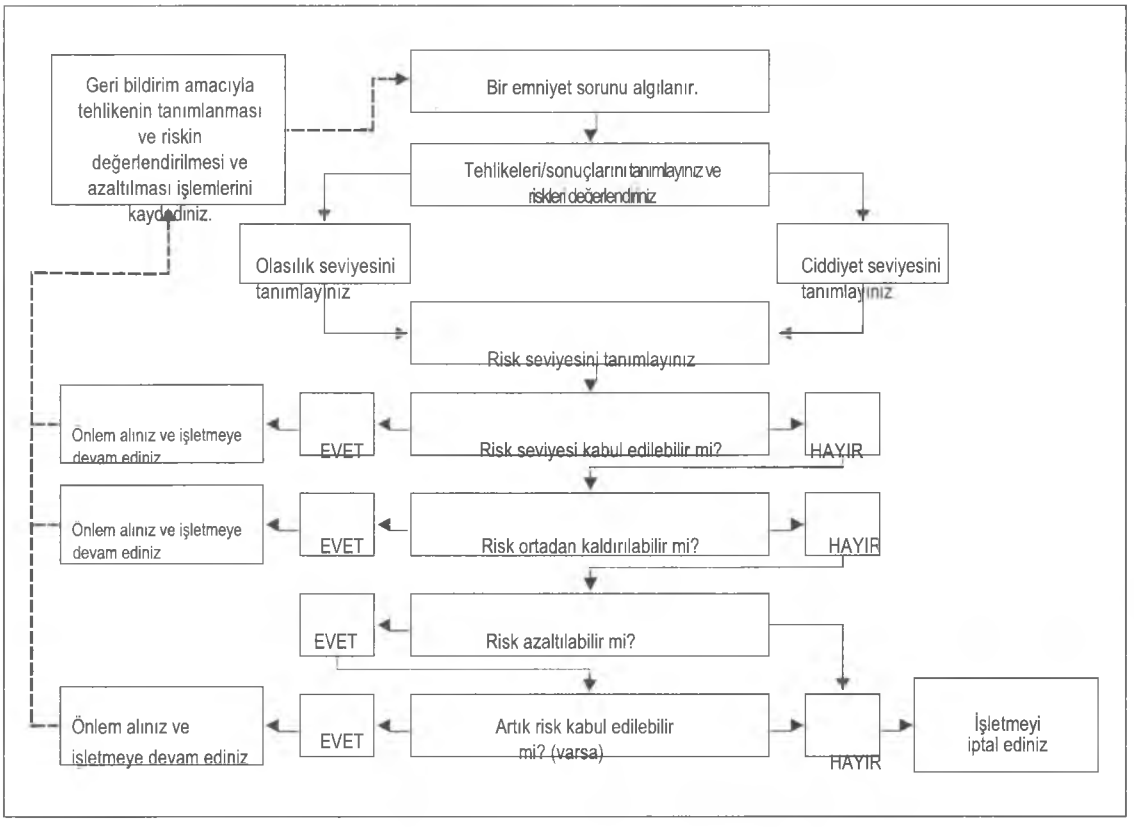
2) maliyet ve

3) emniyet riskinin azaltılması veya ortadan kaldırılması (yani yönetilmesi) için önlem almanın zorluğu.

d) Etkili emniyet riski yönetimi, emniyet riskinin kendisini en aza indirirken, bir emniyet riskinin kabul edilmesinin yararlarını (çoğunlukla, hizmetin sunumundaki zaman ve/veya maliyette azalma) en yüksek seviyeye çıkarmayı amaçlar.

e) Emniyet riskleri ile ilgili kararların mantığı, kabul etmelerini sağlamak için, bu kararlardan etkilenen ilgili taraflara iletilmelidir.

5.8.2 Şekil 5-8'de emniyet riski yönetimi sürecinin tümü sunulmaktadır. Bir emniyet sorunu algılandıktan sonra, emniyet sorunun altında yatan tehlikeler ve tehlikenin potansiyel sonuçları tanımlanır ve emniyet riskinin seviyesini (emniyet riski indeksi) tanımlamak için sonuçlara ait emniyet riskleri değerlendirilir. Emniyet riskleri kabul edilebilir olarak değerlendirilirse, uygun önlem alınır ve operasyon devam eder. Geri bildirim amacıyla (emniyet kütüphanesi), tehlikenin tanımlanması ve riskin değerlendirilmesi ve azaltılması işlemleri kaydedilir.



Şekil 5-8. Emniyet riski yönetimi süreci

5.8.3 Emniyet riskleri kabul edilemez olarak değerlendirilirse, aşağıdaki soruların sorulması gerekir:

a) ***Emniyet riskleri ortadan kaldırılabilir mi?*** Yanıt evetse, uygun önlem alınır ve emniyet kütüphanesine geri bildirimde bulunulur. Yanıt hayırsa, sonraki soru aşağıdaki gibidir:

b) ***Emniyet riskleri azaltılabilir mi?*** Yanıt hayırsa, operasyon iptal edilmelidir. Yanıt evetse, uygun azaltma önlemi alınır ve sonraki soru aşağıdaki şekilde olur:

c) ***Artık emniyet riski kabul edilebilir mi?*** Yanıt evetse, önlem alınır (gerekirse) ve emniyet kütüphanesine geri bildirimde bulunulur. Yanıt hayırsa, operasyon iptal edilmelidir.

5.8.4 5.8.3 c) maddesindeki soru, azaltma stratejilerinin asla emniyet risklerini tamamen azaltmayı sağlayamayacağını göstermektedir. Artık bir emniyet riskinin daima kalacağı kabul edilmelidir ve örgüt artık emniyet risklerinin kontrol altında olmasını sağlamalıdır.

5.8.5 Emniyet riski yönetimi sürecinin pratik bir gösterimini sağlamak için, bu bölümün eklerinde üç farklı emniyet riski yönetimi senaryosu verilmiştir. Ek 1'de bir havaalanındaki emniyet riski yönetimi tatbikat örneği verilmiştir. Ek 2'de bir hava trafik hizmeti sağlayıcısındaki bir emniyet riski yönetimi tatbikat örneği verilmiştir. Ek 3'te bir havayolundaki emniyet riski yönetimi tatbikat örneği verilmiştir.

— — — — — — — — —

Bölüm 5 Ek 1

HERHANGİBİRKENT ULUSLARARASI HAVALİMANI İNŞAAT PLANI

1. SENARYO

1.1 Herhangi bir kent Uluslararası Havaalanında (AIA), biri ana, diğeri yardımcı olmak üzere iki paralel pist bulunmaktadır ve yardımcı pistin yaklaşma ucunun yakınına drenaj yapılması planlanmaktadır. İnşaat alanına erişim için inşaat makineleri ana pistten geçmelidir. Gün içinde çok sayıda operasyon olduğunda, gündüz işletmelerinin etkilenmesini önlemek için, daha az trafik olan geceleri çalışma yapılmasına karar verilmiştir. AIA emniyet yöneticisi, drenajın gece yapılması planının emniyetle ilgili sonuçlarını değerlendirmelidir.

1.2 AIA Emniyet Eylem Grubuna (SAG) inşaat planının emniyetle ilgili sonuçlarını değerlendirilmesinde AIA emniyet yöneticisine destek olma görevi verilmiştir. Sorunun açık ve net bir kısmı, pistten çıkmalara neden olabilecek şekilde, inşaat araçlarının iş alanına gidiş gelişleridir. SAG inşaat planının emniyetle ilgili sonuçlarını değerlendirmek için bir emniyet riski yönetimi süreci uygular.

2. SİSTEM TANIMI

SAG'ın ilk görevlerinden biri, inşaat süresince havaalanında işletmelerin gerçekleştirileceği değiştirilmiş sistemin aşağıdaki gibi açıklanmasıdır:

a) apron ile inşaat anı arasında yüksek miktarda inşaat aracı trafiğini içerecek şekilde, inşaat süresince geceleri pist ortamı;

b) mevcut sürücü eğitim programı ve inşaat araçları için eskortların kullanılması;

c) hava trafiği kontrol kulesi ve telsizi bulunmayan inşaat araçlarıyla telsiz iletişiminin bulunmaması gerçeği ve

d) taksi yolları, pistler ve inşaat alanı için işaretler, uyarılar ve aydınlatma.

3. TEHLİKENİN TANIMLANMA SÜRECİ

SAG'ın ikinci görevi inşaat sırasında havaalanındaki işletmelerini etkileyebilecek tehlikeleri ve olası sonuçlarını aşağıdaki şekilde tanımlamaktır:

a) Genel tehlikeyi belirtmek

1) Havaalanı inşaatı.

b) Tehlikenin belirli bileşenlerini belirtmek

1) Ana pistten geçen inşaat araçları.

c) Genel tehlikenin belirli bileşenlerinin sonuçlarını değerlendirmek

1) İnşaat araçları önceden belirlenen prosedürlerin dışına çıkarak, yanlarında eskort olmadan ana pistten geçebilirler.

2) Uçaklar pistten geçen bir araçla karşı karşıya gelebilir.

4. EMNİYET RİSK DEĞERLENDİRME SÜRECİ

SAG'ın üçüncü görevi tehlikenin sonuçlarına ait emniyet risklerini ve mevcut savunmaları aşağıdaki şekilde tanımlamak ve değerlendirmektir:

a) SAG'ın değerlendirmesi, bir inşaat aracının önceden belirlenen prosedürlerin dışına çıkarak, yanında eskort olmadan ana pistten geçmesi gibi uzak bir olasılık olduğu sonucuna ulaşır.

b) Havaalanında gece hava taşımacılığı işletmeleri yapılmaktadır ve bir uçağın pistten geçen bir araçla karşı karşıya gelmesi gibi uzak bir olasılık vardır.

c) Uçakla inşaat aracının karşı karşıya gelmesi olasılığı uzak olsa da, SAG bu türden bir olay olduğunda, olayın ciddiyetinin yıkıcı olacağını değerlendirir.

d) SAG mevcut savunmaları değerlendirir (sürücü eğitim programı, inşaat araçları için eskortların kullanılması, işaretler, uyarılar ve aydınlatma).

e) Emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG emniyet riski indeksini 3A (mevcut koşullar altında kabul edilemez) olarak değerlendirir.

f) SAG inşaat araçlarının inşaat alanına geliş gidişlerinin oluşturduğu tehlikenin sonuçlarına ait emniyet riskinin, mevcut koşullar altında, kabul edilemez olduğuna ve kontrol/azaltma işleminin gerektiğine karar verir.

5. EMNİYET RİSKİ KONTROL/AZALTMA SÜRECİ

SAG'ın dördüncü ve son görevi tehlikelerin sonuçlarına ait emniyet riskini aşağıdaki şekilde azaltmaktır:

a) SAG inşaat alanına ulaşım için mevcut bir havaalanı çevre araç yolunu kullanarak tehlikenin sonuçlarına ait emniyet riskini kontrol etmeye karar verir. Çevre araç yolunda tüm inşaat araçlarına eskortlar eşlik edecektir.

b) Bu azaltma işlemiyle, SAG inşaat araçlarının eskortsuz olarak ana pistten geçmesi veya bir uçağın pistten geçen bir araçla karşı karşıya gelmesi olasılığını yeniden değerlendirerek, son derece düşük olasılıklı olduğunu belirler. Yine de, bir uçakla inşaat aracı karşı karşıya gelirse, bu tür bir olayın ciddiyeti her halükarda yıkıcı olacaktır.

c) Azaltma işlemi olarak çevre araç yolunun kullanılması, sürüş mesafesinin artması nedeniyle inşaat araçlarının gecikmesine neden olabilir, ama SAG'ın değerlendirmesine göre:

1) Tehlikenin sonuçlarının olasılığını tamamen ortadan kaldırmasa da (inşaat araçları çeşitli koşullar veya bu koşulların kombinasyonu sonucunda yine de ana pistten geçebilir), sonuçlara ait emniyet risklerini (bir inşaat aracının önceden belirlenen prosedürlerin dışına çıkarak, yanında eskort olmadan ana pistten geçmesi ve bir uçağın pistten geçen bir araçla karşı karşıya gelmesi) makul derecede düşük (ALARP) bir seviyeye indirir.

d) Emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG emniyet riski indeksini 1A (kabul edilebilir) olarak yeniden değerlendirir.

e) SAG bu karar verme sürecini, gelecekte de takip edilebilmesi için herhangi bir kent Uluslararası Havaalanı emniyet yöneticisine bildirir.

6. TEHLİKE TANIMLAMA VE EMNİYET RİSKİ YÖNETİMİ GÜNLÜĞÜ

6.1 Tablo 5-Ek 1-1'deki tehlike tanımlama ve emniyet riski yönetimi günlüğü, tanımlanan emniyet risklerinin ve görevlendirilen kişiler tarafından alınan önlemlerin kaydının tutulması için kullanılır. Emniyet riski yönetiminin kanıtı olarak ve gelecekteki emniyet riski değerlendirmelerine referans oluşturması için, kayıt kalıcı olarak "emniyet kütüphanesinde" tutulmalıdır.

6.2 Emniyet riskleri tanımlanmış ve derecelendirilmiş olduğundan, bu risklere karşı mevcut savunmalar tanımlanmalıdır. Daha sonra bu savunmaların yeterliliği değerlendirilmelidir. Yeterli olmadıkları anlaşılırsa, ek önlemlerin alınması gerekecektir. Tüm eylemler için belirli bir kişi (genellikle sorumlu bölüm yöneticisi) atanmalı ve tamamlanması için bir hedef tarih verilmelidir. Bu eylem tamamlanana kadar tehlike tanımlanması ve emniyet riski yönetimi günlüğü silinmemelidir.

Tablo 5-Ek 1-1. Tehlike tanımlama ve emniyet riski yönetimi

İşletme veya etkinlik tipi	*Genel tehlike*	*Tehlikenin belirli bileşenleri*	*Tehlike ile ilgili sonuçlar*	*Emniyet risklerinin kontrolü için mevcut savunmalar ve emniyet riski indeksi*	*Emniyet risklerinin azaltılması için ek eylemler ve sonuçta ortaya çıkan emniyet riski indeksi*
Havaalanı operasyonları	Havaalanı inşaatı	Ana pistten geçen inşaat araçları	a) İnşaat araçları önceden belirlenen prosedürlerin dışına çıkarak, yanlarında eskort olmadan ana pistten geçebilirler. b) Uçaklar pistten geçen bir araçla karşı karşıya gelebilir.	a) SAG'ın değerlendirmesi, bir inşaat aracının önceden belirlenen prosedürlerin dışına çıkarak, yanında eskort olmadan ana pistten geçmesi gibi uzak bir olasılık olduğu sonucuna ulaşır. Havaalanında gece hava taşımacılığı işletmeleri yapılmaktadır ve bir uçağın pistten geçen bir araçla karşı karşıya gelmesi gibi uzak bir olasılık vardır. c) Uçakla inşaat aracının karşı karşıya gelmesi olasılığı uzak olsa da, SAG bu türden bir olay olduğunda, olayın ciddiyetinin yıkıcı olacağını değerlendirir. d) SAG mevcut savunmaları değerlendirir (sürücü eğitim programı, inşaat araçları için eskortların kullanılması, işaretler, uyarılar ve aydınlatma). e) Emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG aşağıdaki değerlendirmeleri yapar: Emniyet riski indeksi: 3A Emniyet riski tahammül edilebilirliği: Mevcut koşullarda kabul edilemez.	a) SAG inşaat alanına ulaşım için mevcut bir havaalanı çevre araç yolunu kullanarak emniyet riskini kontrol etmeye karar verir. Çevre araç yolunda tüm inşaat araçlarına eskortlar eşlik edecektir. b) Bu azaltma işlemiyle, SAG inşaat araçlarının eskortsuz olarak ana pistten geçmesi veya bir uçağın pistten geçen bir araçla karşı karşıya gelmesi olasılığını yeniden değerlendirerek, son derece düşük olasılıklı olduğunu belirler. Yine de, bir uçakla inşaat aracı karşı karşıya gelirse, bu tür bir olayın ciddiyeti her halükarda yıkıcı olacaktır. c) Azaltma işlemi olarak çevre araç yolunun kullanılması, sürüş mesafesinin artması nedeniyle inşaat araçlarının gecikmesine neden olabilir, ama SAG'ın değerlendirmesine göre: 1) Tehlikenin sonuçlarının olasılığını tamamen ortadan kaldırmasa da (inşaat araçları çeşitli koşullar veya bu koşulların kombinasyonu sonucunda yine de ana pistten geçebilir), sonuçlara ait emniyet risklerini (bir inşaat aracının önceden belirlenen prosedürlerin dışına çıkarak, yanında eskort olmadan ana pistten geçmesi ve bir uçağın pistten geçen bir araçla karşı karşıya gelmesi) kabul edilebilir bir seviyeye indirir. d) Emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG aşağıdaki yeniden değerlendirmeleri yapar: Emniyet riski indeksi: 1A Emniyet riski tahammül edilebilirliği: Kabul edilebilir. e) SAG bu karar verme sürecini, gelecekte de takip edilebilmesi için Herhangi bir kent Uluslararası Havaalanı emniyet yöneticisine bildirir.

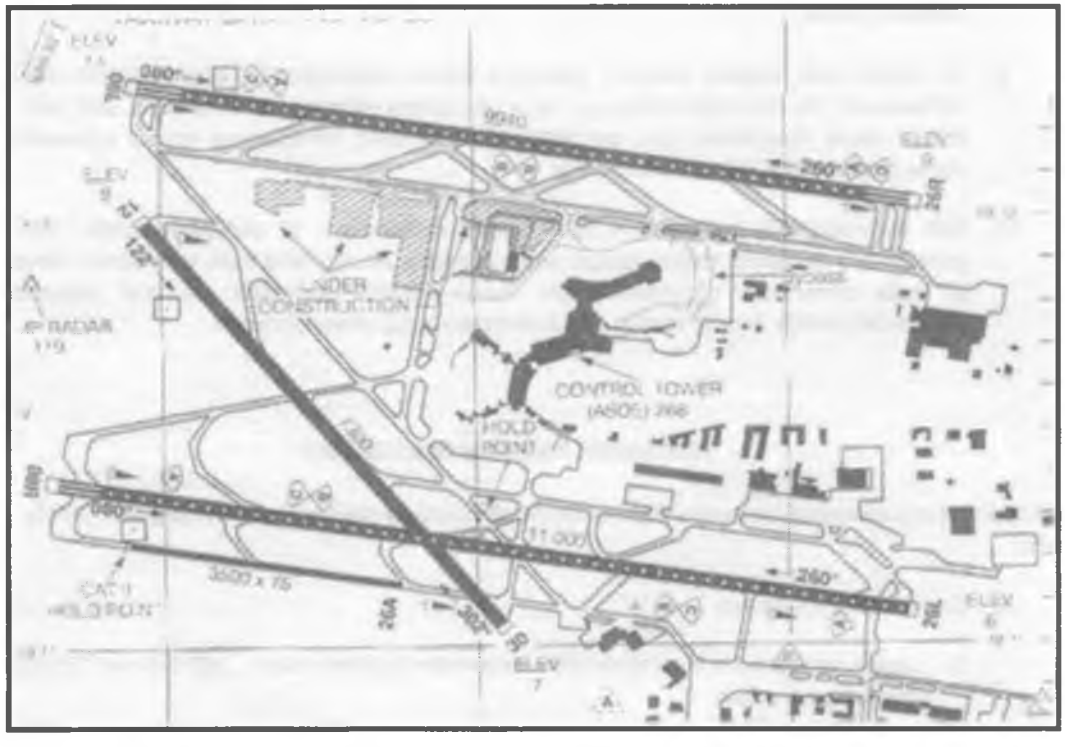
Bölüm 5 Ek 2

KESİŞEN PİST İŞLETMELERİ

1. SENARYO

1.1 Bir hava trafik hizmeti sağlayıcısı, havaalanı kullanıcılarından XYZ Uluslararası Havaalanı'ndaki kesişen pist operasyonları ile ilgili geri bildirim alır. XYZ Uluslararası Havaalanı üç pistten oluşur: 08L/26R, 08R/26L ve 12/30 (Bkz. Şekil 5-Ek 2-1). 26R ve 12 pistlerinde arada bir kesişen pist operasyonları gerçekleştirilmektedir. Hava trafik hizmeti sağlayıcısı, emniyet yöneticisinden XYZ Uluslararası Havaalanı'ndaki 26R ve 12 pistlerindeki kesişen pist operasyonları prosedürlerinin emniyetinin kullanıcılar tarafından dile getirilen şikayetler ışığında yeniden değerlendirilmesini ister.

1.2 Emniyet Eylem Grubundan (SAG) XYZ Uluslararası Havaalanı'ndaki kesişen pist operasyonları prosedürlerinin emniyetinin yeniden değerlendirilmesinde emniyet yöneticisine destek olmaları istenir. SAG, ATS hizmet sağlayıcısı, XYZ Uluslararası Havaalanı'na sefer yapan havayolları ve havayolu pilotları derneğinden, havaalanından ve Devletin denetim kurumundan temsilciler içerir. Genel emniyet sorunu, XYZ Uluslararası Havaalanı'ndan kalkan ve havaalanına inen uçakların uçuş yollarının kesişmesidir. SAG kesişen pist operasyonlarının emniyetini yeniden değerlendirmek için bir emniyet riski yönetimi süreci uygular.



Şekil 5-Ek 2-1. XYX Uluslararası Havaalanı

2. SİSTEM TANIMI

SAG'ın ilk görevlerinden biri, işletmelerin gerçekleştirildiği sistemin aşağıdaki gibi açıklanmasıdır:

a) XYZ Uluslararası Havaalanı'nda üç ana pist ve küçük bir yardımcı pist hizmeti vardır.

b) Havaalanında yılda 325.000 hareket gerçekleşir.

c) 26L-08R pisti 11.000 ft uzunluğundadır ve doğu ve batı gidişleri ve doğu ve batı gelişleri için kullanılmaktadır. 12-30 pisti 7300 ft uzunluğundadır. 12 pisti çoğunlukla gelişler için kullanılır. 30 pisti bazen gidişler ve nadiren gelişler için kullanılır. 12 pisti, fiziksel olarak 08R-26L pistinden geçer ve "kesişen" bir pist olarak kabul edilir. 08L-26R pisti 9.940 ft uzunluğundadır ve temel olarak gelen trafik için ve arada bir giden trafik için kullanılır. 08L pisti henüz gidiş prosedürleri oluşturulmadığı için sadece gelişler için kullanılır.

d) Havaalanındaki uyarılar, işaret sistemleri ve aydınlatma hem denetim kurumlarının hem de ICAO'nun standartlarına uygundur.

e) Kule kontrolü için kullanılan iki kontrol frekansı vardır. Bir frekans güney pistini (26L-08R) ve batı pistini (12-30) kapsar. İkinci frekans kuzey pistini (26R-08L) kapsar.

f) Güney pistlerinde (26L-08R) 12 pistindeki trafikle çakışmayı önlemek için yayınlanmış kesişen pist yaklaşımları vardır. Fiziksel olarak kesişmedikleri için, teknik olarak kesişen pist olarak kabul edilmediklerinden, kuzey pistleri (26R-08L) için yayınlanmış kesişen pist yaklaşımları yoktur. 12 pistinde ILS yaklaşımı olsa da, inişlerin önemli bir bölümü genel olarak görsel yaklaşımlarla bir VFR pistinden yapılır.

g) 12 pistinin trafik bilgileri, 08R-26L pistindeki trafiğe aktarılmaktadır, çünkü iki pistin kesiştiği kabul edilmektedir. Her iki pistteki trafik aynı frekansta kontrol edilmektedir. Ancak, 08L-26R pisti ve 12 pisti fiziksel olarak kesişmediği için, bu pistlerdeki trafik farklı frekanslarda kontrol edilmektedir. Sonuç olarak, trafik bilgileri paylaşılmamaktadır.

h) 26R pistindeki IFR trafiğine IFR trafik ayrımı sağlanırken, 12 pistindeki uçağa VFR ve görsel yaklaşımlara havaalanı kontrol hizmeti sağlanmaktadır. Ancak, hava trafik kontrolörleri bilinen herhangi bir trafik çakışmasını çözümlemek için derhal harekete geçecektir. Standart prosedür 26R-08L pistlerindeki trafiğe öncelik vermek ve 12 pistindeki trafiği yönlendirmektir.

3. TEHLİKENİN TANIMLANMASI SÜRECİ

SAG'ın ikinci görevi havaalanındaki işletmeleri etkileyebilecek tehlikeleri ve olası sonuçlarını aşağıdaki şekilde tanımlamaktır:

a) Genel tehlikeyi belirtmek

1) Uçağın yaklaşmakta veya ayrılmakta olmasından bağımsız olarak, 26R-08L ve 12 pistlerinde kesişen uçuş yolları.

b) Tehlikenin belirli bileşenlerini belirtmek

1) Uçak, 12 pistine inen trafiğe karşı 26R pistine inmeyi reddeder.

2) Uçak, 12 pistine inen trafiğe karşı 26R pistinden kalkar.

3) Uçak, 12 pistine inen trafiğe karşı 08L pistine yaklaşır.

4) Bir uçak, 12 pistine inen trafiğe karşı 08L pistinden 08R pistine veya 08R pistinden 08L pistine yaklaşma hareketinden bir "yana kayma" gerçekleştirir.

c) Genel tehlikenin belirli bileşenlerinin sonuçlarını değerlendirmek

1) Kuyruk türbülansı ile karşılaşma.

2) Diğer trafikten kaçınmak için kaçınma manevrası.

3) Diğer trafikten kaçınmak için manevra sonrasında kontrol kaybı.

4) Dengesiz yaklaşma sonrasında pistin toprak uzantısına çıkma.

5) 12 pistine yaklaşan uçak ile 08L pistine yaklaşan uçak veya 26R pistinden kalkan uçak arasında 26R pistinin kalkış ucunda havada çarpışma (en kötü durum sonucu).

4. EMNİYET RİSK DEĞERLENDİRME SÜRECİ

4.1 SAG XYZ Uluslararası Havaalanı'ndaki 26R-08L ve 12 pistleri için kesişen pist operasyonlarını destekleyen savunmaları belirler. Bu savunmalar, 26R-08L ve 12 pistleri için kesişen uçuş yollarının sonuçlarına ait emniyet risklerinin azalmasına yönelik teknoloji, programlar ve prosedürler biçimindedir.

4.2 Bu savunmalar aşağıdakileri içerir:

a) kontrolör koordinasyon prosedürleri;

b) olumsuz hava koşulları sırasında kaçırılan yaklaşmalar için hava sahasının korunması amacıyla mesafenin arttırılması;

c) 26R pisti gidişler için kullanıldığında 12 pistinden gelişler üzerinde kısıtlamalar;

d) havaalanı yüzey araştırma donanımı (ASDE);

e) piste giriş önleme programı ve vahşi yaşam kontrol programı;

f) Havaalanı içi sürücü ilk ve tekrarlanan eğitimleri ve testleri;

g) yan rüzgar limitlerinin sürekli izlenmesi ve istatistiksel olarak takip edilmesi;

h) yaklaşma radarının bulunması ve kullanılması;

i) pist meşgul tutma süresi standartları;

j) ayrı kule frekansları ve

k) uyarı ve işaret sistemi.

4.3 Mevcut savunmalar temelinde, emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG 26R-08L ve 12 pistleri için kesişen uçuş yollarının sonuçlarına ait emniyet riski indeksini aşağıdaki şekilde değerlendirir:

a) Kuyruk türbülansı ile karşılaşma: olasılık uzak, ciddiyet önemli. Emniyet riski tahammül edilebilirliği: 3C (riskin azaltılması temelinde kabul edilebilir).

b) Diğer trafikten kaçınmak için kaçınma manevrası: olasılık uzak, ciddiyet önemli. Emniyet riski tahammül edilebilirliği: 3C (riskin azaltılması temelinde kabul edilebilir).

c) Diğer trafikten kaçınmak için manevra sonrasında kontrol kaybı: olasılık uzak, ciddiyet tehlikeli. Emniyet riski tahammül edilebilirliği: 3B (riskin azaltılması temelinde kabul edilebilir).

d) Dengesiz yaklaşma sonrasında pistin toprak uzantısına çıkma: olasılık uzak, ciddiyet tehlikeli. Emniyet riski tahammül edilebilirliği: 3B (riskin azaltılması temelinde kabul edilebilir).

e) 12 pistine yaklaşan uçak ile 08L pistine yaklaşan uçak veya 26R pistinden kalkan uçak arasında 26R pistinin kalkış ucunda havada çarpışma: olasılık olası değil, ciddiyet yıkıcı. Emniyet riski tahammül edilebilirliği: 2A (riskin azaltılması temelinde kabul edilebilir).

5.EMNİYET RİSKİ KONTROL/AZALTMA SÜRECİ

5.1 SAG kesişen pistlerdeki operasyonların yasaklanmasının, 26R-08L ve 12 pistleri için kesişen uçuş yollarının olası en kötü sonucunu etkili bir şekilde ortadan kaldıracağını belirler: 26R pistinin kalkış ucunda havada çarpışma. Ancak, emniyet yönetimi önemli sadece etkili değil, aynı zamanda etkin olmalıdır. Kesişen pistlerin kullanılmasını yasaklamak etkin olmayacaktır.

5.2 SAG XYZ Uluslararası Havaalanı'ndaki 26R-08L ve 12 pistleri için kesişen pist operasyonları ile ilgili olarak acil, derhal müdahale edilmesi gereken emniyet sorunları olmadığına karar verir. En kötü senaryo (havada çarpışma) da dahil olmak üzere, XYZ Uluslararası Havaalanı'ndaki 26R-08L ve 12 pistlerindeki kesişen uçuş yollarının sonuçlarına ait emniyet riskleri için mevcut savunmaları, emniyet risklerinin ALARP (makul derecede düşük) tutulması için etkili kontrol yöntemleridir. Yine de, XYZ Uluslararası Havaalanı'ndakl işletmelerin emniyetlerinin güçlendirilmesi için tavsiyelerde bulunurlar. Acil olmasa da, bu tavsiyelerin uygulanması önemli bir emniyet marjı sağlayacaktır.

5.3 Bu tavsiyeler aşağıdakileri içerir:

a) Hava koşulları beklenenden veya hava tahmininden farklı olduğunda, uçuş ekiplerinin pilot raporlarını (PIREP'ler) hava trafik kontrolü birimlerine aktarmasının desteklenmesi için sürekli devam eden bir kampanyanın başlatılması.

b) Bir kesişen pist görüntüleme yardımının (CRDA) XYZ Uluslararası Havaalanı'ndaki önemli bir emniyet ve kapasite arttırma cihazı olarak uygulanmasının uygunluğunun ve etkili olup olmayacağının araştırılması.

c) XYZ Uluslararası Havaalanı'nda CRDA uygulanmazsa, örneğin 26R pistine inmeyi reddeden bir uçağın 12 pistine yaklaşan bir uçağa göre korumalı hava sahası olmasını sağlayacak şekilde inen uçak mesafesinin ayarlanması için ayırma ölçütlerinin ve prosedürlerinin oluşturulması.

d) Geliş tipi çizelgelerinde bir yaklaşma hızı sınırları aralığı belirlenmesi ve hava trafik kontrolörü iletişimi prosedürlerinin, 08L-26R pistindeki trafiğe 12 pistindeki kesişen trafik hakkında bilgi verilmesini sağlayacak şekilde değiştirilmesi.

e) Bir kontrolörün acil durum talimatları verebilmek için başka bir kontrolörün frekansına geçebilmesi için bir acil durum frekansı müdahalesinin kurulması.

5.4 SAG bu karar verme sürecini, gelecekte de takip edilebilmesi için hava trafik hizmeti emniyet yöneticisine bildirir.

6. TEHLİKE TANIMLAMA VE EMNİYET RİSKİ YÖNETİMİ GÜNLÜĞÜ

6.1 Tablo 5-Ek 2-1'deki tehlike tanımlama ve emniyet riski yönetimi günlüğü, tanımlanan emniyet risklerinin ve görevlendirilen kişiler tarafından alınan önlemlerin kaydının tutulması için kullanılır. Emniyet riski yönetiminin kanıtı olarak ve gelecekteki emniyet riski değerlendirmelerine referans oluşturması için, kayıt kalıcı olarak "emniyet kütüphanesinde" tutulmalıdır.

6.2 Emniyet riskleri tanımlanmış ve derecelendirilmiş olduğundan, bu risklere karşı mevcut savunmalar tanımlanmalıdır. Daha sonra bu savunmaların yeterliliği değerlendirilmelidir. Yeterli olmadıkları anlaşılırsa, ek önlemlerin alınması gerekecektir. Tüm eylemler için belirli bir kişi (genellikle sorumlu bölüm yöneticisi) atanmalı ve tamamlanması için bir hedef tarih verilmelidir. Bu eylem tamamlanana kadar tehlike tanımlama ve emniyet riski yönetimi günlüğü silinmemelidir.

Tablo 5-Ek 2-1. Tehlike tanımlama ve emniyet riski yönetimi

İşletme veya etkinlik tipi	*Genel tehlike*	*Tehlikenin belirli bileşenleri*	*Tehlike ile ilgili sonuçlar*	*Emniyet risklerinin kontrolü için mevcut savunmalar ve emniyet riski*	*Emniyet risklerinin azaltılması için ek eylemler ve sonuçta*
Hava trafik kontrolü etkinlikleri	Uçağın yaklaşmakta veya ayrılmakta olmasından bağımsız olarak, 26R-08L ve 12 pistlerinde kesişen uçuş yolları.	a) Uçak, 12 pistine inen trafiğe karşı 26R pistine inmeyi reddeder. b) Uçak, 12 pistine inen trafiğe karşı 26R pistinden kalkar. c) Uçak, 12 pistine inen trafiğe karşı 08L pistine yaklaşır. d) Bir uçak, 12 pistine inen trafiğe karşı 08L pistinden 08R pistine veya 08R pistinden 08L pistine yaklaşma hareketinden bir "yana kayma" gerçekleştirir.	a) Kuyruk türbülansı ile karşılaşma. b) Diğer trafikten kaçınmak için kaçınma manevrası. c) Diğer trafikten kaçınmak için manevra sonrasında kontrol kaybı. d) Dengesiz yaklaşma sonrasında pistin toprak uzantısına çıkma. e) 12 pistine yaklaşan uçak ile 08L pistine yaklaşan uçak veya 26R pistinden kalkan uçak arasında 26R pistinin kalkış ucunda havada çarpışma (en kötü durum sonucu).	• Kontrolör koordinasyon prosedürleri; • Olumsuz hava koşulları sırasında kaçırılan yaklaşmalar için hava sahasının korunması amacıyla mesafenin arttırılması; • 26R pisti gidişler için kullanıldığında 12 pistinden gelişler üzerinde kısıtlamalar; • Havaalanı yüzey araştırma donanımı (ASDE); • Piste giriş önleme programı ve vahşi yaşam kontrol programı; • Havaalanı içi sürücü ilk ve tekrarlanan eğitimleri ve testleri; • Yan rüzgar limitlerinin sürekli izlenmesi ve istatistiksel olarak takip edilmesi; • Yaklaşma radarının bulunması ve kullanılması; • Pist meşgul tutma süresi standartları; • Ayrı kule frekansları ve • uyarı ve işaret sistemi. a) Kuyruk türbülansı ile karşılaşma: Emniyet riski indeksi: 3C Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir. b) Diğer trafikten kaçınmak için kaçınma manevrası: Emniyet riski indeksi: 3C Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir. c) Diğer trafikten kaçınmak için manevra sonrasında kontrol kaybı: Emniyet riski indeksi: 3B Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir. d) Dengesiz yaklaşma sonrasında pistin toprak uzantısına çıkma: Emniyet riski indeksi: 3B Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir. e) 12 pistine yaklaşan uçak ile 08L pistine yaklaşan uçak veya 26 R pistinden kalkan uçak arasında 26R pistinin kalkış ucunda havada çarpışma: Emniyet riski indeksi: 2A Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir.	a) Hava koşulları beklenenden veya hava tahmininden farklı olduğunda, uçuş ekiplerinin pilot raporlarını (PIREP'ler) hava trafik kontrolü birimlerine aktarmasının desteklenmesi için sürekli devam eden bir kampanyanın başlatılması. b) Bir kesişen pist görüntüleme yardımının (CRDA) XYZ Uluslararası Havaalanı'ndaki önemli bir emniyet ve kapasite arttırma cihazı olarak uygulanmasının uygunluğunun ve etkili olup olmayacağının araştırılması. c) XYZ Uluslararası Havaalanı'nda CRDA uygulanmazsa, örneğin 26R pistine inmeyi reddeden bir uçağın 12 pistine yaklaşan bir uçağa göre korumalı hava sahası olmasını sağlayacak şekilde inen uçak mesafesinin ayarlanması için ayırma ölçütlerinin ve prosedürlerinin oluşturulması; d) Geliş tipi çizelgelerinde bir yaklaşma hızı sınırları aralığı belirlenmesi ve hava trafik kontrolörü iletişimi prosedürlerinin, 08L-26R pistindeki trafiğe 12 pistindeki kesişen trafik hakkında bilgi verilmesini sağlayacak şekilde değiştirilmesi. e) Bir kontrolörün acil durum talimatları verebilmek için başka bir kontrolörün frekansına geçebilmesi için bir acil durum frekansı müdahalesinin kurulması.

Bölüm 5 Ek 3

ANDES ULUSLARARASI HAVALİMANI'NDAKİ TİCARİ İŞLETMELER

1. SENARYO

1.1 Safe Airways on beş modern teknolojili çift jet motorlu yolcu uçağına sahip orta boyutlu bir havayolu operatörüdür. Havayolu dağların üzerinde yer alan bir turizm merkezi olan, güzel bir manzara ile çevrelenen ve antik bir uygarlığın kalıntılarını sunan Andes City'ye ticari uçuş faaliyetleri başlatmayı planlamaktadır. Karadan ulaşım tehlikeli yollar üzerinden iki günden fazla süre alabilmektedir; bu nedenle, havayolu ulaşımı en uygun ulaşım aracıdır.

1.2 Andes City'de yaklaşma seyrüsefer yardımcısı olmayan, karmaşık bir coğrafyada yer alan yüksek rakımlı bir havaalanı bulunmaktadır, bu da uçuş işletmelerinin gündüz ve uygun görsel koşullarla sınırlı olmasına neden olmaktadır. Safe Airways üst yönetimi, uçuş işletmeleri direktöründen, uçuş işletmelerinin tüm emniyet gerekliliklerine uygun şekilde ve aynı zamanda uçak performansına ve sınırlamalarına dikkat edilerek maksimum ticari yükle uygulanmasını ister. Planlanan işletmede Andes City'ye akşama doğru bir uçuş olacak ve doksan dakika uzaklıktaki ana üsse hızla dönülecektir.

1.3 Uçuş işletmeleri direktörü, emniyet yöneticisinden Emniyet Eylem Grubunun (SAG) desteğiyle Andes City Uluslararası Havaalanı'na yönelik operasyonel emniyet sonuçlarını değerlendirmesini ister. Sorunun açık ve net bir kısmı, yaklaşma seyrüsefer yardımcıları olmadan karmaşık bir coğrafyada yer alan yüksek rakımlı bir havaalanına yönelik operasyon yapılmasıdır. SAG Andes City Uluslararası Havaalanı'na yönelik işletmelerin emniyetle ilgili sonuçlarını değerlendirmek için bir emniyet riski yönetimi süreci uygular.

2. SİSTEM TANIMI

SAG'ın ilk görevlerinden biri, işletmenin gerçekleştirileceği sistemin aşağıdaki gibi açıklanmasıdır:

a) Andes City Uluslararası Havaalanı, 16000 ft'ten yüksek dağlarla çevrili, 11000 ft rakımındaki bir vadide yer almaktadır.

b) Havaalanında sadece 3400 m (11 155 ft) uzunluğunda, doğu-batı yönünde bir pist (09-27 pisti) bulunmaktadır.

c) Topografya nedeniyle 09 pisti sadece inişler ve 27 pisti sadece kalkışlar için kullanılmaktadır.

d) Aletli alçalma yaklaşımı için, havaalanının 20 mil batısındaki vadide bulunan bir VOR kullanılmaktadır.

e) ILS yaklaşımı yoktur.

f) Ayrılan bir uçağın kalkışına izin verilmesinden sonra, ayrılan uçağın tüm engellerden kurtulduğu rota üzerindeki bir yüksekliğe tırmandığını bildirmesine kadar görsel yaklaşıma izin verilmemektedir.

g) Andes City Uluslararası Havaalanı'na VMC'de görsel yaklaşım, VOR'un 18000 ft üzerinde başlamaktadır. 18000 ft'te yer teması kurulamazsa, VMC yaklaşımlarına ATC tarafından izin verilmemektedir.

h) İniş görsel destekleri yoktur.

i) ATC tarafından Andes City Uluslararası Havaalanı'na görsel yaklaşımını başlatması için onay verilen bir uçak inene ve indikten sonra pistten ayrıldığını anons edene kadar kalkış izni verilmez.

j) Andes City Uluslararası Havaalanı'ndaki hava değişkendir, genellikle tabanı 19000 ile 21000 ft arasında yüksek bir bulut katmanı bulunur.

k) Dış ortam sıcaklığı 10:00 ile 14:00 saatleri arasında yüksektir, bu da uçak performansını etkiler.

l) Kata batik rüzgarlar her gün yaklaşık 16:00'dan sonra 27 pistinden kuyruk rüzgarı ile kalkışı zorunlu kılabilir.

m) Motor yangını, motorun durması veya herhangi bir acil durumda, ağırlık ve performans sınırlamaları engel ayrım sınırı ve net yörüngeye uymanın mümkün olmamasına neden olacağında, havaalanına dönüş zorunludur.

n) Ulusal sivil havacılık kurumu (CAA), operatör sertifikasının bir parçası olarak özel operasyon onayını vermek için, havayolundan bir uçağın yaklaşma, iniş, kalkış, tırmanma ve yol üzerinde aşamalar sırasında net yörünge ve engel ayrım sınırlarına uyabileceğini ve emniyet marjları ve uçak sınırlamaları içinde, karmaşık topografya içinde manevra yapabileceğini kanıtlamasını istemektedir.

o) Dokümantasyon gözden geçirilip onaylandıktan ve kabin ekibi Andes City Uluslararası Havaalanı'ndaki operasyon için özel bir eğitim aldıktan sonra, operasyon başlatılmaya hazır olduğunda, CAA bir test uçuşunun yapılmasını zorunlu tutmaktadır.

3. TEHLİKENİN TANIMLAMA SÜRECİ

SAG'ın ikinci görevi Andes City Uluslararası Havaalanı'ndaki işletmesi etkileyebilecek tehlikeleri ve bu tehlikelerin sonuçlarını aşağıdaki şekilde tanımlamaktır:

a) Genel tehlikeyi belirtmek

1) Karmaşık bir coğrafyada bulunan yüksek rakımdaki bir havaalanında işletme.

b) Tehlikenin belirli bileşenlerini belirtmek

1) Çevre dağlar.

2) Yüksek rakımlı havaalanı.

3) Yaklaşma ve iniş seyrüsefer yardımcılarının bulunmaması.

4) Görsel iniş desteklerinin bulunmaması.

5) Kesişen trafik.

6) Islandığında kayganlaşan pist.

7) Vahşi yaşam.

c) Genel tehlikenin belirli bileşenlerinin sonuçlarını değerlendirmek

1) Aşağıdakiler nedeniyle arazide kontrollü uçuş (CFIT):

i) yaklaşma ve iniş sırasında kritik motor kaybı;

ii) V_1'den sonra kalkış sırasında kritik motor kaybı;

iii) rota üzerindeki tırmanma sırasında kritik motor kaybı;

2) Havada çarpışma.

3) İnişten sonra emniyet pistine çıkış.

4) Kalkışın iptal edilmesinden sonra emniyet pistine çıkış.

5) Kuşlarla çarpışma.

4. EMNİYET RİSK DEĞERLENDİRME SÜRECİ

Not— Bu tatbikatta sadece V1'den sonra kalkış sırasında kritik motor kaybı nedeniyle arazide kontrollü uçuş sonucu ele alınmıştır. Gerçek bir emniyet riski değerlendirmesinde, tüm sonuçlar analiz edilmeli ve tüm emniyet riskleri değerlendirilmeli ve azaltılmalıdır.

4.1 SAG'ın üçüncü görevi tehlikenin sonuçlarına ait emniyet risklerinin ele alınması için mevcut savunmaların etkililiğini değerlendirmektir.

4.2 SAG bu işletmeyle ilgili olarak etkilenebilecek veya eksik olan mevcut emniyet savunmalarını gözden geçirir. Bu savunmalar, temel olarak uçuş ekibinin eğitimi ve benzer işletmelerle ilgili olarak şirketin operasyon el kitabındaki prosedürler ve sınırlamalarla ilgilidir.

4.3 Değerlendirme sırasında belirlenen mevcut savunmalar aşağıdaki gibidir:

a) VMC ve gündüz uçak işletmesi;

b) ulusal AIP'de bulunan havaalanı yerleşimi;

c) havaalanında bulunan ATC prosedürleri;

d) şirket operasyon el kitabı;

e) dağıtım performansı el kitabı;

f) uçak çalıştırma el kitabı;

g) V_1 öncesinde ve sonrasında motor arızası ve kaçırılan yaklaşma prosedürleri hakkında tekrarlanan eğitim;

h) CRM eğitimi.

4.4 SAG, temel olarak karmaşık bir coğrafyada yer alan yüksek rakımlı bir havaalanında belirli bir operasyon ele alınmadığı için, mevcut savunmaların yetersiz olduğuna karar verir.

4.5 Andes City Uluslararası Havaalanı'ndaki geçerli ATC prosedürlerinin yanında operasyon dokümantasyonu da gözden geçirilmiştir.

4.6 Emniyet riski değerlendirme matrisini (Bölüm 5, Şekil 5-4) emniyet riski tahammül edilebilirlik matrisini (Bölüm 5, Şekil 5-5) kullanarak, SAG emniyet riski indeksini 3A (mevcut koşullar altında kabul edilemez) olarak değerlendirir.

5. EMNİYET RİSKİ KONTROL/AZALTMA SÜRECİ

5.1 SAG dördüncü ve son görevi, V1'den sonra kalkış sırasında kritik motor kaybı nedeniyle bir CFIT'in sonuçlarına ait belirlenen emniyet risklerinin kontrol edilmesi ve azaltılmasıdır. Birkaç toplantıdan sonra, SAG aşağıdaki azaltma işlemlerini önerir. Önerilen azaltma işlemleri savunmaları güçlendirmeyi ve emniyet riskini "makul derecede düşük" (ALARP) seviyesine indirmeyi amaçlamaktadır. Bu azaltma işlemleri aşağıdakileri içerir:

a) Karaya dönüş olasılığını da değerlendirerek, V_1'den sonra kritik bir motor kaybı durumunda kalkış ve tırmanma prosedürlerinin geliştirilmesi.

b) Yukarıdaki prosedürler hakkında eğitimin geliştirilmesi ve verilmesi (tam uçuş simülatörü ve her altı ayda bir kalifikasyonların yenilenmesi).

c) Andes City Uluslararası Havaalanı'nın, yenilenmediği sürece sadece bir yıl geçerli olacak şekilde özel ekip kalifikasyonu gerektiren "özel havaalanı operasyonu" olarak değerlendirilmesi.

d) Kabin ekiplerine uygun "özel havaalanı operasyonu" verilmesi. (Bu azaltma işlemi emniyet riskinin bir sonucuna ait olasılığa değil de, ciddiyetine – acil durumda tahliye - yöneliktir.)

e) Özellikle, saat 16:00'dan sonra yüzey rüzgarları hakkında doğru hava durumu bilgilerinin sağlanması.

f) İşletme dokümantasyonunun geliştirilmesi ve CAA tarafından onaylanmak üzere şirket operasyon el kitabı ve dağıtım el kitabına eklenmesi.

g) Açık bir minimum donanım listesi (MEL) kritik öğe politikasının yasaklanması.

h) Bakım güvenilirliği programı altında, bakım departmanı işletmeye ayrılmış uçağın motorunu gözden geçirmelidir.

i) Andes City Uluslararası Havaalanı'ndaki işletmeyle ilgili emniyet risklerinin kontrolü ve azaltılması için uygulanan emniyet önlemleri ve yeni savunmaların izlenmesi. Savunmaların etkililiğinin, değişiklikler uygulandıktan ve CAA tarafından onay verildikten 6 ve 12 ay sonra gözden geçirilmesi planlanmaktadır.

5.2 Bu özel operasyon için geliştirilen yeni savunmaları hesaba katarak, V1'den sonra kalkış sırasında kritik motor kaybı nedeniyle bir CFIT'a ait emniyet riski olası değil (2 — Ortaya çıkma olasılığı çok düşük) olarak değerlendirilir, ancak CFIT'in ciddiyeti hala yıkıcı (A — donanım kullanılamaz hale gelir — çok sayıda ölüm) olarak kalır.

5.3 İşletme artık tahammül edilebilir alandadır ve risk indeksi 2A'dır (riskin azaltılması temelinde kabul edilebilir). Yönetim kararı gerektirebilir (bkz. Bölüm 5, Şekil 5-8). Tehlike tanımlama ve risk yönetimi süreçlerinden elde edilen emniyet verileri ve dokümantasyon şirket "emniyet kütüphanesine" eklenir.

6. AZALTMA ÖNLEMLERİNİN UYGULANMASI İÇİN BİREYSEL SORUMLULUKLAR

Önerilen azaltma önlemlerinin uygulanması için bireysel sorumluluklar aşağıdaki gibidir:

a) Azaltma önlemleri a), f) ve i) — uçuş işletmeleri direktörü;

b) Azaltma önlemleri b), c) ve d) — uçuş eğitimi yöneticisi;

c) Azaltma önlemi e) — dağıtım yöneticisi;

d) Azaltma önlemleri g) ve h) — bakım direktörü;

7. TEHLİKE TANIMLAMA VE EMNİYET RİSKİ YÖNETİMİ GÜNLÜĞÜ

7.1 Tablo 5-Ek 3-1'deki tehlike tanımlama ve emniyet riski yönetimi günlüğü, tanımlanan emniyet risklerinin ve görevlendirilen kişiler tarafından alınan önlemlerin kaydının tutulması için kullanılır. Emniyet riski yönetiminin kanıtı olarak ve gelecekteki emniyet riski değerlendirmelerine referans oluşturması için, kayıt kalıcı olarak "emniyet kütüphanesinde" tutulmalıdır.

7.2 Emniyet riskleri tanımlanmış ve derecelendirilmiş olduğundan, bu risklere karşı mevcut savunmalar tanımlanmalıdır. Daha sonra bu savunmaların yeterliliği değerlendirilmelidir. Yeterli olmadıkları anlaşılırsa, ek önlemlerin alınması gerekecektir. Tüm eylemler için belirli bir kişi (genellikle sorumlu bölüm yöneticisi) atanmalı ve tamamlanması için bir hedef tarih verilmelidir. Bu eylem tamamlanana kadar tehlike tanımlama ve emniyet riski yönetimi günlüğü silinmemelidir.

Tablo 5-Ek 3-1. Tehlike tanımlama ve risk yönetimi

İşletme veya etkinlik tipi	*Genel tehlike*	*Tehlikenin belirti bileşenleri*	*Tehlike ile ilgili sonuçlar*	*Emniyet risklerinin kontrolü için mevcut savunmalar ve emniyet riski indeksi*	*Emniyet risklerinin azaltılması için ek eylemler ve sonuçta ortaya çıkan emniyet riski indeksi*	*Sorumlu kişi*
Uçuş operasyonları	Karmaşık bir coğrafyada bulunan yüksek rakımdaki bir havaalanında işletme.	a) Çevre dağlar. b) Yüksek rakımlı havaalanı. c) Yaklaşma ve iniş seyrüsefer yardımcılarının bulunmaması. d) Görsel iniş desteklerinin bulunmaması. e) Kesişen trafik. f) Islandığında kayganlaşan pist. g) Vahşi yaşam.	a) Aşağıdakiler nedeniyle arazide kontrollü uçuş (CFIT): 1) yaklaşma ve iniş sırasında kritik motor kaybı; 2) V1'den sonra kalkış sırasında kritik motor kaybı; 3) rota üzerindeki tırmanma sırasında kritik motor kaybı; b) Havada çarpışma. c) İnişten sonra emniyet pistine çıkış. d) Kalkışın iptal edilmesinden sonra emniyet pistine çıkış. e) Kuşlarla çarpışma. *Not— Bu tatbikatta sadece V1'den sonra kalkış sırasında kritik motor kaybı nedeniyle arazide kontrollü uçuş sonucu ele alınmıştır. Gerçek değerlendirmede, tüm sonuçlar analiz edilmeli ve tüm emniyet riskleri değerlendirilmeli ve azaltılmalıdır.*	a) VMC ve gündüz uçak işletmesi. b) ulusal AIP'de bulunan havaalanı yerleşimi. c) havaalanında bulunan ATC prosedürleri. d) şirket operasyon el kitabı. e) Dağıtım performansı el kitabı. f) Uçak çalıştırma el kitabı. g) V1 öncesinde ve sonrasında motor arızası ve kaçırılan yaklaşma prosedürleri hakkında tekrarlanan eğitim. h) CRM eğitimi. Emniyet riski indeksi: 3A Emniyet riski tahammül edilebilirliği: Mevcut koşullarda kabul edilemez.	a) Karaya dönüş olasılığını da değerlendirerek, V1'den sonra kritik bir motor kaybı durumunda kalkış ve tırmanma prosedürlerinin geliştirilmesi. b) Yukarıdaki prosedürler hakkında eğitimin geliştirilmesi ve verilmesi (tam uçuş simülatörü ve her altı ayda bir kalifikasyonların yenilenmesi). c) Andes City Uluslararası Havaalanı'nın, yenilenmediği sürece sadece bir yıl geçerli olacak şekilde özel ekip kalifikasyonu gerektiren "özel havaalanı operasyonu" olarak değerlendirilmesi. d) Kabin ekiplerine uygun "özel havaalanı operasyonu" verilmesi. (Bu azaltma işlemi emniyet riskinin bir sonucuna ait olasılığa değil de, ciddiyetine – acil durumda tahliye - yöneliktir.) e) Özellikle, saat 16:00'dan sonra yüzey rüzgarları hakkında doğru hava durumu bilgilerinin sağlanması. f) İşletme dokümantasyonunun geliştirilmesi ve CAA tarafından onaylanmak üzere şirket operasyon el kitabı ve dağıtım el kitabına eklenmesi. g) Açık bir minimum donanım listesi (MEL) kritik öğe politikasının yasaklanması. h) Bakım güvenilirliği programı altında, bakım departmanı işletmeye ayrılmış uçağın motorunu gözden geçirmelidir.	İşletmeler direktörü Eğitim yöneticisi Eğitim yöneticisi Eğitim yöneticisi Dağıtım yöneticisi Operasyonlar direktörü Bakım direktörü Bakım direktörü

İşletme veya etkinlik tipi	*Genel tehlike*	*Tehlikenin belirli bileşenleri*	*Tehlike ile ilgili sonuçlar*	*Emniyet risklerinin kontrolü için mevcut savunmalar ve emniyet riski indeksi*	*Emniyet risklerinin azaltılması için ek eylemler ve sonuçta ortaya çıkan emniyet riski*	*Sorumlu kişi*
					i) Andes City Uluslararası Havaalanı'ndaki işletmeyle ilgili emniyet risklerinin kontrolü ve azaltılması için uygulanan emniyet önlemleri ve yeni savunmaların izlenmesi. Savunmaların etkililiğinin, değişiklikler uygulandıktan ve CAA tarafından onay verildikten 6 ve 12 ay sonra gözden geçirilmesi planlanmaktadır. Emniyet riski indeksi: 2A Emniyet riski tahammül edilebilirliği: Riskin azaltılması temelinde kabul edilebilir. Yönetim kararı gerektirebilir.	İşletmeler direktörü

Bölüm 6

ICAO EMNİYET YÖNETİMİ SARP'LERİ

6.1 HEDEF VE İÇERİKLER

Bu bölümde Annex 1 — *Personele Lisans Verilmesi*, Annex 6 — *Uçakların İşletilmesi*, Annex 8 — *Uçakların Uçuşa Elverişliliği*, Annex 11 — *Hava Trafiği Hizmetleri*, Annex 13 — *Uçak Kazaları ve Olaylarının İncelenmesi* ve Annex 14 — *Havaalanları* bölümlerinde bulunan ICAO emniyet yönetimi SARP'leri sunulmaktadır. Bu bölüm aynı zamanda Devlet emniyet programı (SSP) ile hizmet sağlayıcının emniyet yönetimi sistemi arasındaki ilişkiyi de göstermektedir. Bu bölüm aşağıdaki konuları içerir:

a) ICAO emniyet yönetimi SARP'leri – Genel;

b) Devlet emniyet programı (SSP);

c) Kabul edilebilir emniyet seviyesi (ALoS);

d) Emniyet yönetimi sistemi (SMS);

e) SMS emniyet performansı;

f) Yönetimin hesap verme sorumluluğu;

g) SSP ile SMS arasındaki ilişki ve

h) Uyum ve performans.

6.2 ICAO EMNİYET YÖNETİMİ SARP'LERİ – GENEL

6.2.1 ICAO emniyet yönetimi SARP'leri Annex 1; Annex 6, Kısım I ve III; Annex 8; Annex 11; Annex 13 ve Annex 14'te yer alır. Bu Ekler onaylı eğitim örgütlerinin, uluslararası uçak operatörlerinin, onaylı bakım örgütlerinin, uçak tip tasarımı ve/veya üretiminden sorumlu örgütler, hava trafik hizmeti sağlayıcıların ve sertifikalı havalimanlarının etkinlikleri ile ilgilidir. Annex 1 örneğinde, emniyet yönetimi SARP'leri sadece hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütleri ile sınırlıdır.

6.2.2 Emniyet yönetimi SARP'leri iki hedef gruba yöneliktir: Devletler ve hizmet sağlayıcılar. Bu el kitabının bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Dolayısıyla, bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havalimanlarını kapsar.

6.2.3 ICAO emniyet yönetimi SARP'leri üç farklı gerekliliklere yöneliktir:

a) Bir SSP'nin kabul edilebilir emniyet seviyesi dahil olmak üzere, devlet emniyet programı (SSP) ile ilgili gereklilikler;

b) SMS'nin emniyet performansı dahil olmak üzere, emniyet yönetimi sistemi (SMS) ile ilgili gereklilikler;

c) Hizmetlerin sunulması sırasında emniyetin yönetimi karşısında yönetimin hesap verme sorumluluğu ile ilgili gereklilikler.

6.2.4 ICAO emniyet yönetimi SARP'leri, kabul edilebilir emniyet seviyesi (ALoS) kavramını Devlet tarafından oluşturulan ve bir SSP tarafından güvence sağlanan minimum emniyet derecesinin ifade edilmesinin yöntemi ve emniyet performansı kavramını bir hizmet sağlayıcının ve SMS'sinin emniyet performansını ölçme yöntemi olarak sunar.

6.3 DEVLET EMNİYET PROGRAMI (SSP)

6.3.1 Annex 1, 6, 8, 11, 13 ve 14'te, sivil havacılıkta kabul edilebilir bir emniyet seviyesi elde edilmesi için Devletler tarafın bir Devlet emniyet programı (SSP) oluşturulması gerekliliği yer almaktadır. Bir SSP, emniyetin Devlet tarafından yönetilmesi için bir Emniyet yönetimi sistemidir.

6.3.2 Bir SSP emniyetin geliştirilmesini hedefleyen, bütünleşik bir dizi düzenleme ve etkinlik olarak tanımlanır. Devlet tarafından yerine getirilmesi gereken belirli emniyet etkinliklerini ve Devlet içindeki havacılık etkinliklerinin emniyetli ve etkin şekilde yapılması ile ilgili sorumluluklarını yerine getirmesine destek olmak için Devlet tarafından yürürlüğe sokulan düzenleme ve yönergeleri içerir.

6.3.3 SSP'lerinin oluşturulmasında Devletlere yardımcı olmak için, ICAO bir SSP'nin hem bileşenlerini hem de unsurlarını içeren bir çerçeve geliştirmiştir. Çerçeve dört bileşen ve on bir unsurdan oluşur ve tam haliyle Bölüm 11'de açıklanmıştır. SSP kapsamında yer alan sorumluluklar yeni değildir. Çoğu Devletin zaten bu sorumlulukları yerine getiriyor olması makul bir beklentidir. SSP kavramında yeni olan, bir Devletin emniyetle ilgili sorumluluklarının ve hesap verme sorumluluklarının ilkeli ve sağlam bir şekilde düzenlenmesi ve Devlet tarafından emniyet sorumluluklarının ve emniyetle ile ilgili hesap verme sorumluklarının yerine getirilmesinin etkililik seviyesinin ölçülmesi için bir yöntem önerilmesidir. Belirli ilkelere uyan ve bir standart yapısını izleyen bir Devletin emniyet sorumluluklarının ve emniyetle ile ilgili hesap verme sorumluklarının düzenlenmesi, emniyeti geliştirmeyi amaçlayan düzenlemelerin ve etkinliklerin belgelenmesini, açık ve izlenebilir olmasını sağlar. Bir SSP'nin uzun vadedeki, stratejik hedefi Devlet içinde emniyetin iyileştirilmesi olsa da, bir SSP'nin örgütü iki kısa vadeli, taktik hedefe yönelir: Devlet tarafından emniyet sorumluluklarının ve emniyetle ile ilgili hesap verme sorumluklarının etkili ve etkin bir şekilde yerine getirilmesi ve emniyet sorumluluklarının ve emniyetle ile ilgili hesap verme sorumluklarının Devlet tarafından etkin bir denetlenmesi.

6.3.4 İkinci hedefin, yani emniyet sorumluluklarının ve emniyetle ile ilgili hesap verme sorumluklarının Devlet tarafından etkin bir denetlenmesi hedefinin önemi hafife alınmamalıdır. Günümüzde, ICAO Evrensel Emniyet Denetimi Programı (USOAP) Devletlerin emniyet sorumluluklarını kapsamlı bir şekilde denetlemektedir, ancak Uluslararası Sivil Havacılık Konvansiyonunun Annexlerinde önerilen temel bir mimariyi izlemektedir. Bir devletin emniyeti denetleme işlevinin izlemesi gereken kritik unsurlar tanımlanmıştır ve USOAP denetimleri unsurların ve işlevlerin uygulanma durumunu, uygun olma/uygun olmama temelinde doğrulamaktadır. SSP kavramı olgunluğa ulaştığında ve Devletler tarafından uygulanmaya başlandığında, USOAP'ın SSP'yi sürekli izleme konsepti temelinde bir yaklaşımla, emniyet denetimi işlevinin unsurlarına bağlı olmak yerine, bütüncül bir şekilde denetleyeceği öngörülmektedir.

6.3.5 SSP kavramı aynı zamanda orta vadeli üçüncü bir hedef de içerir: ağırlıklı olarak kural koyucu bir düzenleme ortamından kural koyucu ve performans temelli düzenleme yaklaşımlarını birleştiren bütünleşik bir düzenleme ortamına geçiş. Bu geçişte, hem SSP'nin hem de SMS'nin emniyetin güvence altına alınması bileşeni üzerinde inşa edilen ve bu bölümde daha sonra ele alınan, bir SSP'nin ve bir SMS'nin emniyet performansının ALoS'u kavramı temel önemdedir. Ancak, bu geçiş Devletin emniyet denetimi işlevinin SSP içindeki rolünün ve karşılıklı ilişkilerinin açıkça ortaya konması ile başlamalıdır. Kısa bir açıklama verilmiştir.

6.3.6 Bir Devletin emniyet denetimi işlevi bir SSP'nin parçası ve emniyetin güvence altına alınması bileşeninin temel bir bileşenidir. Devletin emniyet denetimi işlevinin hedeflerine, geleneksel olarak yapıldığı gibi, sivil havacılık yetkililerinin düzenli olarak gerçekleştirdiği yönetimsel kontroller (denetimler, denetlemeler ve araştırmalar) aracılığıyla ulaşılır ve Bölüm 5 ve Bölüm 6.8'de ele alındığı gibi emniyet riski kontrollerinden oluşması gerekmez.

b) ***emniyet seviyesi*** bir sistemin emniyet derecesidir. Sistemin, emniyet bakımından kalitesini temsil eden, görünür hale gelen özelliğidir. Emniyet göstergeleri aracılığıyla ifade edilir;

c) ***emniyet göstergeleri*** sistemin emniyet seviyesini karakterize eden ve/veya tipini belirleyen parametrelerdir;

d) ***emniyet hedefleri*** emniyet seviyesinin somut hedefleridir;

e) **kabul edilebilir emniyet seviyesi** gerçekten uygulanmakta olan bir sistem tarafından sağlanması gereken minimum emniyet derecesidir.

f) ***emniyet göstergesi değeri*** emniyet göstergesinin nicelleştirilmesidir ve

g) ***emniyet hedefi değeri*** emniyet hedefinin nicelleştirilmesidir.

6.4.7 Uygun emniyet göstergelerinin seçilmesi ALoS'un geliştirilmesinin anahtarıdır. Bu seçim, sistemin emniyet seviyesinin temsil edilmesi istenen ayrıntı derecesinin bir işlevi olmalıdır. Emniyet seviyesi geniş, genel bir şekilde temsil edilecekse, yüksek seviyeli/yüksek sonuçlu sistem sonuçlarını (nicel) ve/veya yüksek seviyeli sistem işlevlerini (nitel) temsil eden emniyet göstergelerinin seçilmesi uygundur. Sistemin emniyet seviyesi belirli, dar bir kapsamda temsil edilecekse, düşük seviyeli/düşük sonuçlu sistem sonuçlarını ve/veya düşük seviyeli sistem işlevlerini temsil eden emniyet göstergelerinin seçilmesi uygundur. Her iki durumda, anlamlı emniyet göstergeleri sistem emniyetini karakterize eden sonuçları, süreçleri ve işlevleri temsil etmelidir.

6.4.8 Başka örneklerin yanında, havacılık sistemindeki emniyet göstergelerinin tipik örnekleri aşağıda verilmiştir:

a) ölümcül havayolu kazaları;

b) ciddi olaylar;

c) pistten çıkma olayları;

d) yerde çarpışma olayları;

e) ana havacılık mevzuatının geliştirilmesi/eksikliği:

f) operasyon mevzuatının geliştirilmesi/eksik olması ve

g) düzenlemelere uyum seviyesi.

6.4.9 Başka örneklerin yanında, havacılık sistemindeki emniyet hedeflerinin tipik örnekleri aşağıda verilmiştir:

a) ölümcül havayolu kazalarının azaltılması;

b) ciddi olayların azaltılması;

c) pistten çıkma olaylarının azaltılması;

d) yerde çarpışma olaylarının azaltılması ve

e) üç ayda bir tamamlanan denetimlerin sayısı.

6.4.10 Bu nedenle bir SSP ile ilgili bir ALoS'un geliştirilmesinde ilk adım, söz konusu Devletin havacılık sisteminin emniyet seviyesinin temsil edilmesi istenen ayrıntı derecesine karar verilmesi, ardından Devletin havacılık sisteminin emniyet seviyesini karakterize eden ve tipini belirleyen anlamlı emniyet göstergelerini seçmektir.

Emniyet verilerinin Devlet tarafından erişilebilir olması temsilin ayrıntı derecesine karar verilmesinde ve nitel veya nicel emniyet göstergelerinin seçilmesinde belirleyici etkendir. Emniyet verileri toplama ve analizi yeteneklerini geliştirmiş olan Devletler, geliştirmemiş olanlara göre emniyet seviyesinin daha ayrıntılı bir şekilde temsil edilmesini sağlayacak konumda olacaklardır. İlk gruptaki devletler nicel emniyet göstergeleri tanımlayabileceklerdir, ikinci gruptakiler ise emniyet verileri toplama ve analizi yeteneklerini geliştirirken, başlangıçta nitel emniyet göstergelerini ön planda tutmayı seçebilirler. Emniyet göstergeleri tanımlandıktan sonra, bir sonraki adım iyileştirme hedefleri olarak düşünülebilecek ilgili emniyet hedeflerinin tanımlanması olacaktır.

6.4.11 Emniyet göstergeleri ve emniyet hedefleri seçildikten sonra, söz konusu Devletin havacılık sistemini temsil eden emniyet seviyesi oluşturulabilir. Bu noktada, Devlet sivil havacılıktaki SSP tarafından gerçek uygulamada sağlanması gereken *minimum* emniyet derecesi olan ALoS'un geliştirilmesine geçmeye hazır olmalıdır. ALoS'u geliştirmek için, emniyet göstergelerine değer verilmelidir ve bu değerlerin iyileştirilmesi ve/veya sürdürülmesi ile ilgili hedefler emniyet hedeflerine bağlanmalıdır. Bir SSP ile ilgili ALoS'un emniyet göstergesi değerleri ve emniyet hedefi değerleri aracılığıyla ifade edildiği genel olarak kabul edilse de, aslına bakılırsa ALoS'un gerçek ifadesi emniyet hedefi değerleridir. Şekil 6-1'de emniyet göstergesi değerleri ve emniyet hedefi değerlerinin bir örneği bulunmaktadır. ALoS oluşturulurken aşağıdakilere de dikkat edilmesi gerekir:

a) geçerli emniyet riski seviyesi;

b) emniyet riski toleransı;

c) havacılık sistemindeki iyileştirmelerin maliyetleri/yararları ve

d) sivil havacılık sistemiyle ilgili kamu beklentileri.

Emniyet göstergesi değeri	Emniyet hedefi değeri
1. *[rakam]* operasyon başına ölümcül havayolu kazası *[Oran/rakam]*	→ 1. *[rakam]* operasyon başına ölümcül havayolu kazası sayısına *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* ölümcül havayolu kazası sayısı
2. *[rakam]* operasyon başına pistten çıkma olayı *[Oran/rakam]*	→ 2 *[rakam]* operasyon başına pistten çıkma olayı sayısına *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* pistten çıkma olayı sayısı
3. *[rakam]* operasyon başına yerde çarpışma olayı *[Oran/rakam]*	→ 3 *[rakam]* operasyon başına yerde çarpışma olayı sayısına *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* yerde çarpışma olayı sayısı
4. *İşletmelerin tamamladığı [zaman aralığı]* denetim sayısı *[rakam]*	→ 4 *Tamamlanan [zaman aralığı]* minimum denetim sayısı *[rakam]*

Şekil 6-1. Emniyet göstergesi değerleri ve emniyet hedefi değerleri örneği.

6.4.12 Bir SSP iie ilgili ALoS'un doğru şekilde geliştirilmesi için, iki yakından ilişkili – ve bu nedenle bazen kafa karıştırıcı olabilen – ama son derece ayrı konseptin arasındaki farkın anlaşılması da önemlidir: emniyet ölçümü ve emniyet performansı ölçümü.

6.4.13 ***Emniyet ölçümü*** kaza ve ciddi olay oranları gibi seçilen yüksek seviyeli, yüksek sonuçlu olayların sonuçlarının nicelleştirilmesini ifade eder. Emniyet ölçümü, ana havacılık emniyeti mevzuatının geliştirilme/uygulama durumu ve bu mevzuatın eksikliği, belirli operasyon düzenlemelerinin geliştirilme/uygulama durumu ve bu düzenlemelerin eksikliği ve Devlet içinde düzenlemelere uyum seviyesi gibi seçilen yüksek seviyeli Devlet işlevlerinin nicelleştirilmesine de uygulanabilir. Emniyet ölçümü sürekli bir süreç değil, aksine normalde örneğin yıllık, altı aylık veya üç aylık gibi önceden belirlenmiş zaman aralıklarında gerçekleştirilen bir nokta kontrolüdür. Emniyet ölçümü SSP ile ilişkilidir ve azaltma stratejilerine ait emniyet müdahalelerinin yüksek seviyeli emniyet hedeflerine ne derecede ulaşıldığını gösterir.

6.4.14 ***Emniyet performansı ölçümü*** belirli sayıdaki apron operasyonu başına yabancı madde (FOD) olayı sayısı veya belirli sayıda havaalanı operasyonları başına veya belirli bir zaman aralığı içinde taksi yollarında yetkili olmayan yer aracı girişi olayı sayısı gibi seçilen düşük seviyeli, düşük sonuçlu süreçlerin nicelleştirilmesini ifade eder. Emniyet performansı ölçümü, bir örgüt tarafından örgütün vermek üzere kurulduğu hizmetlerin verilmesi için zorunlu olan, seçilen operasyonel etkinliklerin sürekli olarak izlenmesi ve ölçümünü içeren sürekli bir etkinliktir. Emniyet performansı ölçümü, tamamen olmasa da, çoğunlukla bir SMS ile ilgilidir ve bir SSP veya SMS gibi bir yönetim sisteminin, emniyet ölçümünden (düzenlemelere uyum dahil olmak üzere) kaynaklanan mutlak ölçümlerin ötesinde, gerçek operasyonel performansın bir ölçümünü sağlar. Aynı zamanda, bir SSP'nin parçası olarak oluşturulan emniyet müdahaleleri ve azaltma stratejileri için de geçerlidir.

6.4.15 Bir SSP ile ilgili ALoS emniyet yönetimi ile emniyet performansı ölçümünün makul bir kombinasyonu temelinde geliştirilmelidir. ALoS'un emniyet ölçümünü veya emniyet performansını ne derecede temsil ettiği SSP'nin olgunluğuna bağlıdır. Başlangıçta, bir SSP'nin geliştirilmesi ve uygulanmasından hemen sonra, ALoS ile ilgili emniyet göstergesi değerleri ve emniyet hedef değerleri büyük olasılıkla seçilen yüksek seviyeli/yüksek sonuçlu neticeler (emniyet ölçümü) hakkında nicel eylem bildirimleri aracılığıyla ifade edilecektir. Şekil 6-2'de emniyet ölçümünü temel alan emniyet göstergesi değerleri ve emniyet hedefi değerlerinin bir örneği bulunmaktadır.

6.4.16 SSP olgunlaştıkça ve SSP'nin emniyetin güvence altına alınması bileşeni aracılığıyla emniyet verileri toplama ve analizi becerileri geliştirildikçe, ALoS ile ilgili emniyet göstergesi değerleri ve emniyet hedefi değerleri seçilen yüksek seviyeli/yüksek sonuçlu olaylar (emniyet ölçümü) ile ilgili nicel eylem bildirimleri ve seçilen düşük seviyeli/düşük sonuçlu olaylar (emniyet performansı ölçümü) ile ilgili nicel eylem bildirimlerinin bir kombinasyonu aracılığıyla değiştirilebilir ve ifade edilebilir. SSP'nin olgunluğa ulaştıkça, ALoS ile ilgili emniyet göstergesi değerleri ve emniyet hedef değerleri büyük olasılıkla seçilen düşük seviyeli/düşük sonuçlu neticeler (emniyet performansı ölçümü) hakkında nicel eylem bildirimleri aracılığıyla ifade edilecektir. Şekil 6-3'te emniyet performansı ölçümünü temel alan emniyet göstergesi değerleri ve emniyet hedefi değerlerinin bir örneği bulunmaktadır.

6.4.17 ALoS'un belirli emniyet hedefi değerlerinin ilgili emniyet göstergesi değerlerine göre iyileştirme mi, yoksa bu değerlerin sürdürülmesini mi gerektirdiğini değerlendirirken iki genel yön dikkate alınmalıdır. Önce, ele alınan iyileştirmenin elde edilmesi için Devlet içinde kaynakların bulunup bulunmadığı dikkate alınmalıdır. İkinci olarak, iyileştirmenin elde edilmesi için gerekli görülen eylem plan(lar)ının ne kadar pahalı olduğu dikkate alınmalıdır. Sadece emniyet performansı ölçümü temelinde emniyet hedefi değerlerine uygulanabilir olacak şekilde, dikkate alınması gereken üçüncü bir nokta, iyileştirme ile ele alınan tehlikenin sonuçlarına ait emniyet risklerinin değerlendirilmesinin Bölüm 5'te ele alınan emniyet riski yönetimi sürecinin tahammül edilebilir alanına düşüp düşmediğinin belirlenmesidir. Emniyet hedefi değerleri bir noktada mevcut koşullar altında tahammül edilebilir alana giren bir emniyet riski değerlendirmesini yansıtabilir. Ancak, sistemdeki değişiklikler, büyüme v.s. bu emniyet riski değerlendirmesini geçersiz kılabilir. Bu durumda, emniyet hedefi değeri, ilgili emniyet göstergesi değerinin değişen ortamda geçerli olmasını sağlayacak bir iyileştirmeyi yansıtmalıdır.

Emniyet göstergesi değeri	Emniyet hedefi değeri
1. *[rakam]* gidiş başına CFIT yaklaşma ve iniş kazaları *[rakam]*	1. *[rakam]* operasyon başına CFIT yaklaşma ve iniş kazası sayısına *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* ölümcül havayolu kazası sayısı
2. *[rakam]* operasyon başına pistten çıkma sayısı *[rakam]*	2. *[rakam]* operasyon başına pistten çıkma sayısına *[rakam] göre azalma / [rakam]* operasyon başına maksimum *[rakam]* pistten çıkma olayı sayısı
3. *[x yıl]* ortalamasında yıl başına yerde çarpışma kazaları sayısı *[rakam]*	3. *[x yıl]* ortalamasında yıl başına yerde çarpışma kazası sayısına *[rakam] göre azalma /* maksimum *[rakam]* yerde çarpışma olayı sayısı
4. *Devlet MOR'u aracılığıyla yıllık olarak yakalanan yüksek ciddiyetli olaylar [rakam]*	4. Devlet MOR'u aracılığıyla yıllık olarak yakalanan minimum yüksek ciddiyetli olay sayısı [rakam]
5. *Üç ayda bir operatörlerin tamamladığı* denetim sayısı *[rakam]*	5. *Üç ayda bir operatörlerin tamamladığı minimum* denetim sayısı *[rakam]*
6. QMS uygulanan AIS tesislerinin sayısı *[rakam]* sayısı *[rakam]*	6. [Zaman] aralığında QMS uygulanan AIS tesislerinin
7. *[rakam]* ay/hafta içinde tamamlanan farkların elektronik olarak dosyalanması	7. *[gözden geçirilen rakam]* ay/hafta içinde tamamlanan farkların elektronik olarak dosyalanması

Şekil 6-2. Emniyet ölçümü temelinde emniyet göstergesi değerleri ve emniyet hedefi değerleri örneği

Emniyet göstergesi değeri	Emniyet hedefi değeri
1. *[rakam]* operasyon başına seviye sapmaları *[rakam]* sayısına	1. *[rakam]* operasyon başına seviye sapması *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* seviye sapması sayısı
2. *[rakam]* operasyon başına 5 uluslararası *[Devlet]* havaalanında Kategori B ve C piste giriş olayı sayısı *[rakam]*	2. *[tarih]* aralığına göre 5 uluslararası *[Devlet]* havaalanında Kategori B ve C piste giriş olayı sayısına *[rakam] göre azalma / m*aksimum *[rakam]* Kategori B ve C piste giriş olayı sayısı
3. *[rakam]* operasyon başına TCAS/havada tehlike yaklaşma olayı sayısı *[rakam]*	3. [tarih] aralığına göre TCAS/havada tehlikeli yaklaşma olayı sayısına [rakam] göre azalma / maksimum [rakam] TCAS/havada tehlikeli yaklaşma olayı sayısı
4. *[rakam]* operasyon başına 5 uluslararası *[Devlet]* havaalanında uygun olmayan yaklaşma sayısı *[rakam]*	4. [tarih] aralığına göre 5 uluslararası [Devlet] havaalanında uygun olmayan yaklaşma sayısına [rakam] göre azalma / maksimum [rakam] uygun olmayan yaklaşma sayısı
5. *[rakam]* operasyon başına 5 uluslararası *[Devlet]* havaalanında apron FOD olayı sayısı *[rakam]*	5. [tarih] aralığına göre 5 uluslararası [Devlet] havaalanında apron FOD olayı sayısına [rakam] göre azalma / maksimum [rakam] uygun olmayan yaklaşma sayısı

Şekil 6-3. Emniyet performansı ölçümü temelinde emniyet göstergesi değerleri ve emniyet hedefi değerleri örneği

6.4.19 ALoS eylem planları aracılığıyla sağlanır. Bunlar, bir SSP ile ilgili ALoS'un emniyet hedef değerlerini elde etmek için gerek duyulan araçlar ve yöntemlerdir. Eylem planları güvenilirlik, bulunma, performans ve/veya hassasiyetle ilgili önlemlerin belirlenebileceği operasyonel prosedürler, teknoloji, sistemler ve programları içerir. Arazide kontrollü uçuş (CFIT) kazalarında azalmayla ilgili bir emniyet hedefi için bir eylem planı örneği, sabit alçalmalı iniş prosedürlerinin ve dengeli yaklaşmalar için tasarlanmış iniş prosedürlerinin uygulanması olabilir. Piste giriş olaylarında azalmayla ilgili bir emniyet hedefi için bir eylem planı örneği, kritik donanımın %98 çalışır durumda olmasının beklendiği bir radar sisteminin kullanılmaya başlaması olabilir.

6.4.20 ALoS kavramının, SSP'nin tatmin edici şekilde uygulanıp uygulanmadığının doğrulanması için bir araç olarak, SSP aracılığıyla elde edilebilecek ulusal veya Devlet seviyesinde hedeflere atıfta bulunduğu vurgulanmalıdır. Bu nedenle, daima bir SSP ile ilgili olarak kabul edilebilir emniyet seviyesine referansta bulunulmalıdır. Bir ALoS'un emniyet göstergesi değerleri ve emniyet hedef değerleri, düzenlemelere uyumun ötesinde, bir SSP'nin etkililiğinin sağlanması ve gösterilmesi için ölçülebilir bir yöntem sağlarlar. Bir SSP ulusal ve uluslararası düzenlemeler tarafından getirilen düzenlemeye yönelik tüm gereklilikleri karşılamalıdır. Düzenlemelere uyum hala emniyet yönetiminin temelinde bulunmaktadır. Devlete özel olan ve düzenlemelere uyum tarafından sağlanan temel üzerinde inşa edilen ölçülebilir performans sonuçlarından oluşan bir kombinasyon seçilerek, bir SSP'nin altında yatan emniyet yönetimi süreçlerinin gerçek etkinliği ve etkililiği sağlanabilir.

6.4.21 Bir ALoS'un uygulanması düzenlemelerde ulusal ve uluslararası gerekliliklere uyumun ötesindedir. Bir SSP için bir ALoS oluşturulması, hukuki, düzenlemelere ait veya diğer yerleşik gerekliliklerin yerine geçmez, yine Devletlerin *Uluslararası Sivil Havacılık Konvansiyonu* (ICAO Doc 7300) ve Konvansiyonun annexlerinde bulunan ilgili hükümlerde yer alan yükümlülüklerini ortadan kaldırmaz.

6.4.22 ALoS'un ele alınmasında bir sonuç olarak, Şekil 6-4, 6-5 ve 6-6'da bu bölümde ele alınan şekilde, başlangıç aşamasından bir SSP ile ilgili olgun ALoS'a geçiş, emniyet ölçümünü yansıtan ALoS ve ilgili SMS'lerin emniyet performansı ölçümünü yansıtan ALoS grafik olarak özetlenmektedir.

6.5 EMNİYET YÖNETİMİ SİSTEMİ (SMS)

6.5.1 Annex 1, 6, 8, 11, 13 ve 14'te, Devletlerin SSP'lerinin bir parçası olarak, hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerinin, uçak operatörlerinin, onaylı bakım örgütlerinin, uçak tip tasarımı ve/veya üretiminden sorumlu örgütlerin, hava trafik hizmeti sağlayıcılarının ve sertifikalı havalimanlarının bir emniyet yönetimi sistemi (SMS) uygulamasını zorunlu kılması şartı getirilir. Bir SMS, emniyetin bir örgüt tarafından yönetilmesi için bir yönetim aracıdır. Annexlerde ayrıca, SMS'nin Devlet tarafından kabul edilmesini ve en azından aşağıdakileri sağlamasını şart koşulur:

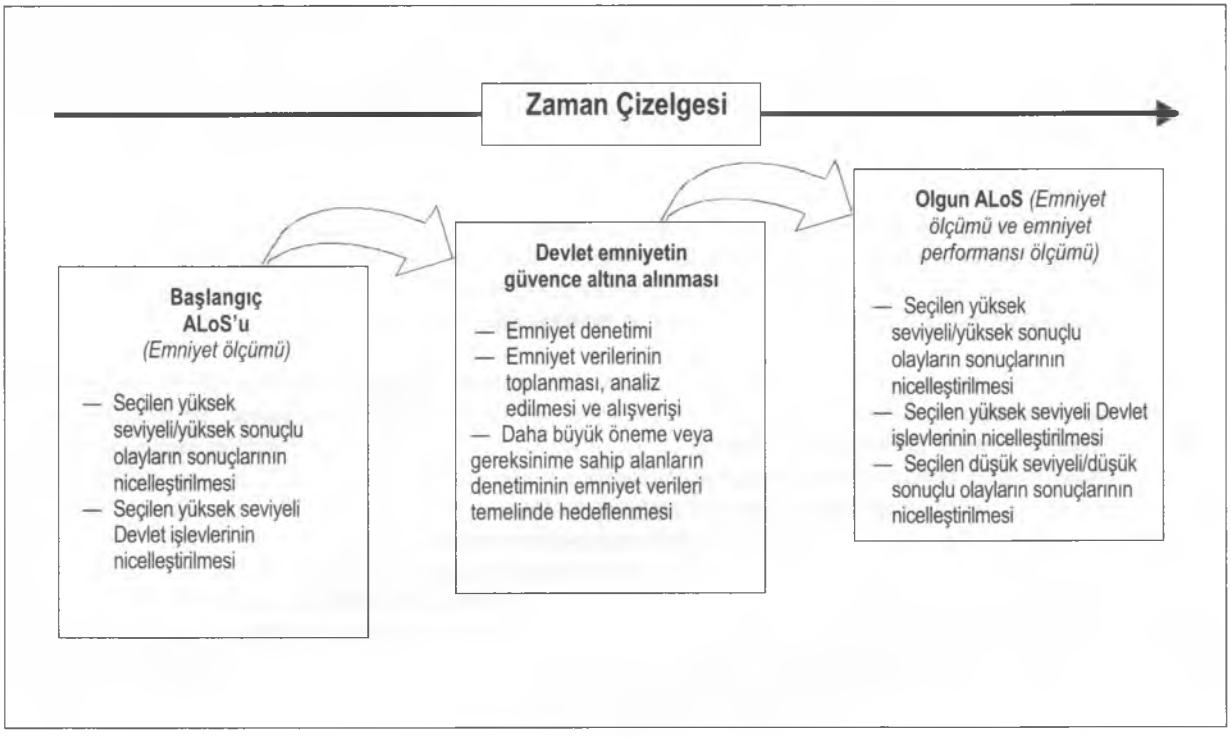
a) emniyet tehlikelerinin tanımlanması;

b) üzerinde uzlaşılan emniyet performansının sürdürülmesi için gerekli olan düzeltme eyleminin uygulanmasının sağlanması;

c) emniyet performansının sürekli olarak izlenmesinin ve düzenli olarak değerlendirilmesinin sağlanması ve

d) emniyet yönetimi sisteminin genel performansının sürekli olarak iyileştirilmesinin hedeflenmesi.

6.5.2 Yukarıda açıklanan ICAO SMS gerekliliklerinde yer alan dört genel süreç (tehlikelerin tanımlanması, tehlikelerin sonuçlarına ait emniyet risklerinin ele alınması için düzeltme eyleminin uygulanması, sürekli izleme ve sürekli iyileştirme) bir örgüt tarafından hizmetlerin verilmesini destekleyen dört temel emniyet sorunu çözme etkinliğini kapsar:



Şekil 6-4. Başlangıçtaki ALoS'tan bir SSP ile ilgili olgun ALoS'a geçiş

a) neyin yanlış olduğunun belirlenmesi (tehlikenin tanımlanması);

b) bir çözüm veya çözümler önerilmesi ve uygulanması (çözüme yönelik eylem);

c) önerilen çözüm veya çözümlerin istendiği gibi çalıştığından emin olunması (sürekli izleme) ve

d) hizmetlerin sunulmasında etkinliğin ve etkililiğin sağlanması için yönetim sisteminin sürekli olarak iyileştirilmesi (SMS'nin sürekli olarak iyileştirilmesi).

6.5.3 Bir SMS gerekli örgüt yapıları, hesap verme sorumlulukları, politikalar ve prosedürler de dahil olmak üzere emniyetin yönetimine sistematik bir yaklaşım olarak tanımlanır. Bir SMS'nin temel noktaları Bölüm 7'de ele alınmaktadır. SSP'de olduğu gibi, bir SMS'nin uygulanmasında hizmet sağlayıcılara yardımcı olmak için ICAO bir SMS çerçevesi geliştirmiştir. Çerçeve dört bileşen ve on iki unsurdan oluşur ve tam haliyle Bölüm 8 ve Bölüm 9'da açıklanmıştır.

6.6 SMS EMNİYET PERFORMANSI

6.6.1 Annex 1, 6, 8, 11 ve 14'te, bir hizmet sağlayıcının SMS'sinin emniyet performansının korunması için düzeltme eylemlerini sağlaması ve bu emniyet performansını sürekli olarak izlemesi ve düzenli olarak değerlendirmesi şart koşulmaktadır.

6.6.2 Emniyet performansı kavramı SMS'nin etkili bir şekilde işletmesinin olduğu gibi, performans temelli bir düzenleme ortamına doğru ilerlemenin de önemli bir parçasıdır. SMS'nin gerçek performansının izlenmesine ve sadece "uygun kutucukları işaretlemek" ile yetinmekten kaçınmaya yardımcı olur.

Sistemin gerçekten tasarım özelliklerine göre çalışıp çalışmadığını – sadece düzenleme gerekliliklerini yerine getirmek değil – ve SMS'nin performansını tasarım beklentileri seviyesine getirmek için nerede harekete geçmek gerekeceğini belirlemek için, bir SMS'nin bir ölçülebilir sonuçlar kümesi tanımlaması gerekir. Bu ölçülebilir performans sonuçları emniyetle ilgili önemli etkinliklerin gerçek performansının mevcut örgüt kontrollerine değerlendirilmesine izin verir, böylece emniyet riskleri makul derecede düşük şekilde (ALARP) yürütülebilir ve gerekli düzeltme önlemleri alınabilir.

6.6.3 Performans temelli bir düzenleme yaklaşımı, mevcut örgüt kontrolleri karşısında emniyetle ilgili önemli etkinliklerin gerçek performanslarının değerlendirilmesini sağlar. Ayrıca, emniyet yönetiminin altında yatan emniyetin sürekli iyileştirilmesi hedefine, sadece SMS'nin etkili bir emniyet performansı göstermesinin güvencesi altına alınmasıyla — belirli emniyet performansı sonuçlarının oluşturulması ve ölçülmesiyle — erişilebilir.

6.6.4 Bir SMS'nin emniyet performansı sadece yüksek sonuçlu neticelerin nicelleştirilmesi (emniyet ölçümü) ile değildir, daha çok düşük sonuçlu süreçlerin nicelleştirilmesi (emniyet performansı ölçümü) ile ilgilidir. Bir SMS'nin emniyet performansı sadece emniyet performansı ölçümünü temsil eder. Emniyet performansı, bir hizmet sağlayıcının emniyet hedeflerini, SMS'nin belirli düşük seviyeli süreçlerinin ölçülebilir emniyet sonuçları biçiminde ifade eder. Devlet ile hizmet sağlayıcılar arasındaki ilişki perspektifinden, emniyet performansı Devlete hizmet sağlayıcılar temel operasyonel işlevleri yerini getirirken, hizmet sağlayıcıların SMS'sinin etkinliğini ve etkililiğini ölçmek için nesnel kanıtları sağlar. Bu tür emniyet performansı üzerinde, hizmet sağlayıcının hizmetlerin sunulması sırasında ulaşması gereken minimum kabul edilebilir değer olarak Devlet ve hizmet sağlayıcılar arasında uzlaşma sağlanmalıdır. Dolayısıyla, bir SMS'nin emniyet performansı Devletin SMS'nin emniyet performansını, SMS'nin düzenlemelere uyumun ne kadar ötesinde çalıştığını ölçmesini sağlayan bir referanstır. Bir SMS'nin emniyet performansını kabul ederken, geçerli emniyet riski seviyesi, sistemdeki iyileştirmelerin maliyeti/yararları ve havacılık sektörünün emniyeti ile ilgili kamuoyu beklentileri gibi etkenlerin dikkate alınması gerekir.

6.6.5 Her bir Devlet içinde, her bir SMS'nin emniyet performansı ile ilgili olarak Devlet ve havacılık örgütleri arasında ayrı ayrı anlaşmaya varılmalıdır. Üzerinde uzlaşılan emniyet performansı bir havacılık örgütün özel operasyonel bağlamların karmaşıklığına ve havacılık örgütün bunlara yönelik kaynaklarının bulunup bulunmadığına uygun olmalıdır. Uygulamada, bir SMS'nin emniyet performansı emniyet performansı gösterge değerleri ve emniyet performansı hedef değerleri ile ifade edilir ve eylem planları aracılığıyla uygulanır.

6.6.6 Emniyet performansı gösterge değerleri bir SMS'nin emniyet performansını yansıtan kısa vadeli, ölçülebilir hedeflerdir. Sayısal olarak ifade edilirler; açık, ölçülebilir ve bir SMS'nin emniyet sorunları ile bağlantılı olmalıdırlar. Emniyet performansı gösterge değerleri sadece emniyet performansı ölçümünü yansıtır. Bir SMS'nin emniyet performansı gösterge değerleri emniyet ölçümünü yansıtmamalıdır. Her bir SMS'nin emniyet performansı üzerinde Devlet ile her bir havacılık örgütü arasında ayrı olarak uzlaşılması gerektiğinden, emniyet performansı gösterge değerleri, örneğin uçak operatörleri, onaylı havaalanı operatörleri ve ATS sağlayıcılar gibi havacılık sektörünün farklı segmentleri arasında değişir. Bir örnek verilmiştir.

6.6.7 SMS'si aracılığıyla, onaylı bir havaalanı operatörü, apron işletmelerinde yabancı nesne (FOD) ile ilgili emniyet konularını belirlemiştir. Aynı zamanda, taksi yollarındaki trafik veya yetkisiz araçların bu yollara girmesi ile ilgili emniyet konularını da belirlemiştir. Böylece, Devletin sivil havacılık denetim kurumu ile yapılan anlaşmaya uygun olarak aşağıdaki emniyet performansı gösterge değerlerini tanımlar: apronda 10000 işletmede bir 15 FOD olayı ve taksi yollarında 10000 işletmede bir 20 yetkisiz araç girişi olayı. Bu emniyet performansı gösterge değerleri 6.6.6'da ele alınan koşulları yerine getirir: sayısal olarak ifade edilirler; açık, ölçülebilir ve havaalanı SMS'sinin emniyet sorunları ile bağlantılıdırlar. Ayrıca, her iki emniyet performansı göstergesi emniyet performansı ölçümünü yansıtmaktadır.

6.6.8 Emniyet performansı hedef değerleri bir SMS'nin emniyet performansını yansıtan uzun vadeli, ölçülebilir hedeflerdir. Emniyet performansı hedef değerleri sayısal olarak ifade edilirler; açık, ölçülebilir, ilgili taraflar tarafından kabul edilebilir ve bir SMS'nin emniyet performansı göstergesi (kısa vadeli hedef) ile bağlantılı olmalıdırlar.

Emniyet hedefi değerleri	1. *[rakam]* gidiş başına CFIT ve yaklaşma ve iniş kazası sayısına *[rakam] göre azalma /* operasyon başına maksimum *[rakam]* ölümcül havayolu kazası sayısı 2. *Üç ayda bir operatörlerin tamamladığı minimum* inceleme sayısı *[rakam]* 3. ...
Eylem planları	1. Sektöre dağıtılan ve eğitim kursları tarafından desteklenen CFIT eğitim paketi. 2. İşe alma politikasının gözden geçirilmesi ve gerekirse güncellenmesi. İnceleme el kitabının güncellenmesi. 3. ...
Emniyet göstergesi değerleri	1. *[rakam]* gidiş başına CFIT ve yaklaşma ve iniş kazaları *[rakam]* 2. *Üç ayda bir operatörlerin tamamladığı* denetim sayısı *[rakam]* 3. ...
Devlet	Yürürlükteki tüm uluslararası standartlara uyacaktır.

Şekil 6-5. Emniyet ölçümünü yansıtan ALoS

Emniyet hedefi değerleri	1. *[tarih]* aralığına göre geliş *[rakam] başına* 5 uluslararası havaalanında uygun olmayan yaklaşma sayısına *[rakam] göre azalma / m*aksimum *[rakam]* uygun olmayan yaklaşma sayısı 2. *[tarih]* aralığına göre operasyon başına *[rakam]* 5 uluslararası *[Devlet]* havaalanında Kategori B ve C piste giriş olayı sayısına *[rakam] göre azalma / m*aksimum *[rakam]* Kategori B ve C piste giriş olayı sayısı 3. ...
Eylem planları	1. Uygulanan sabit alçalmalı iniş (CDA) prosedürleri. Dengeli yaklaşmalar için tasarlanmış geliş prosedürleri. 2. 5 uluslararası *[Devlet]* havaalanında ASDE/X kurulumu 3. ...
Emniyet göstergesi değerleri	1. *[rakam]* operasyon başına 5 uluslararası havaalanında uygun olmayan yaklaşma sayısı *[rakam]* 2. *[rakam]* operasyon başına 5 uluslararası *[Devlet]* havaalanında Kategori B ve C piste giriş olayı sayısı *[rakam]* 3. ...
Devlet	Yürürlükteki tüm uluslararası standartlara uyacaktır.

Şekil 6-6. Emniyet performansı ölçümünü yansıtan ALoS

6.6.9 6.6.7'de ele alınan örnek üzerinden devam edersek, havaalanı Devletin sivil havacılık denetim kurumu ile yapılan anlaşmaya uygun olarak aşağıdaki emniyet performansı hedef değerlerini tanımlar: 2009 Ocak'ına kadar, aprondakI FOD olaylarını 10000 işletmede bir 8'e indirme ve taksi yollarında yetkisiz araç girişi olaylarını 10000 işletmede bir 20 değerinde sürdürme. Bu emniyet performansı hedef değerleri 6.6.6'da ele alınan koşulları yerine getirir: sayısal olarak ifade edilirler; açık, ölçülebilir ve havaalanı SMS'sinin emniyet performansı göstergeleri ile bağlantılıdırlar. Ayrıca, her iki emniyet performansı hedef değerleri emniyet performansı ölçümünü yansıtmaktadır.

6.6.10 Eylem planları, bir SMS'nin emniyet performansı gösterge değerlerini ve emniyet performansı hedef değerlerini elde etmek için gerek duyulan araçlar ve yöntemlerdir. Güvenilirlik, çalışır durumda olma, performans ve/veya hassasiyetle ilgili önlemlerin belirlenebileceği operasyonel prosedürler, teknoloji, sistemler ve programları içerirler. Yukarıda açıklanan SMS'nin emniyet performansı gösterge değerlerini ve emniyet performansı hedef değerlerini elde etmek için uygulanabilecek bir eylem planı örneği aşağıdaki gibi olacaktır: günde üç kez apronda denetimden oluşan bir program uygulama, sürücüler için bir eğitim kursu geliştirme ve uygulama ve (havaalanına özgü) bir taksi yolu işaret sistemi kurma.

6.6.11 Bir SMS'nin emniyet performansının emniyet performansı göstergesi değerleri ve emniyet performansı hedef değerleri farklı veya aynı olabilir. Bir SMS'nin emniyet performansının emniyet performansı göstergesi değerleri ve emniyet performansı hedef değerlerinin farklı olup olmadığını değerlendirirken üç nokta dikkate alınmalıdır. Önce, emniyet performansı değerinin daha zorlu bir emniyet performansı hedef değerine dönüştürülmesi için hizmet sağlayıcıda kaynakların bulunup bulunmadığına dikkat edilmelidir. İkincisi, emniyet performansı değerinin daha zorlu bir emniyet performansı hedef değerine dönüştürülmesi için gereken eylem planlarının ne kadar pahalı olduğuna dikkat edilmelidir. Üçüncüsü ve daha önemlisi, emniyet performansı gösterge değeri ve emniyet performansı hedef değeri aynı kalacaksa, emniyet performansı göstergesi ve emniyet performansı hedefi tarafından ifade edilen tehlikenin sonuçlarına ait emniyet risklerinin değerlendirmesinin Bölüm 5'te ele alınan emniyet riski yönetimi sürecinin tahammül edilebilir alanına düşüp düşmediğinin belirlenmesine dikkat edilmelidir. Emniyet performansı gösterge değeri mevcut koşullar altında tahammül edilebilir alana giren bir emniyet riski değerlendirmesini yansıtabilir. Ancak, sistemdeki değişiklikler, büyüme v.s. bu emniyet riski değerlendirmesini geçersiz kılabilir. Bu durumda, emniyet performansı hedef değeri, değişen ortamda geçerli olması için daha zorlu bir hedef değere dönüştürülmelidir.

6.6.12 Farklı emniyet performansı göstergeleri ve emniyet performansı hedeflerinden oluşan bir yelpaze, tek bir gösterge veya hedefe oranla bir havacılık örgütün SMS'sinin emniyet performansının daha iyi anlaşılmasını sağlayabilir. Başka bir deyişle, bir SMS'nin emniyet performansı daima belirli sayıda emniyet performansı göstergeleri ve emniyet performansı hedefleri ile ifade edilmelidir, asla tek bir gösterge veya hedefle ifade edilmemelidir. Ek örnekler aşağıda verilmiştir.

6.6.13 Bir uçak operatörü uçuş işletmelerinin yaklaşma ve iniş aşamalarını SMS'si tarafından ele alınması gereken önemli emniyet sorunlarından biri olarak belirlemiştir. Aynı zamanda, SMS'sinin emniyet riski yönetimi bileşeni olmasına karşın, ağdaki hassas olmayan yaklaşmalarla hizmet verilen havalimanlarında dengesiz (veya uyumlu olmayan) yaklaşmalarla ilgili bir emniyet sorunu olduğunu belirlemiştir. Böylece, Devletin sivil havacılık denetim kurumu ile yapılan anlaşmaya uygun olarak aşağıdaki emniyet performansı gösterge değerini tanımlar: ağdaki hassas olmayan yaklaşmalarla hizmet verilen havalimanlarında 1000 iniş operasyonu başına 10 dengesiz (veya uyumlu olmayan) yaklaşma. Ardından, uçak operatörü Devletin sivil havacılık denetim kurumu ile yapılan anlaşmaya uygun olarak aşağıdaki emniyet performansı hedef değerini tanımlar: sonraki üç yıl içinde, ağdaki hassas olmayan yaklaşmalarla hizmet verilen havalimanlarında 1000 iniş operasyonu başına dengesiz (veya uyumlu olmayan) yaklaşmaların sayısını yüzde 50 azaltmak. Yukarıda açıklanan SMS'nin emniyet performansı gösterge değerini ve emniyet performansı hedef değerini elde etmek için uygulanabilecek eylem planı örneği aşağıdaki gibi olacaktır: ağdaki hassas olmayan yaklaşmalarla hizmet verilen havalimanlarında sabit alçalmalı iniş (CDA) GPS yaklaşmalarının geliştirilmesi.

6.6.14 Bir ATS sağlayıcısı, havaalanı operasyonlarını SMS'si tarafından ele alınması gereken önemli bir emniyet sorunu olarak belirlemiştir. SMS'sinin emniyet riski yönetimi bileşeni olmasına karşın, piste girişlerle ilgili bir sorun belirlemiştir ve aşağıdaki emniyet performansı gösterge değerini tanımlamıştır: 2009 boyunca milyon işletmede bir 0,8 Kategori A ve B (en ciddi) piste giriş olayı. Buna bağlı olarak, ATS sağlayıcısı aşağıdaki emniyet performansı hedef değerini tanımlar. 2010'a kadar Kategori A ve B (en ciddi) piste giriş olaylarını milyon işletmede 0,5 adete indirmek.

6.6.15 Bir SMS'nin emniyet performansı, mümkün olduğunca, nicel emniyet performansı göstergeleri ve emniyet performansı hedefleri tarafından tanımlanmalıdır. Ancak, pek çok Devlette hizmet sağlayıcıların emniyet verileri toplama ve analizi kabiliyetinin tam olarak gelişmemiş olabileceği unutulmamalıdır. Bu nedenle, bu kabiliyetler geliştirilirken, bir SMS'nin emniyet performansı nicel ve nitel emniyet performansı göstergeleri ve emniyet performansı hedeflerinin bir kombinasyonu aracılığıyla tanımlanabilir. Yine de, hedef SMS'nin emniyet performansı tanımının sadece nicel ölçütlerle elde edilmesi olarak kalmalıdır.

6.6.16 Bir SMS'nin emniyet performansı tanımı düzenlemelerde ulusal ve uluslararası gerekliliklere uyumun ötesinde bir gerekliliktir. Bir SMS için emniyet performansının oluşturulması, hukuki, düzenlemelere ait veya diğer yerleşik gerekliliklerin yerine geçmez, yine hizmet sağlayıcıların ilgili ulusal düzenlemelerde ve *Uluslararası Sivil Havacılık Konvansiyonu* (ICAO Doc 7300) ve Konvansiyonun annexlerinde bulunan ilgili hükümlerde yer alan yükümlülüklerini ortadan kaldırmaz.

6.7 YÖNETİMİN HESAP VERME SORUMLULUĞU

6.7.1 Annex 1, 6, 8, 11, 13 ve 14'teki ICAO emniyet yönetimi SARP'lerinin üçüncü ve sonuncu grubu, hizmetlerin sunulması sırasında emniyetin yönetiminin karşısında yönetimin hesap verme sorumluluğudur. ICAO SARP'lerine göre, kabul edilen bir emniyet yönetimi sistemi, hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütleri, uçak operatörleri, onaylı bakım örgütleri, uçak tip tasarımı ve/veya üretiminden sorumlu örgütler, hava trafik hizmeti sağlayıcıları ve sertifikalı havalimanlarını kapsayacak şekilde emniyetle ilgili hesap verme sorumluluğunun sınırlarını açık bir şekilde tanımlamalıdır, buna üst yönetimin emniyetle ilgili doğrudan hesap verme sorumluluğu da dahildir.

6.7.2 Yönetimin emniyetin yönetilmesine katılması Bölüm 3 ve 8'de ele alınmıştır ve bunun burada daha fazla ele alınması gerekmemektedir. Yine de, dille ilgili bir soruna dikkat çekilmelidir: ICAO emniyet yönetimi gerekliliklerinin hesap verme sorumluluğu teriminin kullanımı. İngilizcede, hesap verme sorumluluğu kavramı sorumluluk kavramından farklıdır. Sorumluluk bir kişinin belirli eylemleri yerine getirmesi gereken durumları ifade ederken, hesap verme sorumluluğu bu yükümlülüğü veya istekliliği bu eylemlerin yerine getirilmesinin sorumluluğunu kabul etmek noktasına kadar genişletmektedir. Emniyet yönetimi terimleri ile ifade edilirse, emniyet sorumlulukları bir kişinin yerine getirmesi gereken görevlerin emniyetle ilgili amaçlarını açıklar. Hesap verme sorumlulukları ise, kişinin doğrudan veya kişinin sorumluluklarını temsil ettikleri de dahil olmak üzere, başkalarının gözetimi ve yönetimi altında yerine getirmesi gereken ifadelerdir. Her iki terim arasında önemli bir fark vardır. Ancak, bu fark sadece İngilizcede yer almaktadır. Bu nedenle, yönetimle ilgili olarak ICAO emniyet yönetimi gereksinimlerinde yer alan sorumluluk terimi, Annex 1, 6, 8, 11, 13 ve 14'ün İngilizce dışındaki dillerdeki versiyonunda yer alan şekliyle, İngilizcedeki hesap verme sorumluluğu terimi anlamında anlaşılmalıdır.

6.7.3 Başarılı bir emniyet yönetimi, tüm yönetim ve denetim seviyelerinde etkin katılım gerektirir. Bu, örgütün yapısında yansıtılmalı ve emniyetle ilgili hesap verme sorumluluklarında yayınlanmalıdır. Örgüt – örgüte ait çizelgeler veya diyagramlarla – sorumlulukları, hesap verme sorumluluklarını ve yetkileri tanımlamalı, belgelemeli ve iletmelidir. Üst yönetimin hesap verme sorumluluğu ve işlevsel sorumlulukları Bölüm 8'de daha ayrıntılı ele alınacaktır.

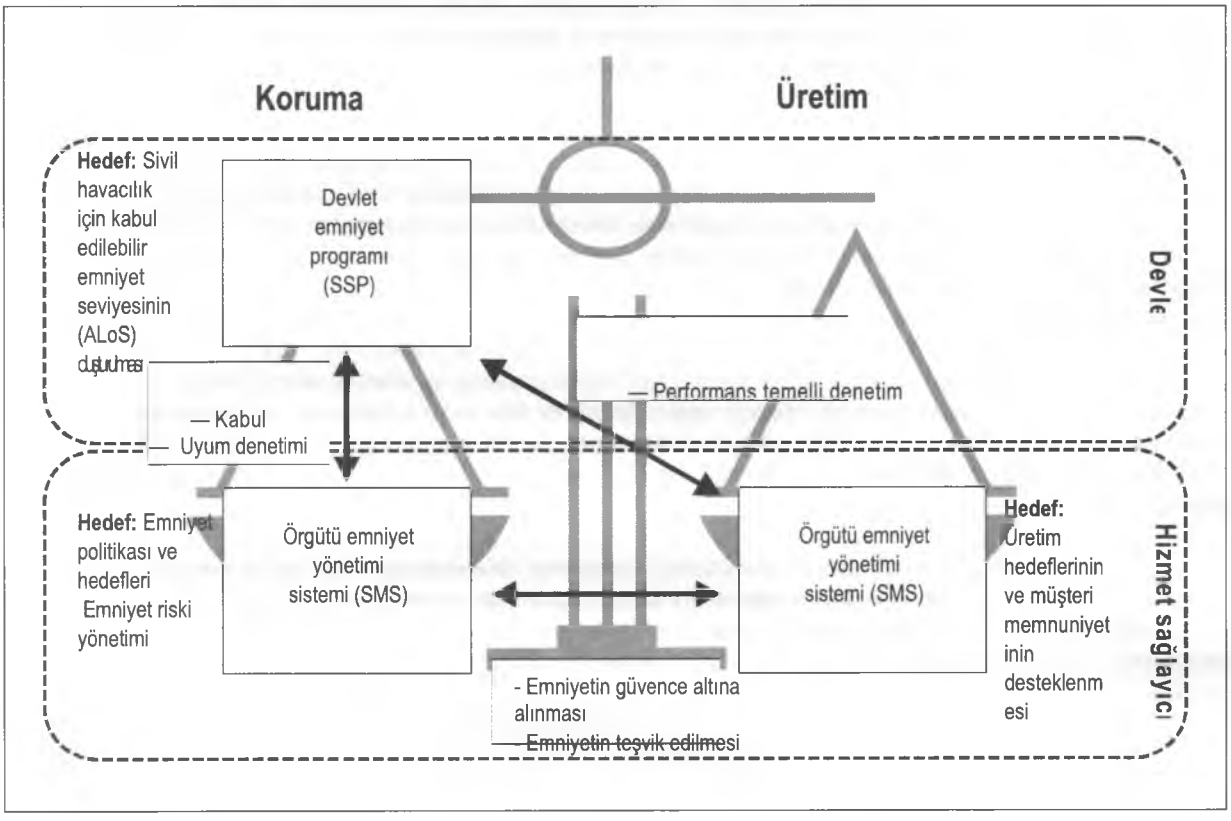
6.8 SSP İLE SMS ARASINDAKİ İLİŞKİ

6.8.1 Bir SSP ile SMS arasındaki ilişkinin açık bir şekilde anlaşılması Devletler içinde emniyet yönetimi eyleminin uyumlu olması için önemlidir. Bu ilişki en basit şekilde aşağıdaki gibi ifade edilebilir: Devletler bir SSP geliştirmek ve oluşturmaktan sorumludur; hizmet sağlayıcılar ise bir SMS geliştirmek ve oluşturmaktan sorumludur. Bu çok önemli bir noktadır: Devletlerin bir SMS geliştirmesi beklenmez; bunun yerine SSP aynı rolüoynar.

Yine de, Devletler SSP'lerindeki etkinliklerinin bir parçası olarak, hizmet sağlayıcının SMS'sinin geliştirilmesini, uygulanmasını ve operasyonel performansı kabul etmek ve denetlemekten sorumludur. Hizmet sağlayıcının SMS'sinin emniyet performansını denetlerken, Bölüm 6.4'te ele alınan bir SSP'nin ALoS kavramı, bir SSP ile bir SMS arasındaki ilişkide temel bir rol oynar. Bir SSP ile bir SMS arasındaki ilişki Şekil 6-7'de gösterilmiştir ve Bölüm 11'de daha ayrıntılı olarak ele alınmıştır.

6.8.2 Bölüm 3'te emniyetin yönetimini bir örgütlenme süreci ve emniyet yönetimini temel bir operasyonel işlev olarak kabul eden bir perspektiften kaynaklanabilecek potansiyel bir yönetim ikilemi ele alınmaktadır. "İki P ikilemi" olarak sunulan bu tür bir ikilem, bir SSP ile SMS arasındaki ilişkiyi açıklamak için uygun bir arka plan sağlamaktadır.

6.8.3 Şekil 6-7'de, SSP koruma ve üretim arasındaki dengenin koruma tarafında yer almaktadır. SSP, emniyet risklerini Devlet seviyesinde kontrol ederek kamu emniyetini sağlamayı hedeflemektedir. Bir SSP'nin bu şekilde üretim hedefleri yoktur. Devletin havacılık örgütlerinden etkinlik beklense de, kar elde etme amaçlı belirli bir ürün veya hizmet sunmazlar. Devletin temel hedefi, SSP'si aracılığıyla, hizmet sağlayıcılar tarafından hizmetlerin sunulması sırasında mümkün olduğunca kamu emniyeti sağlamaktır. Bu hedefe SSP için ALoS'u tanımlayarak ve SSP'nin aşağıdaki iki "operasyonel bileşen" aracılığıyla Devlet içinde emniyet risklerinin kontrolü ile ulaşılır: emniyet riski yönetimi ve emniyetin güvence altına alınması.



Şekil 6-7. SSP ile SMS arasındaki ilişki

6.8.4 Hizmet sağlayıcının SMS'si dengenin koruma tarafında sadece kısmen yer almaktadır. Devletin aksine, hizmet sağlayıcı kar elde etme amaçlı belirli bir ürün veya hizmet sunar. Koruma bakımından, hizmet sağlayıcının SMS'sinin amacı, örgütün uzmanlık alanındaki ürün veya hizmetlerin sunulması ile ilgili etkinlikler ve süreçlerin sonucu olan emniyet risklerinin kontrol edilmesidir. Hizmet sağlayıcı, hizmet sunumu sırasında emniyet risklerinin kontrolünü temel olarak SMS'nin aşağıdaki iki "operasyonel bileşen" aracılığıyla sağlar: emniyet riski yönetimi ve emniyetin güvence altına alınması, burada emniyet politikası ve hedefleri ve emniyetin teşvik edilmesi destekleyici, ama önemli bir rol oynamaktadır.

6.8.5 Devlet, SSP'sinin bir parçası olarak, ilk olarak bir hizmet sağlayıcının SMS'sini kabul eder. Bu kabul, büyük oranda kural koyucu şekildedir: Devlet, büyük olasılıkla sivil havacılık denetim kurumu aracılığıyla, hizmet sağlayıcının SMS'sinde önerilen bileşen ve unsurların Devlet tarafından yürürlüğe sokulmuş olan mevcut düzenlemeler ve yönetmeliklere uygun olduğunu doğrulayacaktır. Kabulün büyük oranda yönetimsel bir süreç olduğunun unutulmaması önemlidir: Devlet bir yönetim sisteminin ayrıntılı planını ve bu planın geliştirilmesi ve uygulanması için bir eylem planını onaylar. Basitçe, kabul çoğunlukla "uygun kutucukların işaretlenmesi" anlamına gelir. Ancak, düzenleme uyumun sağlanmasına karşın, kabul SMS'nin doğru şekilde çalışmasını garanti etmez. Kabul ve uyum denetimi, Şekil 6-7'de SSP ve SMS'yi bağlayan dikey okla gösterilmiştir. Devletin SMS'nin doğru şekilde uygulandığından (yani SMS'nin gerçekten çalıştığından) emin olmasının yolu, hizmetlerin sunulmasını hedefleten etkinliklerin gerçekten uygulanması sırasında denetlemesidir.

6.8.6 SMS performansını doğrulamak için, Devletin sivil havacılık kurumu, uygulanmasının denetimini hizmetlerin sunulmasını amaçlayan etkinlikler sırasında, düzenli olarak gerçekleştirmelidir. Bu uygulamada imkansız olmasa da zor olacaktır, SMS'nin emniyet performans göstergelerinin ve emniyet performansı hedeflerinin nedeni budur. 6.8.5'te ele alınan şekilde kabul ve uyum denetimi kural koyuculuk temelli iken, emniyet performansı göstergeleri ve hedeflerinin denetimi performans temellidir. Böylece bölüm 6.6'da ele alınan emniyet performansı kavramı, bölüm 6.4'te ele alınan SSP'nin ALoS'u kavramını hizmet sağlayıcının SMS'sini kapsayacak şekilde genişletir. Emniyet performansı ile SMS ilişkisi, ALoS ile SSP ilişkisi ile aynıdır.

6.8.7 Bir SMS'nin emniyet performansı ölçümü, emniyet performansı göstergeleri, emniyet performansı hedefleri ve eylem planlarını içerir. Bu önemli, üzerinde uzlaşılmış gösterge ve hedefler, hizmet sağlayıcının hizmetlerinin sunulması ile ilgili etkinlikleri gerçekleştirdiği operasyonel bağlamdaki genel tehlikeleri temsil ederler ve SMS'nin gerçekleştirilmesi ile ilgili adil bir manzara ortaya koyacak şekilde performans temelli denetim süreci sağlarlar. Belirli bir hizmet sağlayıcının işletmesine özel kısa vadeli ve orta vadeli bir öncelikli emniyet hedefleri kümesi tanımlayarak, belirli emniyet hedeflerinin altında yatan tehlikelerin sonuçlarına ait emniyet risklerine karşı azaltma stratejileri uygulayarak ve azaltma stratejilerinin etkililiğinin ölçülmesini sağlayan ölçütler ve zaman çizelgeleri oluşturarak, hizmet sağlayıcı düzenlemelere uyumun ötesinde, denetim kurumuna SMS'nin emniyet performansının doğrulanması için ölçülebilir araçlar sağlamaktadır veya bu araçların eksikliğini bildirmektedir.

6.8.8 Tartışmayı Şekil 6-7'deki koruma ve üretim arasında aracılık sağlayan dengenin üretim tarafına taşırsak, daha önce ele alındığı gibi, bir SSP'nin bu tür üretim hedefleri yoktur, ama bir hizmet sağlayıcının vardır. Bir hizmet sağlayıcının üretim etkinliklerinin hedefi ticari hedeflere ulaşmak ve müşteri memnuniyeti sağlamaktır. SMS üretim hedeflerinin peşinde koşarken hizmet sağlayıcının karşı karşıya gelmek zorunda olduğu tehlikelerin sonuçlarına ait emniyet risklerinin örgütün kontrolü altında kalmasını sağlamak için kullandığı araçtır. Hizmet sağlayıcının SMS'si ilk olarak, emniyet risklerini ve bu riskleri emniyet yönetimi aracılığıyla örgüt kontrolü altında tutmak için gereken azaltma işlemlerini tanımlar. İşletmeler başladığında, emniyet risklerinin kontrolü ve azaltma işlemlerinin izlenmesi emniyetinin teşvik edilmesi ile desteklenen sürekli bir emniyetin güvence altına alınması süreci aralığıyla sağlanır. Emniyet riski yönetimi, emniyetin güvence altına alınması ve emniyetin teşvik edilmesi böylece örgütün üretim ve koruma arasındaki dengeyi sürdürmesi için gereken araçları sağlar.

6.8.9 SMS'nin kabul edilmesi ve düzenlemelere uyum bakımından devletin yönetimsel denetimi ile ilgili olarak, Devletin geleneksel rolü koruma tarafında yer alsa da, bir SSP'de üretim tarafında bir denetim işlevi rolü de vardır. Tehlikenin tanımlanması ve emniyet riski yönetimindeki sorunlar, azaltma stratejilerinin geliştirilmesindeki sorunlarla birlikte, genellikle kaynakların dağıtılması ile ilgilidir. Bu, genellikle kaynakların dağıtılmasında üretim etkinliklerine doğru bir yönelim gösterildiğinde ortaya çıkan durumdur. Tehlikenin tanımlanması ve emniyet riski yönetimindeki ve azaltma stratejilerinin geliştirilmesindeki sorunlar, kaynakların üretim ve korumaya dengesiz olarak dağıtılması nedeniyle, hizmet sağlayıcının SMS'sinin emniyet performansının üzerinde uzlaşılan şekilde gerçekleştirilememesi ile de görünür hale gelecektir.

Bu nedenle, 6.8.7'de ele alındığı gibi performans temelli bir denetimin yürütülmesi, SMS'nin operasyonel performansın hizmet sağlayıcısına özel olarak üzerinde uzlaşılan SMS emniyet performansı ile karşılaştırılarak denetlenmesi sırasında, kaynakların dağıtılmasında ve bir bütün olarak SMS'nin emniyet performansının yerine getirilmesindeki yanlılıklar açık hale gelecektir: kaynakların eksikliği ya emniyet tehlikelerinin tanımlanmamasına ya da sorunlu emniyet riski yönetimine ve buna bağlı olarak SMS'nin kötü bir emniyet performansına sahip olmasına neden olacaktır. Böyle bir durumda, düzenlemelere uygun olsa bile, hizmet sağlayıcının SMS'si etkili olmayacaktır. Şekil 6-7'de, performans temelli kabul ve denetim işlevleri SSP ile örgütün üretim süreçlerini bağlayan çapraz okla temsil edilmiştir.

6.9 UYUM VE PERFORMANS

6.9.1 Havacılıkta, SSP ile SMS aracılığıyla emniyet yönetimi uygulamalarının gerçekçi bir şekilde uygulanmasını başarmaya yönelik bir görüşle, mevcut uyum temelli emniyet yaklaşımını performans temelli bir yaklaşımla tamamlama gereksinimi ile ilgili kanı giderek daha fazla taraftar bulmaktadır. Bu konu, SSP ve eşlikçisi ALoS başlıkları altında bu bölümde ele alınmıştı. Bu kısımda, önemli noktalar vurgulanarak, bir özet sunulmaktadır.

6.9.2 Emniyet yönetimi ve emniyete performans temelli bir yaklaşım arayışı, emniyet riski kontrollerinin uygulanmaya başlanması ve etkili bir şekilde kullanılmasını temel alır. Devletin perspektifinden, kullanabileceği en etkili emniyet riski kontrolleri emniyet düzenlemeleridir.

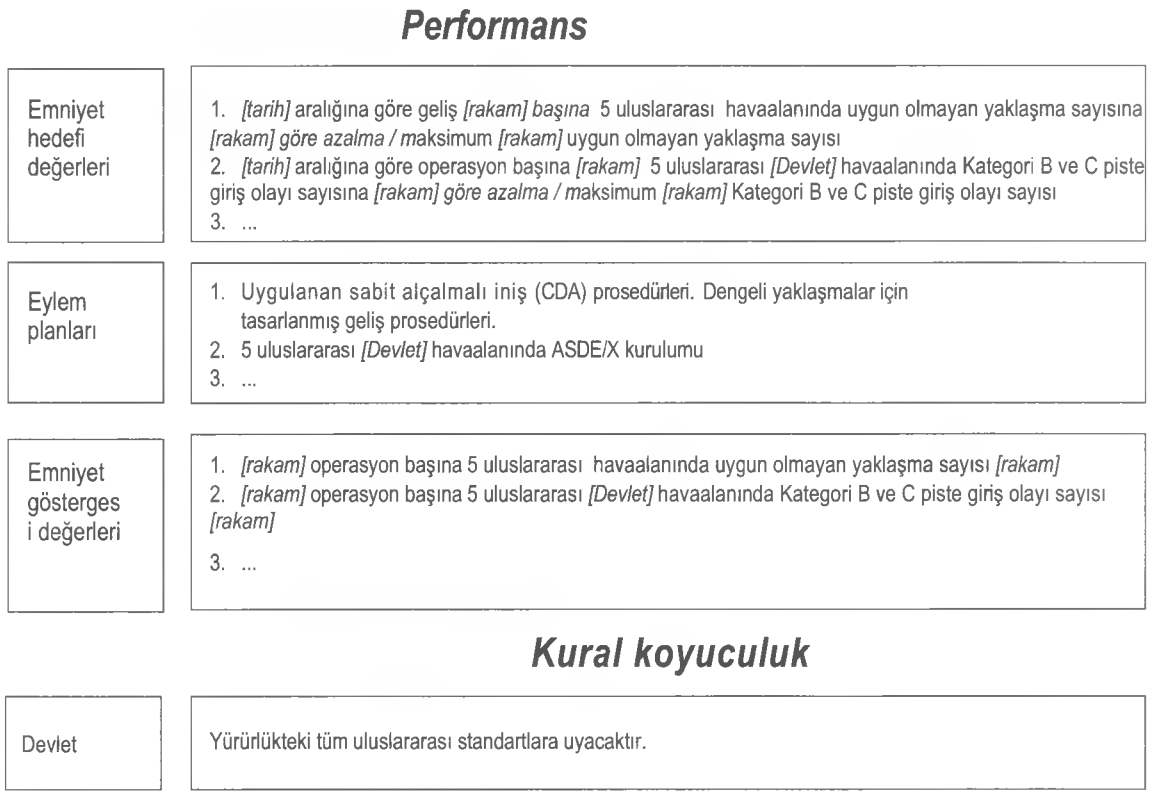
6.9.3 Bölüm 3'te ve bu bölümde ele alındığı gibi, uyum temelli bir emniyet ortamında, emniyet yönetimi yaklaşımı katı ve kural koyucudur. Uyum temelli bir emniyet ortamında, emniyet düzenlemeleri yönetimsel kontroller olarak kullanılır. Katı bir düzenleme çerçevesi, sadece aşağıdaki hedefe yönelik denetimlerle desteklenir: düzenlemelere uyum.

6.9.4 Performans temelli bir emniyet ortamında, yaklaşım esnek ve dinamiktir. Bu tür bir ortamda, emniyet düzenlemeleri emniyet riski kontrolleri olarak kullanılır. Emniyet risklerine yanıt vermek ve kontrol etmek için geliştirilen düzenlemelerin yer aldığı bir düzenleyici çerçeve uygulanır ve düzenleyici çerçeveye uyumun denetimi emniyet risklerinin, aşağıdaki iki hedefle, veri temelli olarak tanımlanması ve önceliklerinin belirlenmesi ile desteklenir: düzenlemelere uyum, ama daha önemlisi, etkili emniyet performansının doğrulanması.

6.9.5 Performans temelli bir emniyet ortamında, hem SSP hem de SMS'nin düzenlemelere uyumun ötesinde, tasarım beklentilerine uygun şekilde çalışıp çalışmadıklarını belirlemek için, bir SSP için ölçülebilir hedeflerden ve bir SMS için ölçülebilir performans hedeflerinden oluşan bir küme tanımlanması gerekir. Ölçülebilir hedefler ve performans hedefleri emniyetle ilgili önemli etkinliklerin gerçek performansının mevcut örgüt kontrollerine değerlendirilmesine izin verir, böylece emniyet riskleri makul derecede düşük şekilde (ALARP) yürütülebilir ve gerekli düzeltme ve koruma önlemleri alınabilir.

6.9.6 Bir SSP ile ilgili ALoS ve bir SMS'nin emniyet performansı ile kavramları hem SSP hem de SMS'nin etkili bir şekilde işletmesi için önemli bileşenlerdir. Düzenlemelere uyumun ötesinde, bir SSP'nin gerçek uygulaması ve bir SMS'nin gerçek performansını izlemek için, performans temelli bir düzenleme ortamının temelini oluştururlar. Sadece belirli emniyet hedeflerinin ve emniyet performansı hedeflerinin oluşturulması ve ölçülmesiyle – bir SSP'nin etkili bir şekilde uygulanmasının ve bir SMS'nin etkili emniyet performansı göstermesinin güvence altına alınmasıyla — bir SSP/SMS'nin altında yatan emniyet performansının sürekli iyileştirilmesi hedefine erişilebilir.

6.9.7 Emniyet göstergeleri ile emniyet hedefleri ve emniyet göstergesi değerleri ve emniyet hedef değerleri, düzenlemelere uyumun ötesinde, sırasıyla bir SSP veya SMS'nin etkililiğinin sağlanması ve gösterilmesi için ölçülebilir bir yöntem sağlarlar. Düzenlemelere uyum, Devlet için olduğu gibi, hizmet sağlayıcılar için de hala emniyet yönetiminin temelinde bulunmaktadır. Şekil 6-8 ve 6-9, kural koyuculuğun ve performansın bir SSP ve SMS içinde nerede ve nasıl yer aldığını göstermek için, sırasıyla bu bölümde ele alınan SSP ve SMS'nin emniyet göstergeleri ve emniyet hedefleri, emniyet performansı göstergeleri, emniyet performansı hedefleri ve eylem planlarını temel almaktadır.



Şekil 6-8. SSP — Performansla birleştirilen kural koyuculuk

6.9.8 Özet olarak, ICAO uyumlu emniyet yönetimi SARP'lerine uygun olarak:

a) Sivil havacılıkta kabul edilebilir emniyet seviyesi (ALoS) elde etmek için, Devletler bir Devlet emniyet programı (SSP) oluşturmalıdır.

b) Erişilecek kabul edilebilir emniyet seviyesi (ALoS) Devlet tarafından oluşturulmalıdır.

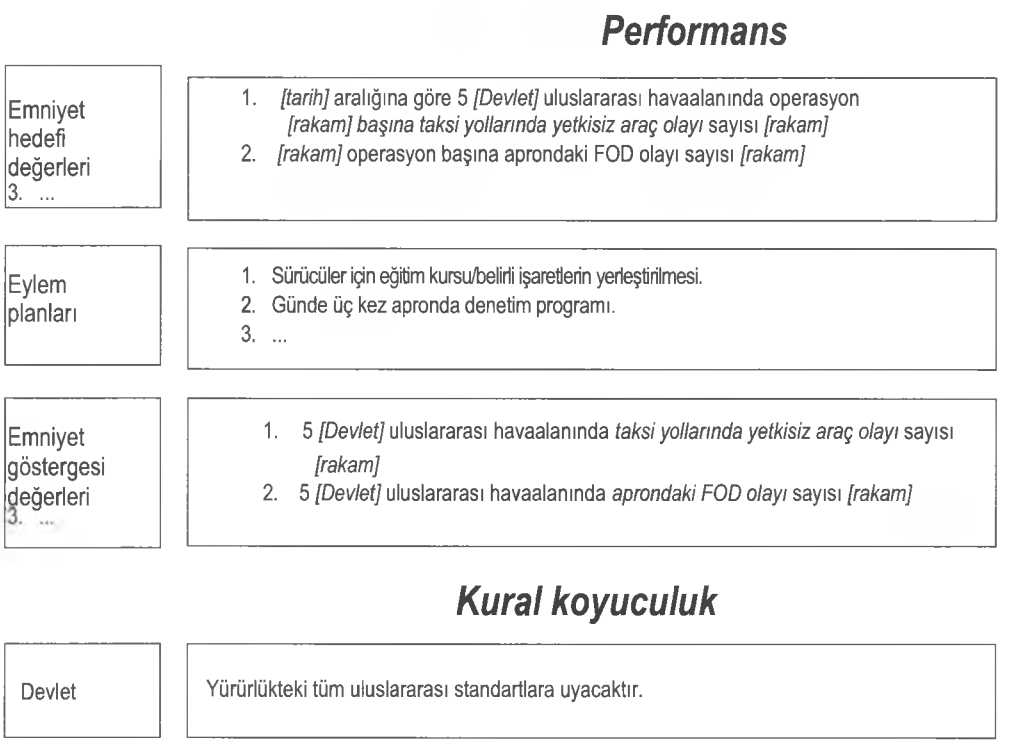
c) Hizmet sağlayıcılar aşağıdaki sağlayan bir emniyet yönetimi sistemi (SMS) uygulamalıdır:

1) emniyet tehlikelerinin tanımlanması;

2) emniyet performansının sürdürülmesi için düzeltme eylemlerinin sağlanması;

3) emniyet performansının sürekli olarak izlenmesinin ve düzenli olarak değerlendirilmesinin sağlanması ve

4) SMS'nin genel performansının sürekli olarak iyileştirilmesinin hedeflenmesi.



Şekil 6-9. SMS — Performansla birleştirilen kural koyuculuk

Bölüm 7

EMNİYET YÖNETİMİ SİSTEMİNE (SMS) GİRİŞ

7.1 HEDEF VE İÇERİKLER

Bu bölümde emniyet yönetimi sistemlerinin (SMS) temel özellikleri açıklanmakta ve sistemin doğru şekilde açıklanmasının (sistem tanımlaması) ve SMS uygulama sürecine başlamadan önce bir boşluk analizi yapılmasının rolü ve önemi ele alınmaktadır. Bu bölümde ayrıca SMS ile kalite yönetim sistemleri (QMS) arasındaki ilişki ele alınmaktadır. Bu bölüm aşağıdaki konuları içerir:

a) Başlangıç konseptleri;

b) SMS özellikleri;

c) Sistem tanımlaması;

d) Boşluk analizi;

e) SMS ve QMS;

f) SSP/SMS ve kaza inceleme süreci;

g) Yönetim sistemlerinin entegrasyonu;

h) Terimlerin açıklanması ve

i) Emniyet sloganları ile emniyet ilkeleri arasındaki fark.

7.2 BAŞLANGIÇ KONSEPTLERİ

7.2.1 Bir SMS bir alet kutusuna benzetilebilir. Bir havacılık örgütün, iş alanındaki hizmetlerinin sunulması sırasında karşılaşması gereken tehlikelerin sonuçlarına ait emniyet risklerini kontrol edebilmek için gereksinim duyduğu araçları içeren bir alet kutusudur. Çoğu durumda, örgütün kendisi hizmetlerin sunulması sırasında tehlikelerin ortaya çıkmasına neden olur. Bir SMS'nin kendisinin bir araç veya süreç olmadığının ifade edilmesi önemlidir. Bir SMS iki temel emniyet yönetimi sürecinin (tehlikenin tanımlanması ve emniyet riski yönetimi) gerçekleştirilmesi için gereken araçların içinde yer aldığı ve korunduğu alet kutusudur. Bir SMS'nin örgüt için sağladığı şey, boyut ve karmaşıklık açısından örgütün boyutu ve karmaşıklığına uygun bir alet kutusudur.

7.2.2 Bir alet kutusu (Şekil 7-1) olarak, bir SMS tehlikenin tanımlanması ve emniyet riski yönetimi için özel araçlara gerek duyulduğunda:

a) eldeki işe uygun araçların örgütün kullanımına hazır olmasını sağlar;

Şekil 7-1. SMS – Bir alet kutusu

b) araçlar ve görevlerin doğru şekilde ilişkilendirilmesini sağlar;

c) araçların örgütün gereksinimlerine ve kısıtlarına uygun olmasını sağlar ve

d) kaynakların gereksiz yere harcanmasına gerek kalmadan, araçların alet kutusu içinde kolaylıkla bulunmasını sağlar.

Bir SMS örgütteki belirli emniyet yönetimi süreçlerinin yürütülmesi için gereken araçların doğru ve zamanında saklanması, gerektiğinde bulunabilmesi ve kullanılabilmesini sağlayan koruyucu bir kabuk olduğundan bu perspektif önemlidir. İçinde doğru araçlar olmadan, bir SMS sadece boş bir kabuktur.

7.2.3 Bölüm 3'ün kapanış özetinde, emniyet yönetiminin bazı karakteristikleri ve ayırıcı özellikleri ifade edilmektedir. Önemli karakteristiklerden biri, emniyet yönetiminin, örgütün genellikle tehlikelerin ortaya çıkmasına neden olabilen, en belirgin (örneğin bir havayolunun uçuş işletmeleri) tek bir etkinliği ile sınırlandırılamamasıdır. Emniyet yönetimi örgütün bütününün tüm operasyonel etkinlikleri dikkate alır. Bir SMS'nin kapsamı örgütün etkinliklerinin çoğunu ve hizmetlerin sunulmasını destekleyen ve tehlikeleri ortaya çıkarma potansiyeline sahip operasyonel etkinliklerin kesinlikle tümünü içine alır. Bir SMS'nin kapsamı doğrudan işletmeleri, bakım, onarım, destek hizmetlerini, eğitimi, kontrolü ve diğer operasyonel etkinlikler içerir. Bir SMS'nin kapsamı, Bölüm 3'te ele alındığı gibi, uygun ve hizmet sunumu ile ilgili olduğu sürece, finans, insan kaynakları ve hukuk gibi operasyonel etkinlikleri destekleyen diğer operasyonel etkinlikleri de doğrudan içine alır.

7.2.4 Bir SMS üst yönetimden başlamalıdır. Bu retorik veya felsefi bir ifade değildir, son derece somut nedenlere dayalı bir ifadedir. Bir örgütün temel operasyonel işlev olarak emniyetin yönetimi, diğer tüm temel operasyonel işlevler gibi kaynak gerektirir. Kaynakların dağıtılması açıkça üst yönetimin bir işlevidir, üst yönetim kaynakların dağıtılmasında hem yetki hem de sorumluluk sahibidir. Üst yönetim örgütün SMS'sinin rolü ve hedefleri hakkında bilgilendirilmezse veya örgütün SMS'sinde uygun bir seviyede yer almazsa, emniyet risklerinin örgüt kabiliyetleri üzerinde sahip olacağı tehdidin kapsamını değerlendiremeyecektir. Bu değerlendirme olmadığında, kaynakların dağıtılması gerçek gereksinimlerin uzağına düşecektir. Başka bir deyişle, Bölüm 3'te ele alınan "iki P ikilemi" yüzeye çıkacak ve çözülmeden kalacaktır.

7.2.5 Bir SMS örgüt genel emniyet seviyesi üzerinde sürekli iyileştirme yapmayı hedefler. Temel bir operasyonel işlev olarak emniyet yönetiminin doğasına uygun olarak, bir SMS sürekli ve günlük olarak tehlikelerin tanımlanmasını, bilgilerin toplanmasını ve analizini, emniyet riski tahminlerini ve azaltma stratejilerinin uygulanmasını içerir. Bir SMS'nin durduğu veya yavaşladığı bir nokta yoktur. Bir SMS örgütün stratejik hedeflerine uygun olan ve temel operasyonel işlevleri destekleyen emniyet seviyelerinin sürdürülmesini ve mümkünse iyileştirilmesini hedefleyen sürekli, asla sona ermeyen bir işletmedir. Bu anlamda, bir SMS bir kazanın gerçekleşmesini bekleyen, ardından benzer kazaların önlenmesi için incelemeden elde edilen bilgilerden mümkün olduğunca çok ders çıkaran ve bu dersleri yayan klasik kaza incelemesi kavramından tamamen farklıdır. Bir SMS, bir kazaya yol açmalarından önce sınırlamak için tehlikeleri etkin bir şekilde araştırır, emniyet risklerini sürekli olarak değerlendirir.

7.2.6 SMS'de havacılıkla ilgili tüm taraflar, çok somut nedenlerle rol oynar. Emniyet riski ile ilgili kararlar alınmadan önce, bu kararlarla ilgili olarak verecekleri bilgilerin dikkate alınacağından emin olmak için havacılık sistemi ile ilgili tarafların belirlenmesi ve işin içine katılması önemlidir.

7.2.7 Ayrıca, SMS etkinliklerinin geniş bir yelpazedeki doğası nedeniyle emniyet riski ile ilgili karar verme sürecine çok sayıda sektörden bilgi girişi yapılması önemlidir. Aşağıda, emniyet riski ile ilgili karar verme sürecine katkıda bulunmaları veya bilgi girişinde bulunmaları istenebilecek ilgili tarafların listesi bulunmaktadır:

a) havacılık profesyonelleri;

b) uçak sahipleri ve operatörler;

c) üreticiler;

d) havacılık düzenleme kurumları;

e) sektör içindeki ticari birlikler;

f) bölgesel hava trafik hizmeti sağlayıcıları;

g) meslek birlikleri ve federasyonlar;

h) uluslararası havacılık örgütleri;

i) araştırma ajansları ve

j) uçuşları kullanan kamuoyu.

7.2.8 İlgili taraflar, ele alınan emniyet riskleri ile iletişimin erkenden ve adil, nesnel ve anlaşılabilir şekilde gerçekleşmesini sağlayarak örgütlerdeki karar vericilere yardımcı olabilir. Emniyet iletişimin güvenilir olması için, olgularla, yönetimin önceki ifadeleriyle ve diğer kurumların mesajları ile tutarlı olması gerekir. Bu mesajlar, ilgili tarafların anlayabileceği terimlerle ifade edilmelidir.

7.3 SMS ÖZELLİKLERİ

7.3.1 Bir SMS'yi karakterize eden üç özellik vardır. Bunlar:

a) sistematik;

b) proaktif ve

c) açık olmasıdır.

7.3.2 Bir SMS, emniyet yönetimi etkinlikleri önceden belirlenen bir plana uygun oldukları ve örgüt içinde tutarlı bir şekilde uygulandıkları için sistematiktir. Tehlikelerin sonuçlarına ait emniyet risklerini kontrol altında tutmak için uzun vadeli bir plan sürekli, günlük bir şekilde geliştirilir, onaylanır, uygulanır ve işletilir. Sistematik ve stratejik doğalarının bir sonucu olarak, SMS etkinlikleri ani dramatik değişimlerin aksine, kademeli ama sürekli iyileştirmeyi hedefler. Bir SMS'nin sistematik doğası aynı zamanda sonuçlardan çok süreçlere odaklanılmasını sağlar. Sonuçların (yani olumsuz olaylar) emniyet risklerinin kontrolünü destekleyen çözümler oluşturduğu kabul edilse de, bir SMS'nin ana odağı, sonuçlardan önce gelen, örgütün hizmetlerinin sunumu sırasında karşılaştığı rutin operasyonel etkinlikler (süreçler) sırasında ortaya çıkan tehlikelerin yakalanmasıdır.

7.3.3 Bir SMS proaktiftir, çünkü emniyeti etkileyen olaylar ortaya çıkmadan önce, tehlikelerin tanımlanmasını ve emniyet risklerinin kontrolünü ve azaltılmasını vurgulayan bir yaklaşım üzerine inşa edilir. Olumsuz bir olay yaşandığında onarım eylemine girişmek ve ardından bir sonraki olumsuz olay yaşanana ve onarım eylemi yeniden uygulanana kadar "uyku moduna" geçmek yerine, emniyet risklerinin örgütün sürekli kontrolü altında tutmayı amaçlayan stratejik planlamayı içerir. Etkili tehlike tanımlama işlemini sürdürmek için, hizmetlerin sunulması için gereken operasyonel etkinlikler sürekli olarak izlenir. Bu da, tehlikelerle ilgili emniyet verilerinin toplanmasını sağlayarak, fikirler veya daha kötüsü yanlı görüşler veya önyargılara dayanarak emniyet riskleri hakkında kararlar formüle edilmesinin aksine, emniyet riskleri ve kontrol edilmeleri hakkında verilere dayanan örgüt kararları alınmasını sağlar.

7.3.4 Son olarak, bir SMS açıktır, çünkü tüm emniyet yönetimi etkinlikleri belgelenir, görülebilir ve dolayısıyla savunulabilir. Emniyet yönetimi etkinlikleri ve buna bağlı olarak örgütün emniyet yönetimi bilgi birikimi herkesin erişimine açık resmi belgelerde formel bir şekilde kaydedilir. Dolayısıyla, emniyet yönetimi etkinlikleri saydamdır. Bu bakımdan, Bölüm 4'te ele alınan "emniyet kütüphanesi" emniyet yönetimi etkinliklerinin ve bilgi birikiminin formel örgüt yapıları içinde belgelenmesini ve sadece bireylerin kafasında kalmasını sağlamada önemli bir rol oynar. Emniyet yönetimi etkinliklerinin ve bilgi birikiminin bireylerin kafasında kaldığı bir durumun gelişmesine neden olan bir örgüt, emniyet etkinliklerinin ve bilgi birikiminin korunması bakımından kendini son derece istikrarsız bir konuma sokar.

7.4 SİSTEM TANIMLAMASI

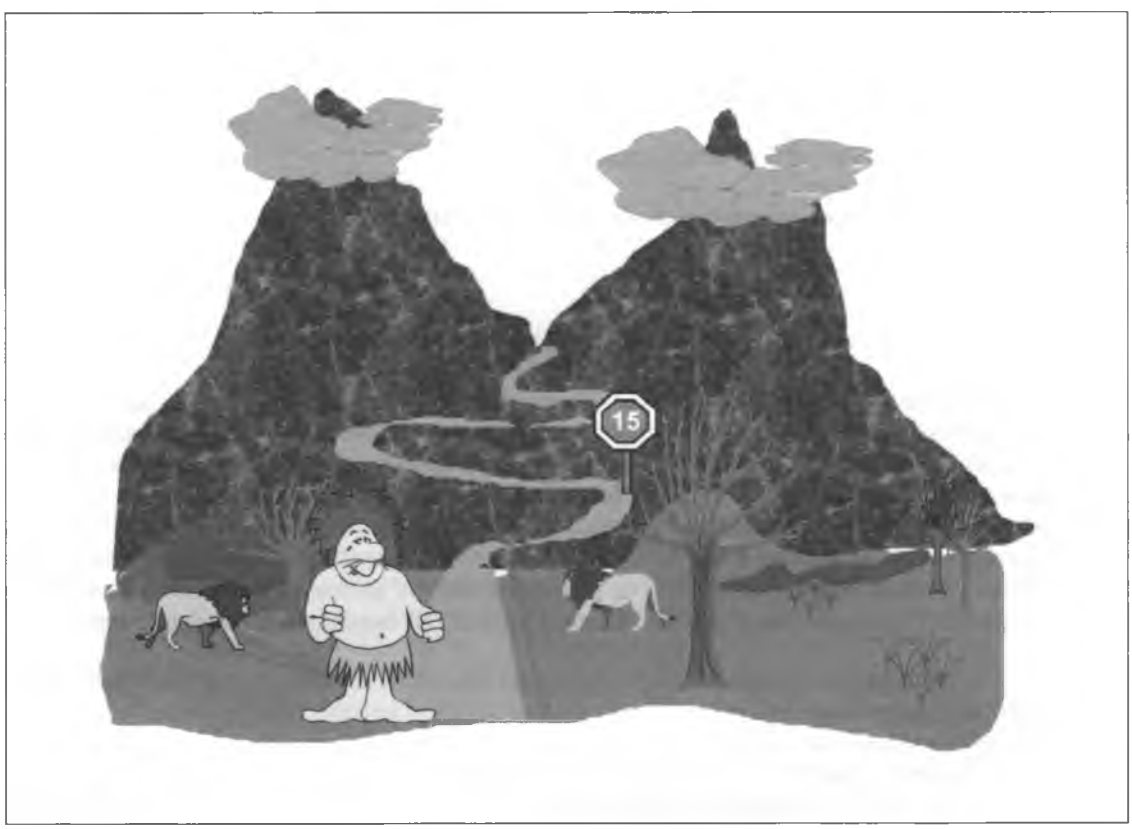
7.4.1 Bir sistem tanımlaması, SMS'nin geliştirilmesinin ilk ön koşuludur. Bölüm 2'de havacılık ortamındaki insanlar, bağlam ve emniyet arasındaki ilişki ele alınmıştır. Bu tartışmada hizmetlerin sunulması sırasındaki emniyet açıklarının kaynaklarının, insanlar ve insanların hizmet sunma etkinliklerini gerçekleştirdikleri operasyonel bağlamın diğer bileşenleri arasındaki arayüzdeki uyumsuzluklarda bulunduğu öne sürülmektedir. İnsanlar ve operasyonel bağlamın diğer bileşenleri arasındaki etkileşimin sonucu olan potansiyel emniyet açıkları, tanımlanabilir ve kontrol edilebilir unsurlara sahip tehlikeler bağlamında özel olarak karakterize edilebilirler. Tehlikeler üretim sistemlerinin benzersiz bileşenleridir ve çoğu tehlike hasar verme potansiyelini sistemin farklı bileşenleri ile operasyonel etkileşimlerin sonucunda ortaya çıkarır.

7.4.2 Aşağıda basit bir örnek verilmiştir. Yakıt havacılık sisteminin bir bileşenidir ve her enerji kaynağı gibi bir tehlikedir. Yeraltındaki depolarda dokunulmadan saklanırken, yakıtın bir tehlike olarak hasar verme potansiyeli düşüktür.

Uçaklar da havacılık sisteminin bileşenleridir. Uçaklara yakıt konması gerekir. İnsanlar uçaklara yakıt ikmali yaparken (hizmetin sunulması için gerekli bir operasyonel etkileşim), yakıtın bir tehlike olarak hasar verme potansiyeli önemli ölçüde artar. Bu durumda, yakıt ikmali işletmelerin örgüt kontrolü altına alınması için yakıt ikmali prosedürleri uygulanır. Bu prosedürler tehlikenin unsurlarının tanımlanması ve kontrolünü temel alır. Tehlikenin unsurlarının tanımlanması ve büyük oranda kontrolü, ilk ve önemli bir adım olarak, sistem tanımlamasına dayanır.

7.4.3 Havacılık ortamındaki insanlar, bağlam ve emniyet arasındaki ilişkinin açıklanması için Bölüm 2'de kullanılan örnek de bir sistem tanımlamasının ifade edilmesinde yararlıdır.

7.4.4 Şekil 7-2'de hizmet sunma etkinliğinin gerçekleştiği ortam gösterilmektedir. Söz konusu hizmet küçük paketlerin insanlar (mağara adamları) tarafından dağların diğer tarafına teslim edilmesidir. Hizmetin sunulmasında yer alan insanlar, kullanacakları araçlar ve yöntemler ve ortamın özelliklerinin kombinasyonu, hizmet sunma etkinliğinin gerçekleşeceği operasyonel ortamını oluştururlar. Söz konusu sistem, paketlerin teslimi ile ilgili bir sosyo-teknik sistemdir (yani insanları ve teknolojiyi bir araya getiren bir sistemdir). Emniyet açıklarının kaynakları, özel olarak insanlar ve insanların hizmet sunma etkinliklerini gerçekleştirdikleri operasyonel bağlamın diğer bileşenleri arasındaki arayüzdeki uyumsuzluklarda bulunan tehlikeler olarak karakterize edildiklerinden, bu tür uyumsuzlukların belirlenmesindeki ilk adım sistemi bileşenleri ve bileşenler arasındaki etkileşimler bakımından tanımlamak olacaktır.



Şekil 7-2. Sistem tanımlaması

7.4.5 Bölüm 2'de ele alınan SHEL modelini kullanarak, bu sistemin bileşenleri ve aralarındaki etkileşim bakımından bir tanımlaması aşağıdaki şekilde olabilir. Sosyo-teknik sistemin işlevi paketlerin teslimatıdır. Diğer sistemlerle arayüzlere sahiptir: topografik bir sistem, hava sistemi, vahşi yaşam sistemi. Sosyal bir bileşen vardır: insanlar. Sistemin işletmesi için temel önemde olan insan performansı konuları vardır: aslanlarla, dağlarla ve havayla etkileşim kurarken insanlar nasıl bir performans göstereceklerdir? Sistemde donanım bileşenleri vardır: dağlardan geçen yol, uyarı işaretleri. Yazılım bileşenleri de vardır: hizmetin sunulması sağlanırken (paketler dağın diğer tarafındaki araç yoluna sağlam halde ulaşması gerekir) sistemin işletmesinde ve sistemle etkileşimde insanlara kılavuzluk sağlayacak dokümantasyon, prosedürler ve eğitim (aslanlarla nasıl başa çıkılır, yoldaki virajlar nasıl bildirilir, havaya karşı nasıl korunur).

7.4.6 Formel veya teknik bir şekilde ifade edilirse, havacılıktaki bir sistem tanımlaması aşağıdakileri içermelidir:

a) sistemin hava taşımacılığı sistemindeki diğer sistemlerle etkileşimleri;

b) sistem işlevleri;

c) sistemin işletmesi için gereken insan performansı ile ilgili konular;

d) sistemin donanım bileşenleri;

e) sistemin işletmesi için kılavuzluk sağlayacak ilgili prosedürler dahil olmak üzere, sistemin yazılım bileşenleri;

f) operasyonel ortam ve

g) sözleşme yapılan ve satın alınan ürün ve hizmetler.

7.4.7 Bu bölümün Ek 1'inde sistem tanımlaması ile ilgili kılavuzluk sağlanmaktadır.

7.5 BOŞLUK ANALİZİ

7.5.1 İnsanlar ve sistemin diğer bileşenleri arasındaki arayüzlerde tehlike olarak tanımlanan emniyet açıklarının kaynaklarının belirlenmesinde ilk adım sistem tanımlamasıdır. Sistem bileşenleri ve etkileşimleri bakımından tanımlandıktan sonra, ikinci adım insanlar ve sistemin diğer bileşenleri arasındaki arayüzlerde tehlike olarak tanımlanan bu emniyet açıklarının, sistemde zaten mevcut olan kaynakların bir analizi aracılığıyla ele alınmasıdır. Analizin iki hedefi vardır. İlk hedef, sistem tanımlaması aracılığıyla tanımlanan farklı bileşenler arasında arayüzlerde ortaya çıkan uyumsuzlukların tanımlanmasıdır. Bu uyumsuzluklar emniyet açıklarıdır. İkinci hedef, bozuk arayüzlerin düzeltilmesi, hizmetleri emniyetli bir şekilde sunar ve görevlerini etkin bir şekilde yerine getirirken insanlara yardım edilmesi için hangi ek kaynaklara ihtiyaç duyulacağının belirlenmesidir. Bu, boşluk analizi olarak adlandırılır.

7.5.2 Bir SMS perspektifinden, bir boşluk analizi temel olarak SMS'nin çalışması için gerekenlerle karşılaştırıldığında, örgüt içinde zaten bulunan emniyet düzenlemelerinin bir analizidir. Bir boşluk analizi önemlidir, çünkü bir SMS'nin geliştirilmesine başlamak için gereken temel örgüt yapıları örgüt içinde zaten mevcut olabilirler: çoğu örgütte bir SMS ile ilgili çeşitli etkinlikler zaten mevcut ve çalışır durumda olacağı için bir SMS'nin tamamen baştan inşa edilmesi nadiren gerekecektir. Bir SMS'nin geliştirilmesi sırasında mevcut örgüt yapılarından yararlanılmalı ve SMS bu yapılar üzerinde geliştirilmelidir.

7.5.3 Şekil 7-2'ye dönüldüğünde ve sistem tarafından sunulan hizmetin insanlar tarafından, küçük paketlerin dağın diğer tarafına teslimatı olduğu akılda tutulursa, basit bir boşluk analizinin örneği verilmiş olur.

Analiz için kılavuz soru şu olmalıdır: hizmeti verecek operasyonel personel (bu örnekte mağara adamı), bu iş yeterli kaynaklarla doğru şekilde donatılmış durumda mı? Bu sorunun yanıtı hem emniyeti (yani personel hizmetin emniyetli şekilde verilmesi için doğru şekilde donatılmış mı?) hem de etkinliği (yani personel hizmetin etkin şekilde verilmesi için doğru şekilde donatılmış mı?) dikkate almalıdır.

7.5.4 Bölüm 2'de ele alınan SHEL modeli bu sorulara yanıt vermek ve boşluk analizinin yönlendirmek için yararlı bir araçtır (bkz. Şekil 7-3). Mağara adamı Personeldir (L). Araç yolu, DUR işareti, hız işareti ve dağ geçidinin üstüne yakın tünel Donanımdır (H). Ağaçlar, aslanlar, dağlar ve bulutlar Ortamdır (E). Görünür olmasa da, mağara adamının aldığı eğitim ve hizmetin verilmesi için mağara adamının uyması gereken prosedürler ve talimatlar Yazılımdır (S). Şekil 7-3'te gösterildiği gibi, boşluk analizi Şekil 7-2'ye kıyasla aşağıdaki sonuçları üretecektir:

a) Mağara adamı, dolambaçlı ve muhtemelen düzgün olmayan bir araç yolundan, dağlar üzerinden geçmelidir, ama yalın ayaktır. Bu nedenle, ayağını incitebilir ve düşebilir (emniyet) ve/veya yavaş ilerleyebilir ve dolayısıyla paketlerin teslimatını geciktirebilir (etkinlik). Boşluk analizine göre, bu durumda mağara adamı (L) ile araç yolu (H) arasındaki arayüzdeki uyumsuzluğu ele almak için ayakkabı sağlanması önemli olacaktır.

b) Dağların tepesindeki geçitteki bulutlar yağmura ve fırtınalara neden olabilir. Bu durumda, şapka sağlanması mağara adamını koruyacak ve mağara adamı (L) ile bulutlar (E) arasındaki arayüzdeki uyumsuzluğun ele alınmasını sağlayacaktır.

Şekil 7-3. Boşluk analizi

c) Aslanlar mağara adamı ve hizmetin sunulması için açık bir tehlikedir. DUR işareti sistemde zaten mevcut bulunan, mağara adamını tehlike (yani özellikle tehlikeli alana girme) konusunda uyarmayı amaçlayan bir kaynaktır. Yine de, kendini savunmayı sağlayacak bir araç uygun bir ek kaynak olacaktır. Bu durumda, mağara adamına bir mızrak sağlanması mağara adamı (L) ile aslanlar (E) arasındaki uyumsuzluğun ele alınmasını sağlayacaktır.

d) DUR işaretine ek olarak, özellikle tehlikeli alana girmeden önce araç yoluna boyanan sarı "tut" çizgileri farkındalığı arttıracak ve mağara adamının dikkatini aslanlara yönelterek, mağara adamı (L) ile aslanlar (E) arasındaki uyumsuzluğun ele alınması için mızrağın ek bir kaynak olarak kullanılmasını sağlayacaktır.

e) Mağara adamının, kaba ve bozuk dağ yolunda yürürken daha iyi denge sahibi olmasının yanında mızrağını tutmak için ellerinin boş kalmasını sağlamak üzere küçük paketleri taşımasını sağlayan bir donanımı yoktur. Paketlerin taşınması için bir sırt çantası, mağara adamı (L) ile aslanlar (E) ve mağara adamı (L) ile araç yolu (H) arasındaki arayüzdeki uyumsuzluğu ele almak için ek bir kaynak olacaktır.

f) Dolambaçlı bir araç yolunun başlangıcında yolcuları dolaylı bir şekilde uyaran bir hız işareti vardır. Hız işareti, araç yolunun devamındaki koşullar hakkında anlaşılır bir mesaj vermemektedir. Bu işe ayrılmış ve açık bir uyarı işareti bu durumda mağara adamı (L) ile araç yolu (E) arasındaki arayüzdeki uyumsuzluğu ele almak için ek bir kaynak olacaktır.

g) Dağın tepesindeki geçidin bir tünelle olduğu hakkında hiçbir uyarı yoktur. Bir uyarı işareti mağara adamı (L) ile yol (E) arasındaki arayüzdeki uyumsuzluğu ele almak için ek bir kaynak olacaktır.

7.5.5 Böylece bir boşluk analizi, insanlar ve operasyonel bağlamın diğer bileşenleri arasındaki etkileşim sonucunda ortaya çıkan tehlikeler bakımından belirtilen emniyet açıklarının ele alınması için sistemde mevcut olan kaynakları, yapıları ve emniyet düzenlemelerini açığa çıkarır. Ayrıca, emniyet açıklarının azaltılması ve operasyonlardaki tehlikelere karşı dayanıklılığın arttırılması için gerekli olacak ek kaynakları, yapıları ve emniyet düzenlemelerini de açığa çıkarır.

7.5.6 Boşluk analizi tamamlandığında ve tamamen belgelendiğinde, eksik veya hatalı oldukları belirlenen kaynaklar, yapılar ve düzenlemeler, mevcut olanlarla birlikte SMS uygulama planının temelini oluşturacaktır. Örgütler SMS uygulama planlarını kendi gereksinimlerine göre biçimlendirebilirler; ancak görüntüleme veya izlemenin kolaylığı bakımından bir çalışma tablosu formatı, Gantt çizelgesi veya MS Project tipi bir düzen önerilir. Gereken SMS bileşenlerinin ve unsurlarının bir araya getirilmesi için, örgütün politikaları, hedefleri, prosedürleri ve süreçleri nasıl oluşturacağının veya değiştireceğinin belirlenmesini sağlamak üzere her bir öğe değerlendirilecektir. Bu bölümün Ek 2'sinde, örgütteki kendi sistemlerini tanımladıktan sonra bir örgütün neyin eksik olduğunu bulmasına yardımcı olarak soru önerileri ile birlikte, hizmet sağlayıcılar için bir örnek verilmiştir.

7.6 SMS ve QMS

7.6.1 Kalite yönetimi havacılık sisteminin pek çok segmentinde uzun zamandır kullanılmaktadır. Pek çok havacılık örgütü kalite kontrolü (QC) ve/veya kalite güvencesini (QA) yıllardır uygulamakta ve işletmektedir.

7.6.2 Bir QA programı örgütün kalite politikasını ve hedeflerini tanımlar ve oluşturur. Örgütün etkinliği iyileştirmek ve hizmetle ilgili riskleri azaltmak için gereken unsurlara sahip olmasını sağlar. Doğru şekilde uygulanırsa, bir QA prosedürlerin geçerli gerekliliklere uygun olarak ve tutarlı bir şekilde yürütülmesini, sorunların belirlenmesini ve çözülmesini ve örgütün prosedürlerini, ürünlerini ve hizmetlerini sürekli olarak gözden geçirmesini ve iyileştirmesini sağlar. Kurumsal hedeflere ulaşılması için, QA sorunları belirlemeli ve prosedürleri iyileştirmelidir.

7.6.3 QA ilkelerinin emniyet yönetimi süreçlerinde uygulanması, örgütün emniyet hedeflerine ulaşmasını desteklemek için gereken sistem çapındaki önlemlerin alındığından emin olunmasını sağlar. Ancak, QA kendi başına kalite dogmasında öne sürüldüğü gibi, "emniyetin güvence altına alınması sağlayamaz". Bir örgütün, hizmetlerinin sunulması ile etkinlikleri sırasında karşılaşması gereken tehlikelerin sonuçlarına ait emniyet risklerinin yönetilmesi ile ilgili en geniş kapsamlı hedefe ulaşılması için gerek duyulan süreçlerin standardizasyonunu sağlamak için bir örgüte yardımcı olan, QA ilkeleri ve konseptlerinin emniyetin güvence altına alınması bileşeni (Bölüm 9'da ele alınmıştır) altında bir SMS'ye entegre edilmesidir.

7.6.4 QA ilkeleri, aşağıdaki unsurlar dahil olmak üzere, bir örgütün tüm yönlerinin performansının izlenmesine yönelik prosedürleri içerir:

a) prosedürlerin (örneğin SOP'ların) tasarımı ve dokümantasyonu;

b) denetim ve test yöntemleri;

c) donanım ve işletmelerin izlenmesi;

d) dahili ve harici denetimler;

e) alınan düzeltme önlemlerinin izlenmesi ve

f) gerektiğinde uygun istatistik analizlerinin kullanılması.

7.6.5 Birkaç havacılık örgütü QC ve QA programlarını, kalite yönetimi sistemleri (QMS) olarak adlandırılan programlar altında entegre etmişlerdir. Kalite güvencesi ile ilgili olarak uluslararası düzlemde kabul edilmiş bazı standartlar günümüzde kullanılmaktadır. Seçilen standartlar, örgütün büyüklüğüne, karmaşıklığına ve ürüne bağlıdır. Örneğin ISO 9001-2000 standardı, ISO tarafından geliştirilen ve pek çok örgüt tarafından şirket içinde bir kalite yönetimi sistemi uygulamak için kullanılan bir uluslararası standartlar kümesidir. Bu tür sistemlerin kullanılması, aynı zamanda tedarikçi veya yüklenicilerin uygun kalite yönetimi sistemlerine sahip olmasını sağlar.

7.6.6 Havacılıktaki QA/QC'nin uzun geçmişine, SMS'nin göreli olarak daha genç olmasına ve belirli SMS süreçlerinin kalite ilkeleri tarafından beslendiğine bakıldığında, SMS ile QMS arasındaki ilişkinin yanlış anlaşılması ve yanlış algılanması potansiyeli gerçektir. Dolayısıyla, bu ilişkinin ve SMS'nin ve QMS'nin genel örgüt hedeflerine ve özellikle de örgütün emniyet hedeflerine ulaşılmasındaki göreli katkısının karşı çıkmak yerine sinerji sağlayan bir perspektiften tanımlanması önemlidir.

7.6.7 SMS ve QMS'nin pek çok ortak yönü olduğunun söylenmesi doğrudur: Her ikisi de:

a) planlanmalı ve yönetilmelidir;

b) ölçüm ve izlemeye dayanmalıdır;

c) örgütteki tüm işlevleri, süreçleri ve kişileri içermelidir ve

d) sürekli olarak iyileştirmeyi amaçlıdır.

7.6.8 SMS ve QMS'nin pek çok ortak yönü olduğundan, bir QMS oluşturmuş ve çalıştırmakta olan bir örgütün SMS'ye ihtiyacı olmadığını veya zaten SMS'ye sahip olduğunu kabul etme yönünde bir eğilim olabilir. Ancak, SMS ve QMS'nin pek çok ortak yönü olduğu gibi, ikisi arasında önemli farklar da vardır, ayrıca örgütün, hizmetlerinin sunulması ile etkinlikleri sırasında karşılaşması gereken tehlikelerin sonuçlarına ait emniyet risklerinin yönetilmesi ile ilgili en geniş kapsamlı hedefe ulaşılmasında QMS'Nin kendi başına yeterince etkili olamayacağı da açıktır.

7.6.9 Kalite yönetimi 1960'larda kullanılmaya başlamıştı, o dönemde insan performansı, örgütten kaynaklanan etkenler ve bunların emniyet üzerindeki etkileri ile ilgili anlayış bugünkü kadar gelişmiş değildi. Bu nedenle, zaman içindeki değişiklikler ve sürekli güncellemeye karşın, kalite yönetimi örneğin bir felakete neden olabilecek karmaşık gizli hata yolu gibi yüksek seviyeli/yüksek sonuçlu sorunların tanımlanmasında daha az etkilidir. Üstelik, denetim bürokrasisi ve formel bir kalite onayı alma süreci kendi kendilerinde sonlanma potansiyeline sahiptir: kurumsal genel merkezin girişinde bir ISO onayı flaması asma hedefi örgütün emniyet uygulamaları oluşturma hedefinden sapmasına ve emniyet açısından odağını yitirmesine neden olabilir.

7.6.10 SMS insan performansı, İnsani Etkenler ve örgütten kaynaklanan etkenlere odaklanır ve uygun olduğunda emniyet memnuniyetine erişmeye katkıda bulunması için bunlara kalite yönetimi tekniklerini ve süreçlerini entegre eder. SMS'nin hedefi örgütün karşı karşıya gelmesi gereken ve çoğu durumda hizmetlerin sunulması sırasında yol açacağı tehlikelerin tanımlanması ve bu tehlikelerin sonuçlarına ait emniyet risklerinin örgüt kontrolü altına alınmasıdır. Geniş anlamda, bu hedefin ilk buyruğu – tehlikenin tanımlanması – SMS'nin emniyet yönetimi ilkeleri ve uygulamalarını temel alan emniyet riski yönetimi bileşeni (Bölüm 9'da ele alınmıştır) aracılığıyla gerçekleştirilir. İkinci buyruk — emniyet risklerinin örgüt kontrolü altına alınması — bir SMS'nin emniyet ve kalite yönetimi ilkeleri ve uygulamalarının entegrasyonunu temel alan emniyetin güvence altına alınması bileşeni (yine Bölüm 9'da ele alınmıştır) aracılığıyla gerçekleştirilir.

7.6.11 Kısaca, öyleyse SMS aşağıdakiler bakımından QMS'den farklıdır:

a) SMS örgütün emniyetle ilgili, insani ve örgütle ilgili yönlerine (yani emniyet memnuniyeti) odaklanırken

b) QMS örgütün ürünleri ve hizmetlerine (yani müşteri memnuniyeti) odaklanır.

7.6.12 SMS ile QMS arasındaki ortak ve farklı yönler anlaşıldıktan sonra, her iki sistem arasında sinerjiye dayanan bir ilişki oluşturulması mümkündür. İlişkinin asla düşmanca değil, birbirini tamamlayıcı olduğu ne kadar vurgulanırsa azdır; bu ilişki aşağıdaki özetlenir:

a) SMS kısmen QMS ilkeleri üzerinde inşa edilir;

b) SMS hem emniyet hem de kalite politikaları ve uygulamalarını içermelidir ve

c) SMS açısından bakıldığında, kalite ilkeleri, politikaları ve uygulamalarının entegrasyonu emniyetin yönetilmesinin desteklenmesine odaklanmalıdır.

7.6.13 SMS ile QMS arasında birbirini tamamlayıcı bir ilişki kurulması, her bir sisteme örgüt emniyet hedeflerine erişilmesinde birbirini tamamlayıcı şekilde katkıda bulunulmasını sağlar:

a) SMS emniyet tehlikelerinin ve sonuçlarının tanımlanması için örgüt süreçlerinin ve prosedürlerinin tasarlanması ve uygulanmasına neden olur ve havacılık işletmeleriyle ilgili emniyet risklerinin örgüt kontrolü altına alınmasını sağlar.

b) QMS'nin SMS'ye entegrasyonu emniyet tehlikelerinin ve sonuçlarının tanımlanması için örgüt süreçlerinin ve prosedürlerinin izlenmesini ve havacılık işletmelerindeki ilgili emniyet risklerinin örgüt kontrolü altına alınmasını, amaçlandığı gibi çalışmalarını ve çalışmadıklarında iyileştirilmelerini sağlar.

7.6.14 Bölüm 6'da ele alına Ekler 1, 6, 8, 11 ve 14'te bulunan ICAO emniyet yönetimi SARP'lerinin SMS ile sınırlı olduğu vurgulanmalıdır. Belirtilen Annexlerde QMS ile ilgili ICAO gereklilikleri yoktur, sadece istisnai olarak Annex 6, Kısım I, Bölüm 8'de onaylı bakım örgütleri (AMO) için bir gereksinim vardır.

7.7 SSP/SMS VE KAZA İNCELEME SÜRECİ

7.7.1 SMS ile QMS arasındaki ilişkide olduğu gibi, SSP veya SMS ve kaza inceleme süreci ve kaza inceleme sürecinin emniyet yönetimi ortamında oynadığı rol arasındaki ilişki, emniyet topluluğunda tartışılan bir konu olmuştur. Tartışmalar, çoğunlukla SMS ile kaza inceleme süreci arasındaki ilişkiye odaklanmış olsa da, SSP de kuşkusuz tartışmanın bir parçası olmalıdır. Tıpkı SMS ile QMS arasındaki ilişkide olduğu gibi, SSP/SMS ile kaza inceleme süreci arasındaki ilişkinin mutlak tamamlayıcılık ve sinerji içeren bir ilişki olduğu asla yeterince vurgulanamaz. Kaza inceleme süreci emniyet yönetimi sürecinin önemli bir aracıdır.

7.7.2 Emniyet yönetimi sürecinde, Bölüm 3'te ele alındığı gibi diğer örgüt süreçlerinin yanında emniyetin yönetimi ile ilgili günlük etkinlikler SSP veya örgütün SMS'si aracılığıyla sağlanır. Bir kaza (veya ciddi bir olay), sırasıyla bir Devlet veya örgütte emniyetin yönetimi için gerekli etkinlikleri yönlendiren yönetim sistemleri olarak SSP veya SMS (veya her ikisinin) nihai başarısızlığını temsil eder. Bu türden nihai bir arıza ortaya çıktığında, emniyet yönetimi etkinliklerinin başarısızlığının nedenlerini bulmak ve arızanın tekrarlanmaması için gerekli önlemleri oluşturmak için kaza inceleme süreci başlatılır. Dolayısıyla, bir emniyet yönetimi ortamında, kaza inceleme sürecinin ayrıcı bir rolü vardır. Sistemdeki tüm emniyet savunmaları, engelleri, kontrolleri ve dengeleyiciler başarısız olduğunda başlatılan, havacılık sistemindeki emniyetin nihai koruyucusudur.

7.8 YÖNETİM SİSTEMLERİNİN ENTEGRASYONU

7.8.1 Havacılık örgütleri bazen "sistemlerden oluşan bir sistem" olarak tanımlanır. Bunun nedeni, havacılık örgütlerinin hizmetlerinin sunulması aracılığıyla üretim hedeflerine ulaşmak için farklı yönetim sistemlerini uygulamaları ve çalıştırmalarının gerekmesidir. Bir havacılık örgütün çalıştırması gereken tipik yönetim sistemleri aşağıdakileri de içerir:

a) kalite yönetimi sistemi (QMS);

b) çevre yönetimi sistemi (EMS);

c) iş sağlığı ve emniyeti yönetimi sistemi (OHSMS);

d) emniyet yönetimi sistemi (SMS) ve

e) Emniyet yönetimi sistemi (SEMS).

7.8.2 Sivil havacılıkta tüm bu farklı yönetim sistemlerini entegre etme eğilimi giderek artmaktadır. Bu entegrasyonun açık avantajları vardır:

a) tekrarların ve dolayısıyla maliyetlerin azaltılması;

b) genel örgüt risklerinin azaltılması ve karlılıkta artış;

c) potansiyel olarak çatışan hedeflerin dengelenmesi;

d) potansiyel olarak çatışan sorumlulukların ve ilişkilerin ortadan kaldırılması ve

e) güç sistemlerinin dağıtılması.

7.8.3 Ancak bütün bu sistemlerin, özellikle de SMS'nin örgüt içindeki diğer yönetim sistemleriyle entegre edilmesi için farklı yöntemler vardır. Havacılık örgütleri kalite, emniyet, iş sağlığı ve emniyeti ve çevre koruma yönetimi sistemlerinin entegre edilmesi için cesaretlendlrilmelidir. Ancak, bu entegrasyon ICAO uyumlu emniyet yönetimi SARP'lerinin ve bu el kitabının kapsamının dışındadır.

7.9 TERİMLERİN AÇIKLANMASI

Hizmet sağlayıcıların ve/veya sivil havacılık denetim kurumlarının sorumluluğu altında gerçekleştirilen farklı emniyet yönetimi etkinlikleri ile ilgili olarak kullanılan terminoloji konusunda ortak bir anlayış geliştirilmesi önemlidir. Aşağıdaki terimler bu el kitabında kullanıldığında, aşağıdaki anlamlara gelmektedirler:

a) ***Emniyet gözetimi*** Devletin operatörlerin/hizmet sağlayıcıların SMS'sine göre yaptığı şeydir;

b) ***Emniyetin güvence altına alınması*** izleme ve ölçüm dahil olmak üzere Devletin kendi SSP'sinin emniyet performansına göre ve operatörlerin/hizmet sağlayıcıların kendi SMS'lerinin emniyet performansına göre yaptığı şeydir ve

c) ***Emniyet denetimi*** Devletin kendi SSP'sinin yapısına göre ve operatörlerin/hizmet sağlayıcıların kendi SMS'lerinin yapısına göre yaptığı şeydir.

Not — Emniyet gözetimi denetimi ICAO USOAP'ın CAA'nın Devlet emniyet programına (SSP) göre ve ICAO SARP'lerine ve ilgili kılavuzluk malzemelerine uygun olarak kendi emniyet gözetimi kapasitelerine göre yaptığı şeydir.

7.10 EMNİYET SLOGANLARI İLE EMNİYET İLKELERİ ARASINDAKİ FARK

7.10.1 Havacılıkta uzun zamandır yerleşik olan, emniyet sorunları hakkında farkındalık uyandırmak için sloganlara dayanma yönünde bir eğilim vardır, bu eğilim sonucunda çoğu zaman sloganlar ilkelerle karıştırılır. Sloganlar ile ilkeler arasında büyük bir fark vardır. İkincisi açıkça sağlam bilgilere dayanan bir kılavuz bilgileri dile getirir ve belirli bir çabanın nasıl gösterileceği hakkında kapsamlı ifadeler sağlar. İlki geleneksel ve bazen sorgulanması gereken yaygın bilgeliğe (halk bilgeliği) dayanan belirsiz referansları dile getirir ve çoğunlukla bir sorunun nasıl çözüleceği hakkında yanıltıcı ifadelerde bulunur. Emniyetin yönetimi ve bir SSP/SMS'nin kullanılmaya başlaması gibi kritik bir çabanın "sloganlara dayanarak" gerçekleştirilmeye çalışması kesinlikle makul değildir. Ancak, bu potansiyel mevcuttur. Bu bölümde, çoğunlukla Bölüm 2 ve 3'te alınan temel emniyet ve emniyet yönetimi konseptlerini uygulayarak, havacılığın en çok tutulan beş emniyet sloganı gözden geçirilmekte ve bu sloganların geçersiz olduğu gösterilmektedir:

a) Havacılıkta, emniyet ilk önceliktir.

b) Emniyet herkesin sorumluluğudur.

c) Bozulmadıysa, niye onarılması gereksin ki?

d) Emniyetin pahalı olduğunu düşünüyorsanız, bir kaza yapmayı deneyin.

e) Kazaların yüzde yetmişi insan hatasından kaynaklanır.

7.10.2 ***Havacılıkta, emniyet ilk önceliktir.*** Üretim sistemlerindeki örgütler, isimlerinin açıkça gösterdiği gibi, otomobil üretimi, petrol çıkarma veya ticari havacılıkta olduğu gibi insanların ve malların hava yoluyla taşınması gibi bir üretim hedefine ulaşmaya çalışmak için oluşturulmuşlardır. Üretim sistemlerindeki örgütler, üretim hedeflerine ulaşma çabalarını sürdürmek için gerekli kaynaklara sahip olabilmeleri için, etkinliklerinin sonucunda para kazanmak zorundadırlar. Bu nedenle, havacılıkta neden emniyetin ilk önceliğe sahip olabileceği görmek zordur; paranın önce geldiğinin düşünülmesi mümkündür. Bölüm 2'de ele alındığı gibi, havacılıkta emniyet havacılık örgütlerinin emniyetli bir şekilde para kazanabilmesi için üretim ve koruma hedeflerine makul, koordineli bir şekilde öncelik verilmesini içeren bir sorundur. Ancak, bu sloganda önceliklerin karıştırılması arada bir hatalı çabalara neden olmuştur. Aslında, olumsuz olaylarla karşı karşıya kaldıklarında işlevsel olmayan örgütlerin en sık kullandıkları argüman, karşı yöndeki kanıtlara rağmen, "şirketimizde, emniyet öncelikli" olmasına karşın söz konusu kötü sonucun başlarına nasıl geldiğini anlayamadıklarıdır. Geçmiş, bu sloganın arkasında gizlenen ve uygun eylemlerle desteklemeyen örgütlerin en kötü emniyet sabıkasına sahip olduklarını göstermiştir.

7.10.3 ***Emniyet herkesin sorumluluğudur.*** Bu slogan kafa karıştırıcıdır. İnsan hasta olduğunda, doktora gider. Hukukla ilgili bir danışmaya ihtiyacı olduğunda, bir avukata danışır. Musluktan su akmazsa, tesisatçıyı arar. Ancak, emniyet sorunları ile karşılaşıldığında, özellikle uzun yıllara dayanan bir deneyimleri varsa, havacılıktaki herkes konunun uzmanı olduğunu öne sürer. Gerçek ise, sadece eğitimli uzmanların günümüzdeki emniyet sorunlarını bağlamla ilişkili, etkili, etkin bir şekilde ele alabileceğidir. Havacılıktaki en iyi yönetilen örgütlerde mesleki yeterliliğe sahip, belirli iş tanımlarına ve tanımlanmış sorumluluklara ve örgüt erişimine sahip özel emniyet personeli bulunur. Bu profesyoneller örgüt emniyet izleyicileri olma sorumluluğunu üstlenirler. Havacılığın yapısında yer alan potansiyel tehlikelere karşı örgütün yapısında yer alan direnci değerlendirmek ve güçlendirmek için, diğer personelin uyacağı planlar koordine ederler. Yönetilmeyen tehlikeler ve emniyet sorunları bulduklarında birilerini suçlamazlar, ama çözüm geliştirmenin bir ön koşulu olarak sorunların belgelenmesi ve tanımlanması üzerinde çalışırlar. Bölüm 8'de bu fikirler derinlemesine ele alınmaktadır.

7.10.4 ***Bozulmadıysa, niye onarılması gereksin ki?*** Bu slogan kaza olmadığı sürece emniyetle ilgili endişelenmeye gerek olmadığını, kimse yaralanmadığı, metal bükülmediği ve örgüt eleştiri veya utançla karşı karşıya gelmediği sürece sistemin emniyetli olduğunu öne sürer. Başka bir deyişle, slogan kazaların veya kaza olmamasının sistemin emniyetinin güvenilir göstergeleri olduğunu öne sürer. Bu düşünce biçiminin alternatif bir şekli, sistemdeki tehlike işaretlerinin sürekli olarak gözetlenmesi için en iyi bilgilere dayanan yapılar ve süreçler kullanılıyorsa, kazaların sadece "sistemde yer alan talihsiz bir gürültü" olduğunu öne sürer. Bölüm 3'te açıklandığı gibi, bu sloganın altında yatan diğer yanlışların ötesinde, sistemdeki sorunları ele almadan önce sistemin bozulmasını beklemek makul olmanın ötesinde külfetli olabilir. Ayrıca, sistem bozulduğunda, insan yaşamı tehlikeye düşecektir, bu da bu yaklaşımla ilgili etik sorulara neden olur. Ancak bir kaza yaşandıktan sonra düzeltme eylemine girişmekten kaynaklanan mali ve insani maliyetler kaçınılmaz olarak yüksek olduğundan, sistemin bozulmadan önce onarılması için zorlayıcı ekonomik ve etik nedenler vardır.

7.10.5 ***Emniyetin pahalı olduğunu düşünüyorsanız, bir kaza yapmayı deneyin.*** Bu sloganın ortaya koyduğu yayın inanç, mesleki davranışlara uyarak, disiplinli olarak ve kurallara uyarak, sistemde nihayetinde kazalara yol açabilecek tüm aksaklıkların tahmin edilmesinin mümkün olduğudur. Basitçe dile getirilirse, düzenlemelere uymak ve "kitaba uygun davranmak" emniyet için yeterli garanti sağlar. Ne yazık ki, Bölüm 3'te ele alınan pratik sapmanın gösterdiği gibi, gerçek dünyada böyle olmaz. En gelişmiş yapılar ve süreçler kullanılsa da, kazalar, tıpkı hastalık ve ölüm gibi nihayetinde istatistiksel bir şans haline gelecektir. İnsanların aile doktorlarını ziyaret etmeleri ve spor programlarına katılmaları gibi, sistem performansının proaktif olarak kontrol edilmesi ve diğer proaktif çabalara girişilmesi mümkün ve makul olsa da, tüm tehlikelerin ortadan kaldırılması mümkün değildir. Tehlikeler havacılık işletmesi bağlamında ayrılmaz bileşenlerdir. Önlemek için en iyi şekilde çaba gösterilse de, havacılıkta arızalarda ve operasyonel hatalar oluşacaktır. Kalifiye personele sahip, üretim hedeflerine uygun kaynaklarla donatılmış ve iyi tasarlanmış prosedürlere sahip, etkin bir örgüt yine de bir kazayla karşılaşırken, kötü yönetilen, ciddi şekilde kaynak eksikliği bulunan, personelinin kalifiye olduğu kuşkulu, standardın altındaki uygulamalara ve kazalardan kıl payı kurtulma geçmişine sahip bir örgüt sadece şans nedeniyle bir kaza yaşamayabilir.

7.10.6 ***Kazaların yüzde yetmişi insan hatasından kaynaklanır.*** Bu slogan, emniyet sloganların ne kadar yanıltıcı olabileceğini gösterdiği için sona bırakılmıştır. Havacılık sistemini ele alalım: insanlar sistemin taslağını kavrar ve kavradıkları şeyden tatmin olduklarında tasarlamaya başlarlar. Daha sonra, insanlar sistemi inşa eder ve çalışır hale geldiğinde, insanlar sistemi çalıştırırlar. Sistemin hedeflerine erişmek için gerekli davranışları göstermeleri için, insanlar sistemin her gün çalışmasını sağlayan diğer insanları eğitir. İnsanlar sistemin performansı hakkında stratejik ve taktik kararlar verirler ve tehlikeler tanımlandığında, insanlar sistemin bu tür tehlikelerden korunması için gerekli önlemleri alırlar. Basitçe söylersek: sistemi insanlar tasarlar, üretir, eğitir, çalıştırır, yönetir ve savunur. Bu nedenle, sistem bozulduğunda, insan hatası nedeniyle olması zorunludur. Bu perspektiften ve gözlem seviyesine bağlı olarak, kazaların yüzde yüzünün insan hatasından kaynaklandığı savunulabilir.

Bölüm 7 Ek 1

SİSTEM TANIMLAMASI İLE İLGİLİ KILAVUZ BİLGİLER

1. GİRİŞ

1.1. Bir sistem tanımlaması, bir örgütteki bir SMS'nin geliştirilmesinin ilk ön koşuludur. Her sistemin yapısında, tehlikelerle karakterize edilen olası emniyet açıklıkları bulunur. Tehlike tanımlama süreci, sadece sistem tanımlamasının kapsamına giren tehlikeleri tanımlayabilir. Bu nedenle, formel tanımlamasına göre, sistemin sınırları sistemin oluşturabileceği veya karşı karşıya gelebileceği tüm olası tehlikeleri kapsayabilecek kadar geniş olmalıdır. Özellikle, tanımlamanın sistem içindeki arayüzleri ve sistemin bir parçası olarak değerlendirildiği daha büyük sistemlerle olan arayüzleri içermesi önemlidir.

1.2 Sistemin ayrıntılı bir tanımlaması aşağıdakileri içermelidir:

a) sistemin amacı;

b) sistemin nasıl kullanılacağı;

c) sistemin işlevleri;

d) sistemin sınırları ve dış arayüzleri ve

e) sistemin içinde çalışacağı ortam.

1.3 Potansiyel kayıpların veya sistemin bozulmasının emniyetle ilgili sonuçları, kısmen sistemin entegre edileceği operasyonel ortamının karakteristiğine bağlı olarak belirlenmelidir. Bu nedenle, ortamın tanımlaması emniyet üzerinde önemli bir etkisi olabilecek tüm etkenleri içermelidir. Bu etkenler örgütten örgüte değişecektir. Bunlar, örneğin hava ve yer trafiği karakteristikleri, havaalanı altyapısı ve hava durumu ile ilgili etkenleri içerebilirler. Sistemin tanımlaması aynı zamanda beklenmedik durum prosedürleri ve örneğin iletişim veya seyrüsefer yardımcılarının arızası gibi diğer normal olmayan işletmeleri de dikkate almalıdır. Bir havaalanının sistem tanımlaması örneği aşağıda ayrıntılı olarak verilmiştir.

2. BİR HAVALİMANININ SİSTEM TANIMLAMASI

Bir havaalanın sistem tanımlaması, havaalanının işletmesi için gerekli tesisleri, donanımı, personeli, süreçleri ve prosedürleri içerir. Bu işlevler aşağıdakileri içerebilir:

1. İşletme yönetimi

1.1 Hareket alanı erişim kontrolü

a) Hava
b) Kara
c) Deniz

1.2 Havaalanı acil durum planlaması

a) Acil durum prosedürleri el kitabı
b) Acil durum simülasyonu uygulamaları

1.3 Kurtarma ve yangınla mücadele

a) Kapasite
   1) Donanım
   2) Köpük/su/kuru toz boşaltma hızı
b) Tesis bakımı
c) Personel eğitimi ve deneyimi
d) Donanım mobilizasyon planı
e) Kapasite azalması (uyarı)
f) Yangın musluğu sistemi

1.4 Hareket alanı denetimi ve bakımı

a) Havaalanı el kitabı
b) Denetim formları
c) Bakım

1.5 Görsel desteklerin bakımı

a) Denetimler
b) Program

1.6 İnşaat yönetimi

a) Çalışmaların kontrolü
b) Tesis yönetimi

1.7 Apron emniyet yönetimi, araç trafiği dahil

a) Havaalanı içi operasyonları için kurallar ve düzenlemeler
b) Havaalanı içi yönetim
   1) Havaalanı içi araç yönetimi
   2) Havaalanı içi araç ehliyeti
   3) Araç incelemesi
   4) Emniyet özellikleri
   5) Uçak hizmeti koordinasyonu
   c) Donanımın park edilmesi
d) Apron disiplini
e) Geriye itme operasyonları
f) Trafik işaretleri
g) Park yeri tahsisi
h) Uçak hasar kontrolü
i) Yakıt dökülme kontrolü
j) Araç ve donanım hasarı kontrolü
k) Apron etkinlik denetimi dahil olmak üzere apron emniyeti kontrol listeleri
l) Yüklenicilere ve alt yüklenicilere verilen etkinlikler

1.8 Vahşi yaşamla ilgili tehlikelerin yönetimi

a) Kuş kontrolü yönetimi
b) Gözlem
c) Kuş çarpması raporu yönetimi

1.9 Engel kontrolü

a) Havaalanı sınırları
b) havaalanının dışı
c) Pist şeridi
d) Düzenleme ve araştırmalar
e) Uçuş rotası altında bina inşaatı onayı

1.10 Kullanılamaz durumdaki uçakların kaldırılması

a) Uçak tipine uygun donanım
b) Hazır olmaya yönelik bakım
c) Başlatma şeması
d) Hizmetlerin dışarıdan alınması prosedürlerinin/kontağın oluşturulması

1.11 Tehlikeli malların taşınması

a) Uçakta tehlikeli malların sınırlanması
b) Depolama ve yükleme
c) Eğitim programlarının oluşturulması
d) Operatörlerin tehlikeli malları kabul etmesi
e) Tehlikeli malları içeren uçak olayları için acil durum müdahale kılavuzu

1.12 Düşük görüş mesafesi ve olumsuz hava koşulları

a) Prosedürler
b) Hava trafik hizmetleri ile koordinasyon
c) Dahil olan örgütlerin sorumluluğu

1.13 Telsiz seyrüsefer yardımcılarının kurulması ve bakımı

a) NOTAMLAR

2. Havaalanı yönetimi

2.1 Slotlarla ilgili görüşmeler ve slotların tahsisi
2.2 Uçuş dağıtımı
2.3 Rehberlik ve yer gösterme
2.4 Hareket alanı yönetimi ve park yeri tahsisi
2.5 CAT II ve CAT III düşük görüş mesafeli işletmeler
2.6 Trafik kurallarının kontrolü ve lisans verme düzenlemeleri
2.7 Temizlik, atıkların kaldırılması ve zararlı kontrolü

3. Yolcu/terminal binası yönetimi

3.1 Yolcuların, bagaj akışının ve tesislerin yönetilmesi

3.2 Yolcular ve halkla ilişkiler
3.3 VIP ve CIP yardımı
3.4 Terk edilen bagajlar
3.5 Portör yardımı
3.6 El arabası yönetimi
3.7 Temizlik ve zararlı kontrolü

4. Hava trafiği ve havacılık operasyonları ve iletişim hizmetleri

4.1 Hava trafik kontrolü (düşük görüş mesafesi işletmelerinde havaalanı kontrolü)
4.2 Uçuş bilgileri ve uyarı hizmetleri
4.3 Havacılık bilgileri hizmetleri (uluslararası NOTAM ofisi ve uçuş öncesi bilgi hizmeti)
4.4 Havacılık iletişimi hizmetleri

5. Emniyet ve emniyet yönetimi

5.1 SMS'nin uygulanması ve izlenmesi

a) Emniyet yöneticisi
b) Tehlikenin tanımlanması ve sonuçların değerlendirilmesi
c) Risklerin değerlendirilmesi, kontrolü ve azaltılması
d) Emniyetin güvence altına alınması
e) Emniyet eylemi grupları
f) Emniyet yönetimi sistemleri el kitabı (SMSM)

5.2 Emniyet programının uygulanması ve izlenmesi
5.3 Havaalanı acil durum planının (AEP) uygulanması ve izlenmesi
5.4 Erişim kartlarının verilmesi için başvuruların işlenmesi

Bölüm 7 Ek 2

HİZMET SAĞLAYICILAR İÇİN BİR SMS BOŞLUK ANALİZİNİN GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

Not - Bu ek bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havalimanlarını kapsar.

1. BOŞLUK ANALİZİ

1.1 Bir SMS'nin uygulanması için bir hizmet sağlayıcının SMS'nin hangi bileşenleri ve unsurlarının mevcut olduğunu ve uygulama gerekliliklerine uyması için hangi bileşenlerin ve unsurların eklenmesi veya değiştirilmesi gerektiğini belirlemek üzere kendi sisteminin bir analizini yapması gerekir. Bu analiz boşluk analizi olarak adlandırılır ve SMS gerekliliklerinin hizmet sağlayıcının mevcut kaynakları ile karşılaştırılmasını içerir.

1.2 Boşluk analizi, kontrol listesi biçiminde, ICAO SMS çerçevesini oluşturan bileşen ve unsurların değerlendirilmesine ve geliştirilmesi gereken bileşen ve unsurların belirlenmesine yardımcı olan bilgileri sağlar. Boşluk analizi tamamlandığında ve belgelendiğinde, SMS uygulama planının temellerinden birini oluşturacaktır.

2. ICAO SMS ÇERÇEVESİ

ICAO SMS çerçevesi dört bileşen ve on iki unsurdan oluşur ve uygulanması örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına uygun olmalıdır.

1. Emniyet politikası ve hedefleri

    1.1 Yönetimin taahhüdü ve sorumluluğu
    1.2 Emniyetle ilgili hesap verme sorumlulukları
    1.3 Emniyetin sağlanmasında önemli rol oynayan personelin atanması
    1.4 Acil müdahale planlamasının koordinasyonu
    1.5 SMS dokümantasyonu

2. Emniyet riski yönetimi

    2.1 Tehlikenin tanımlanması
    2.2 Risk değerlendirmesi ve riskin azaltılması

3. Emniyetin güvence altına alınması

    3.1 Emniyet performansının izlenmesi ve ölçülmesi

3.2 Değişimin yönetilmesi
3.3 SMS'nin sürekli olarak iyileştirilmesi

4. Emniyetin teşvik edilmesi

4.1 Eğitim ve öğretim
4.2 Emniyet iletişimi

3. HİZMET SAĞLAYICILAR İÇİN SMS BOŞLUK ANALİZİ

Aşağıdaki boşluk analizi kontrol listesi bir boşluk analizi yapmak için şablon olarak kullanılabilir. Her soru "Evet" veya "Hayır" yanıtı verilmesi için tasarlanmıştır. Bir "Evet" yanıtı, hizmet sağlayıcının söz konusu ICAO SMS çerçevesi bileşeni veya unsurunu sistemine dahil ettiğini ve gereksinimi karşıladığını veya aştığını gösterir. Bir "Hayır" yanıtı, ICAO SMS çerçevesinin bileşeni/unsuru ve hizmet sağlayıcının sistemi arasında bir boşluk olduğunu gösterir.

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bileşen 1 — EMNİYET POLİTİKASI VE HEDEFLERİ			
Unsur 1.1 - Yönetimin taahhüdü ve sorumluluğu			
Bölüm 8	Bir emniyet politikası mevcut mu?	☐Evet ☐ Hayır	
Bölüm 3 ve 8	Emniyet politikası emniyet yönetimi ile ilgili olarak örgütün taahhüdünü yansıtıyor mu?	☐ Evet ☐ Hayır	
Bölüm 3 ve 8	Emniyet politikası, emniyet politikasının uygulanması için gereken kaynakların sağlanması hakkında açık bir ifade içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 3 ve 8	Emniyet politikası emniyetle ilgili raporlama prosedürlerini içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet politikası hangi tipte operasyonel davranışların kabul edilebilir olduğunu açıkça ifade ediyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet politikası disiplin cezalarının geçerli olmayacağı koşulları içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet politikası, Hesap Vermekten Sorumlu Müdür tarafından imzalanmış mı?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet politikası [örgüt] içinde açıkça onaylanmış şekilde iletilmiş mi?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet politikası [örgütle] uyumlu ve ilgili kalması için düzenli olarak gözden geçiriliyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Tutarlı bir hedef kümesi geliştirmek için formel bir süreç var mı?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet hedefleri emniyet performansı göstergeleri, emniyet performansı hedefleri ve eylem planları ile bağlantılı mı?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyet hedefleri herkese açıklanmış ve dağıtılmış mı?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Unsur 1.2 - Emniyetle ilgili hesap verme sorumlulukları			
Bölüm 8 ve 10	[Örgüt] diğer işlevlerinden bağımsız olarak, [örgüt] adına, SMS'nin uygulanması ve sürdürülmesi için nihai sorumluluğu ve hesap verme sorumluluğunu alacak bir Sorumlu Müdür belirlemiş mi?	☐ Evet ☐ Hayır	
Bölüm 8	Sorumlu Müdür emniyet yönetimi sisteminin doğru şekilde uygulanmasını ve [örgütün] tüm alanlarında gerekliliklere uygun şekilde çalışmasını sağlamaktan sorumlu mudur?	☐ Evet ☐ Hayır	
Bölüm 8	Sorumlu Müdür, operasyon sertifikası altında yürütülmesi onaylanan işletmeler için gereken mali kaynakların tam kontrolüne sahip midir?	☐ Evet ☐ Hayır	
Bölüm 8	Sorumlu Müdür, operasyon sertifikası altında yürütülmesi onaylanan işletmeler için gereken insan kaynaklarının tam kontrolüne sahip midir?	☐ Evet ☐ Hayır	
Bölüm 8	Sorumlu Müdür örgütün işlerinin yürütülmesinden doğrudan sorumlu mudur?	☐ Evet ☐ Hayır	
Bölüm 8	Sorumlu Müdür, operasyon sertifikası altında yürütülmesi onaylanan işletmeler üzerinde nihai yetkiye sahip midir?	☐ Evet ☐ Hayır	
Bölüm 8 ve 10	Örgüt SMS'nin emniyet yönetimi ile ilgili olarak, işlevlerinden bağımsız şekilde, yönetimin tüm üyelerinin ve çalışanların hesap verme sorumluluklarını tanımlamış mıdır?	☐ Evet ☐ Hayır	
Bölüm 8	Emniyetle ilgili sorumluluklar, hesap verme sorumlulukları ve yetkiler belgelenmiş ve [örgüt] içinde iletilmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8	[Örgüt] emniyet riskinin tahammül edilebilirliği ilgili olarak karar verme yetkisine sahip yönetim seviyelerinin bir tanımını yapmış mıdır?	☐ Evet ☐ Hayır	
Unsur 1.3 - Emniyetin sağlanmasında önemli rol oynayan personelin atanması			
Bölüm 8	Örgüt SMS'nin günlük işletmesini yönetmek ve denetlemek için kalifiye bir kişi atamış mıdır?	☐ Evet ☐ Hayır	
Bölüm 8	SMS'nin işletmesini denetleyen kişi gereken iş işlevlerini ve sorumluluklarını yerine getiriyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Örgütün tüm seviyelerindeki personelin emniyetle ilgili yetkileri, sorumlulukları, hesap verme sorumlulukları tanımlanmış ve belgelenmiş mi?	☐ Evet ☐ Hayır	
Unsur 1.4 - Acil müdahale planlamasının koordinasyonu			
Bölüm 8	[Örgüt], örgütün büyüklüğüne, doğasına ve karmaşıklığına uygun bir acil müdahale/beklenmedik durum planlamasına sahip midir?	☐ Evet ☐ Hayır	
Bölüm 8	[Örgüt] acil müdahale/beklenmedik durum prosedürlerini, hizmetlerinin verilmesi sırasında etkileşim kurması gereken diğer örgütlerin acil müdahale/beklenmedik durum prosedürleri ile koordine etmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8	[Örgüt] koordinasyon prosedürlerini bu tür etkileşim içinde yer alan personele dağıtmakta ve iletmekte midir?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Unsur 1.5 - SMS dokümantasyonu			
Bölüm 4 ve 8	[Örgüt] uygun tehlike dokümantasyonu ve dokümantasyonun yönetimi için bir emniyet kütüphanesi geliştirmiş ve sürdürmekte midir?	☐ Evet ☐ Hayır	
Bölüm 4 ve 8	[Örgüt] SMS dokümantasyonunu geliştirmiş ve kağıt üzerinde ve elektronik olarak tutmakta mıdır?	☐ Evet ☐ Hayır	
Bölüm 7, 8 ve 10	SMS dokümantasyonu, SMS'yi ve tüm SMS bileşenleri arasındaki bir araya gelen ilişkileri açıklayacak şekilde geliştirilmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8 ve 10	Hizmet sağlayıcı, SMS'nin örgütün emniyet planına uymasını sağlayan bir SMS uygulama planı geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8 ve 10	SMS uygulama planı uygun bir deneyime sahip bir kişi veya planlama grubu tarafından geliştirilmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8 ve 10	Kişi veya planlama grubu SMS uygulama planının geliştirilmesi için (toplantılar için gereken zaman dahil olacak şekilde) yeterli kaynak almış mıdır?	☐ Evet ☐ Hayır	
Bölüm 8	SMS uygulama planı [örgütün] üst yönetimi tarafından onaylanmış mıdır?	☐ Evet ☐ Hayır	
Bölüm 8	SMS uygulama planı [örgütün] üst yönetimi tarafından düzenli olarak gözden geçirilmekte midir?	☐ Evet ☐ Hayır	
Bölüm 8 ve 10	SMS uygulama planı, SMS'nin aşamalar halinde uygulanmasını önermekte midir?	☐ Evet ☐ Hayır	
Bölüm 8	SMS uygulama planı, hizmet sağlayıcının SMS'si ve hizmetlerinin verilmesi sırasında [örgütün] etkileşim kurması gereken diğer örgütlerin SMS'leri arasındaki koordinasyonu açıkça ele alıyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	Hizmet sağlayıcı, örgütün tüm [örgüt] açısından emniyete yaklaşımının iletilmesinin önemli bir aracı olarak bir emniyet yönetimi sistemleri el kitabı (SMSM) geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 8	SMSM diğerlerinin yanında, emniyet politikası, hedefleri, prosedürleri ve bireysel emniyetle ilgili hesap verme sorumluluklarını içerecek şekilde SMS'nin tüm yönlerini belgeliyor mu?	☐ Evet ☐ Hayır	
Bölüm 8	SMSM emniyet riski yönetiminin başlangıçtaki bir tasarım etkinliği ve emniyetin güvence altına alınmasının sürekli bir etkinlik olarak rolünü açıkça dile getirmekte midir?	☐ Evet ☐ Hayır	
Bölüm 8	SMS ile ilgili dokümantasyonun ilgili kısımları, mümkün olduğunca şirket işletmeleri el kitabı, bakım kontrolü/politika el kitabı ve havaalanı operasyonları el kitabı gibi onaylı dokümantasyona eklenmiş mi?	☐ Evet ☐ Hayır	
Bölüm 8	Hizmet sağlayıcı, operasyonel gerekliliklerin belgelenmesi ve teşvik edilmesi için tüm kayıtların oluşturulmasını ve tutulmasını sağlayan bir kayıt sistemine sahip midir?	☐ Evet ☐ Hayır	
Bölüm 8	Hizmet sağlayıcının kayıt sistemi geçerli düzenleme gerekliliklerine ve sektördeki en iyi uygulamalara uygun mudur?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bölüm 8	Kayıt sistemi kayıtların uygun şekilde tanımlanması, okunabilmesi, saklanması, korunması, arşivlenmesi, alınabilmesi, tutulması süresi ve son işlemlerinin yapılması için gereken kontrol süreçlerini sağlıyor mu?	☐ Evet ☐ Hayır	
Bileşen 2 - EMNİYET RİSKİ YÖNETİMİ			
Unsur 2.1 - Tehlikenin tanımlanması			
Bölüm 3 ve 9	[Örgüt] işletmelerdeki tehlikelerle ilgili olarak bilgilerin etkin bir şekilde toplanması için formel bir emniyet verileri toplama ve işleme sistemine (SDCPS) sahip midir?	☐ Evet ☐ Hayır	
Bölüm 3, 4 ve 9	[Örgütün] SDCPS'sinde emniyet verilerinin toplanması için reaktif, proaktif ve tahmine dayalı yöntemlerin bir kombinasyonunu içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 3, 9 ve 10	[Örgüt] emniyet ve risk yönetimi ile ilgili bilgilerin elde edilmesini sağlayan reaktif süreçlere sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Hizmet sağlayıcı, reaktif emniyet verileri toplama yöntemleri ile ilgili eğitimler geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Hizmet sağlayıcı, reaktif emniyet verileri toplama yöntemleri ile ilgili iletişim yöntemleri geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 9	Reaktif raporlama basit, erişilebilir ve hizmet sağlayıcının büyüklüğüne uygun mudur?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Reaktif raporlar uygun yönetim seviyesinde gözden geçirilmekte midir?	☐ Evet ☐ Hayır	
Bölüm 9	Katkıda bulunanlara raporlarının alındığını bildirilmesi ve analizin sonuçlarını paylaşılması için bir geri bildirim süreci var mıdır?	☐ Evet ☐ Hayır	
Bölüm 3, 9 ve 10	Hizmet sağlayıcı, örgütün etkinliklerinin analizi aracılığıyla emniyet risklerinin tanımlanması için etkin şekilde araştırma sağlayan proaktif süreçlere sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Proaktif emniyet verileri toplama yöntemleri ile ilgili eğitimler var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Hizmet sağlayıcı, proaktif emniyet verileri toplama yöntemleri ile ilgili iletişim yöntemleri geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 9	Proaktif raporlama basit, erişilebilir ve hizmet sağlayıcının büyüklüğüne uygun mudur?	☐ Evet ☐ Hayır	
Bölüm 3, 9 ve 10	Hizmet sağlayıcı, gerçek zamanlı normal işletmelerde ortaya çıktığı sırada sistem performansının yakalanmasını sağlayan tahmine dayalı süreçlere sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9 ve 10	Tahmine dayalı emniyet verileri toplama yöntemleri ile ilgili eğitimler var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Hizmet sağlayıcı, tahmine dayalı emniyet verileri toplama yöntemleri ile ilgili iletişim yöntemleri geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 9	Tahmine dayalı emniyet verileri yakalama süreci hizmet sağlayıcının büyüklüğüne uygun mudur?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Unsur 2.2 - Risk değerlendirmesi ve riskin azaltılması			
Bölüm 9 ve 10	[Örgüt], [örgütteki] işletmelerdeki emniyet risklerinin analizini, değerlendirilmesini ve kontrolünü sağlayan formel bir süreç geliştirmiş ve sürdürmekte midir?	☐ Evet ☐ Hayır	
Bölüm 4, 9 ve 10	[Örgütün] SMS dokümantasyonu tehlikeler, sonuçları ve emniyet riskleri arasındaki ilişkiyi açıkça ifade etmekte midir?	☐ Evet ☐ Hayır	
Bölüm 5 ve 9	Tanımlanan tehlikelerin sonuçları ile ilgili emniyet risklerinin analizi için, olasılık ve tekrarlama ciddiyeti bakımından yapılandırılmış bir süreç var mıdır?	☐ Evet ☐ Hayır	
Bölüm 5 ve 9	Emniyet risklerinin değerlendirilmesi ve emniyet risklerinin tahammül edilebilirliğinin (yani kabul edilebilir emniyet riski) belirlenmesi için örgütün kabul edebileceği ölçütler var mıdır?	☐ Evet ☐ Hayır	
Bölüm 5 ve 9	Hizmet sağlayıcı, raporlanan olayların ve sorunların tekrarlamasını önlemek için düzeltme/koruma eylemleri planını içeren emniyet riski azaltma stratejilerine sahip midir?	☐ Evet ☐ Hayır	
Bileşen 3 — EMNİYET GÜVENCESİ			
Unsur 3.1 - Emniyet performansının izlenmesi ve ölçülmesi			
Bölüm 9 ve 10	[Örgüt], örgütün emniyet performansını ve emniyet riski kontrollerinin etkililiğini doğrulamak için dahili bir süreç uygulamakta mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Bu süreçlerde aşağıdaki araçlar yer almakta mıdır? Emniyet raporlama sistemleri ☐ Evet ☐ Hayır Emniyetle ilgili çalışmalar ☐ Evet ☐ Hayır Emniyetle ilgili gözden geçirme işlemleri ☐ Evet ☐ Hayır Emniyet denetimleri ☐ Evet ☐ Hayır Emniyet araştırmaları ☐ Evet ☐ Hayır Dahili emniyet incelemeleri ☐ Evet ☐ Hayır		
Bölüm 6 ve 9	[Örgütün] emniyet performansı SMS'nin emniyet performansı göstergeleri ve emniyet performansı hedeflerine göre doğrulanmış mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Emniyet raporları uygun yönetim seviyesinde gözden geçirilmekte midir?	☐ Evet ☐ Hayır	
Bölüm 9	Katkıda bulunanlara raporlarının alındığını bildirilmesi ve analizin sonuçlarını paylaşılması için bir geri bildirim süreci var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Tehlikenin tanımlanması müdahale olarak düzeltme ve koruma eylemleri oluşturulmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 9	Dahili incelemeler yapmak için prosedürler bulunmakta mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	İlgili tüm tehlikelerin tanımlanması için olaylar ve sorunların raporlanmasını sağlayan bir süreç var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Hizmet sağlayıcı, geliştirilen düzeltme/koruma önlemlerinin etkililiğini değerlendirmek için bir sürece sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9	Hizmet sağlayıcı, dahili raporlama sürecini ve ilgili düzeltme eylemlerini izlemek için bir sisteme sahip midir?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bölüm 9	Etkili dahili değerlendirmeler yapılması için gereken bağımsızlık ve yetkiye sahip bir denetim işlevi var mı?	☐ Evet ☐ Hayır	
Bölüm 9	Denetim sistemi, hizmet sağlayıcı içindeki tüm işlevleri, etkinlikleri ve örgütleri kapsıyor mu?	☐ Evet ☐ Hayır	
Bölüm 9	Denetim sürecinin tarafsızlığının yanında denetimcilerin nesnelliği ve yeterliliğini sağlamak için seçme/eğitim süreçleri var mı?	☐ Evet ☐ Hayır	
Bölüm 9	Denetim sonuçlarının raporlanması ve kayıtların tutulması için bir prosedür var mı?	☐ Evet ☐ Hayır	
Bölüm 9	Denetim sonuçlarına müdahale olarak zamanında düzeltme ve koruma eylemleri gerçekleştirilmesi için gereklilikleri belirleyen bir prosedür var mı?	☐ Evet ☐ Hayır	
Bölüm 9	Alınan önlemlerin doğrulanmasının kaydının tutulması ve doğrulama sonuçlarının raporlanması için bir prosedür var mı?	☐ Evet ☐ Hayır	
Bölüm 9	Trendlerin izlenmesi ve analiz edilmesi için bir süreç var mı?	☐ Evet ☐ Hayır	
Unsur 3.2 - Değişimin yönetilmesi			
Bölüm 9	[Örgüt], örgütteki yerleşik süreçleri ve hizmetleri etkileyebilecek değişiklikleri belirlemesini sağlayan formel bir süreç geliştirmiş ve sürdürmekte midir?	☐ Evet ☐ Hayır	
Bölüm 9	Değişimin yönetilmesine yönelik formel süreç, işletmeler veya emniyet riskleri ile ilgili önemli personeldeki değişiklikleri analiz ediyor mu?	☐ Evet ☐ Hayır	
Bölüm 9	[Örgüt] değişikliklerin uygulanmasından önce emniyet performansının sağlanması için yerleşik düzenlemelere sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9	[Örgüt] operasyonel ortamındaki değişiklikler nedeniyle artık gerek duyulmayan emniyet riski kontrollerini ortadan kaldırmak veya değiştirmek için bir süreç oluşturmuş mudur?	☐ Evet ☐ Hayır	
Unsur 3.3. - SMS'nin sürekli olarak iyileştirilmesi			
Bölüm 9	[Örgüt], SMS'nin standart altı performans göstermesinin nedenlerinin belirlemesini sağlayan formel bir süreç geliştirmiş ve sürdürmekte midir?	☐ Evet ☐ Hayır	
Bölüm 9	[Örgüt], SMS'nin işletmelerde standart altı performans göstermesinin olası sonuçlarını belirlemek için mekanizmalar oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 9	Örgüt, SMS'nin standart altı performans göstermesinin nedenlerini ortadan kaldırmak ve azaltmak için mekanizmalar oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 9	Örgüt tesislerin, donanımların, dokümantasyonun ve prosedürlerin (denetimler ve araştırmalar v.s. aracılığıyla) proaktif olarak değerlendirilmesi için bir sürece sahip midir?	☐ Evet ☐ Hayır	
Bölüm 9	Örgüt, bireyin emniyet sorumluluklarını yerine getirdiğini doğrulamak için, bireyin performansının proaktif olarak değerlendirilmesi için bir sürece sahip midir?	☐ Evet ☐ Hayır	
Bileşen 4 — EMNİYETİN TEŞVİK EDİLMESİ			
Unsur 4.1 — Eğitim ve öğretim			
Bölüm 9	Personelin SMS görevlerini yerine getirmek için eğitilmiş ve yeterli olması için eğitim gerekliliklerini belirlemek için belgelenmiş bir süreç var mıdır?	☐ Evet ☐ Hayır	

ICAO referansı	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bölüm 9	Emniyet eğitimi bireyin SMS'ye katılma şekline uygun mudur?	☐ Evet ☐ Hayır	
Bölüm 9	Emniyet eğitimi, işe alma sırasında verilen temel eğitime eklenmiş midir?	☐ Evet ☐ Hayır	
Bölüm 9	Etkilenen personel için acil müdahale/beklenmeyen durum eğitimi var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Eğitimin etkililiğini ölçen bir süreç var mıdır?	☐ Evet ☐ Hayır	
Unsur 4.2 - Emniyetle iletişimi			
Bölüm 9	[Örgüt] içinde emniyet yönetimi sisteminin etkili bir şekilde çalışmasına izin veren iletişim süreçleri var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Hizmet sağlayıcının büyüklüğüne uygun iletişim süreçleri (yazılı, elektronik, toplantılarla v.s.) var mıdır?	☐ Evet ☐ Hayır	
Bölüm 9	Emniyet açısından önemli bilgiler, ilgili SMS belgelerine yönlendirme sağlayan uygun bir ortamda oluşturulmuş ve korunuyor mu?	☐ Evet ☐ Hayır	
Bölüm 9	Emniyet açısından önemli bilgiler [örgüt] içinde dağıtılıyor mu ve emniyet iletişiminin etkili olup olmadığı izleniyor mu?	☐ Evet ☐ Hayır	
Bölüm 9	Belirli emniyet önlemlerinin neden alındığını ve emniyet prosedürlerinin kullanılmaya başladığını veya değiştirildiğini açıklayan bir prosedür var mı?	☐ Evet ☐ Hayır	

Bölüm 8

SMS'de PLANLAMA

8.1 HEDEF VE İÇERİKLER

Bu bölümde, bir SMS uygulama planının yapısı da dahil olmak üzere, SMS'nin planlaması ile ilgili gereklilikler açıklanmaktadır. Bu gereklilikler ICAO SMS çerçevesi referans olarak kullanılarak açıklanmaktadır. ICAO SMS çerçevesi tamamıyla tanımlansa da, bu bölümde çerçevenin sadece ilk bileşeni olan emniyet politikası ve hedefler ele alınmıştır; ICAO SMS çerçevesinin diğer üç bileşeni (emniyet riski yönetimi, emniyetin güvence altına alınması ve emniyetin teşvik edilmesi) bölüm 9'da ele alınmaktadır. Bu bölüm aşağıdaki konuları içerir:

a) Bir SMS'nin bileşenleri ve unsurları;

b) ICAO SMS çerçevesi;

c) Yönetimin taahhüdü ve sorumluluğu;

d) Emniyetle ilgili hesap verme sorumlulukları;

e) Emniyetin sağlanmasında önemli rol oynayan personelin atanması;

f) Acil müdahale planlamasının koordinasyonu;

g) SMS dokümantasyonu ve

h) SMS uygulama planı.

8.2 BİR SMS'NİN BİLEŞENLERİ VE UNSURLARI;

8.2.1 Bir SMS'nin altında yatan iki temel operasyonel süreci ve iki temel operasyonel süreci desteklemek için gereken örgütsel düzenlemeleri temsil eden dört SMS bileşeni vardır. Bir SMS'nin dört bileşeni şunlardır:

a) emniyet politikası ve hedefleri;

b) Emniyet riski yönetimi;

c) emniyetin güvence altına alınması ve

d) emniyetin teşvik edilmesi

8.2.2 SMS'nin iki temel operasyonel etkinlik emniyet riski yönetimi ve emniyetin güvence altına alınmasıdır. Emniyet riski yönetimi, hizmetlerin sunulması ile ilgili işletmelerin içinde gerçekleştiği bağlamda yer alan tehlikelerin en başta tanımlanmasını hedefleyen bir erken sistem tasarımı etkinliği olarak kabul edilmelidir. Emniyetin güvence altına alınması, aşağıdakileri hedefleyen sürekli, devam eden bir etkinlik olarak görülmelidir:

a) emniyet risklerinin ve sistemde bir kontrol aracı olarak bulunan savunmalarının sonuçlarının değerlendirilmesi ile ilgili olarak tehlikelerin ve varsayımların en başta tanımlanmasının, sistem zaman içinde evrildikçe geçerli ve uygulanabilir olarak kalmasını sağlamak ve/veya

b) gerektiğinde savunmalardaki değişikliklerin yapılması.

Dolayısıyla, tehlikenin tanımlanması ya sistem tasarımı sırasında ya da orijinal sistemde önemli değişiklikler yapılırken gerçekleştirilen tek noktada veya tek seferlik bir etkinlik olarak görülebilir. Diğer yandan, emniyetin güvence altına alınması hizmetlerin sunulmasını destekleyen işletmelerin tehlikelere karşı uygun şekilde korunmasını sağlamak için sürekli olarak gerçekleştirilen, günlük bir etkinliktir. Basitçe ifade edildiğinde, tehlikenin tanımlanması emniyetin güvence altına alınmasının günlük olarak gerçekleştirilmesini sağlayan bir ilk referans çerçevesini sağlar.

8.2.3 Bu iki temel operasyonel etkinlik, emniyet politikası ve hedeflerinin sağladığı şemsiye altında gerçekleşir ve emniyetin teşvik edilmesi yoluyla desteklenir. SMS'nin bu iki bileşeni zorunlu örgütsel düzenlemeleri kapsar, bu düzenlemeler eksik olduğunda tehlikenin tanımlaması ve emniyet riski yönetimi olanaksız veya ciddi şekilde sorunlu olacaktır. Bu nedenle, emniyet riski yönetiminin ve emniyetin güvence altına alınmasının SMS'nin gerçek "eylemleri" olduğu düşünülebilir; bunlar çalışan bir SMS'nin altında yatan operasyonel etkinliklerdir. Diğer yandan, emniyet politikaları ve hedefleri ve emniyetin teşvik edilmesi, emniyet riski yönetiminin ve emniyetin güvence altına alınmasının altında yatan operasyonel etkinliklerin etkili bir şekilde gerçekleştirilmesini sağlayan desteği ve referans çerçevesini de sağlar.

8.2.4 Önceki paragraflarda ele alınan dört bileşen, gerçek bir yönetim sisteminin (SMS) altında yatan dört kapsayıcı emniyet yönetimi sürecini temsil etmeleri bakımından, bir SMS'nin temel ilkelerini oluştururlar. Her bir bileşen, gerçek yönetim sisteminin tıpkı diğer temel operasyonel işlevler veya örgüt süreçlerinde olduğu gibi emniyetin yönetimini gerçekleştirmek için kullanması gereken belirli alt süreçleri, belirli görevleri veya araçları kapsayan unsurlara ayrılmıştır.

8.2.5 Emniyet politikaları ve hedefleri bileşeni beş unsurdan oluşur:

a) yönetimin taahhüdü ve sorumluluğu;

b) emniyetle ilgili hesap verme sorumlulukları;

c) emniyetin sağlanmasında önemli rol oynayan personelin atanması;

d) acil müdahale planlamasının koordinasyonu ve

e) SMS dokümantasyonu.

8.2.6 Emniyet riski yönetimi bileşeni iki unsurdan oluşur:

a) tehlikenin tanımlanması ve

b) risk değerlendirmesi ve riskin azaltılması.

8.2.7 Emniyetin güvence altına alınması bileşeni üç unsurdan oluşur:

a) emniyet performansının izlenmesi ve ölçülmesi;

b) değişimin yönetilmesi ve

c) SMS'nin sürekli olarak iyileştirilmesi.

8.2.8 Emniyetin teşvik edilmesi bileşeni iki unsurdan oluşur:

a) eğitim ve öğretim ve

b) emniyet iletişimi.

8.3 ICAO SMS ÇERÇEVESİ

Not— ICAO SMS çerçevesinin ayrıntıları bu bölümün sonundaki Ek 1'de bulunmaktadır.

Bölüm 8.2'de ele alınan on iki unsurla birlikte dört bileşen, aşağıdaki şekilde bir hizmet sağlayıcının SMS'sinin geliştirilmesi ve uygulanması için ilkelere dayanan bir kılavuz olması amaçlanan ICAO SMS çerçevesini oluştururlar:

1. Emniyet politikası ve hedefleri

    1.1 Yönetimin taahhüdü ve sorumluluğu
    1.2 Emniyetle ilgili hesap verme sorumlulukları
    1.3 Emniyetin sağlanmasında önemli rol oynayan personelin atanması
    1.4 Acil müdahale planlamasının koordinasyonu
    1.5 SMS dokümantasyonu

2. Emniyet riski yönetimi

    2.1 Tehlikenin tanımlanması
    2.2 Risk değerlendirmesi ve riskin azaltılması.

3. Emniyetin güvence altına alınması

    3.1 Emniyet performansının izlenmesi ve ölçülmesi
    3.2 Değişimin yönetilmesi
    3.3 SMS'nin sürekli olarak iyileştirilmesi

4. Emniyetin teşvik edilmesi

    4.1 Eğitim ve öğretim
    4.2 Emniyet iletişimi

8.4 YÖNETİMİN TAAHHÜDÜ VE SORUMLULUĞU

8.4.1 Herhangi bir örgütte yönetim, hizmetlerin sunulması ile doğrudan ilgili olan veya gerekli olan personel etkinliklerinin veya kaynaklarının kullanımının kontrolünden sorumludur. Örgütün emniyet tehlikelerine maruz kalması, doğrudan hizmetlerin sunulması ile ilgili etkinliklerin bir sonucudur. Yönetim personelin belirli etkinlikleri ve kaynakların kullanımı aracılığıyla, tehlikelerin sonuçları ile ilgili emniyet risklerini etkin bir şekilde kontrol edebilir. Bu etkinliklere örnek olarak, yönetim personeli işe alır, eğitir ve denetler ve hizmet sunma etkinliklerini desteklemek için donanımı tedarik eder. Yönetim personelin örgütün emniyet yönergelerine ve kontrollerine uymasını ve donanımlarının hizmet verebilir durumda kalmasını sağlamalıdır. Dolayısıyla emniyetin yönetilmesi için yönetimin temel sorumluluğu açıktır ve bu sorumluluk gerekli emniyet riski kontrollerini bir araya getiren ayrı bir örgüt sisteminin işletilmesi aracılığıyla gerçekleştirilir. Hizmet sağlayıcının SMS'si, yönetimin bu sorumlulukları yerine getirmesinin bir aracıdır. Bir SMS, işletmelerin emniyetli ve etkin olmasını sağlayan bir yönetim sistemidir.

8.4.2 Örgütün SMS'sinin etkili ve etkin olmasını sağlamanın başlangıç noktası, örgütün emniyet politikasıdır. Üst yönetim örgütün emniyet politikasını geliştirmelidir ve bu politika Hesap Vermekten Sorumlu Müdür tarafından imzalanmalıdır. Emniyet politikasının bir örneği Şekil 8-1'de gösterilmiştir. Genel olarak, emniyet politikası aşağıdakilerin yerine getirilmesini taahhüt etmelidir:

a) en yüksek emniyet standartlarının elde edilmesi;

b) geçerli tüm yasal gerekliliklere ve uluslararası standartlara ve en etkili uygulamalara uyulması;

c) uygun tüm kaynakların sağlanması;

d) emniyeti tüm yöneticilerin sorumluluğu haline getirmek ve

e) politikanın her seviyede anlaşıldığından, uygulandığından ve sürdürüldüğünden emin olmak.

8.4.3 Politika geliştirildikten sonra, üst yönetim emniyet politikasını, açıkça onaylanmış şekilde tüm personele iletmelidir.

8.4.4 Üst yönetim, SMS için ve dolayısıyla bir bütün olarak örgüt için emniyet hedeflerini ve emniyet performansının standartlarını oluşturmalıdır. Emniyet hedefleri örgütün emniyetin yönetimi bakımından ne elde etmek istediğini tanımlamalı ve hedeflere ulaşmak için örgütün atması gereken adımları göstermelidir. Emniyet performansı standartları, örgüt davranışının emniyet performansı karşısında ve dolayısıyla emniyetin yönetimi karşısında ölçülmesini sağlar. Hem emniyet hedefleri hem de emniyet performansı standartları, Bölüm 6'da ele alınan, SMS'nin emniyet performansı göstergeleri, emniyet performansı hedefleri ve eylem planları ile bağlantılandırılmalıdır.

8.4.5 Örgüt Sorumlu Müdürü belirlemelidir ve bu yönetici örgütün SMS'sinin etkili ve etkin bir şekilde gerçekleştirilmesi konusunda nihai sorumluluğa sahip, tek ve tanımlı bir kişi olmalıdır. Örgütün büyüklüğü ve karmaşıklığına bağlı olarak, Sorumlu Müdür aşağıdakilerden biri olabilir:

a) icra kurulu başkanı (CEO);

b) Yönetim kurulu başkanı;

c) bir ortak veya

d) şirket sahibi.

8.4.6. Sorumlu Müdürün kim olacağını, bu kişiye örgüt içinde atanan işlev perspektifinden belirleme eğilimi vardır. Ancak, Sorumlu Müdürün kişinin kim olacağından daha önemlisi SMS'nin emniyet performansının uygun bir şekilde değerlendirilmesi için Sorumlu Müdürün yetkilerinin ve sorumluklarının ne olacağı olmalıdır. Bu yetki ve sorumluluklara aşağıdakiler dahildir, fakat bunlarla sınırlı değildir:

a) insan kaynakları konularında tam yetki;

b) önemli mali konularda yetki;

c) örgütün işlerinin yürütülmesinden doğrudan sorumluluk;

d) Sertifiye edilmiş işletmenin faaliyetleri ile ilgili nihai yetki ve

e) tüm emniyet konularında nihai sorumluluk.

EMNİYET POLİTİKASI BEYANI

Emniyet temel operasyonel işlevlerimizden biridir. Hizmetlerimizi sunarken, en yüksek performans seviyesine ulaşma ve ulusal ve uluslararası standartlara uyma hedefiyle, tüm havacılık etkinliklerimizin örgüt kaynaklarının dengeli bir şekilde dağıtılması ile gerçekleştirilmesini sağlamak için stratejiler ve süreçler geliştirmeye, uygulamaya, bunları sürdürmeye ve sürekli olarak iyileştirmeye kendimizi adıyoruz.

[İcra kurulu başkanı (CEO)/genel müdür/veya örgüte uygun kişi] ile başlayarak tüm yönetim seviyeleri ve personel bu en yüksek seviyedeki emniyet performansının elde edilmesinden sorumludur.

Aşağıdakilere bağlı kalacağız:

- Tüm uygun kaynakların sağlanması ile emniyetin yönetilmesini **desteklemek**; bu emniyetli uygulamaları teşvik eden, emniyetle ilgili etkili raporlama ve iletişimi cesaretlendiren ve örgütteki diğer yönetim sistemlerinin sonuçlarına gösterilen dikkatle aynı dikkati göstererek emniyeti etkin bir şekilde yöneten bir örgüt kültürü ortaya çıkmasını sağlayacaktır;
- Emniyetin yönetilmesini tüm yöneticilerin ve çalışanların temel sorumluluğu haline **getirmek**;
- Tüm personel, yöneticiler ve çalışanlar v.s. için, örgütün emniyet performansının ve emniyet yönetimi sistemimizin performansının sağlanmasına yönelik sorumluluklarının ve hesap verme sorumluluklarının **açıkça** tanımlanması;
- İşletmelerimizden veya etkinliklerimizden kaynaklanan tehlikelerin sonuçlarına ait emniyet risklerin ortadan kaldırılması veya makul derecede düşük (ALARP) noktaya kadar azaltılması için bir tehlike raporlama sistemini de içerecek şekilde tehlike tanımlama ve risk yönetimi süreçlerini **oluşturmak ve çalıştırmak**;
- Açıklama, herhangi bir kuşkunun ötesinde, yasadışı bir eylem, büyük bir ihmal ve düzenlemelere veya prosedürlere kasıtlı veya istekli bir şekilde uyulmamasını göstermediği sürece, tehlike raporlama sistemi aracılığıyla bir emniyet sorununu açıklayan herhangi bir çalışana karşı hiçbir şekilde harekete geçiimemesini **sağlamak**;
- Yasalar ve düzenlemelerde yer alan gereklilik ve standartlara **uymak** ve mümkün olduğunda aşmak;
- Emniyet stratejilerini ve süreçlerini uygulamak için yeterli sayıda kalifiye ve eğitimli insan kaynağının bulunmasını **sağlamak**;
- Tüm personeline yeterli ve uygun havacılık emniyeti bilgileri ve eğitimi sağlandığından, emniyet konularından yeterli olduklarında ve sadece becerilerine uygun görevler verildiğinden **emin olmak;**
- Emniyet performansımızı gerçekçi emniyet performansı göstergelerine ve emniyet performansı hedeflerine göre **oluşturmak ve ölçmek;**
- Emniyet performansımızı uygun emniyet önleminin alınmasını ve etkili olmasını sağlayan yönetim süreçleri aracılığıyla **sürekli olarak iyileştirmek;**
- İşletmelerimizi desteklemek için harici olarak tedarik edilen sistem ve hizmetlerinin emniyet performansı standartlarımıza uygun şekilde sağlandığından **emin olmak;**

(İmza) _____

CEO/Genel Yöneticisi/veya uygun kişi

Şekil 8-1. Emniyet politikası örneği

8.4.7 Bölüm 2'de bir temel örgütlenme süreci olarak kaynakların dağıtılması ele alınmaktadır. Bu nedenle, kaynakların dağıtılması en eski yönetim işlevlerinden biridir. Paragraf 8.4.1'de, sonucunda örgütün emniyet tehlikelerine maruz kaldığı hizmetlerin sunulması ile doğrudan ilgili personel etkinlikleri ve kaynak kullanımlarının kontrol yöntemlerinden biri olarak yönetim işlevi daha ayrıntılı olarak ele alınmaktadır. Yukarıda belirtilenler, 8.4.6'de belirtilen Sorumlu Müdürün sorumlulukları ve yetkilerinin gerekçelerini vurgulamaktadır: Bu tür sorumluluklar veya yetkiler sadece kaynakların dağıtılması veya sadece etkinliklerin kontrolüne aittir. Bu yetkilere ve sorumluluklara sahip olmayan bir Sorumlu Müdür atayan bir örgüt, atanan kişiyi kendisine verilen rolü yerine getirmesini sağlayacak özelliklere sahip olmayan bir konuma sokmaktadır.

8.4.8 Sorumlu Müdür atama işlemi uygun şekilde belgelendiği ve bu bölümde daha sonra ele alındığı gibi örgütün emniyet yönetimi sistemleri el kitabında (SMSM) açıklandığı takdirde SMS'nin yönetimini başka bir kişiye atayabilir. Ancak, Sorumlu Müdürün hesap verme sorumluluğu SMS'nin yönetiminin başka bir kişiye atanmasından etkilenmez: Sorumlu Müdür örgütün SMS'nin yürütülmesi ile ilgili nihai sorumluluğa sahip olmaya devam eder.

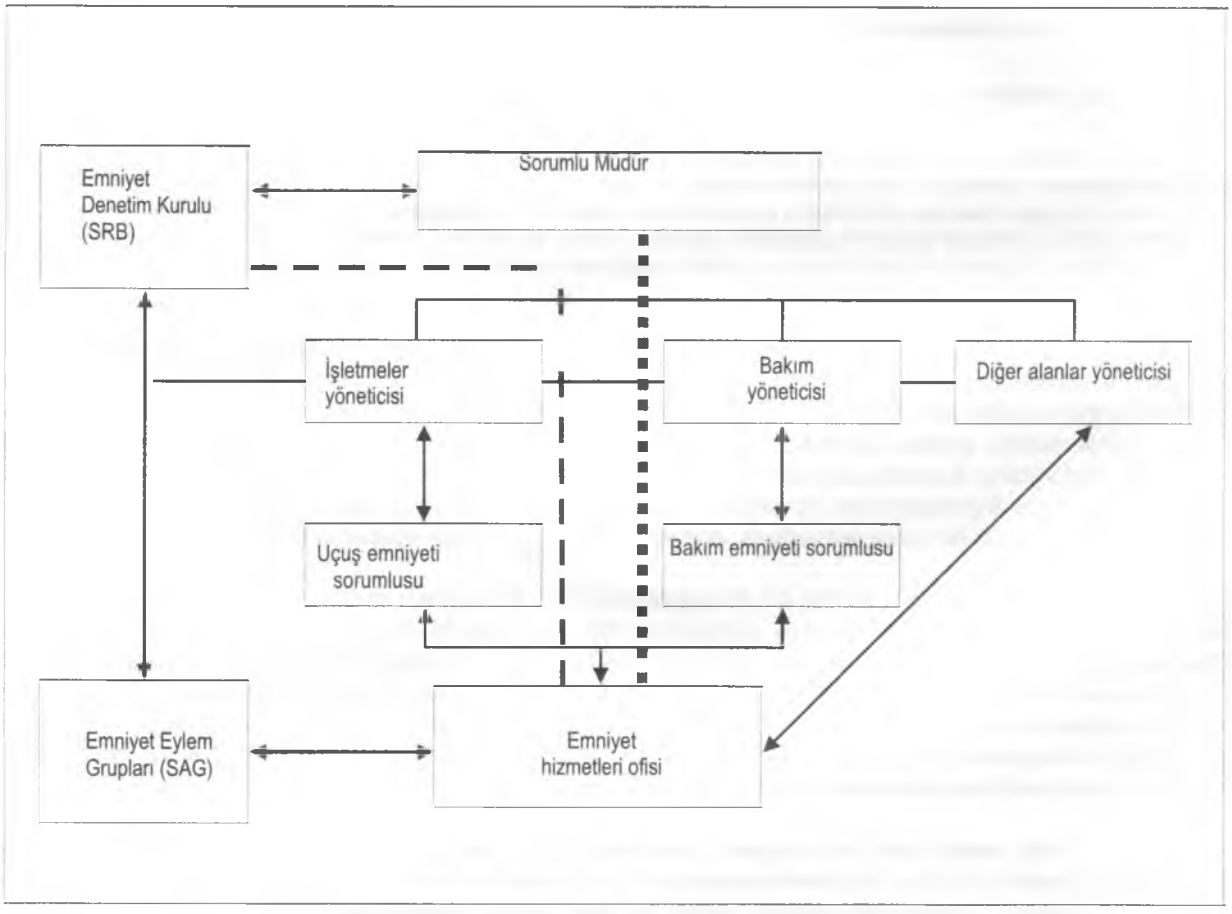
8.5 EMNİYETLE İLGİLİ HESAP VERME SORUMLULUKLARI

8.5.1 Bölüm 3'te emniyet yönetimi örgütün kaynaklarının ve hedeflerinin analizine katkıda bulunan temel bir operasyonel işlev olarak ele alınmaktadır. Bu analiz, örgütün hizmet sunumu gereksinimlerinin tümünü destekleyecek şekilde, kaynakların koruma ve üretim hedefleri arasında dengeli ve gerçekçi bir şekilde dağıtılmasının temelini oluşturur. Paragraf 8.4.1'de SMS işletmelerin emniyetli olmasını sağlayan bir yönetim sistemi olarak ele alınmaktadır. Örgütün hizmet sunumu gereksinimlerinin tümünü destekleyecek şekilde, kaynakların koruma ve üretim hedefleri arasında dengeli ve gerçekçi bir şekilde dağıtılması sağlanmadıkça, işletmelerin emniyetli bir şekilde gerçekleştirilmesi olası değildir. Genel olarak, işletmelerin emniyetli bir şekilde gerçekleştirilmesi ve kaynakların dengeli ve gerçekçi bir şekilde dağıtılabilmesi için emniyetle ilgili hesap verme sorumlulukları, örgütün SMS'sinin kendisi ve özellikle de SMS'nin aşağıdaki unsuru aracılığıyla gerçekleştirilir: Tüm personelin, ama özellikle kritik personelin emniyetle ilgili hesap verme sorumluluklarının tanımlanması.

8.5.2 SMS'nin örgütü ile ilgili olarak yöneticilerin emniyetle ilgili hesap verme sorumlulukları, örgütün SMS'nin örgütün büyüklüğüne, doğasına ve işletmelerin karmaşıklığına ve hizmetlerin sunulması için gereken etkinliklerle ilgili tehlike ve emniyet risklerine uygun bir mimari tanımına bağlıdır. SMS'nin örgütü ile ilgili olarak yöneticilerin emniyetle ilgili hesap verme sorumlulukları, SMS'nin etkili ve etkin bir şekilde yürütülmesi için gereken insani, teknik, mali ve diğer kaynakların dağıtılmasını da içerir.

8.5.3 Seviyelerinden bağımsız olarak, tüm çalışanların iş tanımlarında emniyetle ilgili sorumlulukları ve hesap verme sorumluluklarının yer alması gerekse de, kritik personelinin emniyetle ilgili sorumluluklarının ve yetkilerinin tanımlanması ile ilgili hesap verme sorumlulukları, her bir üst yöneticinin (bölüm yöneticisi veya işlevsel bir birimden sorumlu kişi) iş tanımında, bölümün/işlevsel birimin çalışması ile ilgili sorumlulukların yanında, uygun bir ölçüde, SMS'nin yürütülmesi ile ilgili sorumlulukların eklenmesini de içerir. Temel bir operasyonel işlev olarak emniyet yönetimi perspektifinde, her bir bölüm yöneticisi veya işlevsel bir birimden sorumlu kişi SMS'nin ve emniyet performansının yürütülmesine bir dereceye kadar katılacaktır. Bu katılım elbette, örgütün temel hizmetlerinin sunulmasında doğrudan yer alan operasyonel bölümler veya işlevsel birimlerde (işletmeler, bakım, mühendislik, eğitim ve dağıtım, bundan sonra "bölüm yöneticisi" genel terimi ile adlandırılacaklardır) destek işlevlerinden sorumlu olanlara (insan kaynakları, yönetim, hukuk ve finans) göre daha fazla olmalıdır.

8.5.4 Tüm bölüm yöneticilerinin veya işlevsel bir birimden sorumlu kişilerin, özellikle de bölüm yöneticilerinin emniyetle ilgili sorumlulukları, hesap verme sorumlulukları ve yetkileri, bu bölümde daha ileride ele alınan örgütün emniyet yönetimi sistemleri el kitabında (SMSM) açıklanmalıdır. Emniyetle ilgili sorumluluklar, hesap verme sorumlulukları ve yetkiler, örgütün çeşitli kısımları arasında emniyetin yönetimi ile ilgili arayüzler ve ilişkileri gösteren bir işlev çizelgesinde grafik olarak gösterilmelidir. Şekil 8-2 bir işlev çizelgesi örneğidir.



Şekil 8-2. Emniyetle ilgili hesap verme sorumlulukları

8.5.5 Şekil 8-2'de örgütten çok işlevlerin gösterildiğinin belirtilmesi önemlidir. Emniyet yönetimini bölümler ve işlevsel birimler ve bunların kuruluş içindeki göreli hiyerarşileri bakımından değil, her bir bölüm ve/veya işlevsel birimin temel bir operasyonel süreç olarak emniyeti sağlamasını sağlayan işlevleri bakımından göstermeyi amaçlamaktadır. Bu uyarı önemlidir, çünkü havacılıkta örgüt sayısı kadar örgüt çizelgesi bulunacaktır. Bu nedenle, bu el kitabının amaçlarına uygu olarak, Şekil 8-2 bir örgüt çizelgesi değil, işlevsel bir çizelge olarak kabul edilmelidir.

8.5.6 Emniyet hizmetleri ofisi işlevsel çizelgenin merkezindedir. Emniyet hizmetleri ofisi konsepti emniyetin bir temel operasyonel süreç olarak yönetilmesi kavrayışının anahtarıdır, yönetimin bu amaçla kullandığı sistem olarak SMS için anahtar önemdedir. Emniyet hizmetleri ofisi, süreçler ve operasyonel birimlerin bölüm yöneticileri tarafından hizmetlerin sunulması ile ilgili olarak verilen kararlar bakımından bağımsız ve nötrdür. Bir SMS ortamında, emniyet hizmetleri ofisi dört önemli kurumsal işlevi yerine getirir:

a) tehlike tanımlama sistemini yönetir ve denetler;

b) hizmetin sunulmasında doğrudan yer alan operasyonel birimlerin emniyet performansını izler;

c) üst yönetime emniyet yönetimi konularında tavsiyelerde bulunmak ve

d) bölüm yöneticilerine emniyet yönetimi konularında yardımcı olmak.

8.5.7 Bölüm 2'de ele alınan geleneksel emniyet perspektifinde, emniyet ofisi örgüt içinde tüm emniyet sürecinin tamamen "sahibiydi". Kaza önleme sorumlusu olarak da adlandırılan emniyet sorumlusu emniyet sorunlarını tanımlamak, çözümler önermek, çözümlerin uygulanmasına katılmak ve çözümlerin etkililiğini izlemekten sorumlu kişiydi. Geçtiğimiz yıllarda, emniyet sürecinin tamamen emniyet ofisine "ait olması" kavrayışı, emniyet sorumlusu ile örgütün CEO'su arasında doğrudan bir raporlama ve iletişim bağlantısı oluşturulmasına yönelik geniş kabul gören bir sektör uygulaması tarafından da güçlendirilmekteydi.

8.5.8 Bu yaygın uygulamanın arkasındaki amaç iki yönlüydü. Öncelikle, emniyet ofisi ile CEO arasında doğrudan bir bağlantı kurarak emniyet ofisinin hiyerarşik seviyesini ve görünürlüğünü arttırmayı hedefliyordu. İkincisi, bu doğrudan bağlantı hizmet sunumu ile doğrudan ilgili olan operasyonel etkinlikleri yönetmekten sorumlu olanları (işlevsel bölümlerin yöneticileri) emniyet sorunlarının değerlendirilmesi ve çözümü sürecinden çıkararak nötr bir durum oluşturmayı amaçlıyordu. Buradaki perspektif, bölüm yöneticilerin çeşitli derecelerde ilgili taraflar olabileceği, bunun da emniyet sorunlarının değerlendirilmesi ve çözümünde potansiyel bir çıkar çatışmasına neden olabileceğiydi. Emniyet sorumlusu ile CEO arasındaki doğrudan bağlantı, algılanan bu çıkar çatışmasını ortadan kaldırmak için konmuştu.

8.5.9 İyi niyetli olduğu açık olsa da, bu uygulamanın iki ciddi olumsuz yönü vardı. Birincisi, emniyet sürecinin sahibinin tamamen emniyet ofisi olmasını sağlayarak, işlevsel alt bölüm yöneticilerini emniyetle ilgili karar alma sürecinden çıkarmıştı. Bu "emniyet sorunları bölüm yöneticisinin sorunu değildir; emniyet sorunları emniyet ofisine ve emniyet sorumlusuna aittir" algısının yayılmasına neden olmuştu. Hesap verme sorumluluğu sırası, CEO ile emniyet sorumlusu arasındaki iki taraflı bir diyaloga indirilmişti. CEO'nun iş yükü düşünüldüğünde, bu diyalogun büyük oranda bir monolog haline gelmesi potansiyeli vardı. İkincisi ve daha önemlisi, bilgi birikimi bakımından, operasyonel birimlerin örgüt içinde emniyetle ilgili karar verme sürecine sağlayabileceği değerli katkıları göz ardı ediyordu.

8.5.10 SMS ortamı farklı bir perspektif sunmaktadır. Emniyet ofisi ismi emniyet hizmetleri ofisi olarak değiştirilmiştir, böylece bu ofisin bir temel operasyonel süreç olarak emniyetin yönetilmesi ile ilgili olarak örgüte, üst yönetime ve bölüm yöneticilerine hizmet sunan bir ofis olduğu yansıtılmak amaçlanmıştır. "Ölçemediğini yönetemezsin" kuralı Bölüm 3'te SMS başlığı altında ele alınmıştı. Emniyet hizmetleri ofisi temel olarak bir emniyet verileri toplama ve analizi birimidir. Tahmine dayalı, proaktif ve reaktif yöntemlerin bir kombinasyonu ile (Bölüm 3'te ele alınmıştır), emniyet hizmetleri ofisi hizmet sunma etkinlikleri sırasında tehlikeler hakkında sürekli ve rutin olarak emniyet verileri toplayarak operasyonel amaçlardan sapma (yine Bölüm 3'te ele alınmıştır) sırasında neler olduğunu belirler.

8.5.11 Tehlikeler tanımlandığında, sonuçları değerlendirildiğinde ve bu sonuçların emniyet riskleri değerlendirildiğinde (yani emniyet verilerinden emniyet bilgilerine ulaşıldığında), emniyet bilgileri emniyet sorunlarının çözülmesi için bölüm yöneticilerine gönderilir. Bölüm yöneticileri kendi alanlarında gerçek uzmanlardır ve bu nedenle de etkili ve etkin çözümler tasarlamak ve uygulamak için en uygun kişilerdir. Ayrıca, bölüm yöneticileri emniyet bilgilerini emniyet aklına dönüştürerek ve emniyet hizmetleri ofisi tarafından sağlanan tehlikelerle ilgili bilgilere bir bağlam katarak, emniyet verileri analizi sürecindeki son adımı atabilirler.

8.5.12 Bir bütün olarak örgütte olduğu gibi, emniyet yönetimi ile ilgili ana sorumluluk üretim etkinliklerine "sahip olanlardadır". Tehlikelerle doğrudan karşı karşıya gelinen, örgüt süreçlerindeki bozuklukların tehlikelerin hasar verme potansiyeline sahip sonuçlarına katkıda bulunduğu ve doğrudan denetimin ve kaynak dağıtımının emniyet risklerini ALARP seviyesine indirebileceği yer üretim etkinlikleridir. Ayrıca, sürecin sahipleri tüm örgütlerde söz konusu alanın teknik uzmanlarıdır, dolayısıyla üretimdeki teknik süreçler hakkında en bilgili kişilerdir.

8.5.13 Emniyet bilgileri uygun bölüm yöneticilerine gönderildiğinde, emniyet hizmetleri ofisi rutin emniyet verileri toplama ve analizi etkinliklerine devam eder. Emniyet hizmetleri ofisi ve söz konusu bölüm yöneticileri arasında uzlaşılan bir zaman aralığında, emniyet hizmetleri ofisi, emniyet sorunun devam ettiği alanlardaki bölüm yöneticilerine ilgili emniyet sorunu hakkında yeni emniyet bilgileri sunacaktır.

Emniyet bilgileri, bölüm yöneticileri tarafından uygulanan azaltma çözümlerinin emniyet sorununu çözmeye yardımcı olup olmadığını veya emniyet sorunun sürüp sürmediğini gösterecektir. Sorun devam ediyorsa, başka azaltma çözümleri uygulanır, yeni bir zaman aralığı belirlenir, emniyet verileri toplanır ve analiz edilir ve bu çevrim emniyet verileri analizi emniyet sorunun çözüldüğünü gösterene kadar gerektiği sayıda tekrarlanır. Bu süreç sırasında, bölüm yöneticileri emniyet hizmetleri ofisine değil, bölüm 8.6'da ele alındığı gibi tüm örgütlerin iki formel emniyet biriminden biri aracılığıyla, örgütün SMS'si hakkında nihai sorumluluğa sahip kişi olan Sorumlu Müdüre rapor verir.

8.6 EMNİYETİN SAĞLANMASINDA ÖNEMLİ ROL OYNAYAN PERSONELİN ATANMASI

8.6.1 Emniyet hizmetleri ofisinin etkili bir uygulanması ve çalışmasında önemli bir nokta, ofisteki günlük çalışmalardan sorumlu kişinin atanmasıdır. Bu kişi farklı örgütlerde farklı isimlendirilebilir, ama bu el kitabının amaçlarına uygun olarak emniyet yöneticisi genel terimi kullanılmıştır.

8.6.2 Emniyet yöneticisi, çoğu örgütte, Sorumlu Müdürün SMS'nin günlük yönetim işlevleri için atadığı kişi olacaktır. Emniyet yöneticisi etkili bir SMS geliştirilmesi ve sürdürülmesinden sorumlu kişidir ve bu işin odak noktasıdır. Emniyet yöneticisi aynı zamanda emniyet yönetimi ile ilgili konularda Sorumlu Müdüre ve bölüm yöneticilerine tavsiyelerde bulunur ve emniyet sorunlarını örgüt içinde ve uygun olduğunda dış kurumlarla, yüklenicilerle ve ilgili taraflarla koordine etmek ve iletişimi sağlamaktan sorumludur. Emniyet yöneticisinin işlevleri aşağıdakileri içerir, ama bunlarla sınırlı olması gerekmez:

a) SMS uygulama planını Sorumlu Müdür adına yönetmek;

b) tehlike tanımlamayı ve emniyet riski analizini gerçekleştirmek/kolaylaştırmak;

c) düzeltme eylemlerini izlemek ve sonuçlarını değerlendirmek;

d) örgütün emniyet performansı hakkında periyodik raporlar hazırlamak;

e) kayıtları ve emniyet dokümantasyonunu tutmak;

f) personel emniyet eğitimini planlamak ve organize etmek;

g) emniyet konularında bağımsız öneriler sunmak;

h) havacılık sektöründeki emniyet sorunlarını ve bu sorunların örgütün hizmet sunma amaçlı operasyonlarındaki algılanan etkisini izlemek;

i) (Sorumlu Müdür adına) Devletin denetim kurumu ve diğer Devlet kurumlarıyla emniyetle ilgili konularda koordinasyon ve iletişim sağlamak ve

j) (Sorumlu Müdür adına) uluslararası kurumlarla emniyetle ilgili konularda koordinasyon ve iletişim sağlamak.

8.6.3 Emniyet yöneticisi emniyet hizmetleri ofisinde çalışan tek kişi olabilir veya çoğunlukla emniyet verileri analisti olmak üzere ek personelle destelenebilir. Bu örgütün boyutuna ve hizmetlerin sunulmasını destekleyen operasyonların doğasına ve karmaşıklığına bağlı olacaktır. Emniyet hizmetleri ofisinin büyüklüğünden ve personel seviyesinden bağımsız olarak, işlevleri aynı kalacaktır. Emniyet yöneticisi doğrudan bölüm yöneticileri (işletmeler, bakım, mühendislik, eğitim v.s.) ile birlikte hareket eder. Bu, Şekil 8-2'deki işlevsel çizelgede kesintisiz oklarla gösterilmiştir.

Örgütün boyutu nedeniyle, operasyonel birimlerin başında belirli bir alanda uzmanlığa ve emniyet sorunlarının yönetimi için verilmiş sorumluluğa sahip ayrı bir emniyet sorumlusu varsa, bu emniyet sorumlusu emniyet yöneticisi için ilk iletişim kurulacak kişi olacaktır.

8.6.4 Normal koşullar altında, emniyet yöneticisi Sorumlu Müdür ile iki kanal üzerinden iletişim kurar: Emniyet Eylemi Grubu ve bunun aracılığıyla Emniyet Denetim Kurulu veya doğrudan Emniyet Denetim Kurulu. Bu gruplar bu bölümde daha ileride ele alınmıştır. Acil veya olağandışı durumlarda, emniyet yöneticisi Şekil 8-2'deki ilgili kutucukları bağlayan noktalı çizgili ile gösterildiği gibi Sorumlu Müdüre doğrudan erişim sahibi olmalıdır. Bu iletişim kanalı nadiren kullanılmalıdır ve kullanıldığında uygun şekilde gerekçelendirilmeli ve belgelenmelidir.

8.6.5 Bir SMS ortamında, emniyet yöneticisi tehlikelerle ilgili emniyet verilerinin toplanmasından ve analizinden ve tehlikelerle ve bu tehlikelerin sonuçlarına ait emniyet riskleriyle ilgili emniyet bilgilerinin bölüm yöneticilerine dağıtılmasından sorumlu kişidir. Dolayısıyla, emniyet yöneticisi genellikle kötü haberleri ileten kişi olacaktır. Bu nedenle, emniyet yöneticisi seçim ölçütleri özel önem taşır ve bunlarla sınırlı kalmamak üzere, aşağıdakileri içermelidir:

a) operasyonel yönetim deneyimi;

b) operasyonları destekleyen sistemleri anlamak için teknik bilgi alt yapısı;

c) insanlarla iletişim becerileri;

d) analitik beceriler ve sorun çözme becerileri;

e) proje yönetimi becerileri ve

f) sözlü ve yazılı iletişim becerileri.

Not - Bir emniyet yöneticisi için örnek iş tanımı bu bölümde Ek 2'de yer almaktadır.

8.6.6 Emniyet hizmetleri tarafından tehlikelerin sonuçlarına ait emniyet riskleriyle ilgili bilgilerin dağıtılması, emniyet riski yönetimi sürecinde sadece ilk adımdır. Bu bilgiler bölüm yöneticileri tarafından kullanılmalıdır. Emniyet sorunlarının azaltılması kaçınılmaz olarak kaynak gerektirir. Bazen bu kaynaklar doğrudan bölüm yöneticileri tarafından kullanılabilir durumdadır. Çoklukla ek kaynaklar gerekir ve bu kaynakların dağıtılması bölüm yöneticisinin yetkisinde olmayabilir ve örgütün üst yönetimi tarafından onaylanması gerekebilir. Benzeri şekilde, örgütün üzerinde anlaşılan emniyet performansı ile ilgili olarak azaltma stratejilerinin etkililiği ve etkinliğinin tarafsız bir değerlendirmesinin sağlanması için bir tür formel örgütlenme süreci olması gerekir. Emniyet Denetim Kurulu (SRB) kaynak dağıtımı hedeflerinin elde edilmesi ve azaltma stratejilerinin etkililiği ve etkinliğinin tarafsız şekilde değerlendirilmesi için bir platform sağlar.

8.6.7 SRB Sorumlu Müdürün başkanlığını yaptığı çok yüksek seviyeli bir kuruldur ve işlevsel alanlardan sorumlu bölüm yöneticileri dahil olmak üzere üst düzey yöneticilerden oluşur. Emniyet yöneticisi SRB'de sadece danışman olarak yer alır. SRB açıkça stratejik bir kuruldur, politikalar, kaynak dağıtımı ve örgüt performansının izlenmesi ile ilgili yüksek seviyeli sorunlarla ilgilenir ve olağandışı koşullar gerektirmedikçe nadiren toplanır. SRB:

a) SMS uygulama planının etkili olup olmadığını izler;

b) gerekli bir düzeltme eyleminin zamanında yapılıp yapılmadığını izler;

c) örgütün emniyet politikasına ve hedeflerine göre emniyet performansını izler;

d) örgütün, başka bir temel operasyonel süreçte olduğu gibi emniyet yönetiminin belirtilen kurumsal önceliğini destekleyen, emniyet yönetimi süreçlerinin etkili olup olmadığını izler;

e) alt yüklenicilere verilen işletmelerin emniyet denetiminin etkili olup olmadığını izler;

f) düzenlemelere uyum için gerekenin ötesinde emniyet performansının elde edilmesi için uygun kaynakların ayrılmasını sağlar ve

g) SAG'ye stratejik yönlendirme sağlar.

8.6.8 SRB tarafından bir stratejik yönlendirme geliştirildikten sonra, örgüt içinde stratejilerin uyumlu ve koordineli bir şekilde uygulanması gerekir. Emniyet Eylem Grubunun (SAG) temel rolü budur. SAG bölüm yöneticileri ve ön saflarda yer alan personelin temsilcilerinden oluşan yüksek seviyeli bir kuruldur ve başkanlığını belirlenen bölüm yöneticileri sırayla yapar. Emniyet yöneticisi SAG'ın sekreteridir. SAG açıkça taktik bir kuruldur ve SRB'nin stratejik buyruklarının yerine getirilmesi için uygulama konuları ile ilgilenir. SAG bölüm işletmeleri sırasında karşılan tehlikelerin sonuçlarına ait emniyet risklerinin kontrolünü sağlamaya yönelik belirli etkinliklerle ilgili "kök" uygulama konuları ile ilgilenirken, SRB kendisi tarafından sağlana stratejik yönlendirmeye uyumu sağlamak için bu konuların koordinasyonu ile ilgilenir. SAG:

a) işlevsel alanlardaki operasyonel emniyet performansını denetler ve tehlikenin tanımlanması ve emniyet riski yönetiminin uygun şekilde, emniyetle ilgili farkındalık sağlamak için personelin katılımı ile gerçekleştirilmesini sağlar;

b) tehlikelerin belirlenen sonuçları için azaltma stratejileri ile ilgili çözümleri koordine eder ve emniyet verilerinin elde edilmesi ve personelin geri bildiriminin sağlanması için tatmin edici düzenlemelerin yapılmasını sağlar;

c) emniyetle ilgili olarak operasyonel değişikliklerin etkisini değerlendirir;

d) Düzeltme eylemi planlarının uygulanmasını koordine eder ve tüm personelin emniyet yönetimine tam olarak katılabilmesi için yeterince olanak olmasını sağlamak üzere toplantılar veya brifingler düzenler;

e) düzeltme eyleminin zamanında yapılmasını sağlar;

f) önceki emniyet tavsiyelerinin etkili olup olmadığını gözden geçirir.

g) emniyetin teşvik edilmesini denetler ve personele düzenlemelerde getirilen minimum gerekliliklere uyan veya aşan uygun emniyet, acil durum ve teknik eğitimlerini verildiğinden emin olunmasını sağlar.

8.7 ACİL MÜDAHALE PLANLAMASININ KOORDİNASYONU

8.7.1 Bir acil müdahale planlaması (ERP) bir kaza sonrasında hangi eylemlerin yapılması gerektiğini ve her bir eylemden kimin sorumlu olduğunu yazılı olarak ortaya koyar. Bir ERP'nin amacı, acil durum yetkilerinin dağıtılması ve acil durum sorumluluklarının atanması dahil olmak üzere, normal koşullardan acil durum koşullarına düzenli ve etkin bir şekilde geçilmesini sağlamaktır. Kritik personel tarafından gerçekleştirilecek eylemlerin onayı ve acil durumla başa çıkmak için gösterilen çabaların koordinasyonu da plan içinde yer almaktadır. Genel hedef işletmelere emniyetli bir şekilde devam edilmesi veya normal işletmelere en kısa zamanda dönülmesidir.

8.7.2 Havalimanları bir havaalanı acil durum planı (AEP), hava trafik hizmetleri sağlayıcıları beklenmeyen durum planları ve havayolları acil müdahale planları geliştirmelidir. Havalimanı, ATC ve havayolu işletmeleri birbiriyle çakıştığında, bu planların uyumlu olması mantıklıdır. Bu planların koordinasyonu SMS el kitabında açıklanmalıdır.

8.8 SMS DOKÜMANTASYONU

8.8.1 Bölüm 7'de açıklandığı gibi, SMS'nin belirgin bir özelliği tüm emniyet yönetimi etkinliklerinin belgeli ve görülebilir olmasının gerekmesidir. Dolayısıyla, dokümantasyon bir SMS'nin önemli bir unsurudur.

8.8.2 SMS dokümantasyonu, uygun olduğunda, ilgili ve geçerli tüm ulusal ve uluslararası düzenlemeleri içermeli ve bu düzenlemelere atıfta bulunmalıdır. Aynı zamanda, tehlike bildirim formları, operasyonel emniyetin yönetimi ile ilgili sorumluluk, hesap verme sorumluluğu ve yetki sıraları ve emniyet yönetimi örgütünün yapısı gibi SMS'ye özgü kayıtları ve dokümantasyonu içermelidir. Kayıtların işlenmesi, saklanması, alınması ve korunması dahil olmak üzere kayıt yönetimi için açık kılavuz bilgileri de içermelidir. Ancak, kuşkusuz bir SMS dokümantasyonunun en önemli kısmı SMS el kitabıdır (SMSM).

8.8.3 SMSM örgütün tüm örgüt açısından emniyete yaklaşımının iletilmesinin önemli bir aracıdır. Emniyet politikası, hedefleri, prosedürleri ve bireysel emniyetle ilgili hesap verme sorumluluklarını içerecek şekilde SMS'nin tüm yönlerini belgeler.

8.8.4 SMSM tipik olarak aşağıdakileri içerir:

a) emniyet yönetimi sisteminin kapsamı;

b) emniyet politikası ve hedefleri;

c) emniyetle ilgili hesap verme sorumlulukları;

d) kritik emniyet personeli;

e) dokümantasyon kontrol prosedürleri;

f) acil müdahale planlamasının koordinasyonu;

g) tehlikenin tanımlanması ve risk yönetimi şemaları;

h) emniyet güvencesi;

i) emniyet performansının izlenmesi;

j) emniyet denetimi;

k) değişimin yönetilmesi;

l) emniyetin teşvik edilmesi ve

m) yüklenicilere verilen etkinlikler.

8.9 SMS UYGULAMA PLANI

8.9.1 SMS uygulama planı örgütün emniyetin yönetilmesine yaklaşımını tanımlar. Bu nedenle, hizmetlerin etkili ve etkin bir şekilde sunulmasını desteklerken örgütün emniyet hedeflerine ulaşılmasını sağlayan bir SMS'nin uygulanması için gerçekçi bir stratejidir. Bir örgütün kurumsal emniyet hedeflerine nasıl ulaşacağını ve düzenlemelere dayalı olarak veya başka şekilde, yeni veya gözden geçirilmiş emniyet gerekliliklerini nasıl karşılayacağını açıklar. Plandaki önemli öğeler, normal olarak örgütün iş planına dahil edilmelidir. Birden fazla belgeden oluşabilen bir SMS uygulama planı hangi önlemlerin, kim tarafından ve hangi zaman aralığında alınacağının ayrıntılarını verir.

8.9.2 Örgütün büyüklüğü ve işletmelerinin karmaşıklığına bağlı olarak, SMS uygulama planı bir kişi veya uygun bir deneyim zeminine sahip bir planlama grubu tarafından geliştirilebilir. Planlama grubu, uygulama planındaki ilerlemeyi değerlendirmek için üst yönetimle düzenli olarak toplantı yapmalı ve bu gruba eldeki işe uygun kaynaklar (toplantılar için zaman dahil olmak üzere) sağlanmalıdır.

8.9.3 Bir SMS uygulama planı tipik olarak aşağıdakileri içerir:

a) emniyet politikası ve hedefleri;

b) sistem tanımı;

c) boşluk analizi;

d) SMS bileşenleri;

e) Emniyetle ilgili roller ve sorumluluklar;

f) Tehlike raporlama politikası;

g) çalışanların katılımını sağlayan araçlar;

h) emniyet performansı ölçümü;

i) emniyet iletişimi;

j) emniyet eğitimi ve

k) emniyet performansının yönetim tarafından gözden geçirilmesi.

8.9.4 Tamamlandığında, üst yönetim SMS uygulama planını onaylamalıdır. Bir SMS'nin uygulanması için tipik zaman aralığı bir ile dört yıl arasındadır. Aşamalı bir yaklaşımı da içerecek şekilde, SMS'nin uygulanması Bölüm 10'da ele alınmıştır ve bir SMS uygulama planı ve ilgili zaman aralığını geliştirmenin metodolojisi hakkında kılavuz bilgiler söz konusu bölümün Ek 2'sinde yer almaktadır.

Bölüm 8 Ek 1

EMNİYET YÖNETİMİ SİSTEMLERİ (SMS) ÇERÇEVESİ

Bir SMS, emniyetin bir örgüt tarafından yönetilmesi için bir yönetim aracıdır. Bu ek, bir örgüt tarafından bir emniyet yönetimi sisteminin (SMS) uygulanması ve sürdürülmesi için bir çerçeve sunar. Çerçevenin uygulanması örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına uygun olmalıdır. Çerçeve SMS'nin uygulanması için minimum gereklilikleri temsil eden aşağıdaki dört bileşen ve on iki unsurdan oluşur.

1. Emniyet politikası ve hedefleri

    1.1 Yönetimin taahhüdü ve sorumluluğu
    1.2 Emniyetle ilgili hesap verme sorumlulukları
    1.3 Emniyetin sağlanmasında önemli rol oynayan personelin atanması
    1.4 Acil müdahale planlamasının koordinasyonu
    1.5 SMS dokümantasyonu

2. Emniyet riski yönetimi

    2.1 Tehlikenin tanımlanması
    2.2 Risk değerlendirmesi ve riskin azaltılması.

3. Emniyet güvencesi

    3.1 Emniyet performansının izlenmesi ve ölçülmesi
    3.2 Değişimin yönetilmesi
    3.3 SMS'nin sürekli olarak iyileştirilmesi

4. Emniyetin teşvik edilmesi

    4.1 Eğitim ve öğretim
    4.2 Emniyet iletişimi

1. EMNİYET POLİTİKASI VE HEDEFLERİ

1.1 Yönetimin taahhüdü ve sorumluluğu

[Örgüt] ulusal ve uluslararası gerekliliklere uyması gereken ve örgütün Sorumlu Müdürü tarafından imzalanması gereken emniyet politikasını tanımlamalıdır. Emniyet politikası örgütteki emniyetle ilgili taahhütleri yansıtmalıdır; emniyet politikası için gereken kaynakların sağlanması hakkında açık bir ifade içermelidir ve görülür bir onayla, örgüt içinde iletilmelidir. Emniyet politikası emniyetle ilgili raporlama prosedürlerini içermelidir; hangi tür operasyonel davranışların kabul edilemez olduğunu açıkça ifade etmelidir ve disiplin kovuşturmasının uygulanmayacağı koşulları içermelidir. Emniyet politikası örgütle uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmelidir.

1.2 Emniyetle ilgili hesap verme sorumlulukları

[Örgüt] diğer işlevlerinden bağımsız olarak, [örgüt] adına, SMS'nin uygulanması ve sürdürülmesi için nihai sorumluluğu ve hesap verme sorumluluğunu alacak bir Sorumlu Müdür belirlemiş olmalıdır. Örgüt aynı zamanda SMS'nin emniyet yönetimi ile ilgili olarak, işlevlerinden bağımsız şekilde, yönetimin tüm üyelerinin ve çalışanların hesap verme sorumluluklarını tanımlamış olmalıdır. Emniyetle ilgili sorumluluklar, hesap verme sorumlulukları ve yetkiler belgelenmiş ve örgüt içinde iletilmiş olmalıdır ve emniyet riskinin tahammül edilebilirliğiyle ilgili olarak karar verme yetkisine sahip yönetim seviyelerinin bir tanımını içermelidir.

1.3 Emniyetin sağlanmasında önemli rol oynayan personelin atanması

[Örgüt] etkili bir SMS'nin geliştirilmesi ve sürdürülmesinden sorumlu kişi ve bu işin odak noktası olarak bir emniyet yöneticisi belirlemelidir.

1.4 Acil müdahale planlamasının koordinasyonu

[Örgüt] acil durum operasyonlarından normal işletmelere düzenli ve etkin bir şekilde geçiş ve normal işletmelere dönüş sağlayan bir acil müdahale planının, örgütün hizmetlerinin sunulması sırasında karşı karşıya gelmesi diğer örgütlerin acil müdahale planlarıyla uygun bir şekilde koordine edildiğinden emin olmalıdır.

1.5 SMS dokümantasyonu

[Örgüt] üst yönetim tarafından onaylanan, örgütün emniyet hedeflerine uyacak şekilde örgüt emniyetinin yönetilmesine yaklaşımını tanımlayan bir SMS uygulama planı geliştirmelidir. [Örgüt] emniyet politikalarını ve hedeflerini, SMS gerekliliklerini, SMS süreçlerini ve prosedürlerini, prosedürler ve süreçlerle ilgili sorumlulukları, hesap verme sorumluluklarını ve yetkileri ve SMS çıktılarını açıklayan bir SMS dokümantasyonu geliştirmeli ve sürdürmelidir. Ayrıca SMS dokümantasyonunun bir parçası olarak, emniyetin yönetilmesine yaklaşımını örgüt içinde iletmek için [örgüt] bir emniyet yönetimi sistemleri el kitabı (SMSM) geliştirmeli ve sürdürmelidir.

2. EMNİYET RİSKİ YÖNETİMİ

2.1 Tehlikenin tanımlanması

[Örgüt] işletmelerdeki tehlikelerin tanımlanmasını sağlayan formel bir süreç geliştirmeli ve sürdürmelidir. Tehlikenin tanımlanması, emniyet verilerinin toplanması için reaktif, proaktif ve tahmine dayalı yöntemlerin bir kombinasyonunu temel almalıdır.

2.2 Risk değerlendirmesi ve riskin azaltılması

[Örgüt], [örgütteki] işletmelerdeki emniyet risklerinin analizini, değerlendirilmesini ve kontrolünü sağlayan formel bir süreç geliştirmeli ve sürdürmelidir.

3. EMNİYET GÜVENCESİ

3.1 Emniyet performansının izlenmesi ve ölçülmesi

[Örgüt], örgütün emniyet performansını ve emniyet riski kontrollerinin etkililiğini doğrulamak için gerekli araçları geliştirmeli ve sürdürmelidir. [Örgütün] emniyet performansı SMS'nin emniyet performansı göstergeleri ve emniyet performansı hedeflerine göre doğrulanmalıdır.

3.2 Değişimin yönetilmesi

[Örgüt], değişiklikleri uygulamadan önce emniyet performansından emin olmak için gereken düzenlemeleri açıklama için ve operasyonel ortamdaki değişiklikler nedeniyle artık gerek duyulmayan emniyet riski kontrollerini ortadan kaldırmak veya değiştirmek için, örgütteki yerleşik süreçleri ve hizmetleri etkileyebilecek değişiklikleri belirlemesini sağlayan formel bir süreç geliştirmeli ve sürdürmelidir.

3.3 SMS'nin sürekli olarak iyileştirilmesi

[Örgüt], SMS'nin standart altı performans göstermesinin nedenlerini, SMS'nin işletmelerde standart altı performans göstermesinin olası sonuçlarını belirlemesini ve bu nedenleri ortadan kaldırmasını veya azaltmasını sağlayan formel bir süreç geliştirmiş ve sürdürmekte olmalıdır.

4. EMNİYETİN TEŞVİK EDİLMESİ

4.1 Eğitim ve öğretim

[Örgüt], personelin SMS görevlerinin yerine getirmek için eğitimli ve yeterli olmasını sağlayan bir emniyet eğitimi programı geliştirmeli ve sürdürmelidir. Emniyet eğitiminin kapsamı her bir bireyin SMS'ye katılma şekline uygun olmalıdır.

4.2 EMNİYET İLETİŞİMİ

[Örgüt], tüm personelinin SMS hakkında bilgi sahibi olmasını sağlayan, emniyetle ilgili önemli bilgileri taşıyan ve belirli emniyet önlemlerinin neden alındığını ve emniyet prosedürlerinin neden uygulanmaya başladığını veya değiştirildiğini açıklayan formel bir emniyet iletişimi şekli geliştirmeli ve sürdürmelidir.

Bölüm 8 Ek 2

BİR EMNİYET YÖNETİCİSİ İÇİN ÖRNEK İŞ TANIMI

1. GENEL AMAÇ

Emniyet yöneticisi, örgütün emniyet yönetimi sisteminin (SMS) planlanması, uygulanması ve yürütülmesi için kılavuzluk ve yönlendirme sağlamaktan sorumludur.

2. ÖNEMLİ ROLLER

Emniyet savunucusu

- Mükemmel bir emniyet tavrı ve davranışı sergilemeli, düzenleyici uygulamalara ve kurallara uymalı, tehlikeleri tanımalı ve raporlamalı ve emniyetin etkili bir şekilde raporlanmasını desteklemelidir.

Lider

- Etkili liderlik aracılığıyla emniyet uygulamalarının yeşermesini sağlayan bir örgüt kültürünün modelini oluşturur ve destekler.

İletişimci

- Emniyet sorunlarını yönetimin dikkatine sunmak ve emniyet bilgilerini örgütün personeline, yüklenicilere ve ilgili taraflara iletmek için bir bilgi iletim kanalı görevi yapar.
- Örgüt içindeki emniyet sorunları ile ilgili bilgi sağlar ve bu bilgileri ifade eder.

Geliştirici

- Tehlikenin tanımlanması ve emniyet riski değerlendirme şemalarının ve örgütün SMS'sinin sürekli olarak iyileştirilmesine yardımcı olur.

İlişki kurucu

- Örgütün Emniyet Eylem Grubu (SAG) ile ve emniyet hizmetleri ofisi içinde (SSO) mükemmel iş ilişkileri kurar ve bu ilişkileri sürdürür.

Elçi

- Örgütü devletin, uluslararası örgütlerin ve sektörün komitelerinde (örneğin ICAO, IATA, CAA, AIB v.s.) temsil eder.

Analizci

- Teknik verileri tehlikeler, olaylar ve olayların ortaya çıkışı ile ilgili trendler bakımından analiz eder.

Süreç yönetimi

- Rollerini ve sorumluluklarını yerine getirmek için geçerli süreçleri ve prosedürleri etkili bir şekilde kullanır.
- Süreçlerin etkinliğini arttırma fırsatlarını araştırır.
- Süreçlerin etkililiğini ölçer ve sürekli olarak kalitelerini iyileştirmeye çalışır.

3. SORUMLULUKLAR

3.1 Bu pozisyon değişen koşullarla ve durumlarla çok az gözetimle başa çıkma becerisi gerektirir. Emniyet yöneticisi örgütteki diğer yöneticilerden bağımsız olarak hareket eder.

3.2 Emniyet yöneticisi, emniyetli işletmelerle ilgili konularda üst yönetime ve Sorumlu Müdüre bilgi ve tavsiye sağlamaktan sorumludur. İncelik, diplomasi ve son derece sağlam bir karakter ön koşullarıdır.

3.3 Önceden hiç haber verilmeden veya kısa zaman önce haber verilerek veya normal iş saatleri dışında görevler verilebileceği için bu iş esneklik gerektirir.

4. DOĞASI VE KAPSAMI

Emniyet yöneticisi örgüt içindeki operasyonel personel, üst yöneticiler ve bölüm yöneticileri ile etkileşimde olmalıdır. Emniyet yöneticisi aynı zamanda örgütün dışındaki düzenleyici kurumlar, kuruluşlar ve hizmet sağlayıcılarla olumlu ilişkiler kurmalıdır. Diğer iletişimler, uygun olduğunda çalışma seviyesinde kurulmalıdır.

5. KALİFİKASYONLAR

Sahip olması gereken özellik ve kalifikasyonlar aşağıdakilerden oluşur:

a) örgütün işlevleri (örneğin eğitim yönetimi, uçak işletmeleri, hava trafik yönetimi, havaalanı işletmeleri ve bakım örgütü yönetimi) geniş bir operasyon bilgisi ve deneyimi;

b) emniyet yönetimi ilkeleri ve uygulamaları hakkında sağlam bilgi seviyesi;

c) iyi sözlü ve yazılı iletişim becerileri;

d) gelişmiş kişiler arası iletişim becerileri;

e) bilgisayar okur yazarlığı;

f) hem örgütün içinde hem de dışında tüm seviyelerle ilişki kurma yeteneği;

g) örgüt becerisi;

h) gözetim olmadan çalışma becerisi;

i) iyi analitik beceriler;

j) liderlik becerileri ve otoriter yaklaşım ve

k) iş arkadaşlarının ve yönetimin saygısını kazanma.

6. YETKİ

6.1 Emniyet konuları ile ilgili olarak, emniyet yöneticisi Sorumlu Müdür ve uygun üst ve orta yönetim seviyelerine doğrudan erişim sahibidir.

6.2 Emniyet yöneticisi, işletmenin herhangi bir yönüyle ilgili olarak emniyet denetimleri, araştırmaları ve incelemeleri yapma yetkisine sahiptir.

6.3 Emniyet yöneticisi, örgütün emniyet yönetimi sistemleri el kitabında (SMSM) belirtilen prosedürlere uygun şekilde dahili emniyet olaylarının incelemelerini yapma yetkisine sahiptir.

Bölüm 9

SMS'NİN İŞLETİLMESİ

9.1 HEDEF VE İÇERİKLER

Bu bölümde, ICAO SMS çerçevesini referans olarak kullanarak, SMS'nin işletilmesi ile ilgili gereklilikler açıklanmaktadır. ICAO SMS çerçevesinin ilk bileşeni Bölüm 8'de ele alınmıştı. Bu bölüm çerçevenin kalan üç bileşenini ele almaktadır. Bu bölüm aşağıdaki konuları içerir:

a) Emniyet riski yönetimi – Genel;

b) Tehlikenin tanımlanması;

c) Risk değerlendirmesi ve riskin azaltılması;

d) Emniyet güvencesi – Genel;

e) Emniyet performansının izlenmesi ve ölçülmesi;

f) Emniyet bilgilerinin kaynaklarının korunması;

g) Değişimin yönetilmesi;

h) SMS'nin sürekli olarak iyileştirilmesi;

i) Emniyet riski yönetimi (SRM) ile emniyet güvencesi (SA) arasındaki ilişki;

j) Emniyetin teşvik edilmesi — Eğitim ve

k) Emniyetin teşvik edilmesi - Emniyet iletişimi.

9.2 EMNİYET RİSKİ YÖNETİMİ - GENEL

9.2.1 Bir örgütün emniyeti, emniyet riski yönetimi aracılığıyla, hizmetlerin sunulması ile ilgili kritik etkinliklerdeki tehlikelerin sonuçlarına ait emniyet risklerinin makul oranda düşük (ALARP) seviyeye kadar kontrol edilmesini sağlayarak yönetir. Bu, aşağıdaki iki farklı etkinliği kapsayan genel bir terim olan emniyet riski yönetimi terimiyle adlandırılır: tehlikelerin tanımlanması ve risk değerlendirmesi ve riskin azaltılması.

9.2.2 Emniyet riski yönetimi, tahmin edilen tehlikelerin sonuçlarını azaltmak veya ortadan kaldırmak için uygun emniyet riski kontrollerinin sistem içine gömülü olduğu bir sistem tasarımı üzerinde inşa edilir. Bu, "sistem" ister bir uçak gibi fiziksel bir sistem olsun, isterse de bir havayolu, havaalanı veya bir hava trafik hizmeti sağlayıcısı gibi bir örgüt sistemi olsun geçerlidir. Bu el kitabında, ikincisi – örgüt sistemi – daha sık atıfta bulunulan "sistemdir". Bir örgüt, sistemin görevini yerine getirmek için gerekli yapılar, süreçler ve prosedürler ile insanlar, donanım ve tesislerden oluşan bir sistemdir.

9.3 TEHLİKENİN TANIMLANMASI

9.3.1 Emniyet riski yönetimi, tehlikenin tanımlanmasının temeli olarak sistemin işlevlerinin tanımının yapılması ile başlar (bkz. Bölüm 7). Sistem tanımında, sistemin bileşenleri ve bu bileşenlerin sistemin operasyonel ortam ile arayüzlerinde tehlike olup olmadığı ve sistemde önceden var olan emniyet riski kontrollerinin veya bu kontrollerin eksikliğinin belirlenmesi için analiz edilir (yine Bölüm 7'de ele alınan, boşluk analizi ismi verilen bir süreç). Tehlikeler açıklanan sistem bağlamı içinde analiz edilir, potansiyel olarak zararlı sonuçları tanımlanır ve bu sonuçlar emniyet riskleri (Bölüm 5'te ele alınan, belirlenen sonuçlarının hasar verme potansiyellerinin olasılığı ve sonuçta ortaya çıkan ciddiyeti) bakımından değerlendirilir. Tehlikelerin sonuçlarına ait emniyet risklerinin kabul edilemeyecek kadar yüksek olarak değerlendirildiği durumlarda, ek emniyet riski kontrolleri sisteme eklenmelidir. Bu nedenle, sistem tasarımının değerlendirilmesi ve sistemin tehlikelerin sonuçlarını yeterli ölçüde kontrol ettiğinin doğrulanması, emniyet yönetiminin temel bir unsurudur.

9.3.2 Dolayısıyla, tehlikenin tanımlanması işletmelerindeki tehlikeler ve emniyet riskleri hakkında geri bildirim toplama, kaydetme, bu geri bildirimlere göre hareket etme ve geri bildirimleri oluşturmanın amaçlandığı formel sürecin ilk adımıdır. Doğru bir şekilde başlatılan bir SMS'de, tehlikenin tanımlanmasının kaynakları Bölüm 3'te ele alınan üç yöntemi içermelidir: reaktif, proaktif ve tahmine dayalı yöntemler. Tehlikenin tanımlanması sürecinin kendisi Bölüm 4'de ele alınmaktadır.

9.3.3 Tehlikelerin tanımlanmasına yapısal bir yaklaşım, sistemin operasyonel ortamdaki çoğu tehlikenin mümkün olduğunca tanımlanmasını sağlar. Bu türden bir yapısal yaklaşımın elde edilmesi için uygun teknikler aşağıdakileri içerir:

a) ***Kontrol listeleri.*** Benzer sistemlerdeki deneyim ve mevcut veriler gözden geçirilmeli ve bir tehlike kontrol listesi oluşturulmalıdır. Potansiyel olarak tehlikeli alanların daha fazla değerlendirilmesi gerekir.

b) ***Grup halinde gözden geçirme.*** Grup oturumları tehlike kontrol listesini gözden geçirmek, tehlikeler hakkında daha geniş kapsamlı beyin fırtınaları yapmak veya ayrıntılı bir senaryo analizi yapmak için kullanılabilir.

9.3.4 Tehlikenin tanımlanması oturumları geniş bir yelpazede deneyimli operasyonel ve teknik personel gerektirir ve genellikle yönetilen bir grup tartışması şeklinde gerçekleştirilir. Beyin fırtınası tekniklerini bilen bir oturum yöneticisi, grup oturumlarını yönetmelidir. Normalde, varsa, emniyet yöneticisi bu rolü üstlenir. Burada ele alındığı şekliyle grup oturumlarının kullanılması tehlikenin tanımlanması bağlamında olsa da, aynı grup tanımladıkları tehlikenin sonuçlarına ait emniyet risklerinin olasılığının ve ciddiyetinin değerlendirilmesini de ele alabilir.

9.3.5 Tehlikelerin değerlendirilmesi, en az olası olandan en olası olana kadar tüm olasılıkları dikkate almalıdır. "En kötü durum" koşulları için yeterli bütçe ayrılmalıdır, ama nihai analize dahil edilecek tehlikelerin "anlaşılır" tehlikeler olması da önemlidir. En kötü anlaşılır durumla hesaba katılmaması gerekecek kadar şansa bağlı olan durumun arasındaki sınırın tanımlanması çoğunlukla zordur. Aşağıdaki tanımlar bu tür kararlar verirken kılavuz olarak kullanılmalıdır:

a) ***En kötü durum.*** Beklenen koşullar içinde en istenmeyenler, örneğin son derece yoğun trafik ve son derece kötü hava aksamaları.

b) ***Anlaşılır durum.*** Bu, aşırı koşulların varsayılan kombinasyonunun sistemin hizmet ömrü içinde ortaya çıkmasını beklemenin mantıksız olmadığını gösterir.

9.3.6 Tanımlanan tüm tehlikelere bir tehlike numarası verilmelidir ve tehlike günlüğüne kaydedilmelidir (tehlike günlüklerinin örnekleri Bölüm 5'in eklerinde bulunabilir). Tehlike günlüğü her bir tehlikenin, sonuçlarının tanımlarını, sonuçlara ait emniyet risklerinin olasılığına ve ciddiyetine ait değerlendirmeleri ve çoğunlukla azaltma önlemleri olmak üzere gereken emniyet riski kontrollerini içermelidir. Tehlike günlüğü yeni tehlikeler tanımlandığında güncellenmeli ve yeni emniyet riski kontrolleri (yani yeni azaltma önlemleri) eklenmelidir.

9.4 RİSK DEĞERLENDİRMESİ VE RİSKİN AZALTILMASI

9.4.1 Tehlikeler tanımlandıktan sonra, potansiyel sonuçlarına ait emniyet riskleri değerlendirilmelidir (Bölüm 5). Emniyet riski değerlendirmesi, örgütün kapasitelerini tehdit ettiği belirlenen tehlikelerin sonuçlarına ait emniyet risklerinin analizidir. Emniyet riski analizlerinde geleneksel olarak riskin iki bileşene ayrılır: hasara neden olan bir olay veya koşulun ortaya çıkma olasılığı ve eğer ortaya çıkarsa olay veya koşulun ciddiyeti. Emniyet riskleri ile ilgili karar verme ve kabul işlemleri risk tahammül edilebilirliği matrisi aracılığıyla belirlenir. Bir matrisin gerekli olması kadar, sağduyulu davranmak da gereklidir. Matrisin tanımı ve nihai yapısının tasarlanması hizmet sağlayıcı örgüte bırakılmalıdır ve bu tanım ve yapı denetim örgütü ile yapılan bir anlaşmaya konu olmalıdır. Bunun amacı, bu alandaki geniş farklılıklara uygun davranarak, her bir örgütün emniyetle ilgili karar alma araçlarının kendi işletmelerine ve operasyonel ortama uygun olmasını sağlamaktır.

9.4.2 Önceki adımda emniyet riskleri değerlendirildikten sonra, risklerin ortadan kaldırılması ve/veya ALARP durumuna indirilmesi gerekir. Bu emniyet riskinin azaltılması olarak adlandırılır. Emniyet riski kontrolleri tasarlanmalı ve uygulanmalıdır. Bunlar ek veya değiştirilmiş prosedürler, yeni denetim kontrolleri, eğitimde değişiklikler, ek veya değiştirilmiş donanım veya çeşitli başka ortadan kaldırma/azaltma alternatifleri olabilir. Neredeyse değişmez şekilde bu alternatifler üç geleneksel havacılık savunmasından (teknoloji, eğitim ve düzenlemeler) birinin veya bunların bir kombinasyonunun uygulanmaya veya yeniden uygulanmaya başlamasını içerecektir. Emniyet riski kontrolleri tasarlandıktan sonra, ama sistem henüz "çalıştırılmadan" önce, bu kontrollerin sisteme yeni tehlikeler ekleyip eklemediği değerlendirilmelidir.

9.4.3 Bu noktada, emniyet riski kontrollerinin kabul edilebilir olarak değerlendirilmesi koşuluyla, sistem işletmede kullanılmaya başlamaya/yeniden kullanılmaya başlamaya hazırdır. SMS'nin bundan sonraki bileşeni olan emniyet güvencesi, kalite yönetimi sistemleri tarafından kullanılanlara uygun denetim, analiz, gözden geçirme tekniklerini ve benzer teknikleri kullanır. Bu teknikler, tasarlandıkları gibi uygulanmaya devam etmelerini ve dinamik operasyonel ortamda etkili olmaya devam etmelerini sağlamak için emniyet riski kontrollerini izlemek için kullanılır.

9.5 EMNİYET GÜVENCESİ – GENEL

9.5.1 Emniyet riski yönetimi, emniyet yönetimi çevrimini tamamlamak için emniyet performansı hakkında geri bildirime ihtiyaç duyar. İzleme ve geri bildirimler aracılığıyla, SMS performansı değerlendirilebilir ve sistemde gereken değişiklikler yapılabilir. Ek olarak, emniyet güvencesi ilgili taraflara sistemi emniyet performansı seviyesi hakkında bir gösterge sağlar.

9.5.2 Güvence "güven veren bir şey" olarak tanımlanabilir. SMS'deki emniyet riski yönetimi süreci, örgütün kendi operasyonel süreçleri ve içinde çalıştığı ortamları iyi bir şekilde kavraması ile başlar; tehlikenin tanımlanması, emniyet riski değerlendirmesi ve emniyet risklerinin azaltılması ile ilerler ve uygun emniyet riski kontrollerinin geliştirilmesi ve uygulanması ile olgunlaşır. Tehlikelerin sonuçlarına ait emniyet riskleri için kontroller tasarlandıktan, emniyet risklerini kontrol edebilecekleri değerlendirildikten ve kullanılmaya başladıktan sonra, emniyet güvencesi emniyet riski yönetiminin yerine geçer.

9.5.3 Emniyet riski kontrolleri geliştirildikten ve uygulandıktan sonra, mevcut kalmaları ve amaçlandıkları gibi çalışmaları örgütün sorumluluğundadır. Yukarıdaki "güvence" tanımı altında, bu örgüt tarafından kontrollerin performansının ve etkililiği konusunda güven sağlamak için üstlenilen süreçler ve etkinlikleri içerir. Örgüt, operasyonel ortamdaki yeni ve azaltılmamış tehlikelerin ortaya çıkması konusunda ve operasyonel süreçlere, tesislerde, donanım koşullarında veya insan performansında mevcut emniyet riski kontrollerinin etkililiğini azaltabilecek bozulmalar konusunda uyarı verebilecek değişikliklerin farkına varıldığından emin olmak için işletmelerini ve ortamını sürekli olarak izlemeye devam etmelidir. Bu, gözden geçirme ve gerekirse, mevcut emniyet riski kontrollerinin düzeltilmesi veya yenilerinin geliştirilmesi için emniyet riski yönetimine dönülmesi gerektiği konusunda uyarı sağlayacaktır.

9.5.4 Bu kontrollerin sürekli olarak incelenmesi, analizi ve değerlendirilmesi için bir süreç, sistemin günlük çalışması boyunca uygulanmaya devam etmelidir. Emniyet güvencesi süreci, emniyet riskli kontrollerinin etkili olup olmadığının analizi, belgelenmesi, denetlenmesi ve yönetim tarafından gözden geçirilmesi gerekliliği bakımından kalite güvencesi sürecinin yansımasıdır.

Aradaki fark, emniyet güvencesinde vurgunun emniyet riski kontrollerinin yerinde, uygulanmakta olduğunun ve etkili olarak kaldığının güvencesinin sağlanması olmasıdır. Kalite güvencesindeki geleneksel vurgu, tipik olarak müşteri memnuniyeti üzerindedir, bu da uygun perspektiflerden bakıldığında, emniyetin sağlanması ile tamamen paralel olabilir veya olmayabilir. Kısa bir açıklama verilmiştir.

9.5.5 Havacılıktaki kalite güvencesi geleneksel olarak bakım ve üretim işletmeleriyle ilişkilendirilmiştir ve eğitimdeki ve kontrollerdeki sınırlı kullanımı dışında uçuşla ilgili işletmelerde daha az kullanılmıştır. Daha önceki bazı düzenlemelerde kalite güvencesi programlarına yer veriliyordu, ancak bunlardaki gereklilikler genellikle kapsamlı veya örgütün tüm işlevleri üzerinde iyi bir şekilde tanımlanmış değildi. Ancak, kalite güvencesinin sık sık emniyetten çok müşteri memnuniyeti ve ticari hedeflere ulaşmakla ilişkilendirilmesine karşın, tanıdık bir terim olduğu olgusu hala geçerlidir. Yine de, örgüt hedeflerine ulaşmayı sağlayan bir araç olarak, kalite güvencesi teknikleri emniyet güvencesine de uygulanabilir. Bu teknikleri emniyet güvencesi için kullanmak için, örgüt emniyetle ilgili hedeflerini belirler ve ölçerken dikkatli olmalıdır.

9.5.6 En önemli nokta, örgütün tüm operasyonel süreçleri emniyet riski kontrollerinin emniyet riski yönetimi ilkelerinin sağlam bir şekilde uygulanmasını sağlayacakları şekilde tasarlaması ve uygulaması ve bu kontrollerin güvencesini sağlamasıdır. Örgütün güvence süreci için başlık seçimi — "kalite" veya "güvence" — SMS'deki emniyet odağı sürdürüldüğü sürece daha az önemlidir.

9.5.7 Bölüm 6'da emniyet yönetimi için uyum ve performans temelli yaklaşımlar ele alınmaktadır. Uygun bir perspektiften bakılmadığında, performansın sağlanması sırasında gözden kaçırılabilecek bir nokta, düzenlemelere uygun güvencesinin dahil edilmesidir. Bölüm 6'da emniyet riski kontrolleri olarak düzenleme kavrayışı tanılıtılıyordu. Bu durumda, düzenlemeler emniyet riski yönetimi sürecinin ayrılmaz bir parçasıdır. Uygun bir şekilde uygulanan bir SMS'de, emniyet riski güvencesi ile düzenlemelere uyum güvencesi arasında çatışma yoktur. Düzenlemeler sistem tasarımının bir parçası olmalıdır ve düzenlemelere uyum ve emniyet riski yönetimi aynı bütünün parçalarıdır. Düzenlemelere uyulması hala geçerli bir beklentidir ve SMS'nin performansında "güven sağlamayı" amaçlayan bir etkinlik olarak emniyet güvencesi anlamında ele alınmalıdır.

9.5.8 Sonuç olarak, üst yönetim işletmelerin emniyeti sürdürülürken, aynı zamanda işin yaşama olasılığının sürdürülmesi için emniyetin sağlanması ve müşteri memnuniyeti hedeflerinin dengelenmesini sağlamalıdır. SMS ve QMS hedeflerinin entegrasyonu kaynak tasarrufu sağlayabilirse de, emniyetin sağlanması ve müşteri memnuniyeti hedeflerinin arasındaki uyumsuzluklar bulunması olasılığı ikisinin birbirinin yerine kullanılamayacağını veya aynı paralelde olmayabileceği göstermektedir. Bu tür bir entegrasyonun sağlanması örgütün yönetimine bağlıdır. Emniyet yönetimi perspektifinden, sistem performansının değerlendirilmesi ve sistem performansının geçerli operasyonel ortamda emniyet risklerini kontrol etmeye devam ettiğinin doğrulanması hala temel sorun olmaya devam etmektedir.

9.5.9 Son olarak, emniyet güvencesi etkinlikleri raporlar, çalışmalar, araştırmalar, denetimler, değerlendirmeler v.s.'deki bulgulara karşı düzeltme eylemlerinin geliştirilmesini ve bunların zamanında ve etkili bir şekilde uygulanmasını sağlayan prosedürleri içermelidir. Düzeltme eylemlerinin geliştirilmesi ve uygulanması için örgütün sorumluluğu, bulgularda atıfta bulunulan operasyonel bölümlere ait olmalıdır. Yeni tehlikeler bulunmuşsa, yeni emniyet riski kontrollerinin geliştirilmesi gerekip gerekmediğini belirlemek için emniyet yönetimi süreci kullanılmalıdır.

9.6 EMNİYET PERFORMANSININ İZLENMESİ VE ÖLÇÜLMESİ

9.6.1 Emniyet güvencesinin temel görevi kontroldür. Bu, örgütün emniyet performansının emniyet politikası ve onaylı emniyet hedeflerine göre doğrulandığı süreç olan gü performansının izlenmesi ve ölçümü ile sağlanır. Emniyet güvencesi kontrolü, örgütün hizmetlerinin sunulmasında operasyonel personelin katılması gereken etkinliklerin sonuçlarının izlenmesi ve ölçülmesi ile yapılır.

9.6.2 Uluslararası kalite yönetimi standardı olan ISO-9000'de süreç aşağıdaki şekilde tanımlanır: "... girdileri çıktılara dönüştüren bir dizi birbiri ile ilişkili etkinlik." Temel olarak "insanların yaptıkları şey" olarak "etkinliklere" yapılan vurgu, Bölüm 2 ve 3'teki emniyet ve emniyet yönetimi tartışmalarında insan hatasına ve iş yeri koşullarına o kadar vurgu yapılmasının da nedenidir ve nihayetinde emniyet riski yönetimine taşınmıştır. Çoğu tehlikenin temelinde bu koşullar vardır ve yine çoğu emniyet riski kontrolünün odağında da bu koşullar vardır. Dolayısıyla, emniyet performansı ve izleme süreci altındaki çoğu güvence etkinliği, hizmetlerin sunulması için gereken etkinliklerde insanların nasıl performans gösterdiklerini etkileyen işyeri koşullarına odaklanmıştır. Yine bu nedenle de, SHEL modeli — hizmetlerin sunulmasını sağlayan operasyonel etkinliklerin yerine getirilmesini destekleyen sistemlerden oluşan bir model — sistem tanımı ve boşluk analizi için kılavuz olarak önerilmiştir.

9.6.3 Aşağıda, emniyet performansının izlenmesi ve ölçümü aracılığıyla "emniyet güvencesi vermek" için ele alınması gereken genel konuların veya alanların bir listesi verilmiştir:

a) ***Sorumluluk.*** İşletme etkinliklerinin (planlama, organize etme, yönetme, kontrol) yönetiminden ve nihai olarak yerine getirilmesinden kimin sorumlu olduğu.

b) ***Yetki.*** Prosedürleri kimin yönetip yönetemeyeceği, kontrol edip edemeyeceği veya değiştirip değiştiremeyeceği ve emniyet riski kabulü kararları gibi önemli kararları kimin alabileceği.

c) ***Prosedürler.*** İşletme etkinliklerini yerine getirmek ve "ne" (hedefler) sorusunu "nasıl" (pratik etkinlikler) sorusuna çevirmek için belirli yöntemler.

d) ***Kontroller.*** İşletme etkinliklerini yolunda tutmak için tasarlanmış donanım, yazılım, özel prosedürler veya prosedür adımları ve denetim uygulamaları dahil olmak üzere sistemin unsurları.

e) ***Arayüzler.*** Bölümler arasındaki yetki sıraları, çalışanlar arasındaki iletişim sıraları, prosedürlerin tutarlılığı ve örgütler, iş birimleri ve çalışanlar arasında sorumluluğun açık bir şekilde dağıtılması gibi şeylerin incelenmesi.

f) ***Süreç önlemleri.*** Sorumlu taraflara gerekli eylemlerin yerine getirildiği, gerekli çıktıların üretildiği ve beklenen sonuçları ulaşıldığı hakkında geri bildirim sağlama araçları.

9.6.4 Emniyet performansı ve izleme ile ilgili bilgiler formel denetim ve değerlendirme, emniyetle ilgili olayların incelenmesi, hizmetlerin sunulması ile ilgili günlük etkinliklerin sürekli izlenmesi ve tehlike raporlama sistemleri aracılığıyla çalışanlardan alınan bilgiler gibi çeşitli kaynaklardan gelir. Bu bilgi kaynaklarından her biri her örgütte belirli bir seviyede bulunur. Ancak, bu kaynakların ne olması gerektiği veya nasıl "görünmeleri gerektiği" ile ilgili özellikler operasyon seviyesinde bırakılmalıdır, örgütlerin bunları örgüt büyüklüğü ve tipine uygun kapsam ve ölçekte ayarlamalarına izin verilmelidir. Emniyet performansının izlenmesi ve ölçülmesi için bilgi kaynakları aşağıdakileri içerir:

a) tehlike raporlama;

b) emniyetle ile çalışmalar;

c) emniyetle ilgili gözden geçirmeler;

d) denetimler;

e) emniyet araştırmaları ve

f) dahili emniyet incelemeleri.

9.6.5 Tehlikenin raporlanması ve tehlike raporlama sistemleri tehlikenin tanımlanmasının önemli unsurlarıdır. Gerçek sistem performansını operasyonel personelden daha iyi kimse bilemez. "Kitaba" göre nasıl çalışması gerektiğinin karşısında, günlük olarak gerçekten nasıl çalıştığını öğrenmek isteyen bir örgüt, bunu operasyonel personeline sormalıdır, bu da raporlama sistemlerinin önemini gösterir. Üç tür raporlama sistemi vardır:

a) zorunlu raporlama sistemleri;

b) gönüllü raporlama sistemleri ve

c) gizli raporlama sistemleri.

9.6.6 ***Zorunlu raporlama sistemlerinde***, insanlardan belirli tipte olay ve tehlikeleri rapor etmeleri istenir. Bunun için, kimin rapor vereceğini ve neyin raporlanacağını gösteren ayrıntılı düzenlemeler gerekir. Zorunlu sistemler genel olarak "donanım" konuları ile ilgilendiklerinden, operasyonel etkinliklerin diğer yönlerinden çok teknik arızalar hakkında bilgi toplama eğilimindedirler. Bu yanlılığın üstesinden gelmeye yardımcı olmak için, gönüllü raporlama sistemi diğer yönler hakkında daha fazla bilgi almayı amaçlarlar.

9.6.7 ***Gönüllü raporlama sistemlerinde*** rapor veren, bunun için herhangi hukuki veya yönetimsel bir zorunluluğu olmadan, gönüllü olay veya tehlike bilgileri sunar. Bu sistemlerde, düzenleyici kurumlar ve/veya örgütler raporlama için bir teşvik sunabilirler. Örneğin, hataları veya kasıtsız ihlalleri gösteren, raporlanmış olaylar için ceza işlemleri uygulanmayabilir. Raporlanan bilgiler rapor verenlere karşı kullanılmamalıdır, yani bu sistemler cezalandırıcı olmamalıdır ve bilgilerin raporlanmasını cesaretlendirmek için bilgi kaynaklarına koruma sunulmalıdır.

9.6.8 ***Gizli raporlama sistemleri*** rapor verenin kimliğini korur. Bu, gönüllü raporlama sistemlerinin cezalandırıcı olmamasını sağlamanın yöntemlerinden biridir. Gizlilik genellikle kimlik verilerinin kaldırılmasıyla ve rapor verenin kimliğini gösteren bilgilerin sadece raporlanan olayların takibi veya bu olaylardaki "boşlukların doldurulması" için "bekçiler" tarafından bilinmesini sağlayarak elde edilir. Gizli olay raporlama sistemleri, ceza veya utanç korkusu olmadan insan hatalarına neden olan tehlikelerin ortaya çıkmasını kolaylaştırır ve tehlikelerle ilgili bilgilerin daha geniş kapsamlı olarak alınmasını sağlar.

9.6.9 Raporlama sistemlerinin altında yatan temel süreçler standartlaştırılmış olsa da, gerçek raporlama gereklilikleri Devletler ve örgütler arasında değişebilir. Aynı zamanda, raporlama sistemlerinin başarısını sağlamak için, operasyonel personelin rapor verme konusunda normal olarak gönülsüz olduğunun belirtilmesi de önemlidir. Bu ifade her tür raporlama için geçerlidir, özellikle de hataların kişinin kendisi tarafından raporlanması söz konusu olduğunda geçerlidir. Bu gönülsüzlüğün nedenleri şunlardır: sadece en sık karşılaşılan üçünü belirtmek gerekirse misilleme, kendi kendini suçlama ve utanç. Bölüm 2'de ele alınan, tehlike tanımlama sistemlerinde emniyet raporlamasının önemi ile ilgili eğitim ve emniyet bilgilerinin kaynaklarının korunması (bölüm 9.7'de ele alınmıştır) raporlamadaki gönülsüzlüğü ortadan kaldırmak ve etkili bir emniyet raporlaması ortamı sağlamak için önemli stratejilerdir. Başarılı emniyet raporlama sistemlerinin tipik özellikleri aşağıdakilerden oluşur:

a) raporların verilmesi kolaydır;

b) raporların sonucu olarak disiplin cezası verilmez;

c) raporlar gizlidir ve

d) geri bildirim hızlı, erişilebilir ve bilgilendiricidir.

9.6.10 ***Emniyetle ilgili çalışmalar*** büyük emniyet sorunlarını kapsayan büyük kapsamlı analizlerdir. Bazı yaygın emniyet sorunları en iyi şekilde mümkün olan en geniş bağlamda incelendiklerinde anlaşılabilir. Bir örgüt küresel bir doğaya sahip veya sektör veya Devlet ölçeğinde ele alınmış bir emniyet sorunu ile karşılaşabilir. Örneğin, bir havayolu yaklaşma ve inişle ilgili olaylarda bir artış yaşayabilir (dengesiz yaklaşmalar, sert inişler, aşırı hızlı inişler v.s.). Küresel seviyede, sektör yaklaşma ve iniş kazalarının (ALA) sıklığı ve ciddiyetini ele almış ve önemli çalışmalar yapmış, pek çok emniyet tavsiyesi oluşturmuş ve uçuşun kritik yaklaşma ve iniş aşamalarında bu olayların azaltmak için küresel önlemler almıştır.

Dolayısıyla, söz konusu havayolu bu küresel tavsiyeler ve çalışmalar içinde kendi şirket için emniyet analizi için ikna edici argümanlar bulabilir. Bu tür argümanlar, önemli miktarda veri, uygun analiz ve etkili iletişim gerektiren büyük ölçekli değişimlerin yapılması için gereklidir. Tek tek olaylar ve anekdotlara dayanan bilgileri temel alan emniyet argümanları yeterli olmayabilir. Doğaları nedeniyle, emniyetle ilgili çalışmalar belirli, tek tek tehlikelerin tanımlanmasından çok, sistem emniyet sorunlarının ele alınması için daha uygundur.

9.6.11 ***Emniyetle ilgili gözden geçirme işlemleri*** yeni teknolojilerin kullanılmaya başlaması, prosedürlerin değiştirilmesi veya uygulanması sırasında veya işletmelerde yapısal bir değişim yapılan durumlarda gerçekleştirilir. Emniyetle ilgili gözden geçirme işlemleri, bölüm 9.8'de ele alınan, değişimin yönetilmesinin temel bir bileşenidir. İlgili değişimle bağlantılı, açıkça tanımlanmış bir hedefleri vardır. Örneğin, bir havaalanı yüzey araştırma donanımı (ASDE) uygulamayı düşünmektedir. Bu nedenle, emniyetle ilgili gözden geçirme işleminin hedefi, proje ile ilgili emniyet yönetimi etkinliklerinin uygun ve etkili olup olmadıklarını değerlendirerek XYZ havaalanında ASDE'nin uygulanmasıyla ilgili emniyet risklerini değerlendirmek olacaktır. Emniyetle ilgili gözden geçirme işlemleri, önerilen değişiklikler sonucunda aşağıdaki emniyet yönetimi etkinliklerinin etkili bir şekilde uygulanıp uygulanmadığını araştıran Emniyet Eylem Grupları (SAG) tarafından gerçekleştirilir:

a) tehlikelerin tanımlanması ve risk değerlendirmesi ve riskin azaltılması;

b) emniyet ölçümü;

c) yönetimin hesap verme sorumlulukları;

d) operasyonel personelin becerileri;

e) teknik sistemler ve.

f) anormal işletmeler.

9.6.12 Önerilen değişiklikler sonucunda her bir emniyet yönetimi etkinliğinin uygulanıp uygulanmadığı gözden geçirildikten sonra, SAG her bir etkinlik için bir tehlike konularını, bölüm yöneticisi tarafından önerilen yanıt/azaltma işlemini ve tehlikelerin ele alınmasında azaltma işlemlerinin uygunluğunu ve etkili olup olmadığının değerlendirmesini içeren bir liste hazırlar. Azaltma işlemi gerçekten tehlikeye yönelik olması durumunda uygun olacaktır. Azaltma işlemi, emniyet risklerini ALARP düzeyine indirmek için normal çalışma koşulları altındaki emniyet risklerini sürekli olarak yönetirse etkili olacaktır. SAG aynı zamanda her bir tehlikeye önem ve acillik derecesi vererek, yanıtların/azaltma işlemlerinin öncelikleri konusunda bir öneride bulunur. Böylece emniyetle ilgili gözden geçirmeler, emniyet ve etkili bir değişim için bir yol haritası sağlayarak, değişim süreleri boyunca emniyet performansının sürmesinin sağlarlar.

9.6.13 ***Denetimler*** örgütün SMS'sinin bütünlüğüne odaklanır ve emniyet riski kontrollerinin durumunu periyodik olarak değerlendirirler. Diğer gerekliliklerde olduğu gibi, denetim gereklilikleri de işlevsel seviyede bırakılır, böylece örgütün karmaşıklığına uygun, geniş bir karmaşıklık yelpazesi sağlanır. Denetimler hizmetin sunulması ile ilgili etkinliklere doğrudan katılan birimler için "harici" olsalar da, bir bütün olarak örgütün kendisi için "dahilidir". Denetimlerin teknik süreçlerin derinlemesine denetimleri olması gerekmez, aksine bölüm birimlerinin emniyet yönetimi işlevlerinin, etkinliklerinin ve kaynaklarının güvenceye alınmasını amaçlarlar. Denetimler SMS'nin yapısının personel politikası, onaylı prosedürler ve talimatlara uyum, donanım ve tesislerin çalıştırılması ve gereken performans seviyelerinin korunması v.s. için gereken yeterlilik seviyeleri ve eğitim bakımından sağlam olmasını sağlamak için kullanılır.

9.6.14 ***Emniyet araştırmaları*** günlük işletmelerdeki sorunlu alanlar veya darboğazlar, operasyonel personelin algıları ve fikirleri ve uyuşmazlık veya kafa karışıklıklarına neden olan alanlar gibi belirli bir işletmenin belirli unsurlarını veya prosedürlerini inceler. Emniyet araştırmalarında kontrol listeleri, anketler ve resmi olmayan gizli görüşmeler kullanılabilir. Araştırmalar öznel olduğundan, düzeltme eylemi alınmadan önce doğrulama yapılması gerekir. Araştırmalar önemli emniyet bilgileri için ucuz bir kaynak oluşturabilir.

9.6.15 ***Dahili emniyet incelemeleri*** incelenip Devlete rapor edilmesi gerekmeyen olayları veya durumları içerir, bazı durumlarda söz konusu olay Devlet tarafından incelemeye alınmasa da, örgütler dahili incelemeler yapabilirler.

Dahili emniyet incelemelerinin kapsamında bulunan olayların örnekleri aşağıdaki gibidir: uçuş sırasında türbülans (uçuş işletmeleri); frekans sıkışması (ATC); malzeme hatası (bakım) ve apron aracı işletmeleri (havaalanı).

9.6.16 Sonuç olarak, emniyet performansının bilgi kaynaklarının izlenmesinin bir örgütün SMS'sine katkısı aşağıdaki şekilde özetlenebilir:

a) tehlike raporlaması işletmelerindeki tehlikeler hakkında temel bilgi kaynağıdır;

b) emniyet çalışmaları genel emniyet sorunları ve/veya sistemli emniyet arızaları hakkında bir bilgi kaynağıdır;

c) emniyetle ilgili gözden geçirme işlemleri değişimin yönetilmesi ile bağlantılıdır ve değişen operasyonel koşullar altında emniyet performansının sürdürülmesini sağlar;

d) denetimler SMS yapılarının ve süreçlerinin bütünlüğünü sağlar;

e) emniyet araştırmaları günlük işletmelerindeki belirli sorunlu alanlar hakkında uzman algılarının ve fikirlerinin örneklerinin alınmasını sağlar;
ve

f) dahili emniyet incelemeleri Devlet tarafından incelenmesi zorunlu tutulmayan küçük ölçekli sonuçları ele alır.

9.7 EMNİYET BİLGİLERİNİN KAYNAKLARININ KORUNMASI

9.7.1 Uluslararası sivil havacılığın olağanüstü emniyet geçmişi, başka şeylerin yanında, iki önemli etkene bağlıdır: emniyet bilgilerinin geliştirilmesi ve serbest şekilde alışverişine dayanan sürekli bir öğrenme süreci ve hataları önleyici eylemlere dönüştürebilme becerisi. Modern sivil havacılıkta emniyetin sürdürülmesini hedefleyen çabaların ampirik verilere dayanması gerektiği uzun zamandır kabul edilen bir gerçektir. Sivil havacılıkta kullanılabilecek bu tür verilerin farklı kaynakları vardır. Bir araya geldiklerinde, havacılık işletmelerinin güçlü ve zayıf yönlerinin sağlam bir şekilde anlaşılmasının temelini oluştururlar.

9.7.2 Yıllar boyunca, kaza ve olay incelemelerinden elde edilen bilgiler, donanım tasarımı, bakım prosedürleri, uçuş ekibi eğitimi, hava trafik kontrol sistemleri, havaalanı tasarımı ve işlevleri, hava durumu destek hizmetleri ve hava ulaşımı sisteminin diğer emniyet bakımından kritik konuları hakkında iyileştirmeler yapmayı amaçlayan etkinliklerin belkemiğini oluşturmuştur. Geçtiğimiz yıllarda, teknolojik araçların mevcudiyeti emniyet verilerinin toplanmasının hızlanarak gelişmesine neden olmuştur (kaza ve olay incelemesi ve raporlaması ile birlikte, bundan sonra emniyet verilerini toplama ve işleme sistemleri veya SDCPS olarak adlandırılacaktır). Bölüm 3'te ele alındığı gibi, SDCPS bir SMS için yaşamsal önemdedir ve düzeltmeye yönelik emniyet eylemlerinin ve devam eden stratejilerin uygulanması için kullanılan bilgileri üretir.

9.7.3 SDCPS sivil havacılığın operasyonel hatalar hakkında daha derin bir kavrayış kazanmasını sağlamıştır: neden ortaya çıktıkları, ortaya çıkma sıklıklarını en aza indirmek için neler yapılabileceği ve emniyet üzerindeki olumsuz etkilerinin nasıl ortadan kaldırılabileceği. Havacılıkta tehlikelerin büyük çoğunluğu kasıtsız olan operasyonel hatalara yol açtığı tartışmasızdır. İyi eğitimli, iyi niyetli insanlar, iyi tasarlanmış bir donanıma bakım yaparken, çalıştırırken veya kontrol ederken hata yapmaktadır. Hataların kasıtlı eylemlerin, malzemenin yanlış kullanımının, sabotaj veya ihlallerin sonucu olduğu nadir durumlar dışında, cezalandırma sistemleri hesap verme sorumluluğu zincirinin kopmamasını sağlamaktadır. Kasıtsız operasyonel hataların daha iyi anlaşılması ve kötüye kullanım durumunda kuralların uygun şekilde işletilmesini birleştiren bu ikili yaklaşım, emniyet açısından sivil havacılığın işine yaramış, bu arada ihlalde bulunanlar için kaçış olmamasını sağlamıştır.

9.7.4 Ancak, geçtiğimiz yıllarda sivil havacılıkta olaylara neden operasyonel hatalar ele alınırken, SDCPS'den elde edilen bilgilerin disiplin veya cezalandırma amacıyla kullanılmasına yönelik bir eğilim ortaya çıkmıştır. Davalarda kanıt olarak da kabul edilmiş, bu da bu tür olaylarda yer alan bireylerin ceza almasına neden olmuştur. Kasıtsız operasyonel hatalardan kaynaklanan havacılık olaylarında cezai kovuşturmada bulunmak, havacılıktaki emniyetin iyileştirilmesi olan emniyet bilgilerinin geliştirilmesini ve serbestçe iletilmesini engelleyebilir.

9.7.5 Uluslararası sivil havacılık komünitesindeki birkaç girişim, SDCPS'nin korunma altına sağlamaya çalışmışlardır. Ancak, sorunun hassasiyeti düşünüldüğünde, sivil havacılığın çabalarında bir amaç birliği ve tutarlılık sağlayan bir çerçeve önemlidir. Emniyet bilgilerinin korunmasını sağlamaya yönelik çabalar emniyet bilgilerinin korunması gerekliliği ile kaza soruşturmalarındaki sorumluluk arasında hassas bir denge oluşturmalıdır. Bu bağlamda, Taraf Ülkelerde kaza soruşturmaları ile ilgili yasalara uyumlu olmayan önerilerde bulunmaktan kaçınmak için dikkatli bir yaklaşım sergilenmelidir.

9.7.6 ICAO Toplantılarının 35. oturumunda, kaynakların korunması ve emniyet bilgilerinin serbest akışı konusu ele alınmış ve Toplantı Kararı A35-17 — *Havacılık emniyetini iyileştirmek için emniyet verileri toplama ve işleme sistemlerinden elde edilen bilgilerin korunması* kararı alınmıştır. Bu karar ICAO Konseyine "Devletlere, Devlet içinde kaza soruşturmalarının uygun şekilde yapılmasını sağlarken, ilgili tüm emniyet verileri toplama ve işleme sistemlerinden elde edilen bilgilerin korunması için ulusal yasaları ve düzenlemeleri sokmalarında yardımcı olacak uygun hukuki kılavuzluğun geliştirilmesi" görevini vermiştir.

9.7.7 Toplantı Kararı A35-17'de istenen hukuki kılavuzluğun geliştirilmesinin ilk adımı olarak, ICAO bazı Devletlerden SDCPS'den elde edilen bilgilerin korunması ile ilgili yasaların ve düzenlemelerin örneklerini göstermelerini istemiştir. Ardından, ICAO Devletlerden alınan materyalin analizini yapmış, sağlanan yasalar ve düzenlemelerde ortak noktalar ve kavramsal noktalar aramıştır.

9.7.8 Sağlanan hukuki kılavuz (Annex 13 İlave E — *Uçak Kazaları ve Olayları İncelemesi* içinde bulunur*)* Devletlerin kaza soruşturmalarının uygun şekilde yapılmasını sağlarken, SDCPS'den elde edilen bilgilerin korunması için ulusal yasaları ve düzenlemeleri sokmalarında yardımcı olmayı amaçlar. Amaç, sadece havacılık emniyetinin iyileştirilmesi için toplanan bilgilerin uygun olmayan kullanımını önlemektir. Devletlerin yasalarını ve düzenlemelerini ulusal politikaları ve uygulamalarına uygun şekilde tasarlama esnekliğine sahip olması gerektiğini unutmadan, hukuki kılavuzluk emniyet bilgilerini korumak için yasa ve düzenlemeleri yürürlüğe sokan Devletin belirli gerekliliklerine uyarlanabilecek bir dizi ilke biçimini almıştır. Kılavuzun kısa bir özeti aşağıda yer almaktadır.

9.7.9 Hukuki kılavuz aşağıdakileri ifade eden genel ilkeleri içerir:

a) Emniyet bilgilerinin uygun olmayan şekilde kullanılmaktan korunmasının tek amacı, zamanında ve uygun önleyici önlemlerin alınabilmesi ve havacılık emniyetinin iyileştirilebilmesi için bu bilgilerin sürekli olarak mevcut olmasını sağlamaktır;

b) Emniyet bilgilerinin korunmasının amacı Devletlerde kaza soruşturmalarının uygun şekilde yürütülmesine müdahale etmek değildir;

c) Emniyet bilgilerini koruyan ulusal yasa ve düzenlemeler havacılık emniyetinin iyileştirilmesi için emniyet bilgilerinin korunması gerekliliği ile kaza soruşturmalarının uygun bir şekilde yürütülmesi gerekliliği arasında bir denge kurulmasını sağlamalıdır;

d) Emniyet bilgilerini koruyan ulusal yasa ve düzenlemeler, bu bilgilerin uygun olmayan şekilde kullanılmasını önlemelidir ve

e) Belirli koşullar altında nitelikli emniyet bilgilerine koruma sağlamak Devletin emniyet sorumlulukları arasındadır.

9.7.10 Kılavuzda, koruma ilkeleri aşağıdaki şekilde yer alır:

a) Emniyet bilgileri, aşağıdakileri içeren, ama bunlarla sınırlı kalması gerekmeyen belirli koşullara göre uygun olmayan kullanımdan korunma hakkına sahip olmalıdır: bilgilerin toplanmasının sadece emniyet amaçlarıyla olması ve bilgilerin açıklanmasının mevcudiyetlerinin sürmesini engelleyecek olması;

b) Koruma, içerdiği emniyet bilgilerinin doğası temelinde her bir SDCPS'ye özel olmalıdır;

c) Belirtilen koşullara uygun olarak, nitelikli emniyet bilgilerinin korunmasının sağlanması için formel bir prosedür oluşturulmalıdır;

d) Emniyet bilgileri toplanma amaçlarından farklı bir şekilde kullanılmamalıdır;
ve

e) Emniyet bilgilerinin disiplin, kamu, idari ve ceza kovuşturmalarında kullanılması sadece ulusal yasa tarafından uygun korumalar altında yapılmalıdır.

9.7.11 Kılavuz, emniyet bilgilerinin korunmasındaki istisnaların sadece ulusal yasa ve düzenlemeler tarafından ve aşağıdaki durumlarda verilmesini sağlar:

a) olayın yasaya göre hasar vermek kastı ile yapılan veya hasar oluşabileceği bilgisi ile yapılan bir eylem, taksirli eylem, ağır ihmal veya kasıtlı suistimale denk bir eylem nedeni ile ortaya çıktığının kanıtının bulunması;

b) uygun bir otoritenin, koşulların olayın makul olarak hasar vermek kastı ile yapılan veya hasar oluşabileceği bilgisi ile yapılan bir eylem, taksirli eylem, ağır ihmal veya kasıtlı suistimale denk bir eylem nedeni ile ortaya çıktığını gösterdiğini belirlemesi;

c) uygun bir otorite tarafından yapılan bir değerlendirmede, emniyet bilgilerinin açıklanmasının adaletin yerine gelmesi için zorunlu olduğunu belirlemesi ve bilgilerin açıklanmasının, bu açıklamanın emniyet bilgilerinin gelecekteki mevcudiyeti üzerinde ulusal ve uluslararası alanda sahip olabileceği olumsuz etkilerden daha önemli olması.

9.7.12 Kılavuz aynı zamanda kamuya açıklama konusunu da ele alır, yukarıda verilen koruma ve istisna hükümlerine bağlı olarak, emniyet bilgilerinin açıklanmasını isteyen bir kimse, bu açıklamanın yapılmasının gerekçesini ortaya koymak zorundadır. Emniyet bilgilerinin açıklanması için formel ölçütler oluşturulmalı ve bunlarla sınırlı kalmamak üzere, aşağıdakileri de içermelidir:

a) emniyet bilgilerinin açıklanması emniyeti tehlikeye atan koşulların düzeltilmesi ve/veya politikaların ve düzenlemelerin değiştirilmesi için zorunludur;

b) emniyet bilgilerinin açıklanması, emniyetin iyileştirilmesi için bu bilgilerin gelecekte de mevcut olmasını engellememektedir;

c) emniyet bilgilerinde bulunan ilgili kişisel bilgilerin açıklanması yürürlükteki gizlilik yasalarına uygundur ve

d) emniyet bilgilerinin açıklanması, kimlik bilgileri kaldırılarak, özetlenerek ve toplu halde yapılmalıdır.

9.7.13 Kılavuz, her bir SDCPS için ayrı bir yeddiemin olması gerektiğini önererek, emniyet bilgilerini koruyan yedieminin sorumluluklarını da ele alır. Aşağıdaki durumlar dışında, bilgilerin açıklanması konusunda her türlü korumayı sağlamak emniyet bilgileri yedieminin sorumluluğundadır:

a) emniyet bilgileri yediemini bilginin kaynağının bilgilerin açıklanması için rızasına sahiptir veya

b) emniyet bilgileri yediemini emniyet bilgilerinin açıklanmasının istisna ilkelerine uygun olduğu kanaatindedir.

9.7.14 Son olarak, kılavuz kaydedilen bilgilerin korunmasını ele alır ve kokpit ses kaydedicileri (CVR'ler) gibimevzuata göre gerekli olan işyeri kayıtlarının operasyonel personelin diğer mesleklerdeki kişilerin maruz kalmadıkları bir gizlilik ihlali oluşturmakta olarak algılanabileceklerini dikkate alara, aşağıdakileri önerir:

a) yukarıda verilen koruma ve istisna ilkelerine bağlı olarak, yasalar ve düzenlemelerde mevzuata göre yapılması gereken işyeri kayıtları öncelikli korumalı bilgiler, yani daha fazla korunması gereken bilgiler olarak kabul edilmelidir.

b) ulusal yasa ve düzenlemeler bu tür kayıtlarla ilgili olarak gizlilikleri ve kamu tarafından erişim bakımından özel önlemler almalıdır. Mevzuata göre gerekli olan işyeri kayıtlarının korunması için alınan bu önlemler gizlilik emirlerinin verilmesini de içerebilir.

9.8 DEĞİŞİMİN YÖNETİMİ

9.8.1 Havacılık örgütleri genişleme, daralma, mevcut sistemlerdeki, donanımlardaki, programlar, ürün ve hizmetlerdeki değişiklikler ve yeni donanım veya prosedürlerin kullanılmaya başlaması nedeniyle kalıcı değişimlerle karşı karşıya kalabilirler. Bir değişiklik olduğunda, işletmeye kasıtsız olarak tehlikeler eklenebilir. Emniyet yönetimi uygulamaları, değişimin yan ürünü olan tehlikelerin sistematik ve proaktif olarak tanımlanmasını ve tehlikelerin sonuçlarına ait emniyet risklerinin yönetmek için stratejilerin geliştirilmesini, uygulanmasını ve ardından değerlendirilmesini gerektirir. 9.6.11'de ele alınan emniyetle ilgili gözden geçirmeler, değişim durumlarında önemli bir bilgi ve karar verme kaynağıdır.

9.8.2 Değişiklik yeni tehlikelerin ortaya çıkmasına neden olabilir, mevcut emniyet riski azaltma stratejilerinin uygun olup olmamalarını etkileyebilir ve/veya mevcut emniyet riski azaltma stratejilerinin etkili olup olmamalarını etkileyebilir. Değişiklikler örgütün içinde veya dışında olabilir. Örgütün dışında gerçekleşen değişimlerin örnekleri arasında düzenlemelerdeki koşullardaki değişiklikler, emniyet gerekliliklerindeki değişiklikler ve hava trafik kontrolünün yeniden düzenlemesi bulunur. Örgütün içinde gerçekleşen değişimlerin örnekleri arasında, yönetim değişiklikleri, yeni donanım ve yeni prosedürler yer alır.

9.8.3 Formel bir değişim yönetimi süreci aşağıdaki üç noktayı hesaba katmalıdır:

a) ***Sistem ve etkinliklerin kritikliği.*** Kritiklik emniyet riski ile yakından ilgilidir. Kritiklik yanlış çalıştırılan bir donanımın veya yanlış gerçekleştirilen bir etkinliğin potansiyel sonuçları ile ilgilidir; temel olarak "bu donanım/etkinlik emniyetli sistem işletmeleri için ne kadar önemlidir?" sorusunu yanıtlar. Bu sistemin tasarımı sürecinde dikkate alınması gereken bir nokta olsa da, bir değişim durumunda da ilgili hale gelir. Açıktır ki, bazı etkinlikler hizmetlerin emniyetli olarak sunulması için diğerlerinden daha önemlidir. Örneğin, daha önce üçüncü taraflara ait bir yükleniciye bakım yaptıran bir örgütte, örgüt kendi bakım örgütünü uygulamaya başladıktan sonra, önemli bir bakımdan sonra hizmete dönen bir uçağın hizmete dönüşü ile ilgili etkinlikler veya prosedürlerdeki değişimler, ikram etkinliklerindeki değişimlerle ilgili benzer bir senaryoya göre emniyet bakımından daha kritik olacaktır. Potansiyel olarak ortaya çıkabilecek emniyet risklerinin kontrol edilebilmesi için düzeltme eylemlerinin yapılabilmesi için, daha kritik donanım ve etkinlikler değişimden sonra gözden geçirilmelidir.

b) ***Sistemlerin ve operasyonel ortamların stabilitesi.*** Değişimler büyüme, yeni varış noktalarına işletmeler, filolardaki değişiklikler, sözleşmeli hizmetlerdeki değişiklikler veya örgütün doğrudan kontrolü altında olan diğer değişiklikler gibi programlı bir değişikliğin sonucu olabilir. Ekonomik veya mali durum, işçilerdeki huzursuzluklar, politik veya düzenleme ortamlarındaki değişiklikler, hava durumundaki sezonsal değişiklikler gibi fiziksel ortamdaki değişiklikler gibi operasyonel ortamdaki değişiklikler de önemlidir. Bu etkenler örgütün doğrudan kontrolü altında olmasa da, bunlara yanıt vermek için örgütün önlem alması gerekir. Sistemlerde veya operasyonel ortamlarda sık değişiklikler olması, yöneticilerin önemli bilgileri daha dengeli durumlara göre daha sık güncellemeleri gerekir. Bu, değişimin yönetilmesinde dikkate alınması gereken önemli bir noktadır.

c) ***Geçmiş performans.*** Kritik sistemlerin geçmiş performansları gelecekteki performanslarını sağlam bir göstergesidir.
Emniyet güvencesinin kapalı devre doğası burada etkili olur. Emniyet güvencesi sürecindeki trend analizleri, emniyet performansı önlemlerinin zaman içinde izlenmesi ve bu bilginin değişim durumlarında gelecekteki etkinliklerin planlanmasına katılması için kullanılmalıdır. Ayrıca, geçmiş denetimlerin, değerlendirmelerin, incelemelerin veya raporların sonucunda sorunlar bulunduğunda ve düzeltildiğinde, bu bilgilerin düzeltmeye yönelik eylemlerin etkililiğini sağlamak için dikkate alınması önemlidir.

9.8.4 Bundan sonra, formel bir değişim yönetimi süreci ile örgüt içinde yerleşik süreçleri, prosedürleri, ürünleri ve hizmetleri etkileyebilecek değişiklikler tanımlanabilir. Değişiklikleri uygulamadan önce, formel bir değişim yönetimi süreci emniyet performansını sağlayacak düzenlemeleri tanımlamalıdır. Bu sürecin sonucu, örgüt tarafından hizmetlerin sunulması sırasındaki değişikliklerden kaynaklanan emniyet risklerinin ALARP düzeyine indirilmesidir.

9.8.5 Bölüm 7'de sistemin bir SMS'nin planlanmasındaki temel öncül etkinliklerinden biri olarak tanımlanmasının (sistem tanımı) önemi ele alınmaktadır. Sistem tanımının hedefi, temel sistem için temel bir tehlike analizi belirlemektir. Sistem evrildikçe, sistemdeki (veya sistemin çalışma bağlamını sağlayan ortamdaki) küçük görünen, ama kademeli olarak artan değişiklikler zaman içinde birikebilir, bu da ilk sistem tanımını yanlış hale getirebilir. Bu nedenle, formel değişimin yönetimi sürecinin parçası olarak, değişim koşulları bulunmasa bile, sistem tanımı ve temel tehlike analizi, geçerliliklerinin sürdüğünü belirlemek için periyodik olarak gözden geçirilmelidir. Bir örgüt sistemde değişiklikler yapıldıktan sonra ve bunun ardından periyodik olarak, hizmetlerin sunulduğu ortamın açık bir temsilini sunmaya devam ettiğinden emin olmak için, sistemini, bu sistemin beklenen ve gerçek operasyonel ortamı gözden geçirmelidir.

9.9 SMS'NİN SÜREKLİ OLARAK İYİLEŞTİRİLMESİ

9.9.1 Güvence, sürekli iyileştirme çevresi ilkesi üzerinde inşa edilir. Kalite güvencesinin kalitede sürekli iyileştirmeyi kolaylaştırdığı gibi, emniyet güvencesi operasyonel sistemin sürekli doğrulanması ve güncellenmesi ile düzenlemelere uyum da dahil olmak üzere, emniyet performansının kontrol edilmesini sağlar. Bu hedeflere benzer araçların uygulanması ile ulaşılır: dahili değerlendirmeler ve bağımsız denetimler (hem dahili hem de harici), katı belge kontrolleri ve emniyet kontrolleri ve azaltma eylemlerinin sürekli olarak izlenmesi.

9.9.2 ***Dahili değerlendirmeler*** örgütün operasyonel etkinliklerinin ve SMS'ye özgü işlevlerin değerlendirilmesini içerir. Bu amaçla yapılan değerlendirmeler, değerlendirilen teknik süreçten işlevsel olarak bağımsız olan kişiler veya örgütler tarafından yapılmalıdır (yani uzman bir emniyet veya kalite güvencesi bölümü veya üst yönetim tarafından yönetilen başka bir alt örgüt). Dahili değerlendirme işlevi aynı zamanda emniyet yönetimi işlevleri, politika oluşturma, emniyet riski yönetimi, emniyet güvencesi ve emniyetin teşvik edilmesinin denetlenmesini ve değerlendirilmesini gerektirir. Bu denetimler, belirlenen yönetim sorumlularına SMS için SMS'nin kendisinin süreçlerinin envanterini yapma sorumluluğunu verir.

9.9.3 ***Dahili denetimler*** yöneticilerin karar vermek ve operasyonel etkinlikleri yolunda tutmak için bilgi almak üzere kullanabilecekleri önemli bir araçtır. Emniyet yönetimi ile ilgili temel sorumluluk, örgütün hizmetlerinin sunumunu destekleyen teknik etkinliklerinin "sahibi olan" kişilere aittir. Tehlikelerle en çok doğrudan karşı karşıya gelinen, emniyet risklerine katkıda bulunan etkinliklerdeki bozuklukların ve doğrudan denetim ve kaynak dağıtımının emniyet risklerini ALARP seviyesine indirebileceği yer burasıdır. Dahili denetimler çoğunlukla bir örgütün etkinlikleri ile ilgili bir test veya bu etkinliklerin "derecelendirilmesi" olarak kabul edilse de, emniyet riski kontrolleri uygulandıktan sonra, hizmetlerin sunulmasını destekleyen etkinliklerden sorumlu müdürlere, bu etkinliklerin çalışmaya devam edip etmediklerini ve operasyonel emniyeti sürdürmede etkili olup olmadıklarını kontrol etmede yardımcı olmak için kullanılan, emniyet güvencesinin önemli araçlarıdır.

9.9.4 SMS'nin ***harici denetimleri*** düzenleyici kurum, kod paylaşımı ortakları, müşteri örgütleri veya örgüt tarafından seçilen diğer üçüncü taraflar tarafından gerçekleştirilebilir. Bu denetimler sadece gözetim sistemiyle güçlü bir arayüz sağlamaz, aynı zamanda ikincil bir güvence sistemi sağlar.

9.9.5 Dolayısıyla, SMS'nin sürekli olarak iyileştirilmesinin amacı, standardın altındaki performansların dolaysız nedenlerinin ve bu performansların SMS'nin çalışmasındaki sonuçlarını belirlenmesi ve emniyet güvencesi etkinlikleri aracılığıyla belirlenen standardın altındaki performanslar içeren durumların düzeltilmesidir. Sürekli iyileştirme dahili değerlendirmeler, dahili ve harici denetimler aracılığıyla elde edilir ve aşağıdakiler için geçerlidir:

a) Örneğin dahili değerlendirmeler aracılığıyla, tesislerin, donanımın, dokümantasyonun ve prosedürlerin proaktif olarak değerlendirilmesi;

b) Örneğin periyodik yeterlilik kontrolleri (değerlendirme/denetleme formu) aracılığıyla, bireyin emniyetle ilgili sorumluluklarını yerine getirdiğinin doğrulanması için bireyin performansının proaktif olarak değerlendirilmesi ve

c) Örneğin, dahili ve harici denetimler aracılığıyla, sistemin emniyet risklerinin kontrolü ve azaltılmasındaki etkililiğinin doğrulanması için reaktif değerlendirmeler.

9.9.6 Sonuç olarak, sürekli iyileştirme sadece örgüt teknik işletmelerin ve düzeltme eylemlerinin etkili olup olmadığı konusunda sürekli olarak farkındalık gösterirse ortaya çıkabilir. Aslında, emniyet kontrollerinin ve azaltma eylemlerinin sürekli izlenmesi olmadan, emniyet yönetiminin hedeflerine ulaşıp ulaşamadığını söylemenin yolu yoktur. Benzer şekilde, bir SMS'nin amacını etkin bir şekilde yerine getirip getirmediğini ölçmenin yolu da yoktur.

9.10 EMNİYET RİSKİ YÖNETİMİ (SRM) İLE EMNİYET GÜVENCESİ (SA) ARASINDAKİ İLİŞKİ

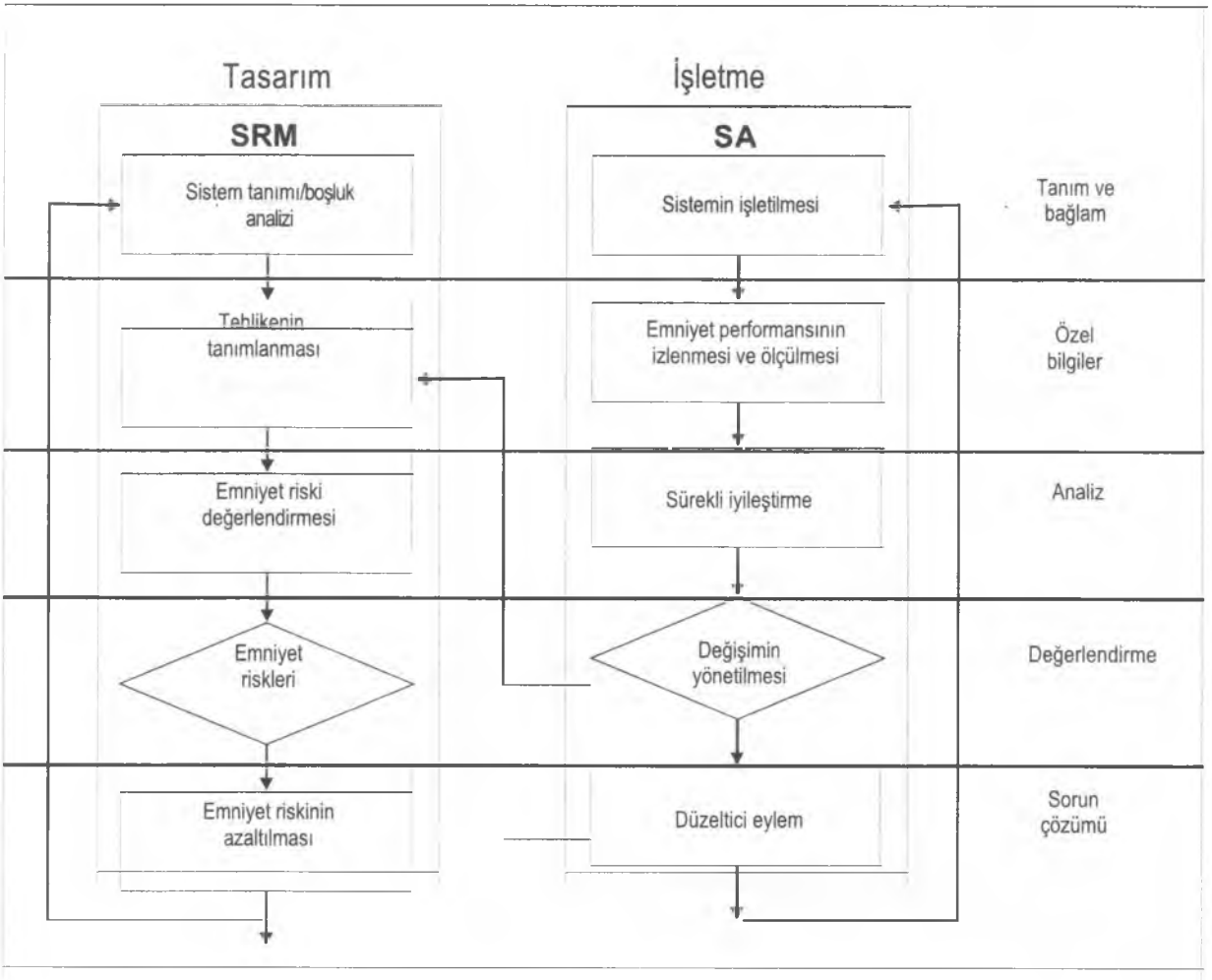
9.10.1 Emniyet riski yönetimi ile emniyet güvencesi arasındaki ilişkinin incelikleri sık sık kafa karıştırıcı olabilmektedir. Etkili risk yönetiminde ve emniyet güvencesinde, hem hizmet sağlayıcı hem de sivil havacılık denetim kumru için ilk görevlerden biri, örgüt sisteminin ve etkinliklerinin yapısı ve yapılandırılması hakkında kapsamlı bir anlayış sahibi olmaktır. Önemli miktarda tehlike ve emniyet riski bu etkinliklerin yanlış tasarlanmasından veya sistem ve operasyonel ortam arasındaki uyumsuzluktan kaynaklanır. Bu durumlarda, operasyonel emniyete yönelik tehlikeler yeterince anlaşılmayabilir ve dolayısıyla yeterince kontrol edilemeyebilir.

9.10.2 Bir SMS'nin emniyet riski yönetimi işlevi, tehlikelerin başlangıçta tanımlanmasını ve emniyet risklerinin değerlendirilmesini sağlar. Örgüt içinde emniyet riski kontrolleri geliştirilir ve emniyet riskini ALARP düzeyine indirebilecekleri belirlendiğinde, günlük işletmelerde kullanılırlar. Bu noktada, emniyet riski kontrollerinin amaçlandığı gibi uygulandığından ve amaçlanan hedeflerine ulaşmaya devam ettiklerinden emin olmak için, emniyet güvencesi işlevi devreye girer. Emniyet güvencesi işlevi aynı zamanda operasyonel ortamdaki değişiklikler nedeniyle yeni emniyet riski kontrolleri gerekliliğinin tanımlanmasını sağlar.

9.10.3 Bir SMS'de sistemin emniyet gereklilikleri örgütün hizmet sunumunu destekleyen etkinliklerdeki emniyet risklerinin nesnel olarak değerlendirilmesinden geliştirilir ve bu değerlendirmeyi temel alır. Sistemin güvence tarafı örgütün (kendisine ve uygun üçüncü taraflara) bu gerekliliklerin nesnel kanıtların toplanması ve analizi ile yerine getirildiğini kanıtlaması üzerine odaklanır.

9.10.4 Dolayısıyla, bir SMS'nin emniyet riski yönetimi işlevi hizmet sunumunu destekleyen işletmelerdeki emniyet risklerinin değerlendirilmesi ve aynı zamanda değerlendirilen risklerin ALARP düzeyine indirilmesi için kontrollerin geliştirilmesini sağlar. Aynı zamanda, bu etkinliklerle ilgili emniyet kararlarını destekler. Tamamlandığına, SMS'nin emniyet güvencesi işlevi bir QMS'deki kalite güvencesi işlevine son derece benzer şekilde çalışır. Aslında, SMS'nin emniyet güvencesi işlevleri neredeyse doğrudan uluslararası kalite yönetimi standardı olan ISO 9001-2000'den alınmıştır. Daha önce ele alındığı gibi, önemli bir fark vardır: tipik QMS gereklilikleri müşteri gereklilikleriyken ve müşteri memnuniyetini temel alırken, SMS gereklilikleri emniyet gereklilikleridir ve emniyetin sağlanmasını temel alırlar.

9.10.5 İki işlevin bir SMS'nin tümleşik süreçleri içindeki rollerinin tekrarlanması önemlidir. Emniyet riski yönetimi (SRM) süreci, tehlikelerin başlangıçta tanımlanmasını ve risklerin değerlendirilmesini sağlar. Emniyet riski kontrolleri geliştirilir ve emniyet riskini ALARP düzeyine indirebilecekleri belirlendiğinde, günlük işletmelerde kullanılırlar. Bu noktada, emniyet güvencesi (SA) işlevi devreye girer. Emniyet güvencesi, örgüt kontrollerinin uygulandığının ve tüm tiplerdeki kontrollerin amaçlanan hedeflerine ulaşmaya devam ettiğinin güvencesini sağlar. Bu sistem aynı zamdan operasyonel ortamdaki değişiklikler nedeniyle yeni kontrollerin eklenmesi gerekliliğinin değerlendirilmesini sağlar. Şekil 9-1'de bu konsept görsel biçimde gösterilmiştir.



Şekil 9-1. Emniyet riski yönetimi ile emniyet güvencesi arasındaki ilişki

9.11 EMNİYETİN TEŞVİK EDİLMESİ — EĞİTİM

9.11.1 Bir örgütteki emniyet çabaları zorunlu kılınarak veya politikaların tamamen mekanik olarak uygulanması ile başarıya ulaşamaz. Emniyetin teşvik edilmesi hem bireysel hem de örgüt içindeki davranışları belirleyen tavrı ortaya koyar ve örgütün politikaları, prosedürleri ve süreçlerindeki boşlukları doldurarak, emniyet çabalarına bir amaç anlayışı katar.

9.11.2 Emniyet politikasında ve hedeflerinde belirtilen pek çok süreç ve prosedür ve SMS'nin emniyet riski yönetimi ve emniyet güvencesi bileşenleri, bir SMS'nin yapısal temel taşlarını sağlar. Ancak, örgüt aynı zamanda operasyonel personel ile örgütün yönetimi arasındaki iletişimi sağlayan süreçleri ve prosedürleri belirlemelidir. Örgütler hedeflerini ve örgütün etkinliklerinin ve önemli olayların mevcut durumunu iletmek için her tür çabayı göstermelidir. Benzer şekilde, örgütler açık bir ortamda yukarıya doğru iletişim için bir yöntem sağlamalıdır.

9.11.3 Emniyetin teşvik edilmesi aşağıdakileri içerir:

a) Emniyetle ilgili yeterlilik dahil olmak üzere eğitim ve öğretim ve

b) emniyet iletişimi.

9.11.4 Emniyet yöneticisi örgütün belirli işletmeleri ve operasyonel birimleriyle ilgili emniyet konuları hakkında geçerli bilgileri ve eğitimi sağlar. Örgütteki seviyelerinden bağımsız olarak tüm personele uygun eğitimin sağlanması, yönetimin SMS'nin etkili şekilde gerçekleştirilmesine taahhüdünün bir göstergesidir. Emniyet eğitimi ve öğretimi aşağıdakileri içermelidir:

a) eğitim gerekliliklerinin belirlenmesi için belgelenmiş bir süreç;

b) eğitimin etkililiğini ölçen bir doğrulama süreci;

c) işe alma sırasında (genel emniyet) işe özel eğitim;

d) İnsani Etkenler ve örgüt etkenlerini içerecek şekilde, SMS'yle ilgili işe alma/başlangıç eğitimi; ve

e) tekrarlanan emniyet eğitimi.

9.11.5 Örgütün içindeki her bir etkinlik alanında eğitim gereklilikleri ve etkinlikleri belgelenmelidir. Çalışanın eğitim gerekliliklerinin belirlenmesi ve izlenmesi ve personelin planlanan eğitimi aldığının doğrulanmasına yardımcı olmak için yönetim de dahil olmak üzere her çalışan için bir eğitim dosyası oluşturulmalıdır. Eğitim programları örgütün gerekiiliklerine ve karmaşıklığına uyarlanmalıdır.

9.11.6 Bir örgütteki emniyet eğitimi personelin emniyet yönetimi ile ilgili görevlerini yerine getirecek şekilde eğitilmiş ve yeterli olmasını sağlamalıdır. SMS el kitabı (SMSM) operasyonel personel, yöneticileri ve denetimciler, üst yöneticiler ve Sorumlu Müdür için başlangıç eğitimi ve tekrarlanan emniyet eğitimi standartlarını belirtmelidir. Emniyet eğitiminin miktarı bir bireyin sorumluluklarına ve SMS'ye katılma şekline uygun olmalıdır. SMSM'de aynı zamanda içerik, sıklık, doğrulama ve emniyet eğitimi kayıtlarının yönetimi de dahil olmak üzere emniyet eğitimi sorumlulukları da belirtilmelidir.

9.11.7 Emniyet eğitimi bir yapıtaşı yaklaşımı izlemelidir. İşletme personeli için emniyet eğitimi, tüm çalışma ve emniyet prosedürlerinin izlenmesi ve tehlikelerin tanınması ve raporlanması dahil olmak üzere emniyet sorumluluklarını da dikkate almalıdır. Eğitim hedefleri örgütün emniyet politikasını ve SMS temel ilkelerini ve genel bakışını da içermelidir. İçerik tehlikelerin, sonuçların ve risklerin tanımını, roller ve sorumluluklar dahil olmak üzere emniyet riski yönetimi sürecini ve son derece temel olarak emniyet raporlamasını ve örgütün emniyet raporlama sistemlerini içermelidir.

9.11.8 Yöneticiler ve denetmenler için emniyet eğitimi, SMS'nin desteklenmesi ve operasyonel personelin tehlikenin raporlanmasına katılması dahil olmak üzere emniyet sorumluluklarını dikkate almalıdır. İşletme personeli için oluşturulan eğitim hedeflerine ek olarak, yöneticiler ve denetmenler için eğitim hedefleri emniyet süreci, tehlikenin tanımlanması ve emniyet risk değerlendirmesi ve azaltılması ile değişimin yönetimi hakkında ayrıntılı bilgiler içermelidir. İşletme personeli için belirtilen içeriğe ek olarak, denetmenler ve yöneticiler için eğitimin içeriğinde emniyet verileri analizi de yer almalıdır.

9.11.9 Üst yöneticiler için emniyet eğitimi ulusal ve örgüt düzeyindeki emniyet gerekliliklerine uyum, kaynakların dağıtılması, etkili bir bölümler arası iletişim sağlanması ve SMS'nin etkin bir şekilde desteklenmesi gibi emniyet sorumluluklarını içermelidir. Önceki iki çalışan grubunun hedeflerine ek olarak, üst yöneticiler için emniyet eğitimi emniyet güvencesi ve emniyetin teşvik edilmesini, emniyet rolleri ve sorumluluklarını ve kabul edilebilir emniyet seviyeleri oluşturulmasını içermelidir (Şekil 9-2).

9.11.10 Son olarak, emniyet eğitimi Sorumlu Müdür için özel bir emniyet eğitimi içermelidir. Bu eğitim oturumu makul oranda kısa olmalıdır (yarım günü aşmamalıdır) ve Sorumlu Müdüre SMS rolleri ve sorumlulukları, emniyet politikası ve hedefleri, emniyet riski yönetimi ve emniyet güvencesi dahil olmak üzere örgütün SMS'si hakkında genel bir farkındalık sağlamalıdır.

9.12 EMNİYETİN TEŞVİK EDİLMESİ - EMNİYET İLETİŞİMİ

9.12.1 Örgüt SMS hedeflerini ve prosedürlerini tüm operasyonel personeline iletmelidir ve SMS örgütün hizmetlerin sunulmasını destekleyen işletmelerinde tüm yönleriyle görünür olmalıdır. Emniyet yöneticisi örgütün SMS programının performansını bültenler ve brifingler aracılığıyla iletmelidir. Emniyet yöneticisi aynı zamanda, hem örgüt içinde hem de diğer örgütlerden, incelemeler ve olay geçmişleri veya deneyimleri aracılığıyla öğrenilen derslerin geniş bir kapsamda dağıtılmasını sağlamalıdır. Emniyet yöneticisi ile örgüt içindeki operasyonel personel iletişim akışı sağlanmalıdır. İşletme personeli tehlikeleri tanımlamaları ve raporlamaları ile etkin bir şekilde teşvik edilirse, emniyet performansı daha etkin olacaktır. Bu nedenle, emniyet iletişimi aşağıdakileri hedefler:

a) tüm personelin SMS'den tamamen haberdar olmasını sağlamak;

b) emniyet için önemli bilgileri aktarmak;

c) bazı önlemlerin neden alındığını açıklamak;

d) emniyet prosedürlerin neden kullanılmaya başladıklarını veya değiştirildiklerini açıklamak ve

e) "bilinmesi iyi olacak" bilgileri aktarmak.

9.12.2 Örgüt içindeki iletişimin örnekleri şunlardır:

a) emniyet yönetimi sistemleri el kitabı (SMSM);

b) emniyet süreçleri ve prosedürleri;

c) emniyet haberleri, notları, bültenleri ve

d) web siteleri veya e-posta.

Şekil 9-2. Emniyet eğitimi

Bölüm 10

SMS'NİN UYGULANMASI İÇİN AŞAMALI YAKLAŞIM

10.1 HEDEF VE İÇERİKLER

Bu bölümün amacı SMS'nin aşamalar halinde uygulanması için bir öneri sunmaktır. Bu bölüm aşağıdaki konuları içerir:

a) SMS'nin uygulanması için niye aşamalı bir yaklaşım uygulanmalıdır;

b) Aşama I - SMS uygulamasının planlanması;

c) Aşama II – Reaktif emniyet yönetimi süreçleri;

d) Aşama III – Koruyucu ve öngörüye dayanan emniyet yönetimi süreçleri;

e) Aşama IV – İşletmede emniyet güvencesinin sağlanması.

10.2 SMS'NİN UYGULANMASI İÇİN NİYE AŞAMALI BİR YAKLAŞIM UYGULANMALIDIR?

10.2.1 Bir SMS'nin uygulanması doğrudan bir süreçtir. Yine de, sivil havacılık denetim kurumu tarafından yayınlanan kılavuz materyalin bulunup bulunmaması, hizmet sağlayıcının SMS bilgisi ve uygulama için gerekli kaynaklar gibi bir dizi etkene bağlı olarak, bu doğrudan süreç zorlu bir göreve dönüşebilir.

10.2.2 Proje yönetiminde, karmaşık projelerde en iyi ilerleme yönteminin işin genel karmaşıklığını, tüm işi daha küçük, yönetebilir alt bileşenler ayırarak ortadan kaldırmak olduğu önemli bir kuraldır. Bu şekilde, bunaltıcı ve bazen kafa karıştırıcı olan karmaşıklık ve bunun altında yatan iş yükü, sadece yönetilebilir bir iş yükü gerektiren daha basit ve saydam etkinlik gruplarına dönüştürülebilir. Benzer şekilde, SMS'nin "bir seferde" uygulanması için gereken kaynaklar örgüt içinde bulunmayabilir. Dolayısıyla, genel karmaşıklığın daha küçük etkinlik gruplarına bölünmesi, kısmi veya daha küçük kaynaklar bütün halinde etkinlik alt gruplarına ayrılmasını sağlar. Kaynakların bu şekilde kısmi olarak ayrılması her bir etkinlik gerekliliklerıyle ve örgütün kaynaklarıyla uyumlu olmalıdır. Bu nedenle, SMS'nin uygulanması için aşamalı bir yaklaşım uygulanmasını iki nedeni aşağıdaki gibidir:

a) bir SMS'nin uygulanmasında, kaynakların dağıtılması da dahil olmak üzere izlenebilecek yönetilebilir adımları sağlar ve

b) SMS'nin uygulanması ile ilgili iş yükünü etkin bir şekilde yönetir.

10.2.3 Önceki ikisinden tamamen farklı, ama eşit miktarda önemli olan üçüncü bir neden "kozmetik uyumdan" kaçınmaktır. Bir örgüt hedefini etkili bir SMS'nin gerçekçi bir şekilde uygulanması olarak belirlemelidir, sadece sembollerinin uygulanması olarak değil. Bu gerekliliklere boğulmuş ve SMS'yi yeterli olmayan bir süre içinde tümüyle uygulamak için gerekli kaynaklara sahip olmayan bir örgüt için, sadece sivil havacılık kurumunun taleplerine ve koşullarına uyacak evrakları hazırlama fikri çekici olabilir. Başka bir deyişle, makul olmayacak derecede zorlu uygulama gerekliliklerinin sonucunda "uygun kutucukları işaretleme" olarak adlandırılan bir durum gelişebilir.

Böyle bir durumda, ortaya çıkan SMS, kağıt üzerinde eksiksiz ve uyumlu olmasına karşın, boş bir kabuktan başka bir şey olmayacaktır. Küçük, kademeli ve en önemlisi ölçülebilir adımlar sağlanarak, kozmetik uyum ve "uygun kutucukları işaretleme" yaklaşımları desteklenmemiş olur. SMS'nin tamamen uygulanması kesinlikle daha uzun sürecektir, ama ortaya çıkan SMSN'nin sağlamlığı her bir uygulama aşaması tamamlandığında daha da güçlenecektir ve daha karmaşık emniyet yönetimi süreçleri içeren daha sonraki adımlara geçmeden önce daha basit emniyet yönetimi süreçleri başlatılmış olacaktır.

10.2.4 Özet olarak, bir SMS'nin aşamalı olarak uygulanması önerisi aşağıdakileri amaçlamaktadır:

a) bir SMS'nin uygulanmasında, kaynakların dağıtılması da dahil olmak üzere izlenebilecek yönetilebilir adımları sağlamak;

b) SMS'nin uygulanması ile ilgili iş yükünü etkin bir şekilde yönetmek ve

c) sadece boş bir kabuk (yani "uygun kutucukların işaretlenmesi") değil, sağlam bir SMS sağlar.

10.2.5 Bir SMS için dört uygulama aşaması önerilmektedir. Her bir aşama, Bölüm 8'de ele alınan ICAO SMS çerçevesinin bir bileşeni ile ilgilidir. Her bir aşamanın uygulanması, ilgili aşama sırasında ICAO SMS çerçevesinin her bir bileşenine ait belirli unsurların eklenmesini temel alır.

10.3 AŞAMA I - SMS UYGULAMASININ PLANLANMASI

10.3.1 SMS'nin uygulanmasının 1. aşamasının amacı, SMS gerekliliklerinin nasıl yerine getirileceği ve örgütün çalışma etkinliklerine nasıl entegre edileceği konusunda bir taslak sağlamak ve bunun yanında SMS'nin uygulanması için bir hesap verme sorumluluğu çerçevesi sağlamaktır.

10.3.2 Aşama I arasında, temel planlama yapılır ve sorumluluklar belirlenir. Aşama I'in merkezinde boşluk analizi vardır. Boşluk analizi ile, örgüt emniyet yönetimi süreçlerinin geçerli durumunu belirleyebilir ve daha sonraki emniyet yönetimi süreçlerinin geliştirilmesi için ayrıntılı planlamalara başlayabilir. Aşama I'in önemli bir çıktısı SMS uygulama planıdır.

10.3.3 Aşama I tamamlandığında, aşağıdaki etkinlikler ilgili gereklilikler ve kılavuz materyalde belirtildiği gibi, sivil havacılık denetim kurumunun beklentilerini karşılayacak şekilde sonlandırılmalıdır:

a) Sorumlu Müdürün ve yöneticilerin emniyetle ilgili hesap verme sorumluluklarının belirlenmesi. Bu etkinlik ICAO SMS çerçevesinin 1.1 ve 1.2 numaralı unsurlarını temel almaktadır ve Bölüm 8'de ele alınmıştır.

b) Örgüt içinde SMS'nin uygulanmasından sorumlu kişinin (veya planlama grubunun) belirlenmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 8'de ele alınmıştır.

c) Sistemin tanımlanması (hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütleri, uçak operatörleri, onaylı bakım örgütleri, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcıları ve sertifikalı havalimanları). Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 7'de ele alınmıştır. Sistem tanımı ile ilgili kılavuz bilgiler Bölüm 7 Ek 1'de verilmiştir.

d) Örgütün mevcut kaynaklarını bir SMS'nin kurulması için ulusal ve uluslararası gerekliliklerle karşılaştırarak bir boşluk analizi gerçekleştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 7'de ele alınmıştır. Bir hizmet sağlayıcı için bir SMS boşluk analizinin geliştirilmesi ile ilgili kılavuz bilgiler Bölüm 7 Ek 2'de verilmiştir.

e) Örgütün SMS'yi ulusal gereklilikler ve uluslararası SARP'ler, sistem tanımı ve boşluk analizi temelinde nasıl uygulayacağı açıklayan bir SMS uygulama planının geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 8'de ele alınmıştır.

f) Emniyet politikası ve hedefleri ile ilgili dokümantasyonun geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve bir emniyet politikası beyanı örneği de içeren Bölüm 8'de ele alınmıştır.

g) Emniyet iletişiminin geliştirilmesi ve iletişim araçlarının sağlanması. Bu etkinlik ICAO SMS çerçevesinin 4.2 numaralı unsurunu temel almaktadır ve Bölüm 9'de ele alınmıştır.

10.4 AŞAMA II – REAKTİF EMNİYET YÖNETİMİ SÜREÇLERİ

10.4.1 Aşama II'nin amacı, mevcut emniyet yönetimi süreçlerindeki potansiyel bozuklukları düzeltirken, aynı zamanda önemli emniyet yönetimi süreçlerinin uygulanmasıdır. Çoğu örgüt, farklı uygulama seviyelerinde ve farklı etkililik derecelerinde, temel emniyet yönetimi etkinliklerine sahiptir. Bu etkinlikler, incelemeler ve denetim raporlarını, kaza raporları ve olay incelemelerinden alınan bilgilerin analizini ve çalışan raporlarını içerebilir. Bu aşamanın amacı mevcut etkinliklerin güçlendirilmesi ve henüz mevcut olmayanların geliştirilmesidir. Ancak, ileriye dönük sistemlerin henüz geliştirilmesi ve uygulanması gerektiğinden, bu aşama reaktif olarak kabul edilir. Aşama I'in sonuna doğru, örgüt reaktif emniyet verileri toplama yöntemleri aracılığıyla elde edilen bilgiler temelinde koordineli emniyet analizleri yapmaya hazır olacaktır.

10.4.2 Aşama II tamamlandığında, aşağıdaki etkinlikler ilgili gereklilikler ve kılavuz materyalde belirtildiği gibi, sivil havacılık denetim kurumunun beklentilerini karşılayacak şekilde sonlandırılmalıdır:

a) SMS uygulama planının, reaktif süreçler temelinde emniyet riski yönetimini içeren yönlerinin uygulanması. Bu etkinlik ICAO SMS çerçevesinin 2.1 ve 2.2 numaralı unsurlarını temel almaktadır ve Bölüm 3 ve 8'de ele alınmıştır.

b) SMS uygulama planı bileşenleri ve reaktif süreçler temelinde emniyet riski yönetimi ile ilgili eğitimin verilmesi. Bu etkinlik ICAO SMS çerçevesinin 4.1 numaralı unsurunu temel almaktadır ve Bölüm 3, 8 ve 9'da ele alınmıştır.

c) SMS uygulama planı bileşenleri ve reaktif süreçler temelinde emniyet riski yönetimi ile ilgili dokümantasyonun geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 3, 8 ve 9'da ele alınmıştır.

d) Formel emniyet iletişimi araçlarının geliştirilmesi ve sürdürülmesi. Bu etkinlik ICAO SMS çerçevesinin 4.2 numaralı unsurunu temel almaktadır ve Bölüm 9'de ele alınmıştır.

10.5 AŞAMA III – PROAKTİF VE TAHMİNE DAYALI EMNİYET YÖNETİMİ SÜREÇLERİ

10.5.1 Aşama III'ün amacı ileriye dönük emniyet yönetimi sürecini yapılandırmaktır. Emniyet bilgileri yönetimi ve analitik süreçler düzeltilir. Aşama III'ün sonuna doğru, örgüt reaktif, proaktif ve tahmine dayalı emniyet verileri toplama yöntemleri aracılığıyla elde edilen bilgiler temelinde koordineli emniyet analizleri yapmaya hazır olacaktır.

10.5.2 Aşama III tamamlandığında, aşağıdaki etkinlikler ilgili gereklilikler ve kılavuz materyalde belirtildiği gibi, sivil havacılık denetim kurumunun beklentilerini karşılayacak şekilde sonlandırılmalıdır:

a) SMS uygulama planının, proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimini içeren yönlerinin uygulanması. Bu etkinlik ICAO SMS çerçevesinin 2.1 ve 2.2 numaralı unsurlarını temel almaktadır ve Bölüm 3 ve 8'de ele alınmıştır.

b) SMS uygulama planı bileşenleri ve proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimi ile ilgili eğitimin geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 4.1 numaralı unsurunu temel almaktadır ve Bölüm 3, 8 ve 9'da ele alınmıştır.

c) SMS uygulama planı bileşenleri ve proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimi ile ilgili dokümantasyonun geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 3, 8 ve 9'da ele alınmıştır.

d) Formel emniyet iletişimi araçlarının geliştirilmesi ve sürdürülmesi. Bu etkinlik ICAO SMS çerçevesinin 4.2 numaralı unsurunu temel almaktadır ve Bölüm 9'da ele alınmıştır.

10.6 AŞAMA IV – OPERASYONEL EMNİYETİN GÜVENCE ALTINA ALINMASI

10.6.1 Aşama IV SMS'nin son aşamasıdır. Bu aşamada işletmedeki emniyet güvencesi değişen operasyonel gereklilikleri altında emniyet riski kontrollerinin etkililiğini korumak için periyodik izleme, geri bildirim ve sürekli düzeltme eylemlerinin uygulanması aracılığıyla değerlendirilir. Aşama IV'ün sonunda, emniyet bilgileri yönetimi ve analitik süreçler emniyet operasyonel süreçlerin zaman içinde ve operasyonel ortamdaki değişim zamanları sırasında sürdürülmesini sağlar.

10.6.2 Aşama IV tamamlandığında, aşağıdaki etkinlikler ilgili gereklilikler ve kılavuz materyalde belirtildiği gibi, sivil havacılık denetim kurumunun beklentilerini karşılayacak şekilde sonlandırılmalıdır:

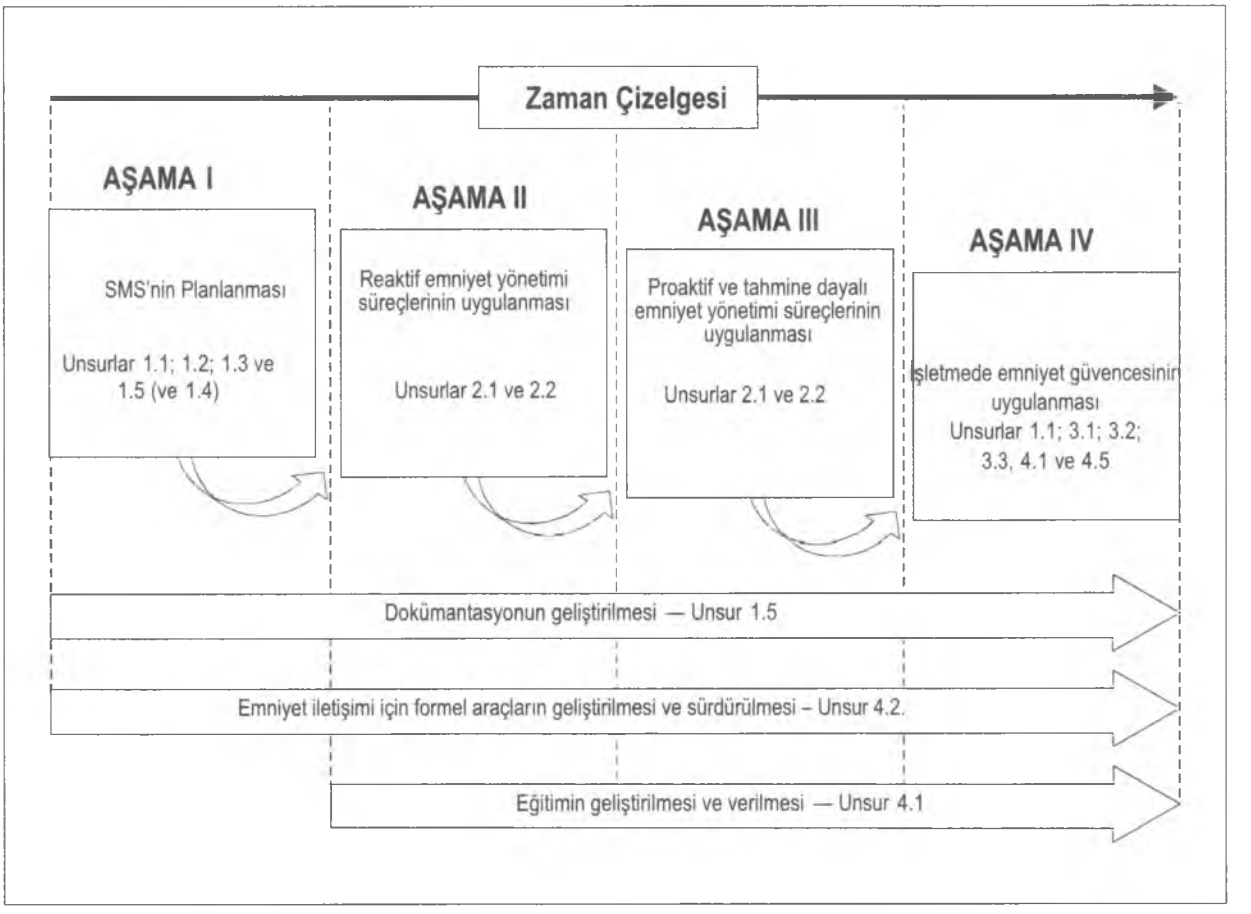
a) Emniyet performansı göstergelerinin, emniyet performansı hedeflerinin geliştirilmesi ve bunlar üzerinde uzlaşmaya varılması ve SMS'nin sürekli olarak iyileştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.1, 3.1, 3.2 ve 3.3 numaralı unsurlarını temel almaktadır ve Bölüm 6 ve 9'da ele alınmıştır.

b) İşletmede emniyet güvencesi ile ilgili eğitimin geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 4.1 numaralı unsurunu temel almaktadır ve Bölüm 9'de ele alınmıştır.

c) İşletmede emniyet güvencesi ile ilgili dokümantasyonun geliştirilmesi. Bu etkinlik ICAO SMS çerçevesinin 1.5 numaralı unsurunu temel almaktadır ve Bölüm 9'de ele alınmıştır.

d) Formel emniyet iletişimi araçlarının geliştirilmesi ve sürdürülmesi. Bu etkinlik ICAO SMS çerçevesinin 4.2 numaralı unsurunu temel almaktadır ve Bölüm 9'de ele alınmıştır.

10.6.3 SMS'nin uygulanmasının farklı aşamalarının ve ilgili unsurların bir özeti Şekil 10-1'de gösterilmiştir.



Şekil 10-1. SMS'nin uygulanmasının farklı aşamalarının özeti

Bölüm 10 Ek 1

BİR DEVLETİN SMS İLE İLGİLİ YÖNETMELİKLERİNİN GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

1. YASAL TEMEL

Bu düzenleme [Devletin geçerli sivil havacılık düzenleme(ler)i, hava trafiği emir(ler)i veya düzenleyici standart(lar)ındaki] yasa koyucu otorite altında yayınlanmıştır.

2. KAPSAM VE UYGULANABİLİRLİK

2.1 Kapsam

2.1.1 Bu düzenleme, bir hizmet sağlayıcının Annex 1 — *Personele Lisans Verilmesi*, Annex 6 — *Uçakların İşletilmesi*, Kısım I – *Uluslararası Ticari Hava Taşımacılığı – Uçaklar* ve Kısım II – *Uluslararası İşletmeler – Helikopterler*, Annex 8 — *Uçakların Uçuşa Elverişliliği*, Annex 11 — *Hava Trafiği Hizmetleri*, Annex 14 — *Havalimanları,* Cilt I – *Havalimanı Tasarımı ve İşletimi* bölümlerine uygun şekilde işletilen emniyet yönetimi sistemi (SMS) için gereklilikleri belirtir.

2.1.2 Bu düzenleme bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havalimanlarını kapsar.

2.1.3 Bu düzenleme, iş emniyeti, çevrenin korunması veya müşteri hizmetleri veya ürün kalitesinden çok, emniyetle ilgili süreçleri, prosedürleri ve etkinliklere yöneliktir.

2.1.4 Hizmet sağlayıcı, diğer örgütlerden sözleşme veya taşeronluk sözleşmesi ile alınan veya satın alınan hizmetlerin veya ürünlerin emniyetinden sorumludur.

2.1.5 Bu düzenleme kabul edilebilir en düşük gereklilikleri ortaya koymaktadır; hizmet sağlayıcı daha katı f-gereklilikler koyabilir.

2.2 Uygulanabilirlik ve kabul

2.2.1 *[Tarih(ler)inden itibaren] geçerli olmak üzere,* bir hizmet sağlayıcı, aşağıdaki minimum koşulları sağlayan, [Devlet] tarafından kabul edilebilir bir emniyet yönetimi sistemine (SMS) sahip olmalıdır:

2.2.1.1 emniyet tehlikelerinin tanımlanması;

2.2.1.2 üzerinde uzlaşılan emniyet performansının sürdürülmesi için gerekli olan düzeltme eyleminin uygulanmasının sağlanması;

2.2.1.3 emniyet performansının sürekli olarak izlenmesinin ve düzenli olarak değerlendirilmesinin sağlanması ve

2.2.1.4 emniyet yönetimi sisteminin genel performansının sürekli olarak iyileştirilmesinin hedeflenmesi.

2.2.2 Devlet tarafından kabul edilebilir olması için, bir hizmet sağlayıcının SMS'si bu düzenlemede ortaya konan koşulları yerine getirmelidir.

Bilgi notu— SMS ile ilgili bir düzenleme, SMS'nin kabul süreci ile ilgili bilgileri içermelidir. Kabul süreci, uygun olduğunda, SMS'nin kabulü için başvuru, başvurunun teslim edilme prosedürleri, kabulün süresi, kabulün yenilenmesi ve kabulün askıya alınması ve/veya iptalini içermelidir.

3. REFERANSLAR

3.1 Bu düzenleme, Annex 1 — *Personele Lisans Verilmesi*, Annex 6 — *Uçakların İşletilmesi*, Kısım I – *Uluslararası Ticari Hava Taşımacılığı – Uçaklar* ve Kısım II – *Uluslararası İşletmeler – Helikopterler*, Annex 8 — *Uçakların Uçuşa Elverişliliği*, Annex 11 — *Hava Trafiği Hizmetleri*, Annex 14 — *Havalimanları*, Cilt I – *Havalimanı Tasarımı ve İşletimi* ve ICAO *Emniyet Yönetimi El Kitabı (SMM)* (Doc 9859) ile uyumludur.

3.2 Bu düzenleme *[Devletin yürürlükteki düzenleyici ve/veya kılavuz materyali] ile uyumludur.*

4. TANIMLAR

Not— Bu liste sadece kılavuzluk sağlamak için verilmiştir.

- Kaza
- Kabul edilebilir emniyet seviyesi (ALoS)
- Sorumlu Müdür
- Sonuç
- Sürekli izleme
- Boşluk analizi
- Tehlike
- Olay
- Dahili emniyet incelemeleri
- Azaltma
- Ortaya çıkan olay
- Gözetim
- Tahmine dayalı
- Proaktif
- Olasılık
- Prosedür
- Süreç
- Reaktif
- Risk
- Emniyet
- Emniyet değerlendirmesi
- Emniyet güvencesi

- Emniyet denetimi
- Emniyet yöneticisi
- Emniyet performansı
- Emniyet performansı göstergesi
- Emniyet performansı hedefi
- Emniyet politikası
- Emniyet gerekliliği
- Emniyet riski
- Emniyet araştırması
- Emniyet yönetimi sistemi (SMS)
- Devlet emniyet programı (SSP)
- Ciddiyet
- Sistem tanımı.

5. GENEL

Bir hizmet sağlayıcı, sahip olduğu operasyon onayı altında yapılması yetkisine sahip olduğu işletmelerin ve işletmelerle ilgili tehlikelerin ve emniyet risklerinin büyüklüğüne, doğasına ve karmaşıklığına uygun bir emniyet yönetimi sistemi (SMS) geliştirmeli, oluşturmalı, sürdürmeli ve bu sisteme sadık kalmalıdır.

6. EMNİYET POLİTİKASI VE HEDEFLERİ

6.1 Genel gereklilikler

6.1.1 Bir hizmet sağlayıcı örgütün emniyet politikasını tanımlamalıdır.

6.1.2 Emniyet politikası, örgütün Sorumlu Müdürü tarafından imzalanmalıdır.

6.1.3 Emniyet politikası, SMS'nin emniyet performansı bakımından yönetim ve çalışanların sorumluluklarını içermelidir.

6.1.4 Emniyet politikası, uygulanması için gereken kaynakların sağlanması hakkında açık bir ifade içermelidir.

6.1.5 Emniyet politikası örgüt içinde açıkça onaylanmış şekilde iletilmelidir.

6.1.6 Emniyet politikası, *diğerlerinin yanında*, aşağıdakileri de içermelidir:

6.1.6.1 emniyet seviyesinde sürekli bir iyileştirme taahhüdü;

6.1.6.2 tehlike raporlama prosedürleri ve

6.1.6.3 çalışanlar tarafından tehlikenin raporlanmasından sonra disiplin cezasının uygulanmayacağı koşullar.

6.1.7 Emniyet politikası geçerli yasal gereklilikler ve uluslararası standartlara, sektördeki en iyi uygulamalara uygun olmalıdır ve örgütün emniyetle konusundaki taahhüdünü yansıtmalıdır.

6.1.8 Emniyet politikası örgütle uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmelidir.

6.1.9 Hizmet sağlayıcı SMS için emniyet hedeflerini oluşturmalıdır.

6.1.10 Emniyet hedefleri, hizmet sağlayıcının SMS'sindeki emniyet performansı göstergeleri, emniyet performansı hedefleri ve eylem planları ile bağlantılı olmalıdır.

6.2 SMS örgüt düzenlemeleri ve emniyetle ilgili sorumluluklar ve hesap verme sorumlulukları

6.2.1 Bir hizmet sağlayıcı, bu düzenlemedeki gerekliliklerin yerine getirilmesinde hizmet sağlayıcı adına sorumlu ve hesap vermekten sorumlu olan bir Sorumlu Müdür atamalı ve [Devlete] bu kişinin ismini bildirmelidir.

6.2.2 Sorumlu Müdür, diğer işlevlerinden bağımsız olarak, [örgüt] adına, SMS'nin uygulanması ve sürdürülmesi için nihai sorumluluğu ve hesap verme sorumluluğunu alacak, tanınabilir tek bir kişi olmalıdır.

6.2.3 Sorumlu Müdür:

6.2.3.1 İşletme sertifikası altında yürütülmesi onaylanan işletmeler için gereken insan kaynaklarının tam kontrolüne sahip olmalıdır;

6.2.3.2 İşletme sertifikası altında yürütülmesi onaylanan işletmeler için gereken mali kaynakların tam kontrolüne sahip olmalıdır;

6.2.3.3 İşletme sertifikası altında yürütülmesi onaylanan işletmeler üzerinde nihai yetkiye sahip olmalıdır.

6.2.3.4 örgütün işlerinin yürütülmesinden doğrudan sorumlu olmalıdır ve

6.2.3.5 tüm emniyet konularında nihai sorumluluk sahibi olmalıdır.

6.2.4 Bir hizmet sağlayıcı, örgütün SMS'sinin uygulanması, SMS'ye bağlılık ve SMS'nin sürdürülmesi için örgüt içinde gerekli düzenlemeleri yapmalıdır.

6.2.5 Bir hizmet sağlayıcı, diğer sorumluluklarından bağımsız olarak, çalışanların yanında yönetimin tüm üyelerinin emniyetle ilgili sorumluluklarını, hesap verme sorumluluklarını ve yetkilerini belirlemelidir.

6.2.6 Emniyetle ilgili sorumluluklar, hesap verme sorumlulukları ve yetkiler tanımlanmış, belgelenmiş ve örgüt içinde iletilmiş olmalıdır.

6.2.7 Bir hizmet sağlayıcı, etkili bir SMS'nin geliştirilmesi ve sürdürülmesinden sorumlu kişi ve bu işin odak noktası olarak yönetimden bir kişiyi emniyet yöneticisi olarak belirlemelidir.

6.2.8 Emniyet yöneticisi, *diğerlerinin yanında*:

6.2.8.1 SMS için gereken süreçlerin geliştirilmesini, uygulanmasını, sürdürülmesini ve bu süreçlere bağlı kalınmasını sağlamalıdır;

6.2.8.2 SMS'nin performansı ve iyileştirme gerekip gerekmediği konusunda Sorumlu Müdüre rapor vermelidir ve

6.2.8.3 örgüt içinde emniyetin teşvik edilmesini sağlamalıdır.

6.3 Acil müdahale planlamasının koordinasyonu

6.3.1 Bir hizmet sağlayıcı acil müdahale planının, hizmetlerinin verilmesi sırasında etkileşim kurması gereken diğer örgütlerin acil müdahale planları ile uygun bir şekilde koordine edilmesini sağlamalıdır.

6.3.2 Acil müdahale planının koordinasyonu, normal işletmelerden acil duruma düzenli ve etkin bir şekilde geçilmesini ve normal işletmelere dönülmesini sağlamalıdır.

6.3.3 Acil müdahale planının koordinasyonu, *diğerlerinin yanında*, aşağıdakileri içermelidir:

6.3.3.1 acil durum yetkisinin dağıtılması;

6.3.3.2 koordine edilen etkinlikler sırasında acil durum sorumluluklarının atanması;

6.3.3.3 acil durumla başa çıkma çabalarının koordinasyonu ve

6.3.3.4 diğer örgütlerin acil müdahale planlarına uyum.

6.4 Dokümantasyon

6.4.1 Bir hizmet sağlayıcı aşağıdakilerin tanımlanması için SMS dokümantasyonunu geliştirmeli ve sürdürmelidir:

6.4.1.1 emniyet politikası ve hedefleri;

6.4.1.2 SMS gereklilikleri;

6.4.1.3 SMS süreçleri ve prosedürleri;

6.4.1.4 süreçler ve prosedürlerle ilgili sorumluluklar, hesap verme sorumlulukları ve yetkiler ve

6.4.1.5 SMS çıktıları.

6.4.2 Bir hizmet sağlayıcı, SMS dokümantasyonunun bir parçası olarak, bir sistem tanımını tamamlamalıdır.

6.4.3 Sistem tanımı aşağıdakileri içermelidir:

6.4.3.1 sistemin hava taşımacılığı sistemindeki diğer sistemlerle etkileşimleri;

6.4.3.2 sistem işlevleri;

6.4.3.3 sistemin çalışması için gereken insan performansı ile ilgili konular;

6.4.3.4 sistemin donanım bileşenleri;

6.4.3.5 sistemin yazılım bileşenleri;

6.4.3.6 sistemin çalıştırılması ve kullanımı için kılavuzluk sağlayan ilgili prosedürler;

6.4.3.7 operasyonel ortam ve

6.4.3.8 sözleşme yapılan, taşerona verilen ve satın alınan ürün ve hizmetler.

6.4.4 Bir hizmet sağlayıcı, SMS dokümantasyonunun bir parçası olarak, aşağıdakileri sağlamak üzere bir boşluk analizini tamamlamalıdır.

6.4.4.1 örgüt içinde mevcut olarak emniyet düzenlemelerinin ve yapılarının belirlenmesi ve

6.4.4.2 örgütün SMS'sinin uygulanması ve sürdürülmesi için gereken ek emniyet düzenlemelerinin belirlenmesi.

6.4.5 Bir hizmet sağlayıcı, SMS dokümantasyonunun bir parçası olarak, bir SMS uygulama planı geliştirmeli, bu plana uymalı ve planı sürdürmelidir.

6.4.6 SMS uygulama planı, örgütün emniyet hedeflerinin yerine getirilmesini sağlayacak şekilde emniyetin yönetilmesi için örgütün geliştirmesi gereken yaklaşımın tanımı olmalıdır.

6.4.7 SMS uygulama planı, hizmet sağlayıcının SMS'si ve hizmetlerinin verilmesi sırasında hizmet sağlayıcının etkileşim kurması gereken diğer örgütlerin SMS'leri arasındaki koordinasyonu açıkça ele alıyor mu?

6.4.8 SMS uygulama planı aşağıdakileri içermelidir:

6.4.8.1 emniyet politikası ve hedefleri;

6.4.8.2 sistem tanımı;

6.4.8.3 boşluk analizi;

6.4.8.4 SMS bileşenleri;

6.4.8.5 Emniyetle ilgili roller ve sorumluluklar;

6.4.8.6 Tehlike raporlama politikası;

6.4.8.7 çalışanların katılımını sağlayan araçlar;

6.4.8.8 emniyet performansı ölçümü;

6.4.8.9 emniyet eğitimi;

6.4.8.10 emniyet iletişimi ve

6.4.8.11 emniyet performansının yönetim tarafından gözden geçirilmesi.

6.4.9 SMS uygulama planı örgütün üst yönetimi tarafından onaylanmalıdır.

6.4.10 Bir hizmet sağlayıcı, SMS dokümantasyonunun bir parçası olarak, örgütün emniyetin yönetilmesine yaklaşımını örgüt içinde iletmek için bir emniyet yönetimi sistemleri el kitabı (SMSM) geliştirmeli ve sürdürmelidir.

6.4.11 SMSM, aşağıdakiler dahil olmak üzere SMS'nin tüm yönlerini ve içeriğini belgelemelidir:

6.4.11.1 emniyet yönetimi sisteminin kapsamı;

6.4.11.2 emniyet politikası ve hedefleri;

6.4.11.3 emniyetle ilgili hesap verme sorumlulukları;

6.4.11.4 kritik emniyet personeli;

6.4.11.5 dokümantasyon kontrol prosedürleri;

6.4.11.6 acil müdahale planlamasının koordinasyonu;

6.4.11.7 tehlikenin tanımlanması ve emniyet riski yönetimi şemaları;

6.4.11.8 emniyet performansının izlenmesi;

6.4.11.9 emniyet denetimi;

6.4.11.10 değişimin yönetilmesi prosedürleri;

6.4.11.11 emniyetin teşvik edilmesi ve

6.4.11.12 sözleşme ile alınan etkinliklerin kontrolü.

Bilgi notu —SMS dokümantasyonunun geliştirilmesi ve bakımı için genel kılavuz bilgiler ICAO Annex 6, Kısım I'e Annex H ve ICAO Annex 6, Kısım III'e Annex, Operatör Uçuş Emniyeti Belgeleri Sistemi'nde bulunabilir.

7. EMNİYET RİSKİ YÖNETİMİ

7.1 Genel

7.1.1 Bir hizmet sağlayıcı işletmelerdeki tehlikelerin tanımlanmasını sağlayan formel bir süreç geliştirmeli ve sürdürmelidir.

7.1.2 Bir hizmet sağlayıcı tehlikelerin tanımlanması ve emniyet risklerinin analizini, değerlendirilmesini ve azaltılmasını sağlayan emniyet verileri toplama ve işleme sistemlerini (SDCPS) geliştirmeli ve sürdürmelidir.

7.1.3 Bir hizmet sağlayıcının SDCPS'sinde emniyet verilerinin toplanması için reaktif, proaktif ve tahmine dayalı yöntemler bulunmalıdır.

7.2 Tehlikenin tanımlanması

7.2.1 Bir hizmet sağlayıcı işletmelerde tehlikelerle ilgili olarak, emniyet verileri toplamanın reaktif, proaktif ve tahmine dayalı yöntemlerini bir araya getiren geri bildirimlerin etkili bir şekilde toplanması, kaydedilmesi, oluşturulması ve bu geri bildirimlere göre davranmak için formel araçlar geliştirmeli ve sürdürmelidir. Emniyet verilerinin toplanması için formel araçlar zorunlu, gönüllü ve gizli raporlama sistemlerini içermelidir.

7.2.2 Tehlikenin tanımlanması süreci aşağıdaki adımları içermelidir:

7.2.2.1 tehlikelerin, olayların veya emniyet sorunlarının raporlanması;

7.2.2.2 emniyet verilerin toplanması ve saklanması;

7.2.2.3 emniyet verilerinin analizi ve

7.2.2.4 emniyet verilerinden elde edilen emniyet bilgilerinin dağıtımı.

7.3 Risk değerlendirmesi ve riskin azaltılması

7.3.1 Bir hizmet sağlayıcı, hizmetlerinin sunulması sırasındaki tehlikelerin sonuçlarına ait emniyet risklerinin analizini, değerlendirilmesini ve kontrolünü sağlayan formel bir süreç geliştirmeli ve sürdürmelidir.

7.3.2 Bu düzenlemenin 7.2 numaralı bölümünde açıklanan tehlikenin tanımlanması süreçleri aracılığıyla tanımlanan her bir tehlikenin sonuçlarına ait emniyet riskleri, olasılıkları ve ortaya çıkmalarının ciddiyeti bakımından analiz edilmeli ve tahammül edilebilirlikleri değerlendirilmelidir.

7.3.3 Örgüt emniyet riskinin tahammül edilebilirliği ile ilgili olarak karar verme yetkisine sahip yönetim seviyelerinin bir tanımını yapmalıdır.

7.3.4 Örgüt, tahammül edilebilir olarak değerlendirilen her bir emniyet riski için emniyet kontrolleri tanımlamalıdır.

8. EMNİYET GÜVENCESİ

8.1 Genel

8.1.1 Bir hizmet sağlayıcı, paragraf 7'deji tehlikenin tanımlanması ve emniyet riski yönetimi etkinliklerinin sonucunda geliştirilen emniyet riski kontrollerinin amaçlanan hedeflerine ulaşmasını sağlamak için emniyet güvencesi süreçleri geliştirmeli ve sürdürmelidir.

8.1.2 Emniyet güvencesi süreçleri, etkinlikler ve/veya işletmelerin örgüt içinden veya dışarıdan temin edilmelerinden bağımsız olarak bir SMS için geçerli olmalıdır.

8.2 Emniyet performansının izlenmesi ve ölçülmesi

8.2.1 Bir hizmet sağlayıcı, SMS emniyet güvencesi etkinliklerinin bir parçası olarak, SMS'nin emniyet performansı göstergelerine ve emniyet performansı hedeflerine göre örgütün emniyet performansını ve emniyet riski kontrollerinin etkili olduğunu doğrulamak için gerekli araçları geliştirmeli ve sürdürmelidir.

8.2.2 Emniyet performansını izleme ve ölçme araçları aşağıdakileri içermelidir:

8.2.2.1 tehlike raporlama sistemleri;

8.2.2.2 emniyet denetimleri;

8.2.2.3 emniyet araştırmaları;

8.2.2.4 emniyetle ilgili gözden geçirmeler;

8.2.2.5 emniyet araştırmaları ve

8.2.2.6 dahili emniyet incelemeleri.

8.2.3 Tehlike raporlama prosedürleri, disiplin cezalarının/idari cezaların geçerli olmayacağı koşullar dahil olmak üzere, etkili bir raporlama sağlamak için gerekli koşulları belirlemelidir.

8.3 Değişimin yönetilmesi

8.3.1 Bir hizmet sağlayıcı, SMS emniyet güvencesi etkinliklerinin bir parçası olarak, değişimin yönetilmesi için formel bir süreç geliştirmeli ve sürdürmelidir.

8.3.2 Formel değişimin yönetilmesi süreci:

8.3.2.1 örgüt içindeki yerleşik süreçleri ve hizmetleri etkileyebilecek değişiklikleri belirlemelidir;

8.3.2.2 değişikliklerin uygulanmasından önce emniyet performansının sağlanması için gereken düzenlemeleri yapmalıdır ve

8.3.2.3 operasyonel ortamdaki değişiklikler nedeniyle artık gerek duyulmayan emniyet riski kontrollerini ortadan kaldırmalı veya değiştirmelidir.

8.4 Emniyet sisteminin sürekli olarak iyileştirilmesi

8.4.1 Bir hizmet sağlayıcı, SMS emniyet güvencesi etkinliklerinin bir parçası olarak, SMS'nin standart altı performans göstermesinin nedenlerini, SMS'nin işletmelerde standart altı performans göstermesinin olası sonuçlarını belirlemesini ve SMS'nin sürekli olarak iyileştirilmesini sağlamak için standart altı performans içeren durumları düzeltmesini sağlayan formel süreçler geliştirmiş ve sürdürmekte olmalıdır.

8.4.2 Hizmet sağlayıcının SMS'sinin sürekli olarak iyileştirilmesi aşağıdakileri içermelidir:

8.4.2.1 emniyet risklerinin kontrolü için stratejilerin etkili olup olmadıklarının doğrulanması için, tesislerin, donanımın, dokümantasyonun ve prosedürlerin proaktif ve reaktif değerlendirmeleri ve

8.4.2.2 emniyet sorumluluklarını yerine getirdiklerinin doğrulanması için bireylerin performansının proaktif olarak değerlendirilmesi.

9. EMNİYETİN TEŞVİK EDİLMESİ

9.1 Genel

Hizmet sağlayıcılar, örgütün emniyet hedeflerine ulaşılabilecek bir ortam yaratmak için formel emniyet eğitimi ve emniyet iletişimi etkinlikleri geliştirmeli ve sürdürmelidir.

9.2 Emniyet eğitimi

9.2.1 Bir hizmet sağlayıcı, emniyetin teşvik edilmesi etkinliklerinin bir parçası olarak, personelin SMS görevlerinin yerine getirmek için eğitimli ve yeterli olmasını sağlayan bir emniyet eğitimi programı geliştirmeli ve sürdürmelidir.

9.2.2 Emniyet eğitiminin kapsamı her bir bireyin SMS'ye katılma şekline uygun olmalıdır.

9.2.3 Sorumlu Müdür aşağıdaki konularda emniyet farkındalığı eğitimi almalıdır:

9.2.3.1 emniyet politikası ve hedefleri;

9.2.3.2 SMS ile ilgili roller ve sorumluluklar;

9.2.3.3 SMS standartları ve

9.2.3.4 emniyet güvencesi.

9.3 EMNİYET İLETİŞİMİ

9.3.1 Bir hizmet sağlayıcı, emniyetin teşvik edilmesi etkinliklerinin bir parçası olarak, aşağıdaki amaçlarla emniyet iletişimi için formel bir süreç geliştirmeli ve sürdürmelidir:

9.3.1.1 tüm personelin SMS'den tamamen haberdar olmasını sağlamak;

9.3.1.2 emniyet için önemli bilgileri aktarmak;

9.3.1.3 bazı emniyet önlemlerinin neden alındığını açıklamak;

9.3.1.4 emniyet prosedürlerin neden kullanılmaya başladıklarını veya değiştirildiklerini açıklamak ve

9.3.1.5 genel emniyet bilgilerini aktarmak.

9.3.2 Emniyet iletişiminin formel araçları, *diğerlerinin yanında*, aşağıdakileri de içerir:

9.3.2.1 emniyet politikaları ve prosedürler;

9.3.2.2 haberler;

9.3.2.3 bültenler ve

9.3.2.4 web siteleri.

10. KALİTE POLİTİKASI

Bir hizmet sağlayıcı, örgütün kalite politikasının SMS'nin etkinlikleri ile uyumlu olmasını ve bu etkinliklerin yerine getirilmesini sağlamalıdır.

11. SMS'NİN UYGULANMASI

11.1 Bu düzenleme, bir hizmet sağlayıcının SMS'sinin, 11.2 ile 11.5 arasında açıklanan şekilde, dört aşamayı kapsayan aşamalı bir uygulama ile uygulanmasını önermektedir, ama zorunlu kılmamaktadır.

11.2 ***Aşama I*** - Planlama SMS gerekliliklerinin nasıl yerine getirileceği ve örgütün çalışma etkinliklerine nasıl entegre edileceği konusunda bir taslak sağlamalı ve bunun yanında SMS'nin uygulanması için bir hesap verme sorumluluğu çerçevesi sağlamalıdır.

11.2.1 Sorumlu Müdürün ve yöneticilerin emniyetle ilgili hesap verme sorumluluklarının belirlenmesi;

11.2.2 Örgüt içinde SMS'nin uygulanmasından sorumlu kişinin (veya planlama grubunun) belirlenmesi;

11.2.3 Sistemin tanımlanması (ATO'lar, uçak operatörleri, AMO'lar, uçak tip tasarımı ve/veya üretiminden sorumlu örgütler, ATC hizmeti sağlayıcıları ve sertifikalı havalimanları);

11.2.4 Örgütün mevcut kaynaklarını bir SMS'nin kurulması için ulusal ve uluslararası gerekliliklerle karşılaştırarak bir boşluk analizi gerçekleştirilmesi,

11.2.5 Örgütün SMS'yi ulusal gereklilikler ve uluslararası SARP'ler, sistem tanımı ve boşluk analizi temelinde nasıl uygulayacağı açıklayan bir SMS uygulama planının geliştirilmesi;

11.2.6 Emniyet politikası ve hedefleri ile ilgili dokümantasyonun geliştirilmesi ve

11.2.7 Emniyet iletişiminin geliştirilmesi ve iletişim araçlarının sağlanması.

11.3 ***Aşama II*** – Reaktif süreçler, SMS uygulama planının, reaktif süreçler temelinde emniyet riski yönetimini içeren unsurlarını uygulamaya koymalıdır:

11.3.1 reaktif süreçler kullanarak tehlikenin tanımlanması ve emniyet riski yönetimi;

11.3.2 aşağıdakilerle ilgili eğitim:

11.3.2.1 SMS uygulama planı bileşenleri ve

11.3.2.2 emniyet riski yönetimi (reaktif süreçler).

11.3.4 aşağıdakilerle ilgili dokümantasyon:

11.3.4.1 SMS uygulama planı bileşenleri ve

11.3.4.2 emniyet riski yönetimi (reaktif süreçler).

11.4 ***Aşama III*** – Proaktif ve tahmine dayalı süreçler, SMS uygulama planının, proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimini içeren unsurlarını uygulamaya koymalıdır:

11.4.1 proaktif ve tahmine dayalı süreçler kullanarak tehlikenin tanımlanması ve emniyet riski yönetimi;

11.4.2 aşağıdakilerle ilgili eğitim:

11.4.2.1 SMS uygulama planı bileşenleri ve

11.4.2.2 emniyet riski yönetimi (proaktif ve tahmine dayalı süreçler).

11.4.3 aşağıdakilerle ilgili dokümantasyon:

11.4.3.1 SMS uygulama planı bileşenleri ve

11.4.3.2 emniyet riski yönetimi (proaktif ve tahmine dayalı süreçler).

11.5 ***Aşama IV*** – Operasyonel emniyetin güvence altına alınması, işletmede emniyet güvencesi uygulamaya koymalıdır:

11.5.1 Emniyet performansı göstergelerinin ve emniyet performansı hedeflerinin geliştirilmesi ve bunlar üzerinde uzlaşma;

11.5.2 SMS'nin sürekli olarak iyileştirilmesi;

11.5.3 işletmede emniyet güvencesi ile ilgili eğitim;

11.5.4 işletmede emniyet güvencesi ile ilgili dokümantasyon ve

11.5.5 formel emniyet iletişimi araçlarının geliştirilmesi ve sürdürülmesi.

— — — — — — — — — —

Bölüm 10 Ek 2

SERVİS SAĞLAYICILAR İÇİN BİR SMS UYGULAMA PLANININ GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

ARKA PLAN

1. Bu ek, örgütlerinin emniyetin yönetilmesine yaklaşımını tanımlayan bir SMS uygulama planının geliştirilmesinde hizmet sağlayıcılara yardımcı olacak kılavuz bilgiler sağlar. SMS uygulama planı örgütün üst yönetimi tarafından onaylanmalıdır ve ulusal düzenlemeler, uluslararası Standartlar ve Tavsiye Edilen Uygulamalar (SARP'ler), sistem tanımı ve boşluk analizi temelinde geliştirilmelidir.

2. Bir SMS uygulama planının geliştirilmesi aynı zamanda aşağıdakileri sağlayacaktır:

a) örgütün emniyet hedeflerine uyacak bir SMS'nin uygulanması için gerçekçi bir strateji hazırlamada hizmet sağlayıcı sağlayıcılara yardımcı olmak;

b) bir SMS'nin uygulanmasında izlenebilecek yönetilebilir adımları sağlamak ve

c) SMS'nin uygulanması için bir hesap verme sorumluluğu çerçevesi sağlamak.

3. SMS'nin uygulanması ile ilgili iş yükünün etkili bir şekilde yönetilmesi için aşamalı bir yaklaşım önerilmektedir. Her bir aşama ICAO SMS çerçevesinin belirli unsurlarının kullanılmaya başlamasını temel alır.

4. Her bir aşamanın uygulanmasının zamanı örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına uygun olmalıdır.

Not 1 – Bu ekte SMS uygulama planının geliştirilmesi için bir Gantt çizelgesi yer almaktadır. Bu kılavuz bilgiler sadece referans amacıyla verilmiştir ve hizmet sağlayıcıların gerekliliklerine uyacak şekilde ayarlanabilir. Model Gantt çizelgesi için bir proje yönetimi dosyası www.icao.int/fsix veya www.icao.int/anb/safetymanagement. adresinden indirilebilir.

Not 2 - Bu ek bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havalimanlarını kapsar.

SMS Uygulama Planı

1. AŞAMA I - SMS UYGULAMASININ PLANLANMASI

1.1 ***Sorumlu Müdür***

- Sorumlu Müdürün ve SMS uygulama planını geliştirecek kişi veya planlama grubunun belirlenmesi (Bölüm 8'de ele alınmıştır).

1.2 ***Sistem tanımı ve boşluk analizi*** (Bölüm 7'de ele alınmıştır).

Sistem tanımı

- Bir örgütteki bir SMS'nin geliştirilmesinin ilk ön koşulu olan sistem tanımının yapılması. Sistem içindeki arayüzleri ve hava taşımacılığı sistemindeki diğer sistemlerle arayüzleri içermelidir. Sistem tanımı ile ilgili kılavuz bilgiler Bölüm 7 Ek 1'de verilmiştir.

Boşluk analizi

- Örgüt içindeki mevcut emniyet düzenlemelerinin ve eksik olanların belirlenmesi için ICAO SMS çerçevesinin dört bileşeni ve on iki unsuru karşısında bir boşluk analizi gerçekleştirilmesi. Bir SMS Boşluk analizinin geliştirilmesi ile ilgili kılavuz bilgiler Bölüm 7 Ek 2'de bulunmaktadır.

- Boşluk analizinin sonuçları temelinde, kişi veya planlama grubu aşağıdakileri dikkate alarak SMS uygulama planını geliştirebilir:

  — SMS'nin uygulanmasını engelleyebilecek potansiyel boşlukların belirlenmesi ve
  — bu boşlukların dikkate alınması için stratejilerin geliştirilmesi.

1.3 **Emniyet politikası ve hedefler** (Bölüm 8'de ele alınmıştır)

Emniyet politikası

- Bir emniyet politikası oluşturmak.

- Sorumlu Müdürün emniyet politikasını imzalamasını sağlamak.

- Emniyet politikasını örgüt içinde açıkça onaylanmış şekilde iletmek.

- Emniyet politikasının örgütle uyumlu ve ilgili kalması için bir gözden geçirme programı oluşturmak.

  Emniyet politikası beyanının bir örneği Bölüm 8'de gösterilmiştir.

Emniyet hedefleri

- Aşağıdakiler bakımından emniyet performansı standartlarını geliştirerek, SMS için emniyet hedeflerini oluşturmak:

— emniyet performansı göstergeleri;
— emniyet performansı hedefleri ve
— eylem planları.

- Alt yükleniciler için SMS gerekliliklerini oluşturmak:

— SMS gerekliliklerinin sözleşme yapma sürecinde yazılması için bir prosedür oluşturmak ve
— ihale dokümantasyonunda SMS gerekliliklerini oluşturmak.

1.4 **Emniyetle ilgili hesap verme sorumlulukları ve emniyetin sağlanmasında önemli rol oynayan personelin atanması**

(bu el kitabının 8. Bölümünde ele alınmıştır)

SMS örgüt yapısı

- Emniyet hizmetleri ofisini oluşturmak.
- Etkili bir SMS geliştirilmesi ve sürdürülmesinden sorumlu kişi ve bu işin odak noktası olarak bir emniyet yöneticisi atamak.
- Emniyet hizmetleri ofisi ve Sorumlu Müdür, Emniyet Eylem Grubu (SAG) ve Emniyet Denetim Grubu (SRB) arasında iletişim sıralarını değerlendirmek ve oluşturmak.
- İşlevsel iletişim sıralarının örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına uygun olmasını sağlamak
- Emniyet Denetim Kurulunun (SRB) başkanlığını Sorumlu Müdürün yapmasını sağlamak.
- SRB'ye, işlevsel alanlardan sorumlu bölüm yöneticileri de dahil olmak üzere, üst yöneticiler atamak.
- SRB'ye uygun stratejik işlevler atamak.
- Emniyet Eylem Grubunu (SAG) oluşturmak.
- Bölüm yöneticilerini ve ön saflardaki personelin temsilcilerini SAG'a atamak.
- SRB'ye uygun taktiksel işlevler atamak.
- Emniyetle ilgili sorumlulukları, hesap verme sorumluluklarını ve yetkileri belgelemek ve örgüt içinde iletmek, buna emniyet riskinin tahammül edilebilirliğiyle ilgili olarak karar verme yetkisine sahip yönetim seviyelerinin bir tanımı da dahil olmalıdır.
- Emniyet hizmetleri ofisinin gerektiğinde SRB ve SAG ile toplantı yapabilmesi için bir toplantı programı oluşturmak.

1.5 **Acil müdahale planının (ERP) koordinasyonu** (Bölüm 8'de ele alınmıştır)

İç koordinasyon

- Yetkilerin dağıtılması ve acil durum sorumluluklarının atanması ile ilgili olarak ERP'nin genel hatlarını gözden geçirmek.
- Acil durum ve normal işletmelere geri dönüş sırasında kritik personelin eylemleri için koordinasyon prosedürleri oluşturmak.

Dış koordinasyon

- Acil durumlar sırasında örgütle etkileşim kuracak dış kurum ve kuruluşları belirlemek.
- Bu kuruluşların ERP'lerini değerlendirmek.
- Farklı ERP'ler arasında koordinasyonu sağlamak.
- Örgütün emniyet yönetimi sistemleri el kitabında (SMSM) farklı ERP'ler arasında koordinasyonu sağlamak.

1.6 **SMS dokümantasyonu** (Bölüm 8'de ele alınmıştır)

SMS dokümantasyonu

- SMS'ye özel kayıtları ve dokümantasyonu toplama ve saklama mekanizmasını oluşturmak.
- İlgili ve geçerli tüm ulusal düzenlemelere ve uluslararası standartlara atıfta bulunmak.
- SMS uygulama planını ve SMSM'yi içeren kayıtların yönetimi için kılavuz ilkeler geliştirmek.

SMS uygulama planı

- SMS uygulama planının geliştirilmesinden sorumlu kişiyi atamak veya planlama grubunu oluşturmak.
- SMS uygulama planını oluşturan tüm geçerli belgeleri toplamak.
- İlerlemeyi değerlendirmek için üst yönetimle düzenli toplantılar yapmak.
- Eldeki işlere uygun (toplantılara ayrılan zaman dahil olmak üzere) kaynaklar ayırmak.
- SMS uygulama planındaki önemli öğeleri örgütün iş planına eklemek.
- SMS'nin uygulanması için gereken eğitim ve planlama ile maliyetleri belirlemek.
- Örgütteki farklı yönetim seviyeleri arasında SMS uygulama planının geliştirilmesi ve uygulanmaya başlanması için zaman ayırmak.
- SMS'nin uygulanması için bir bütçe hazırlamak.
- SMS'nin uygulanması için başlangıç bütçesini onaylamak.
- SMS uygulama planını onaylanması için üst yönetime sunmak.

Emniyet yönetimi sistemleri el kitabı (SMSM)

- Örgütün tüm örgüt açısından emniyete yaklaşımının iletilmesi için SMSM'nin taslağını hazırlamak.
- Aşamalı SMS yaklaşımı ilerledikçe, SMSM'nin (sürekli güncellenen bir belgedir) içeriklerini genişletmek, gözden geçirmek ve düzeltmek.

1.7 **Emniyetin teşvik edilmesi — Eğitim** (Bölüm 9'da ele alınmıştır)

Emniyet eğitimi

- Eğitim gerekliliklerinin belirlenmesi için belgelenmiş bir süreç geliştirmek.
- Eğitimin etkililiğini ölçen bir doğrulama süreci geliştirmek.
- Emniyet eğitimini aşağıdakileri dikkate alarak geliştirmek:
  - — işe alma sırasında (genel emniyet) işe özel eğitim;
  - — insani Etkenler ve örgüt etkenlerini içerecek şekilde, SMS'yle ilgili işe alma/başlangıç eğitimi;
  - — tekrarlanan eğitim
- Eğitimle ilgili maliyetleri belirlemek.
- Tüm personelin bireysel sorumluluklarına ve SMS'ye katılımlarına göre uygun eğitimi almasını organize etmek ve programları hazırlamak.
- Yönetim dahil olmak üzere, her bir personel için eğitim dosyaları geliştirmek.

1.8 **Emniyetin teşvik edilmesi — Emniyet iletişimi** (Bölüm 9'da ele alınmıştır)

- Aşağıdakiler dahil olmak üzere, Aşama I'deki örgüt bilgilerinin aktarılması için bir yöntem oluşturmak:
  - — emniyet haberleri, notları, bültenleri;
  - — web siteleri;
  - — e-posta.

1.9 **Uygulama için zaman aralığı ve teslim edilebilen parçalar**

Aşama I'in uygulanması için tahmin edilen zaman aralığı, örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına bağlı olarak 1 ile 6 ay arasında olabilir.

Teslim edilebilen parçalar

1) Emniyet politikasının Sorumlu Müdür tarafından imzalanması.
2) Emniyet politikasının tüm personele iletilmesi.
3) Sistem tanımının tamamlanması.
4) Boşluk analizinin tamamlanması.
5) SMS örgüt yapısının hazırlanması.
6) SMS uygulama planının onaylanması.
7) SMS planlama aşamasındaki eğitimin verilmesi.

8) SMSM'nin ilk taslağının yayınlanması.

9) Emniyet konularının iletişimi için araçların oluşturulması.

2. AŞAMA II – REAKTİF EMNİYET YÖNETİMİ SÜREÇLERİ

2.1 **Reaktif süreçler temelinde tehlikenin tanımlanması ve analiz**
(Bölüm 3, 4 ve 9'da ele alınmıştır)

Tehlikenin tanımlanması

- Tehlikelerle ilgili reaktif bilgilerin toplanmasında kullanılacak dahili ve harici kaynakları belirlemek.
- Tehlikelerin reaktif olarak tanımlanması için yapılandırılmış bir yaklaşım uygulamak.

2.2 **Reaktif süreçler temelinde emniyet riski yönetimi**
(Bölüm 5 ve 9'da ele alınmıştır)

Emniyet riski değerlendirmesi

- Örgütün operasyonel ortama uygun bir emniyet riski matrisi geliştirmek ve uyarlamak.
- Emniyet riski matrisi talimatlarını geliştirmek ve bunları eğitim programına eklemek.

2.3 **Eğitim** (Bölüm 9'da ele alınmıştır)

- Ön saflardaki personel, yöneticiler ve denetmenler için aşağıdakiler hakkında bir emniyet eğitimi programı geliştirmek:
  - — ilgili SMS uygulama planı bileşenleri;
  - — reaktif süreçler temelinde tehlikenin tanımlanması ve emniyet riski yönetimi (ön saflardaki personel tetikleyici olaylara bağlı olarak tehlikelerin tanımlanması ve raporlanması ve denetmenler tehlike ve emniyet riski yönetimi hakkında eğitilir);
  - — tehlike raporlama formu/şablonu.

2.4 **Reaktif süreçlerle ilgili dokümantasyon** (Bölüm 4 ve 9'da ele alınmıştır)

- Bir emniyet kütüphanesi oluşturmak.
- Reaktif emniyet yönetimi süreçleri ile ilgili bilgileri SMSM'ye eklemek. (Reaktif emniyet yönetimi süreçleri ile ilgili bilgiler, daha sonraki bir aşamada emniyet performansı göstergeleri ve hedeflerini oluşturmak için kullanılacaktır.)
- Reaktif süreçler temelinde tehlikenin tanımlanması ve emniyet riski yönetimi için gereklilikleri, gerekirse yükleniciler için ihale dokümantasyonuna yazmak ve yükleniciler ve alt yüklenicileri yazılı olarak bilgilendirmek.

2.5 **Emniyetin teşvik edilmesi — Emniyet iletişimi** (Bölüm 9'da ele alınmıştır)

- Aşama II'deki örgüt bilgilerinin aktarılması için bir yöntem oluşturmak:

  - emniyet haberleri, notları, bültenleri;
  - web siteleri;
  - e-posta.

2.6 **Uygulama için zaman aralığı ve teslim edilebilen parçalar**

Aşama II'nin uygulanması için tahmin edilen zaman aralığı, örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına bağlı olarak 9 ile 12 ay arasında olabilir.

Teslim edilebilen parçalar

1) Emniyet kütüphanesinin oluşturulması.

2) Reaktif emniyet yönetimi süreçlerinin uygulanması.

3) SMS uygulama planı bileşenleri ve reaktif süreçler temelinde emniyet riski yönetimi ile ilgili eğitimin verilmesinin tamamlanması.

4) Reaktif süreçlerden elde edilen emniyet verilerini temel alan emniyet açısından önemli bilgilerin örgüt içinde dağıtılması.

3. AŞAMA III – PROAKTİF VE TAHMİNE DAYALI EMNİYET YÖNETİMİ SÜREÇLERİ

3.1 **Proaktif ve tahmine dayalı süreçler temelinde tehlikenin tanımlanması ve analiz**
(Bölüm 3, 4 ve 9'da ele alınmıştır)

Tehlikenin tanımlanması

- Tehlikelerle ilgili proaktif ve tahmine dayalı bilgilerin toplanmasında kullanılacak dahili ve harici kaynakları belirlemek.

- Tehlikelerin proaktif ve tahmine dayalı olarak tanımlanması için yapılandırılmış bir yaklaşım uygulamak.

3.2 **Proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimi**
(Bölüm 5 ve 9'da ele alınmıştır)

Emniyet riski değerlendirmesi

- Örgütün operasyonel ortama uygun bir emniyet riski matrisi geliştirmek ve uyarlamak.

- Emniyet riski matrisi talimatlarını geliştirmek ve bunları eğitim programına eklemek.

3.3 **Eğitim** (Bölüm 9'da ele alınmıştır)

- Emniyet hizmetleri ofisinin personelini, emniyetle ilgili verilerin toplanması için belirli proaktif ve tahmine dayalı araçlar hakkında eğitmek.

- Denetmenleri ve ön saflardaki personeli proaktif ve tahmine dayalı süreçler hakkında bilgilendirmek.

- Ön saflardaki personel, yöneticiler ve denetmenler için aşağıdakiler hakkında bir emniyet eğitimi programı geliştirmek:

  — ilgili SMS uygulama planı bileşenleri;
  — proaktif ve tahmine dayalı süreçler temelinde tehlikenin tanımlanması ve emniyet riski yönetimi (ön saflardaki personel daha az ciddiyete sahip tetikleyici olaylardan kaynaklanan veya gerçek zamanlı normal işletmeler sırasında ortaya çıkan tehlikelerin tanımlanması ve raporlanması hakkında eğitilir ve denetmenler proaktif ve tahmine dayalı süreçler temelinde tehlike ve emniyet riski yönetimi hakkında eğitilir);

3.4 **Proaktif ve tahmine dayalı süreçlerle ilgili dokümantasyon**
(bu el kitabının 4 ve 9. bölümlerinde ele alınmıştır)

- Emniyet kütüphanesinde proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetiminden elde edilen bilgileri saklamak.

- Proaktif ve tahmine dayalı emniyet yönetimi süreçleri ile ilgili bilgileri SMSM'ye eklemek.

- Emniyet performansı göstergelerini ve emniyet performansı hedeflerini geliştirmek.

- Proaktif ve tahmine dayalı süreçler temelinde tehlikenin tanımlanması ve emniyet riski yönetimi için gereklilikleri, gerekirse yükleniciler için ihale dokümantasyonuna yazmak ve yükleniciler ve alt yüklenicileri yazılı olarak bilgilendirmek.

3.5 **Emniyetin teşvik edilmesi — Emniyet iletişimi** (Bölüm 9'da ele alınmıştır)

- Aşama III'deki örgüt bilgilerinin aktarılması için bir yöntem oluşturmak:

  - emniyet haberleri, notları, bültenleri;
  - web siteleri;
  - e-posta.

3.6 **Uygulama için zaman aralığı ve teslim edilebilen parçalar**

Aşama III'ün uygulanması için tahmin edilen zaman aralığı, örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına bağlı olarak 12 ile 16 ay arasında olabilir.

Teslim edilebilen parçalar

1) Tehlikenin tanımlanması ile ilgili bilgilerin toplanması için proaktif ve tahmine dayalı araçların ilk test aşamasının oluşturulması.

2) Proaktif ve tahmine dayalı emniyet yönetimi süreçlerinin uygulanması.

3) SMS uygulama planı bileşenleri ve proaktif ve tahmine dayalı süreçler temelinde emniyet riski yönetimi ile ilgili eğitimin verilmesinin tamamlanması.

4) Emniyet performansı göstergelerinin ve emniyet performansı hedeflerinin geliştirilmesi.

5) Reaktif, proaktif ve tahmine dayalı süreçlerden elde edilen emniyet verilerini temel alan emniyet açısından önemli bilgilerin örgüt içinde dağıtılması.

4. AŞAMA IV – OPERASYONEL EMNİYETİN GÜVENCE ALTINA ALINMASI

4.1 **SMS'nin emniyet performansı** (Bölüm 9'da ele alınmıştır)

- Emniyet performansı göstergelerini oluşturmak.
- Emniyet performansı hedeflerini oluşturmak.
- Eylem planlarını oluşturmak.
- Gerektiğinde, eylem planları ile ilgili olarak güvenilirlik, mevcudiyet ve/veya hassasiyet bakımlarından önlemler tanımlamak.
- Devletin denetim kurumu ile emniyet performansının ölçümü konusunda uzlaşmak.

4.2 **Emniyet performansının izlenmesi ve ölçümü** (Bölüm 9'da ele alınmıştır)

- Emniyet performansı ve izlenmesi için bilgi kaynaklarını tanımlamak ve geliştirmek.

4.3 **Değişimin yönetilmesi** (Bölüm 9'da ele alınmıştır)

- Aşağıdakileri dikkate alan formel bir değişimin yönetilmesi süreci oluşturmak:
  - sistem ve etkinliklerin kritikliği;
  - sistemlerin ve operasyonel ortamların stabilitesi;
  - geçmiş performans.
- Yerleşik süreçleri, prosedürleri, ürünleri ve hizmetlerin etkileyebilecek değişiklikleri tanımlamak.
- Değişiklikleri uygulamadan önce, emniyet performansını sağlamak üzere yapılması gereken düzenlemeleri tanımlamak.

4.4 **SMS'nin sürekli olarak iyileştirilmesi** (Bölüm 9'da ele alınmıştır)

- Dahili değerlendirmeler için formlar geliştirmek ve değerlendirilen teknik süreçlerden bağımsız olmayı sağlamak.
- Dahili bir denetim süreci tanımlamak.
- Harici bir denetim süreci tanımlamak.

- Tesislerin, donanımların, dokümantasyonun ve prosedürlerin proaktif olarak değerlendirilmesi için, denetimler ve araştırmalar aracılığıyla tamamlanacak bir program tanımlamak.

- Bireyin performansının proaktif olarak değerlendirilmesi için bir program hazırlamak.

- İşletmede emniyetin güvence altına alınması ile ilgili dokümantasyonu geliştirilmek.

4.5 **Eğitim** (Bölüm 9'da ele alınmıştır)

- Emniyetin güvence altına alınmasının sağlanması aşamasında yer alan personel için operasyonda emniyetin güvence altına alınmasının sağlanması ile ilgili eğitimi geliştirmek.

4.6 **Emniyetin teşvik edilmesi — Emniyet iletişimi** (Bölüm 9'da ele alınmıştır)

- Aşama IV'teki örgüt bilgilerinin aktarılması için bir yöntem oluşturmak:

  - emniyet haberleri, notları, bültenleri;
  - web siteleri;
  - e-posta.

4.7 **Uygulama için zaman aralığı ve teslim edilebilen parçalar**

Aşama IV'ün uygulanması için tahmin edilen zaman aralığı, örgütün büyüklüğü ve verilen hizmetlerin karmaşıklığına bağlı olarak 9 ile 12 ay arasında olabilir.

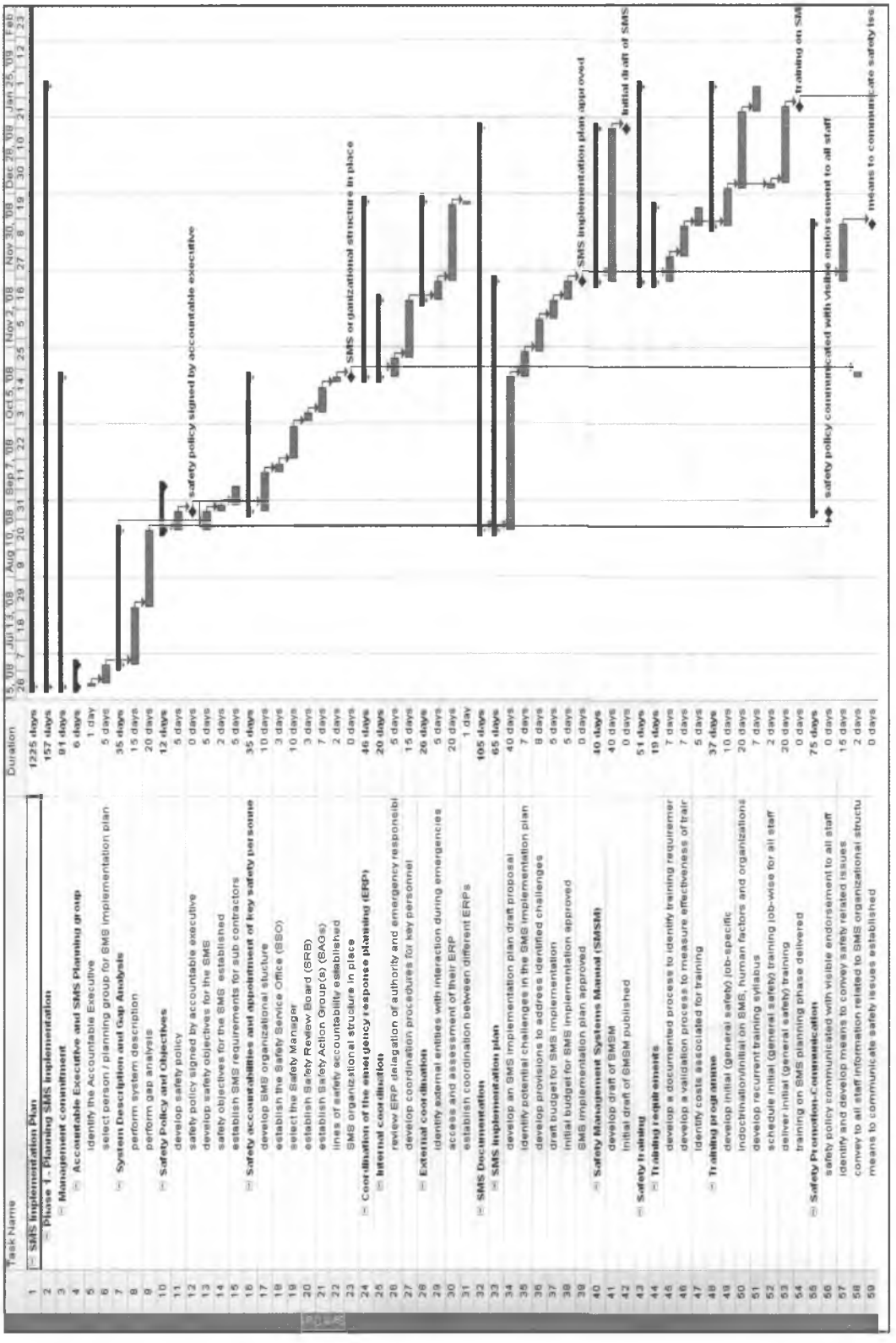
Teslim edilebilen parçalar

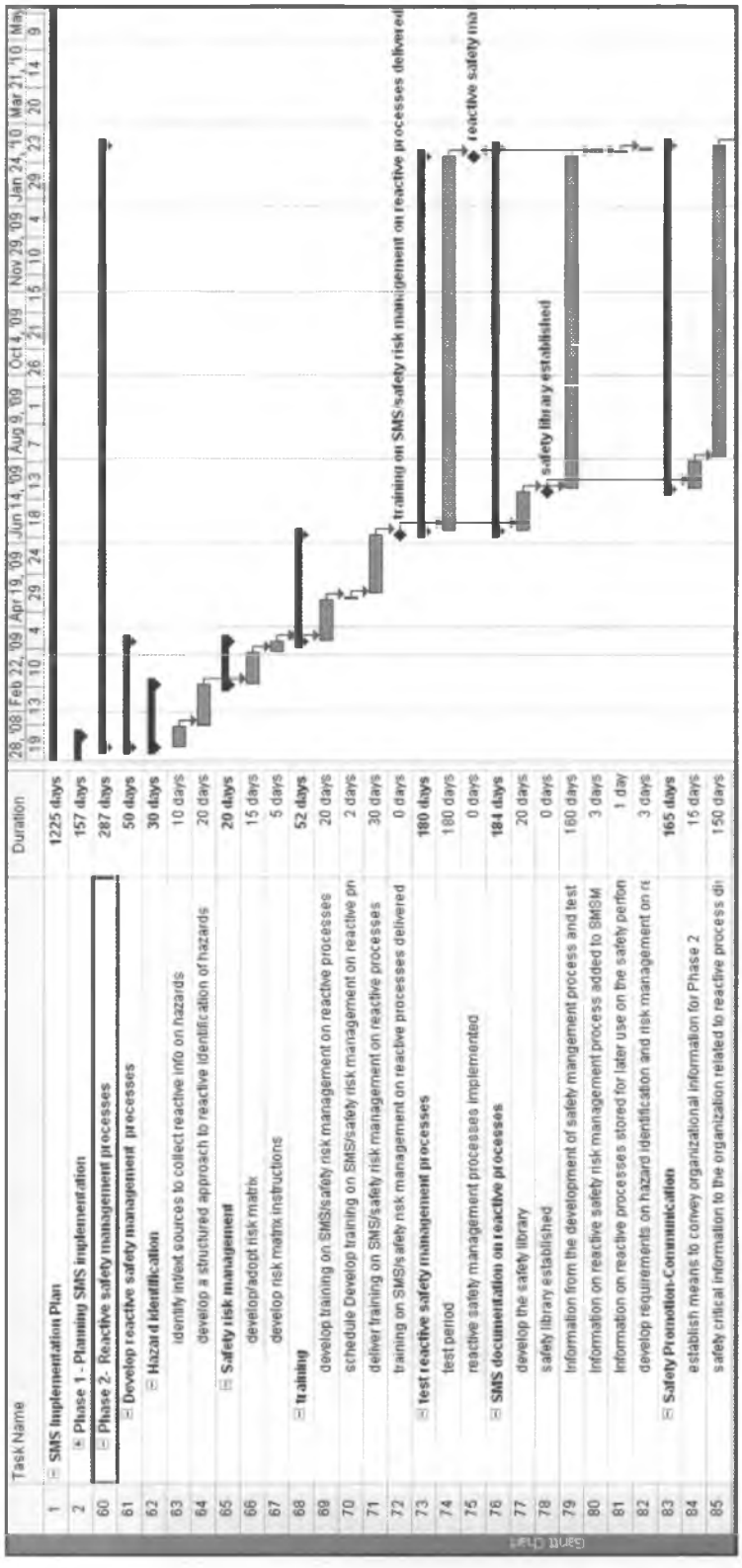
1) Emniyet performansı göstergelerinin ve emniyet performansı hedefleri hakkında Devletin denetim kurumu ile uzlaşmaya varılması.

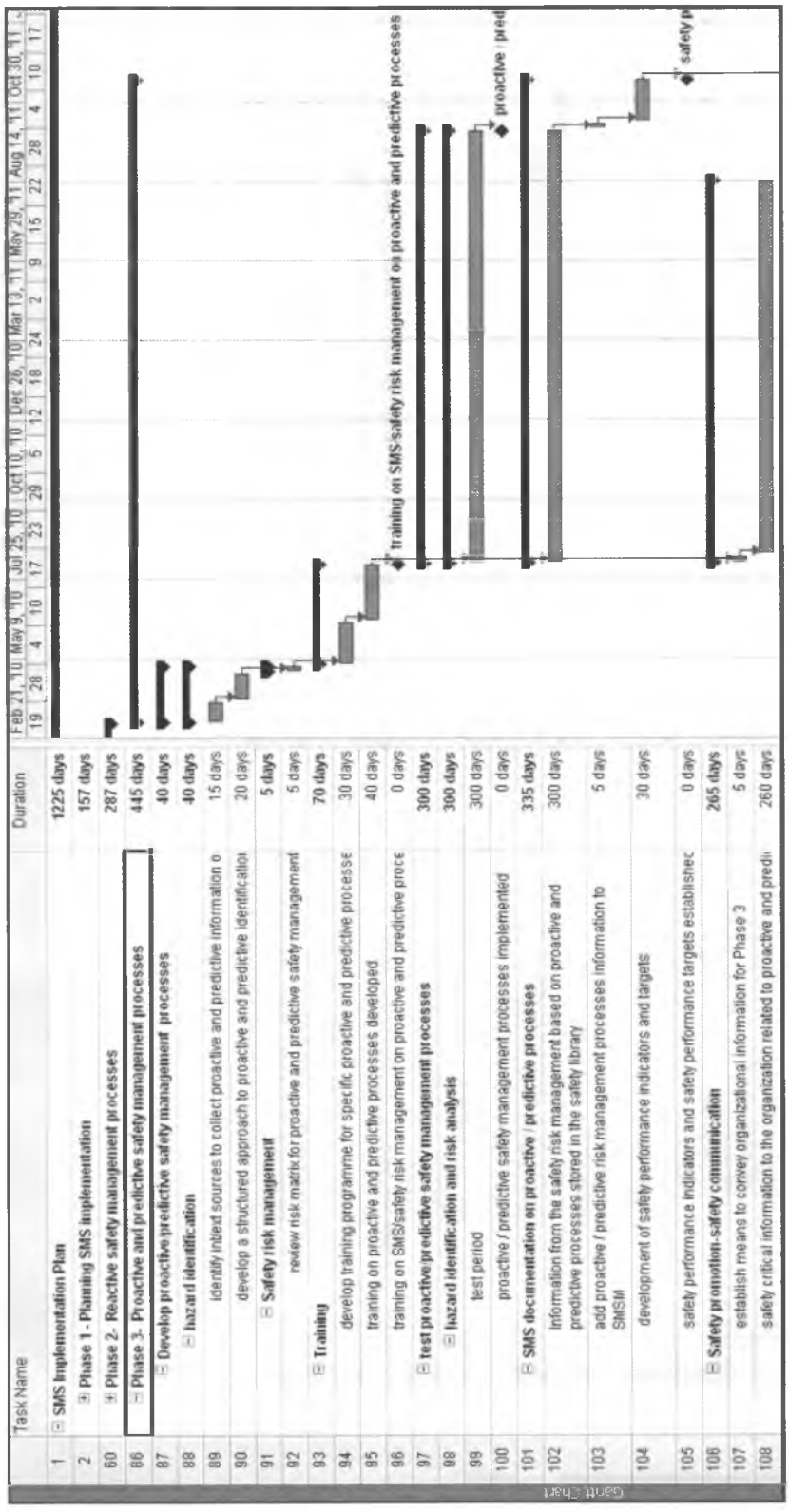
2) İşletme personeli, yöneticiler ve denetmenler için emniyetin güvence altına alınması eğitiminin tamamlanması.

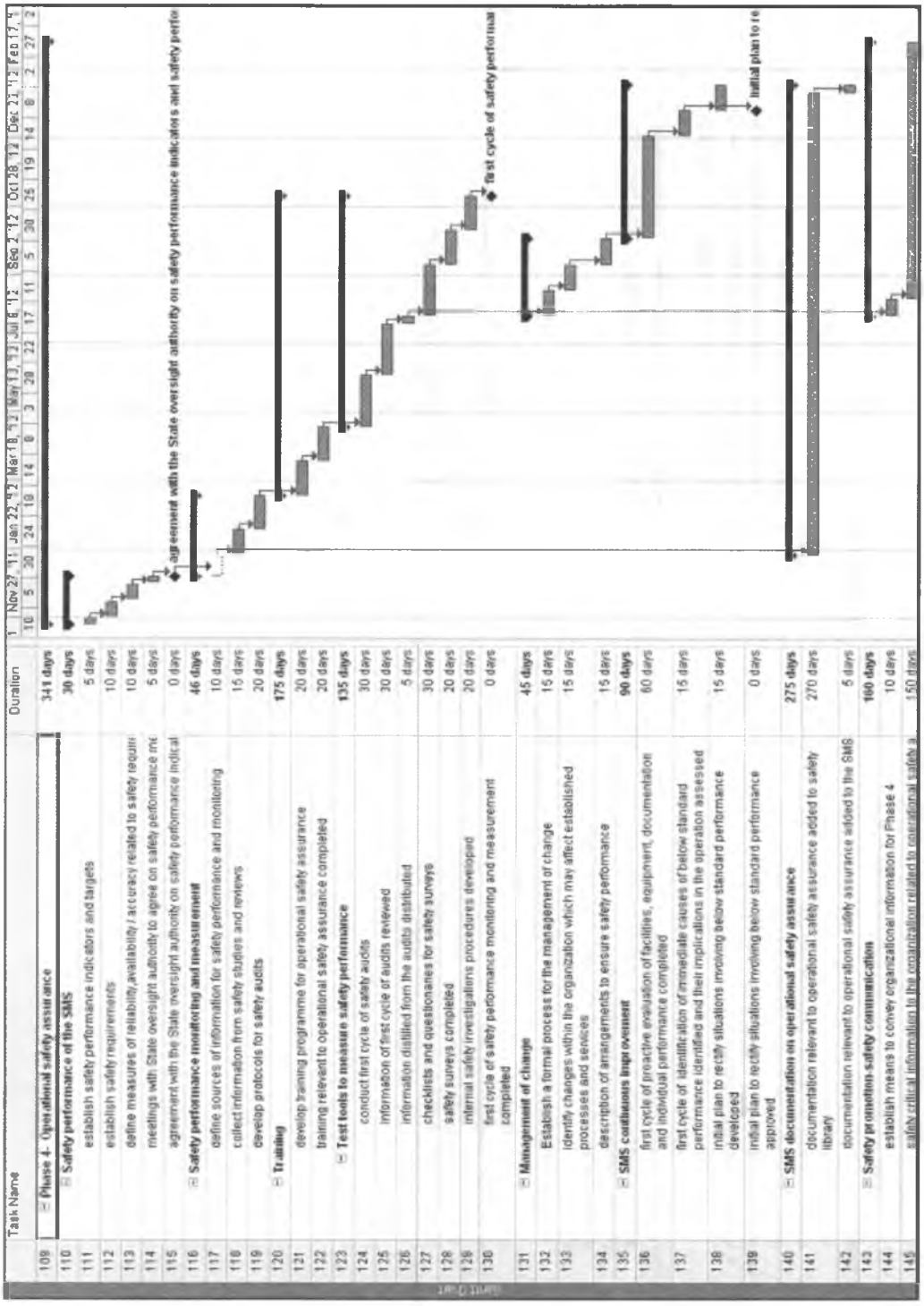
3) İşletmede emniyetin güvence altına alınmasının sağlanması ile ilgili dokümantasyonunun emniyet kütüphanesine eklenmesi.

Gantt Çizelgesi - SMS uygulama planı




Task Name
Duration
28, '08 | Feb 22, '09 | Apr 19, '09 | Jun 14, '09 | Aug 9, '09 | Oct 4, '09 | Nov 29, '09 | Jan 24, '10 | Mar 21, '10
1 SMS Implementation Plan 1225 days
2 Phase 1 - Planning SMS implementation 157 days
60 Phase 2- Reactive safety management processes 287 days
61 Develop reactive safety management processes 50 days
62 Hazard identification 30 days
63 identify in/ext sources to collect reactive info on hazards 10 days
64 develop a structured approach to reactive identification of hazards 20 days
65 Safety risk management 20 days
66 develop/adopt risk matrix 15 days
67 develop risk matrix instructions 5 days
68 training 52 days
69 develop training on SMS/safety risk management on reactive processes 20 days
70 schedule Develop training on SMS/safety risk management on reactive pr 2 days
71 deliver training on SMS/safety risk management on reactive processes 30 days
72 training on SMS/safety risk management on reactive processes delivered 0 days
73 test reactive safety management processes 180 days
74 test period 180 days
75 reactive safety management processes implemented 0 days
76 SMS documentation on reactive processes 184 days
77 develop the safety library 20 days
78 safety library established 0 days
79 Information from the development of safety mangement process and test 160 days
80 Information on reactive safety risk management process added to SMSM 3 days
81 Information on reactive processes stored for later use on the safety perfon 1 day
82 develop requirements on hazard identification and risk management on ri 3 days
83 Safety Promotion-Communication 165 days
84 establish means to convey organizational information for Phase 2 15 days
85 safety critical information to the organization related to reactive process di 150 days
training on SMS/safety risk management on reactive processes delivered
safety library established
reactive safety ma
Gantt Chart


Task Name
Duration
Feb 21, '10
May 9, '10
Jul 25, '10
Oct 10, '10
Dec 26, '10
Mar 13, '11
May 29, '11
Aug 14, '11
Oct 30, '11
SMS Implementation Plan 1225 days
Phase 1 - Planning SMS implementation 157 days
Phase 2- Reactive safety management processes 287 days
Phase 3- Proactive and predictive safety management processes 445 days
Develop proactive predictive safety management processes 40 days
hazard identification 40 days
identify inted sources to collect proactive and predictive information o 15 days
develop a structured approach to proactive and predictive identificatio 20 days
Safety risk management 5 days
review risk matrix for proactive and predictive safety management 5 days
Training 70 days
develop training programme for specific proactive and predictive processe 30 days
training on proactive and predictive processes developed 40 days
training on SMS/safety risk management on proactive and predictive proce 0 days
test proactive predictive safety management processes 300 days
hazard identification and risk analysis 300 days
test period 300 days
proactive / predictive safety management processes implemented 0 days
SMS documentation on proactive / predictive processes 335 days
information from the safety risk management based on proactive and predictive processes stored in the safety library 300 days
add proactive / predictive risk management processes information to SMSM 5 days
development of safety performance indicators and targets 30 days
safety performance indicators and safety performance targets establishec 0 days
Safety promotion-safety communication 265 days
establish means to convey organizational information for Phase 3 5 days
safety critical information to the organization related to proactive and predi 260 days
training on SMS:safety risk management on proactive and predictive processes
proactive / pred
safety p
Gantt Chart


Task Name
Duration
Phase 4- Operational safety assurance 341 days
Safety performance of the SMS 30 days
establish safety performance indicators and targets 5 days
establish safety requirements 10 days
define measures of reliability, availability / accuracy related to safety requir 10 days
meetings with State oversight authority to agree on safety performance ind 5 days
agreement with the State oversight authority on safety performance indicat 0 days
Safety performance monitoring and measurement 46 days
define sources of information for safety performance and monitoring 10 days
collect information from safety studies and reviews 15 days
develop protocols for safety audits 20 days
Training 175 days
develop training programme for operational safety assurance 20 days
training relevant to operational safety assurance completed 20 days
Test tools to measure safety performance 135 days
conduct first cycle of safety audits 30 days
information of first cycle of audits reviewed 30 days
information distilled from the audits distributed 5 days
checklists and questionnaires for safety surveys 30 days
safety surveys completed 20 days
internal safety investigations procedures developed 20 days
first cycle of safety performance monitoring and measurement completed 0 days
Management of change 45 days
Establish a formal process for the management of change 15 days
identify changes within the organization which may affect established processes and services 15 days
description of arrangements to ensure safety performance 15 days
SMS continuous improvement 90 days
first cycle of proactive evaluation of facilities, equipment, documentation and individual performance completed 60 days
first cycle of identification of immediate causes of below standard performance identified and their implications in the operation assessed 15 days
initial plan to rectify situations involving below standard performance developed 15 days
initial plan to rectify situations involving below standard performance approved 0 days
SMS documentation on operational safety assurance 275 days
documentation relevant to operational safety assurance added to safety library 270 days
documentation relevant to operational safety assurance added to the SMS 5 days
Safety promotion-safety communication 160 days
establish means to convey organizational information for Phase 4 10 days
safety critical information in the organization related to operational safety a 150 days
Nov 27 '11
Jan 22 '12
Mar 18 '12
May 13 '12
Jul 8 '12
Sep 2 '12
Oct 28 '12
Dec 23 '12
Feb 17
agreement with the State oversight authority on safety performance indicators and safety perfor
first cycle of safety performan
Initial plan to re

Bölüm 11

DEVLET EMNİYET PROGRAMI (SSP)

11.1 HEDEF VE İÇERİKLER

Bu bölüm emniyetin yönetimine yönelik olarak hem kural koyucu hem de performans temelli yaklaşımların unsurlarını birleştiren bir Devlet emniyet programının (SSP) geliştirilmesi ve uygulanması için bir çerçeve sunmaktadır. Bu bölüm aynı zamanda, hizmet sağlayıcılar tarafından bir SMS'nin uygulanmasının bir ön koşulu olarak bir SSP'nin gerçekçi bir şekilde uygulanmasının önemini ele almaktadır. Bu bölüm aşağıdaki konuları içerir:

a) Bir SSP'nin bileşenleri ve unsurları;

b) ICAO SSP çerçevesi;

c) SSP'nin geliştirilmesi;

d) SSP'nin uygulanması ve

e) SMS'nin uygulanmasının desteklenmesinde SSP'nin rolü.

11.2 BİR SSP'NİN BİLEŞENLERİ VE UNSURLARI;

11.2.1 Bir SSP, emniyetin Devlet tarafından yönetilmesi için bir Emniyet yönetimi sistemidir. Bir SSP'nin uygulanması, Devletin havacılık sisteminin büyüklüğü ve karmaşıklığına uygun olmalıdır ve Devlet içindeki sivil havacılık işlevlerinin bireysel unsurlarından sorumlu çok sayıda otorite arasında koordinasyon gerektirir.

8.2.1 Bir SSP'nin üstlenmesi gereken iki temel operasyonel etkinliği ve bu temel operasyonel etkinlikleri desteklemek için gereken örgütsel düzenlemeleri temsil eden dört SSP bileşeni vardır. Bir SSP'nin dört bileşeni şunlardır:

a) Devletin emniyet politikası ve hedefleri;

b) Devletin emniyet riski yönetimi;

c) Devlet tarafından emniyetin güvence altına alınması ve

d) Devlet tarafından emniyetin teşvik edilmesi.

11.2.3 Emniyet müdahaleleri ve azaltma stratejilerinin bakış açısında, SSP'nin iki temel operasyonel etkinlik Devletin emniyet riski yönetimi ve Devletin emniyetin güvence altına alınmasıdır. Bu iki temel operasyonel etkinlik, Devletin emniyet politikası ve hedeflerinin sağladığı şemsiye altında gerçekleşir ve Devlet tarafından emniyetin teşvik edilmesi yoluyla desteklenir. Bölüm 8, 8.2 ve 8.3'te sunulan bir SMS'nin dengi bileşenlerin çoğu SSP için de geçerlidir. Ancak, bir fark vardır: SSP'de, formel olarak Devlet politikası ve hedeflerinin bir unsuru olarak kabul edilse de, kaza ve ciddi olay inceleme süreci aynı zamanda emniyet verilerinin analizine ve alınıp verilmesine ve aynı zamanda da daha önemli konuların (Devlet tarafından emniyetin güvence altına alınması) denetiminin hedeflenmesine katkıda bulunan temel bir operasyonel etkinliktir.

11.2.4 11.2.2'de ele alınan dört bileşen, gerçek bir yönetim sisteminin (SSP) altında yatan dört kapsayıcı emniyet yönetimi sürecini temsil etmeleri bakımından, bir SSP'nin temel ilkelerini oluştururlar. Her bir bileşen, gerçek Devlet yönetim sisteminin emniyetin kural koyucu ve performans temelli yaklaşımları bir araya getirecek ele alması veya kullanması gereken belirli alt süreçleri, belirli etkinlikleri veya araçları kapsayan unsurlara ayrılmıştır ve hizmet sağlayıcılar tarafından SMS'nin uygulanmasını destekler.

11.2.5 Devlet emniyet politikaları ve hedefleri bileşeni dört unsurdan oluşur:

a) Devlet emniyet mevzuatı çerçevesi;

b) Devletin emniyet sorumlulukları ve hesap verme sorumlulukları;

c) kaza ve olay incelemesi ve

d) yaptırım politikası.

11.2.6 Devlet emniyet riski yönetimi bileşeni iki unsurdan oluşur:

a) hizmet sağlayıcının SMS'si için emniyet gereklilikleri;

b) hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

11.2.7 Devlet tarafından emniyetin güvence altına alınması bileşeni üç unsurdan oluşur:

a) emniyet denetimi;

b) emniyet verilerinin toplanması, analiz edilmesi ve alışverişi ve

c) daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

11.2.8 Devlet tarafından emniyetin teşvik edilmesi bileşeni iki unsurdan oluşur:

a) dahili eğitim, iletişim ve emniyet bilgilerinin dağıtılması ve

b) harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

Not - SSP bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havaalanlarını kapsar.

11.3 ICAO SSP ÇERÇEVESİ

Not— ICAO SSP çerçevesi hakkında ayrıntılı bilgiler bu bölümün sonundaki Ek 1'de bulunmaktadır.

11.3.1 Bölüm 11.2'de ele alınan on iki unsurla birlikte dört bileşen, aşağıdaki şekilde bir SSP'nin geliştirilmesi, uygulanması ve sürdürülmesi için ilkelere dayanan bir kılavuz olması amaçlanan ICAO SSP çerçevesini oluştururlar:

1. Devletin emniyet politikası ve hedefleri

   1.1 Devlet emniyet mevzuatı çerçevesi
   1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları
   1.3 Kaza ve olay incelemeleri
   1.4 Yaptırım politikası

2. Devletin emniyet riski yönetimi

   2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri
   2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

3. Devlet tarafından emniyetin güvence altına alınması

   3.1 Emniyet denetimi
   3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi
   3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

4. Devlet tarafından emniyetin teşvik edilmesi

   4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.
   4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

11.3.2 Bu bölümde tanımlanan SSP çerçevesi ve Bölüm 8'de belirtilen emniyet yönetimi sistemi (SMS) çerçevesi, birbirini tamamlayan, ama ayrı çerçeveler olarak görülmelidir.

11.4 SSP'NİN GELİŞTİRİLMESİ

11.4.1 Devletlerin SSP'lerini ICAO SSP çerçevesinin dört bileşeni ve on bir unsuru etrafında geliştirmeleri önerilir.

11.4.2 ***Devletin emniyet politikası ve hedefleri***. Devletin, havacılık etkinliklerinde emniyetin yönetimini nasıl denetleyeceğinin tanımıdır. Buna SSP ile ilgili olarak farklı Devlet örgütlerinin gerekliliklerinin, sorumluluklarının ve hesap verme sorumluluklarının ve aynı zamanda SSP tarafından ulaşılması istenen kabul edilebilir emniyet seviyesinin (ALoS) tanımları da dahildir.

11.4.3 Aşağıdaki paragraflarda ele alınan üç SSP bileşeni, sadece sorumluluklar, hesap verme sorumlulukları ve yükümlülüklerden oluşan genel bir çerçevenin parçası olarak etkili bir şekilde uygulanabilir. Bu genel çerçeve, altında emniyet riski yönetimi, emniyetin güvence altına alınması ve Devlet tarafından emniyetin teşvik edilmesinin gerçekleşebileceği "koruyucu bir şemsiye" haline gelir. Devletin emniyet politikası ve hedefleri bileşeni, yönetim ve personeline Devletin sivil havacılık otoritesinin emniyet yönetimi çabalarını yolunda tutan açık politikaları, prosedürleri, yönetim kontrollerini, dokümantasyonu ve düzeltme süreçlerini sağlar. Bu bileşen aynı zamanda Devletin giderek karmaşıklaşan ve sürekli değişen hava taşımacılığı sisteminde emniyet konusunda liderliği sağlamasına güven oluşturmak için önemlidir. Bu bileşen altındaki merkezi önemde bir etkinlik, Devletin emniyet politikasının geliştirilmesidir. Bu bölümün 2. eki bir Devlet emniyet politikası beyanı geliştirilmesi için kılavuzluk sağlamaktadır.

11.4.4 ***Devletin emniyet riski yönetimi.*** Devletin, havacılık etkinliklerinde tehlikeleri nasıl tanımlayacağının ve tehlikelerin sonuçlarına ait emniyet risklerini nasıl değerlendireceğinin tanımıdır. Bu, Devletin emniyeti nasıl yöneteceğini belirleyen kontrollerin (kurallar ve/veya düzenlemeler) oluşturulmasını, hizmet sağlayıcının SMS'nin nasıl çalıştığını belirleyen kurallar ve/veya düzenlemelerin oluşturulması ve hizmet sağlayıcının SMS'sinin emniyet performansı üzerinde uzlaşmayı içerir.

11.4.5 Emniyet yönetimi ilkeleri, kural koyma ve politika geliştirme ile başlayarak, Devletin sivil havacılık kurumunu çoğu etkinliğini etkiler. Sadece en yakın zamanda gerçekleşen kazanın nedenlerinin peşinde koşmak yerine, SSP kural koyma işlemi Devletin havacılık sistemin kapsamlı analizlerini temel alır. Düzenlemeler belirlenen tehlikeleri ve tehlikelerin sonuçlarına ait emniyet risklerinin analizini temel alır. Düzenlemelerin kendileri, hizmet sağlayıcının SMS'sine entegre edildiklerinde, risk kontrolünün çerçevelerini oluştururlar.

11.4.6 ***Devlet tarafından emniyetin güvence altına alınması.*** Devletin, Devlet için emniyet yönetimini ve hizmet sağlayıcının SMS'sinin işletilmesinin yerleşik kontrolleri (düzenlemelere uyum) izlemesini nasıl sağlayacağının; Devlet tarafından yapılan emniyet ölçümü ve hizmet sağlayıcılar tarafından yapılan emniyet performansı ölçümünün bir kombinasyonu aracılığıyla SSP'nin gerçekçi bir uygulamasına (ALoS) nasıl ulaşılacağının ve hizmet sağlayıcının SMS'sinin gerçek performansının (emniyet performansı) nasıl gösterileceğinin (emniyet performansı ölçümü) tanımıdır. Bu, uyumun doğrulanması ve performansın ölçülmesi için gereken zorunlu düzenlemelerin (gözetim, incelemeler, denetimler, emniyet verilerinin analizi v.s.) oluşturulmasını da içerir.

11.4.7 ***SSP gözetim etkinlikleri.*** Kural koymanın ötesinde, SSP gözetim etkinlikleri analizler tarafından desteklenir ve Devletin sivil havacılık kurumunun kaynak dağıtımı öncelikleri analizle belirlenen tehlikelerin sonuçlarına ait emniyet risklerini temel alır. Sertifikasyon ve sürüp giden operasyonel emniyet kararları, hizmet sağlayıcının süreçlerinin, ürünlerinin ve/veya hizmetlerinin performanslarının değerlendirilmesini temel alır. Tanımlanan tehlikeleri ele alan düzenlemelerden daha ileriye gidildiğinde, uyum kararları bir hizmet sağlayıcının SMS'sinin hizmet sağlayıcının kendine özgü operasyonel ortamdaki düzenlemelerdeki tehlikeyi ele almadığı temelinde verilir. Devlet tarafından emniyetin güvence altına alınması süreçleri, hizmet sağlayıcının SMS'sindeki değerlendirmelerde gösterildiği gibi hizmet sağlayıcının emniyet yönetimi kapasitesine güven uyandırmak için kullanılır. ICAO Doc 9734, Kısım A, *Bir Devletin Emniyet Denetimi Sisteminin Oluşturulması ve Yönetimi* belgesinde belirtilen sekiz kritik unsurun izlenmesi için belirli mekanizmalarının oluşturulmasının SSP'ye göre gerekli olmadığının vurgulanması önemlidir.

11.4.8 ***Devlet tarafından emniyetin teşvik edilmesi***. Devlet tarafından emniyet eğitimi, iletişimi ve emniyet bilgilerin yayılmasını sağlamak için yapılan düzenlemelerin tanımıdır. Bir SSP altında, bu iki taraflı bir destektir, hem Devletin havacılık örgütleri içinde hem de devletin gözetim altında tuttuğu hizmet sağlayıcılar içinde gerçekleştirilir. Bu, eğitim sağlanması ve emniyet bilgilerinin iletişiminin sağlanması için gerekli araçların oluşturulmasını da içerir.

11.4.9 Yukarıdakilerin hiçbiri Devletin ve havacılık örgütlerinin Devletin düzenlemelerini ve standartlarının tesis edilmesindeki rolünü veya Devlet sivil havacılık personelinin yüksek bir bilgi ve beceri seviyesine sahip olması gerekliliğini değiştirmez. Aksine, emniyet riski analizi, sistem değerlendirme ve yönetimi sistemi değerlendirme gibi alanlarda ve havacılık sektörünün üretim hedeflerine ulaşması için gerekli olan pek çok yeni teknolojide ek beceriler gerektirir. Bu, Devlete eğitim, işe alma ve insan kaynakları yönetimi aracılığıyla bu yeterlilikleri sağlama sorumluluğu yükler.

11.4.10 SSP'nin geliştirilmesinde, emniyet yönetimi ilkeleri SSP'nin Devlet ve SMS'nin hizmet sağlayıcılar tarafından paralel olarak geliştirilmesi için kavramsal bir platform sağlar. Emniyet yönetimi ilkelerinden geliştirilen ve bu ilkeleri temel alan bir SSP, aksi takdirde Devletin sivil havacılık örgütleri içindeki harici ve dahili emniyet süreçleri ve hizmet sağlayıcıların dahili emniyet süreçleri arasında kaçınılmaz olarak gelişecek boşluğu kapatır (bkz. Şekil 11-1). SSP'nin bir parçası olarak, kazaları olayları veya emniyet standartlarına uyulmamasını beklemek yerine, hizmet sağlayıcılara emniyet yönetimi kapasitelerini en baştan göstermek için Devlet hizmet sağlayıcının uyması gereken SMS gerekliliklerini bildirir. Bu hem Devletin hem de hizmet sağlayıcıların emniyet risklerinin önüne geçmesini sağlar. SSP'ye göre SMS gereklilikleri aynı zamanda Devlet ve hizmet sağlayıcıların emniyet sorunlarının çözümünde daha etkin bir şekilde etkileşim kurmalarını sağlayan yapılandırılmış bir çerçeve sunar. Bu şekilde SSP ve SMS'nin paylaşılan, etkileşimli doğası meyve vermiş olur.

11.5 SSP'NİN UYGULANMASI

11.5.1 SSP'nin uygulanması, bir SSP'nin önceki paragraflarda ele alınan dört bileşeninden her biriyle ilgili süreçlerin tanımlanması ile kolaylaştırılır.

Bu süreçler bundan sonra bir SSP'nin her bir bileşeninin ayrı unsurlarına dönüştürülebilir ve Bölüm 8'de ele alınan SMS çerçevesine benzer şekilde, unsur ve bileşenlerin kombinasyonu SSP'nin çerçevesi haline gelir. Bu tür bir çerçevenin mevcut olması, SSP'nin uygulanması için ilkelere dayanan bir kılavuz sağlar. ICAO SSP'nin uygulanmasını kolaylaştırmak için bir SSP'nin geliştirilmesini sağlayacak kılavuz bilgileri geliştirmiştir ve ICAO SSP çerçevesi bu bölümün 1. Ekinde yer almaktadır. Bu bölümün 5. Ekinde bir SMS uygulama planının geliştirilmesi ile ilgili kılavuz bilgiler yer almaktadır.

11.5.2 Bir Devlet tarafından geliştirilen SSP'nin örneği olarak, BK Sivil Havacılık Yayınları (CAP) 784 tarafından yayınlanan, Birleşik Krallık Devlet emniyet programına BK CAA web sitesi aracılığıyla erişilebilir: www.caa.co.uk.

11.6 SMS'NİN UYGULANMASININ DESTEKLENMESİNDE SSP'NİN ROLÜ

11.6.1 Bir SSP'nin amaçlarından biri hizmet sağlayıcılar tarafından SMS'nin uygulanmasını destekleyen bir bağlam oluşturmaktır. Hizmet sağlayıcının SMS'si bir düzenleme boşluğunda veya tamamen uyuma yönelik bir ortamda etkili bir şekilde çalışamaz. Bu tür ortamlarda, hizmet sağlayıcılar sadece SMS'nin parçalarını uygulayacak ve gösterecekler ve Devlet yetkilileri sadece SMS'nin parçalarını değerlendireceklerdir. Hizmet sağlayıcının SMS'si sadece SSP tarafından sağlanan koruyucu şemsiye altında yeşerebilir. Bu nedenle, SSP hizmet sağlayıcılar tarafından SMS'nin etkili bir şekilde uygulanmasını sağlayan temel bir etkendir. Bu nedenle, Ek 5'te sunulan SMS'nin genel bir şekilde uygulanması kapsamında, ikisi küresel ve ikisi de özel dört adım, SMS'nin hizmet sağlayıcılar tarafından uygulanmasını desteklemeyi amaçlar.

Şekil 11-1. SMS Devletin ve hizmet sağlayıcıların emniyet süreçleri arasındaki boşluğu doldurur

11.6.2 Genel olarak, SSP'sinin uygulanması sırasında bir Devletin atması gereken ilk adım, Devlet içinde bir SSP'nin unsurlarının mevcut olup olmadıklarını ve olgunluk durumlarını belirlemek için bir boşluk analizi yapmaktır. Bir SSP için gerçekleştirilen bir boşluk analizi örneği bu bölümün 3. Ekinde yer almaktadır. Boşluk analizinden sonra, Devlet SSP'nin çalışmasını yöneten ulusal mevzuatın ve operasyonel düzenlemelerin taslağını hazırlayacak konumdadır. Bunlara, hizmet sağlayıcılar için SMS gereklilikleri de dahil olacaktır.

11.6.3 SSP'nin uygulanmasında ilk adımlardan biri, Devlet kurumunun personeli için bir eğitim programı geliştirmektir. Eğitim programının iki temel hedefi olmalıdır. İlk hedef, Annex 1, 6, 8, 11, 13 ve 14 ve ilgili kılavuz materyallerinde yer alan emniyet yönetimi ile ilgili ICAO SARP'leri dahil olmak üzere emniyet yönetimi konseptleri hakkında bilgi sağlamaktır. Eğitimin bu yönü, SSP'nin geneli için geçerlidir. İkinci hedef, ulusal düzenlemeler ve ilgili ICAO SARP'lerine uygun olarak, bir SMS'nin önemli bileşenlerinin uygulanmasının nasıl kabul edileceği ve denetleneceği ile ilgili bilgilerin geliştirilmesidir. Eğitimin bu yönü SMS'nin uygulanmasının desteklenmesini amaçlar.

11.6.4 Özellikle SMS'nin uygulanmasını destekleyen bir SSP'nin uygulanmasındaki ilk adım, hizmet sağlayıcılar için SMS gerekliliklerinin ve SMS'nin uygulanması için kılavuz materyalin geliştirilmesidir. Bir Devletin SMS ile ilgili düzenlemesinin geliştirilmesi ile ilgili kılavuz bilgiler Bölüm 10 Ek 1'de bulunmaktadır. Bu kılavuz bilgilerde ICAO SMS çerçevesinin Bölüm 8'de ele alınan bileşenleri ve unsurlarına atıfta bulunulmaktadır. Bu el kitabı ve ICAO SMS ve SSP eğitim kursları, kılavuz materyalin geliştirilmesi için bilgi kaynaklarıdır.

11.6.5 Özellikle SMS'nin uygulanmasını destekleyen bir SSP'nin uygulanmasındaki ikinci adım, sivil havacılık denetim kurumunun yaptırım politikasının gözden geçirilmesidir. Bu adım, özellikle ifade edilmesi gerekir.

11.6.6 Hem SSP hem de SMS'nin özü, kazaları, olayları veya emniyet standartlarına uyulmamasını beklemek yerine, Devlet ve sektörü içinde emniyet yönetimi kapasitelerinin geliştirilmesiyle emniyet risklerinin önüne geçmektir. Bu el kitabının çeşitli kısımlarında ele alındığı gibi yönetimin temellerinden biri ölçmedir, çünkü ölçülemeyen bir şeyin yönetilmesi mümkün değildir. Ölçme işlemi ise verilere ihtiyaç duyar. Dolayısıyla, emniyet verilerinin toplanması, analizi ve alışverişi, 11.4.10'da ele alınan SSP ve SMS'nin etkileşimli doğasının kalbinde yer almaktadır.

11.6.7 Sırasıyla SSP ve SMS altında normal emniyet yönetimi etkinlikleri sırasında, Devlet ve hizmet sağlayıcılar emniyet verilerinin alışverişi yapacaktır. Devlet tarafından hizmet sağlayıcıdan alınan emniyet verileri özellik verileri olacaktır, Devlet bu verilerin bir kısmını toplu veriye dönüştürecektir. Tüm bu verilerin önemli bir kısmı, hizmet sağlayıcının SMS süreçlerinin normal akışı aracılığıyla belirlenen emniyet sorunları ile ilgili olacaktır. Sivil havacılık denetim kurumunun bu verilere müdahalesi yaptırım eylemi olursa, Devletteki emniyet yönetimi süreci durma noktasına gelecektir. Bu nedenle, SSP'nin bir parçası olarak, sivil havacılık kurumunun yaptırım politikasını SMS ortamında çalışan hizmet sağlayıcılarla arasında proaktif ve tahmine dayalı emniyet yönetimi verilerinin sürekli akışını ve alışverişini sağlayacak şekilde gözden geçirmesi önemlidir. Bu gözden geçirme için aşağıdaki kılavuz ilkeler önerilmektedir:

a) hizmet sağlayıcıların belirli emniyet sorunları ile dahili olarak, SMS'leri bağlamında ilgilenmesine izin verilmelidir;

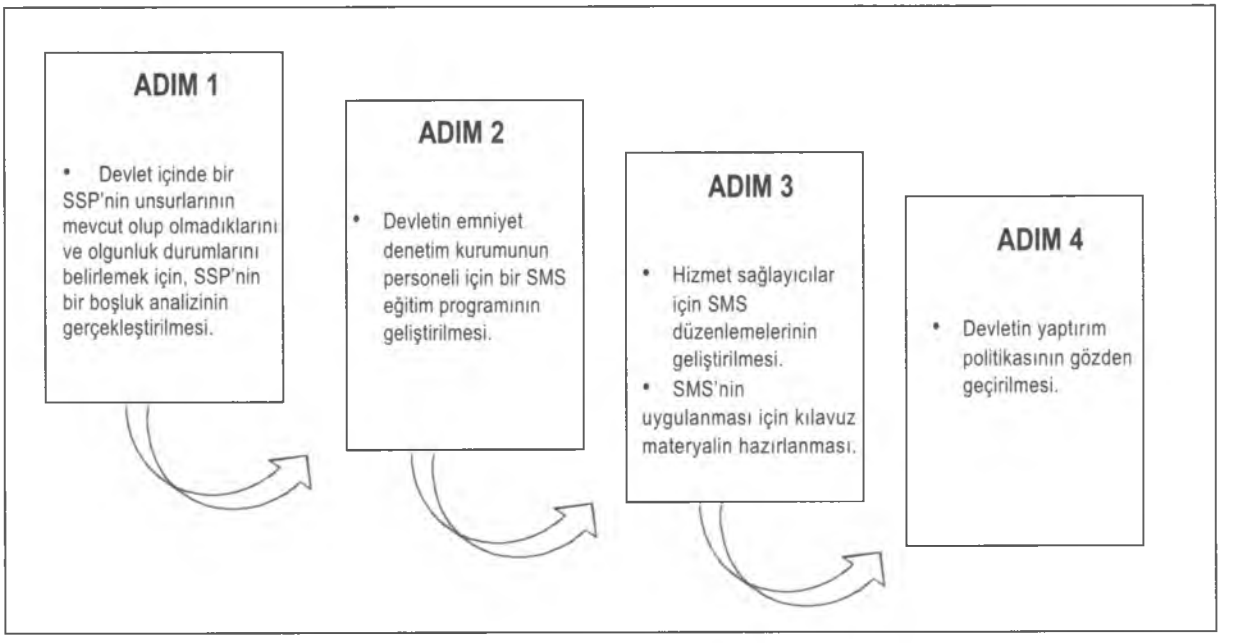
b) hizmet sağlayıcılar Devlete sapmalar ve/veya küçük ihlaller dahil olmak üzere emniyet sorununun açık bir tanımı ve çözümü için Devleti tatmin eden bir azaltma planını sunmalıdır;

c) azaltma planı, Devletin azaltma etkinliklerin tatmin edici bir şekilde ilerleyip ilerlemediğini izleyebilmesi için zaman aralıklarını da içermelidir ve

d) ağır ihmal, taksirli eylem veya kasıtlı suiistimaller kapsamlı bir şekilde oluşturulmuş olan yaptırım prosedürleri ile karşılanmalıdır.

Bu bölümün 4. ekinde bir SMS ortamında bir Devletin yaptırım politikası ve yaptırım prosedürlerinin geliştirilmesi ile ilgili kılavuz bilgiler verilmektedir.

11.6.8 SMS'nin uygulanmasında SSP'nin rolünün ve önerilen eylemlerin bir özeti Şekil 11-2'de gösterilmiştir.



Şekil 11-2. SMS'nin uygulanmasının desteklenmesinin SSP'nin rolünün özeti

Bölüm 11 Ek 1

DEVLET EMNİYET PROGRAMI (SSP) ÇERÇEVESİ

Not - Bu ek bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havaalanlarını kapsar.

Bu ek, bir örgüt tarafından bir Devlet emniyet programının (SSP) bir Devlet tarafından uygulanması ve sürdürülmesi için bir çerçeve sunar. Çerçeve aşağıdaki dört bileşen ve on bir unsurdan oluşur:

1. Devletin emniyet politikası ve hedefleri

    1.1 Devlet emniyet mevzuatı çerçevesi
    1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları
    1.3 Kaza ve olay incelemeleri
    1.4 Yaptırım politikası

2. Devletin emniyet riski yönetimi

    2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri
    2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

3. Devlet tarafından emniyetin güvence altına alınması

    3.1 Emniyet denetimi
    3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi
    3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

4. Devlet tarafından emniyetin teşvik edilmesi

    4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.
    4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

Her bir unsurun kısa bir tanımı aşağıda yer almaktadır.

1. DEVLETİN EMNİYET POLİTİKASI VE HEDEFLERİ

1.1 Devlet emniyet mevzuatı çerçevesi

Devlet, uluslararası ve ulusal standartlara uygun şekilde, Devletin Devlet içinde emniyetin yönetimini nasıl sağlayacağını tanımlayan ulusal bir emniyet mevzuatı çerçevesini ve özel düzenlemeleri yayınlamıştır. Bu, Devletin havacılık örgütlerinin Devlet içindeki emniyetin yönetilmesi ile ilgili belirli etkinliklere katılmasını ve bu örgütlerin rollerinin, sorumluluklarının ve ilişkilerinin oluşturulmasını içerir. Emniyet mevzuatı çerçevesi ve özel düzenlemeler Devletle uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmelidir.

1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları

Devlet, SSP'nin oluşturulması ve sürdürülmesi ile ilgili gereklilikleri, sorumlulukları ve hesap verme sorumluluklarını belirlemiş, tanımlamış ve belgelemiş olmalıdır. Bu, SSP'nin Devletin emniyet hedeflerini karşılayacak şekilde planlanması, organize edilmesi, geliştirilmesi, sürdürülmesi, kontrolü ve sürekli olarak iyileştirilmesi için yönergeleri de içerir. Aynı zamanda, SSP'nin uygulanması için gereken kaynakların sağlanması hakkında açık bir ifade içermelidir.

1.3 Kaza ve olay incelemeleri

Devlet, tek amacı kazaların ve olayların önlenmesi olan ve suçlama veya yükümlülüklerin dağıtılması olmayan bağımsız bir kaza ve olay inceleme süreci oluşturmuş olmalıdır. Bu incelemeler, Devletin emniyet yönetimini destekliyor olmalıdır. SSP'nin işletilmesi sırasında, Devlet kaza ve olay inceleme örgütün diğer Devlet havacılık örgütlerinden bağımsızlığını korumalıdır.

1.4 Yaptırım politikası

Devlet, hizmet sağlayıcıların belirli emniyet sapmalarını içeren eylemlerin, dahili olarak, hizmet sağlayıcının emniyet yönetimi sistemi (SMS) bağlamı içinde ve uygun Devlet kurumunu tatmin edecek şekilde ele almasına ve çözmesine izin verilen koşulları ve şartları belirleyen bir yaptırım politikası yayınlamış olmalıdır. Yaptırım politikası aynı zamanda, emniyet sapmalarının yerleşik yaptırım prosedürleri aracılığıyla ele alınabileceği koşulları ve şartları da belirlemelidir.

2. DEVLETİN EMNİYET RİSKİ YÖNETİMİ

2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri

Devlet, hizmet sağlayıcıların tehlikeleri nasıl tanımlayacaklarını ve emniyet risklerini nasıl yöneteceklerini belirleyen kontrolleri oluşturmuş olmalıdır. Bunlara hizmet sağlayıcının SMS'si için geçerli olan gereklilikler, belirli operasyonel düzenlemeler ve uygulama politikaları da dahildir. Gereklilikler, belirli operasyonel düzenlemeler ve uygulama politikaları, hizmet sağlayıcılarla uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmelidir.

2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

Devlet, hizmet sağlayıcılarla SMS'lerinin emniyet performansı hakkında uzlaşmaya varmış olmalıdır. Hizmet sağlayıcının SMS'sinin üzerinde uzlaşılan emniyet performansı, hizmet sağlayıcılarla uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmelidir.

3. DEVLET EMNİYET GÜVENCESİ

3.1 Emniyet denetimi

Devlet, emniyet denetimi işlevinin sekiz önemli unsurunun etkili bir şekilde izlenmesini sağlayan mekanizmalar kurmuş olmalıdır. Devlet aynı zamanda hizmet sağlayıcılar tarafından tehlikelerin tanımlanmasını ve emniyet risklerinin yönetilmesinin yerleşik düzenleyici kontrollere (gereklilikler, özel operasyonel düzenlemeler ve uygulama politikaları) göre yapılmasını sağlayacak mekanizmaları oluşturmuş olmalıdır. Bu mekanizmalar, düzenleyici emniyet riski kontrollerinin hizmet sağlayıcının SMS'sine uygun bir şekilde entegre edilmesini, tasarlandıkları gibi uygulanmalarını ve düzenleyici kontrollerin emniyet riskleri üzerinde amaçlanan etkiye sahip olmasını sağlayan incelemeler, denetimler ve araştırmaları içerir.

3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi

Devlet, hem bireysel hem de toplu Devlet seviyesinde tehlikeler ve emniyet risklerinin elde edilmesini ve saklamasını sağlayan mekanizmalar oluşturmuştur. Devlet aynı zamanda saklanan verilerden bilgi elde etmek ve emniyet bilgilerinin uygun şekilde hizmet sağlayıcılar ve/veya diğer Devletlerle alışverişini sağlamak için gereken mekanizmaları oluşturmuş olmalıdır.

3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

Devlet, incelemeler, denetimler ve araştırmaları tehlikeler, bu tehlikelerin operasyonlardaki sonuçları ve değerlendirilen emniyet risklerine ait verilerin analizi ile belirlenen şekilde, daha önemli emniyet sorunu veya gereksinimi olan alanlara yönlendirerek önceliklerini belirlemek için gerekli prosedürleri oluşturmuş olmalıdır.

4. DEVLET TARAFINDAN EMNİYETİN TEŞVİK EDİLMESİ

4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

Devlet, Devlet havacılık örgütleri içinde, etkili ve etkin bir SSP'nin yeşermesini sağlayan bir örgüt kültürünün geliştirilmesini desteklemek için eğitim sağlar ve farkındalığı ve emniyetin ilgili bilgilerin iki yönlü iletişimini destekler.

4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması

Devlet, hizmet sağlayıcılar arasında, etkili ve etkin bir SMS'nin yeşermesini sağlayan bir örgüt kültürünün geliştirilmesini desteklemek için eğitim sağlar ve farkındalığı ve emniyetle ilgili bilgilerin iki yönlü iletişimini destekler.

— — — — — — — — —

Bölüm 11 Ek 2

BİR DEVLETİN EMNİYET POLİTİKASI BEYANININ GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

Sivil havacılık emniyetinin yönetimi, [Devletin] en önemli sorumluluklarından biridir. [Devlet], denetimi altında gerçekleşen tüm havacılık etkinliklerinin en yüksek emniyet performansı seviyesine ulaşması ve ulusal ve uluslararası standartlara uymasını sağlamak için, stratejiler ve süreçler geliştirmeye, uygulamaya, bunları sürdürmeye ve sürekli olarak iyileştirmeye kendini adamış olmalıdır.

[Devlet] havacılık sertifikalarının sahiplerinden, yönetim sistemlerinin bir SMS yaklaşımını yeterli derecede yansıttığını göstermeleri istenecektir. Bu yaklaşımın beklenen sonucu, sivil havacılık sektöründeki emniyet raporlamaları da dahil olmak üzere emniyet yönetimi ve emniyet uygulamalarının iyileştirilmesidir.

[Devlette], Sorumlu Müdür [örgüte uygun kişi] ile başlayarak tüm yönetim seviyeleri [Devlet içinde] bu en yüksek seviyedeki emniyet performansının elde edilmesinden sorumludur.

[Devlet] aşağıdakilere bağlı kalır:

a) Devletin havacılık sisteminin kapsamlı bir analizi temelinde, emniyet yönetimi ilkeleri üzerine kurulan genel kural koyma prosedürlerinin ve özel operasyon politikalarının geliştirilmesi;

b) düzenlemelerin geliştirilmesi ilgili konularda havacılık sektörünün tüm segmentlerine danışmak;

c) etkili bir emniyet raporlaması ve iletişimi sistemi aracılığıyla Devlet içinde emniyetin yönetilmesini desteklemek;

d) emniyet sorunlarının çözülmesinde hizmet sağlayıcılarla etkili bir şekilde etkileşim kurmak;

e) [Devlet emniyet denetimi kurumu] içinde, hem emniyetle ilgili olarak hem de diğer konularda, yeterli kaynak sağlandığının ve personelin sorumluluklarını yerine getirmek için gerekli becerilere ve eğitime sahip olmasını sağlamak;

f) analizlerle ve emniyet riskleri temelinde öncelik verilen kaynak dağıtımı ile destekleyerek, hem performans temelli hem de uyuma yönelik denetim etkinliklerini gerçekleştirmek;

g) uluslararası emniyet gerekliliklerine ve standartlara uymak ve mümkün olduğunda aşmak;

h) havacılık sektörünü emniyet yönetimi konseptleri ve ilkeleri konusunda desteklemek ve eğitmek;

i) havacılık örgütlerinde SMS'nin uygulanmasını denetlemek;

j) denetim altındaki tüm etkinliklerin en yüksek emniyet standartlarını karşılamasını sağlamak;

k) emniyet verileri koruma, toplama ve işleme sistemleri (SDCPS) için, insanların tehlikeler hakkında emniyetle ilgili önemli bilgileri sağlamak için cesaretlendirilmelerini ve [Devlet] ile hizmet sağlayıcılar arasında sürekli bir emniyet yönetimi verileri akışı ve alışverişi olmasını sağlayacak hükümler oluşturmak;

l) SSP'mizin açıkça tanımlanmış emniyet göstergeleri ve emniyet hedefleri karşısında gerçekçi bir şekilde uygulanmasını sağlamak ve bunu ölçmek;

m) SSP veya SMS altında oluşturulan herhangi bir SDCPS'den elde edilen hiçbir bilginin, ağır ihmal veya kasıtlı suiistimal durumları dışında, bir yaptırım eyleminin temeli olarak kullanılmamasını sağlayan bir yaptırım politikası yayınlamak.

Bu politika [Devletin emniyet denetimi kurumu] ile ilgili etkinliklerde yer alan tüm personel tarafından anlaşılmalı, uygulanmalı ve dikkate alınmalıdır.

(İmza) _____
Sorumlu Müdür

– – – – – – – – – – –

Bölüm 11 Ek 3

BİR DEVLET EMNİYET PROGRAMI (SSP) BOŞLUK ANALİZİNİN GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

Not - Bu kılavuz bilgiler bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havaalanlarını kapsar.

1. BOŞLUK ANALİZİ

1.1. Bir SSP'nin uygulanması için bir Devletin SSP'nin hangi bileşenleri ve unsurlarının mevcut olduğunu ve uygulama gerekliliklerine uyması için hangi bileşenlerin ve unsurların eklenmesi veya değiştirilmesi gerektiğini belirlemek üzere kendi emniyet sisteminin bir analizini yapması gerekir. Bu analiz boşluk analizi olarak adlandırılır ve SSP gerekliliklerinin Devletin mevcut kaynakları ile karşılaştırılmasını içerir.

1.2 Boşluk analizi, kontrol listesi biçiminde, ICAO SSP çerçevesini oluşturan bileşen ve unsurların değerlendirilmesine ve geliştirilmesi gereken bileşen ve unsurların belirlenmesine yardımcı olan bilgileri sağlar. Boşluk analizi tamamlandığında ve belgelendiğinde, SSP uygulama planının temellerinden birini oluşturur.

2. ICAO SSP ÇERÇEVESİ

ICAO SSP çerçevesi, aşağıda açıklanan dört bileşen ve on bir unsurdan oluşur:

1. Devletin emniyet politikası ve hedefleri
    - 1.1 Devlet emniyet mevzuatı çerçevesi
    - 1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları
    - 1.3 Kaza ve olay incelemeleri
    - 1.4 Yaptırım politikası
2. Devletin emniyet riski yönetimi
    - 2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri
    - 2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.
3. Devlet tarafından emniyetin güvence altına alınması
    - 3.1 Emniyet denetimi
    - 3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi
    - 3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

4. Devlet tarafından emniyetin desteklenmesi

4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.
4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

3. DEVLET EMNİYET PROGRAMI (SSP) BOŞLUK ANALİZİ

Aşağıdaki boşluk analizi kontrol listesi bir boşluk analizi yapmak için şablon olarak kullanılabilir. Her soru "Evet" veya "Hayır" yanıtı verilmesi için tasarlanmıştır. Bir "Evet" yanıtı, Devletin söz konusu ICAO SSP çerçevesi bileşeni veya unsurunu emniyet sistemine dahil ettiğini ve gereklilikleri karşıladığını veya aştığını gösterir. Bir "Hayır" yanıtı, ICAO SSP çerçevesinin bileşeni/unsuru ve Devletin emniyet sistemi arasında bir boşluk olduğunu gösterir.

ICAO referansı (Doc 9859)	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bileşen 1 — DEVLETİN EMNİYET POLİTİKALARI VE HEDEFLERİ			
Unsur 1.1 - Devlet emniyet mevzuatı çerçevesi			
Bölüm 11	[Devlet], Devlet içinde emniyetin yönetimini tanımlayan ulusal emniyet mevzuatı çerçevesini ve özel düzenlemeleri yayınladı mı?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet], Devlet içindeki emniyetin yönetilmesi ile ilgili olarak, her bir [Devlet] havacılık örgütün katılması gereken belirli etkinlikleri tanımladı mı?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet], havacılık örgütleri tarafından [Devlet] içinde emniyetin yönetilmesi ile ilgili gereklilikler, sorumlulukları ve hesap verme sorumluluklarını oluşturdu mu?	☐ Evet ☐ Hayır	
Bölüm 11	Emniyet mevzuatı çerçevesi ve özel düzenlemeler Devletle uyumlu ve ilgili kalması için düzenli olarak gözden geçiriliyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] emniyet mevzuatı çerçevesi ve özel düzenlemeler uluslararası standartlara göre güncel kalmaları için düzenli olarak gözden geçiriliyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] bir emniyet politikası oluşturdu mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] emniyet politikası [Devlet] SSP Sorumlu Müdür veya [Devlet] içindeki yetkili merci tarafından imzalanmış mı?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] emniyet politikası periyodik olarak gözden geçiriliyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] emniyet politikası, emniyetle ilgili sorumluluklarının farkına varmaları için, görülebilir bir onayla, [Devletin] tüm havacılık örgütlerinde tüm personele iletilmiş mi?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet], bileşenleri ve unsurları arasındaki ilişkileri de içerecek şekilde, SSP'yi açıklayan bir belge geliştirmiş mi?	☐ Evet ☐ Hayır	

ICAO referansı (Doc 9859)	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bölüm 11	[Devlet], SSP etkinliklerinin belgelenmesi ve desteklenmesi için tüm kayıtların oluşturulmasını ve tutulmasını sağlayan bir kayıt sistemine sahip midir?	☐ Evet ☐ Hayır	
Bölüm 11	Kayıt sistemi kayıtların uygun şekilde tanımlanması, okunabilmesi, saklanması, korunması, arşivlenmesi, alınabilmesi, tutulması süresi ve son işlemlerinin yapılması için gereken kontrol süreçlerini sağlıyor mu?	☐ Evet ☐ Hayır	
Unsur 1.2 - Devletin emniyet sorumlulukları ve hesap verme sorumlulukları			
Bölüm 11	[Devlet], SSP'nin oluşturulması ve sürdürülmesi ile ilgili olarak Devletin gereklilikleri, sorumlulukları ve hesap verme sorumluluklarını belirlemiş ve tanımlamış mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Gereklilikler, SSP'nin Devletin emniyet hedeflerini karşılayacak şekilde planlanması, organize edilmesi, geliştirilmesi, kontrolü ve sürekli olarak iyileştirilmesi için gerekli yönergeleri ve etkinlikleri de içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Gereklilikler, SSP'nin uygulanması ve sürdürülmesi için gereken kaynakların sağlanması hakkında açık bir ifade içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP'nin uygulanması, işletilmesi ve gözetimi için doğrudan sorumlu olacak nitelikli bir kişi olarak bir Sorumlu Müdür belirledi ve atadı mı?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP Sorumlu Müdürü gereken iş işlevlerini ve sorumluluklarını yerine getiriyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP Sorumlu Müdürü, farklı Devlet havacılık örgütlerini SSP'ye göre uygun şekilde koordine ediyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP Sorumlu Müdürü, SSP'nin doğru şekilde yürütülmesi için gerekli kaynakların kontrolüne sahip mi?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP Sorumlu Müdürü, [Devlet] havacılık örgütlerinin tüm personelinin, SSP'ye göre sorumluluklarını, hesap verme sorumluluklarını ve yetkilerini ve tüm emniyet yönetimi süreçlerini, kararlarını ve eylemlerini anladığından emin mi?	☐ Evet ☐ Hayır	
Bölüm 11	Tüm seviyelerdeki emniyetle ilgili sorumluluklar ve hesap verme sorumlulukları tanımlanmış ve belgelenmiş mi?	☐ Evet ☐ Hayır	
Unsur 1.3 - Kaza ve olay incelemeleri			
Bölüm 11	[Devlet], emniyetin yönetilmesinin bir parçası olarak, tek amacı kazaların ve olayların önlenmesi olan ve suçlama veya yükümlülüklerin dağıtılması olmayan bağımsız bir kaza ve olay inceleme süreci oluşturmuş mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] kaza ve olay inceleme örgütün diğer Devlet havacılık örgütlerinden bağımsızlığını koruyor mu?	☐ Evet ☐ Hayır	
Unsur 1.4 – Yaptırım politikası			
Bölüm 11	[Devlet] bir yaptırım politikası yayınlamış mıdır?	☐ Evet ☐ Hayır	

ICAO referansı (Doc 9859)	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bölüm 11	Yaptırım politikası, hizmet sağlayıcıların belirli emniyet sapmalarını içeren eylemlerin, dahili olarak, hizmet sağlayıcının emniyet yönetimi sistemi (SMS) bağlamı içinde ve uygun Devlet kurumunu tatmin edecek şekilde ele almasına ve çözmesine izin verilen koşulları ve şartları belirliyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Yaptırım politikası, emniyet sapmalarının yerleşik yaptırım prosedürleri aracılığıyla ele alınabileceği koşulları ve şartları belirliyor mu?	☐ Evet ☐ Hayır	
Bileşen 2 – DEVLETİN EMNİYET RİSKİ YÖNETİMİ			
Unsur 2.1 - Hizmet sağlayıcının SMS'si için emniyet gereklilikleri			
Bölüm 11	[Devlet], hizmet sağlayıcıların tehlikeleri nasıl tanımlayacaklarını ve emniyet risklerini nasıl yöneteceklerini belirleyen kontrolleri oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 11	Kontroller hizmet sağlayıcının SMS'si için geçerli olan gereklilikler, belirli operasyonel düzenlemeler ve uygulama politikaları içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Gereklilikler, özel operasyonel düzenlemeler ve uygulama politikaları belirlenen tehlikeleri ve tehlikelerin sonuçlarına ait emniyet risklerinin analizini temel alıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Gereklilikler, belirli operasyonel düzenlemeler ve uygulama politikaları, hizmet sağlayıcılarla uyumlu ve ilgili kalması için düzenli olarak gözden geçirilmiş mi?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] içinde tanımlanan tehlikeler ile ilgili emniyet risklerini hizmet sağlayıcıların nasıl yöneteceği konusunda, olasılık ve tekrarlama ciddiyeti bakımından yapılandırılmış bir süreç var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Emniyet sorunlarının, tehlikelerin veya ortaya çıkan olayların etkili bir şekilde raporlanmasını sağlayan bir [Devlet] politikası var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Emniyet sorunlarının, tehlikelerin veya ortaya çıkan olayların raporlanmasını ile ilgili [Devlet] politikası disiplin cezalarından ve/veya idari cezalardan korunmayı sağlayan koşulları içeriyor mu?	☐ Evet ☐ Hayır	
Unsur 2.2 - Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma			
Bölüm 11	[Devlet], her bir hizmet sağlayıcıyla SMS'lerinin emniyet performansı hakkında uzlaşmaya varmış mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Üzerinde uzlaşılan emniyet performansı hizmet sağlayıcının özel operasyonel bağlamın karmaşıklığına uygun mudur?	☐ Evet ☐ Hayır	
Bölüm 11	Üzerinde uzlaşılan emniyet performansı, hizmet sağlayıcının emniyet risklerini ele almak için sahip olduğu kaynakları dikkate alıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Üzerinde uzlaşılan emniyet performansı, tek bir gösterge veya hedef yerine, çok sayıda emniyet göstergesi ve emniyet hedefi ve aynı zamanda eylem planları ifade edilmiş mi?	☐ Evet ☐ Hayır	
Bölüm 11	Üzerinde uzlaşılan emniyet performansı, hizmet sağlayıcıyla uyumlu ve ilgili kalması için düzenli olarak gözden geçiriliyor mu?	☐ Evet ☐ Hayır	

ICAO referansı (Doc 9859)	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bileşen 3 — DEVLETİN EMNİYET GÜVENCESİ			
Unsur 3.1 – Emniyet denetimi			
Bölüm 11	[Devlet] hizmet sağlayıcılar tarafından tehlikelerin tanımlanması ve emniyet risklerinin yönetilmesinin yerleşik düzenleyici kontrollere göre yapılmasını sağlayacak mekanizmaları oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 11	Yerleşik mekanizmalar, düzenleyici emniyet riski kontrollerinin hizmet sağlayıcıların SMS'sine uygun şekilde entegre edilmesini sağlayacak şekilde incelemeleri, denetimleri ve araştırmaları içeriyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Yerleşik mekanizmalar, düzenleyici emniyet riski kontrollerinin tasarlandığı şekilde uygulanmasını sağlıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Yerleşik mekanizmalar, düzenleyici emniyet riski kontrollerinin emniyet riskleri üzerinde tasarlanan etkiye sahip olmasını sağlıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] ALoS'u ile ilgili olarak düzenli ve periyodik gözden geçirme işlemleri yapılıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	Gözden geçirme işlemleri [Devletin] SSP'sini ve ALoS'unu etkileyebilecek değişiklikleri, en iyi uygulamaların Devlet için paylaşılmasını ve iyileştirilmesine yönelik tavsiyeleri dikkate alıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devletin] SSP'si ve ALoS'unun, Devlet içindeki havacılık operasyonlarının kapsamı ve karmaşıklığına uygun kalıp kalmadığını değerlendirmek için düzenli ve periyodik gözden geçirme işlemleri yapılıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	SSP ile ilgili değişikliklerin etkililiğini değerlendirmek için bir süreç var mıdır?	☐ Evet ☐ Hayır	
Unsur 3.2 — Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi			
Bölüm 11	[Devlet], hem bireysel hem de toplu Devlet seviyesinde tehlikeler ve emniyet risklerinin elde edilmesini ve saklamasını sağlayan mekanizmalar oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] saklanan verilerden bilgi elde etmek ve emniyet bilgilerinin uygun şekilde hizmet sağlayıcılar ve/veya diğer Devletlerle alışverişini desteklemek için gereken mekanizmaları oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] SSP'si ile ilgili kabul edilebilir bir emniyet seviyesi (ALoS)oluşturmuş mudur?	☐ Evet ☐ Hayır	
Bölüm 11	SSP ile ilgili [Devlet] ALoS'u emniyet ölçümü ile emniyet performansı ölçümünün unsurlarını bir araya getirmekte midir?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] ALoS'u, [Devlet] içindeki havacılık etkinliklerinin karmaşıklığına uygun mudur?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] içinde SSP'nin gerçekçi bir şekilde uygulanıp uygulanmadığını ölçmek için bir dizi parametre geliştirmek ve bu parametreleri sürdürmek için formel bir süreç var mıdır?	☐ Evet ☐ Hayır	
Unsur 3.3 — Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi			
Bölüm 11	[Devlet] daha büyük emniyet sorunu veya gereksinimi olan alanlara yönelik incelemelerin, denetimlerin ve araştırmaların önceliklerini belirlemek için prosedürler geliştirmiş midir?	☐ Evet ☐ Hayır	
Bölüm 11	İncelemelerin ve denetimlerin önceliklerinin belirlenmesi tehlikeler, operasyonlardaki sonuçları ve değerlendirilen emniyet riskleri ile ilgili verilerin analizi sonucunda mı yapılmıştır?	☐ Evet ☐ Hayır	

ICAO referansı (Doc 9859)	*Analiz edilecek konu veya yanıtlanacak soru*	*Yanıt*	*Uygulama durumu*
Bileşen 4 — DEVLET TARAFINDAN EMNİYETİN TEŞVİK EDİLMESİ			
Unsur 4.1 - Dahili eğitim, iletişim ve emniyet bilgilerinin dağıtılması.			
Bölüm 11	[Devlet], [Devlet] havacılık örgütleri içinde emniyetle ilgili bilgilerle ilgili olarak dahili eğitim, farkındalık ve iki yönlü iletişim sağlıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] içinde SSP işlevleri ve ürünleri hakkındaki bilgilerin [Devlet] havacılık örgütlerine zamanında sağlanmasını sağlayacak iletişim süreçler var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Emniyet bilgilerinin [Devlet] havacılık örgütlerinde dağıtılmasını sağlayacak bir süreç ve bu sürecin etkili olup olmadığını izlemek için bir yöntem var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] havacılık örgütlerinin büyüklüğüne uygun iletişim süreçleri (yazılı, elektronik, toplantılarla v.s.) var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	SSP işlevleri ve ürünleri ile ilgili bilgiler ve emniyet bilgileri uygun bir ortamda tutuluyor mu?	☐ Evet ☐ Hayır	
Unsur 4.2 - Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması			
Bölüm 11	[Devlet], [Devlet] havacılık örgütleri içinde emniyetle ilgili bilgilerle ilgili olarak harici eğitim, emniyet riskleri ile ilgili farkındalık ve emniyetle ilgili bilgilerin iki yönlü iletişimini sağlıyor mu?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] içinde SSP'nin ulusal ve uluslararası olarak desteklenmesini sağlayan iletişim süreçleri var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	Emniyet bilgilerinin [Devlet] hizmet sağlayıcılarına harici olarak dağıtılmasını sağlayacak formel bir süreç ve bu sürecin etkili olup olmadığını izlemek için bir yöntem var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] içinde SSP işlevleri ve ürünleri hakkındaki bilgilerin [Devlet] hizmet sağlayıcılarına zamanında sağlanmasını sağlayacak iletişim süreçler var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	[Devlet] hizmet sağlayıcılarının büyüklüğüne uygun iletişim süreçleri (yazılı, elektronik, toplantılarla v.s.) var mıdır?	☐ Evet ☐ Hayır	
Bölüm 11	SSP işlevleri ve ürünleri ile ilgili bilgiler ve emniyet bilgileri uygun bir ortamda oluşturuluyor ve tutuluyor mu?	☐ Evet ☐ Hayır	

— — — — — — — — —

Bölüm 11 Ek 4

BİR SMS ORTAMINDA BİR DEVLET UYGULAMA POLİTİKASI VE UYGULAMA PROSEDÜRLERİNİN GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

YAPTIRIM POLİTİKASI

1. GİRİŞ

Bu yaptırım politikası [Devletin geçerli sivil havacılık düzenleme(ler)i, hava trafiği emir(ler)i veya düzenleyici standart(lar)ındaki] yasa koyucu otorite altında yayınlanmıştır.

2. İLKELER

2.1 Bu yaptırım politikası [Devletin CAA'sı] tarafından hizmet sağlayıcıların emniyet etkinliklerinin değerlendirilmesine yönelik kapasitesinin ve düzenlemelerin kapsamlı bir şekilde gözden geçirilmesinin zirve noktasıdır.

2.2 Emniyet yönetimi sistemlerinin (SMS) uygulanması [Devletin CAA'sının] bu gelişmekte olan emniyet çerçevesi için esnek bir yaptırım yaklaşımı geliştirmesini ve aynı zamanda yaptırım işlevlerinin adilce, pratik ve tutarlı bir şekilde gerçekleştirilmesini gerektirir. Bir SMS ortamında esnek bir yaptırım yaklaşımı iki genel ilkeye dayanmalıdır.

2.3 İlk genel ilke, hizmet sağlayıcıların belirli emniyet sapmalarını içeren eylemleri, dahili olarak, hizmet sağlayıcının SMS'si bağlamı içinde ve otoriteyi tatmin edecek şekilde ele almasına ve çözmesine izin veren yaptırım prosedürlerinin geliştirilmesidir. [Devletin Sivil Havacılık Yasası] ve [Devletin Sivil Havacılık Düzenlemelerinin] kasıtlı olarak ihlal edildiği durumlar incelenmeli ve uygunsa alışılagelmiş yaptırıma konu edilmelidir.

2.4 İkinci genel ilke, SMS'ye uygun olarak oluşturulan emniyet verileri toplama ve işleme sistemlerinden (SDCPS) elde edilen bilgilerin yaptırım eyleminin temeli olarak kullanılmamasıdır.

3. KAPSAM

3.1 Bu yaptırım politikası beyanının ve ilgili yaptırım prosedürlerinin altında yatan ilkeler ICAO Annex 1 — *Personele Lisans Verilmesi*, Annex 6 — *Uçakların İşletilmesi*, Kısım I – *Uluslararası Ticari Hava Taşımacılığı – Uçaklar* ve Kısım II – *Uluslararası Operasyonlar – Helikopterler*; Annex 8 — *Uçakların Uçuşa Elverişliliği*, Annex 11 — *Hava Trafiği Hizmetleri*, Annex 14 — *Havaalanları,* Cilt I – *Havaalanı Tasarımı ve İşletimi* bölümlerine uygun şekilde işletilen hizmet sağlayıcılar için geçerlidir.

3.2 Bu kılavuz bilgiler bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havaalanlarını kapsar.

4. GENEL

4.1 [Hizmet sağlayıcı], sahip olduğu operasyon onayı altında yapılması yetkisine sahip olduğu operasyonların ve operasyonlarla ilgili tehlikelerin ve emniyet risklerinin büyüklüğüne, doğasına ve karmaşıklığına uygun bir SMS oluşturmalı, sürdürmeli ve bu sisteme sadık kalmalıdır.

4.2 SMS'nin uygulanmasını destekleyen bir yaptırım politikası geliştirmek için, [Devletin CAA] denetleyicileri hizmet sağlayıcılarla açık bir iletişim kurmalıdırlar.

4.3 Bir SMS'ye uygun şekilde çalışmakta olan bir hizmet sağlayıcı, kasıtsız olarak [Sivil Havacılık Yasası veya Sivil Havacılık Düzenlemelerini] ihlal ederse, belirli gözden geçirme prosedürleri kullanılacaktır. Bu prosedürler, hizmet sağlayıcının denetlenmesinden sorumlu [Devletin CAA] denetleyicisinin, SMS ile yönetilen örgütle diyaloga girmesine olanak sağlayacaktır. Bu diyalogun amacı, önerilen düzeltme önlemleri ve ihlale neden olan sorunları yeterince ele alan bir eylem planı üzerinde uzlaşmak ve hizmet sağlayıcıya bunları uygulamak için makul bir süre sağlamaktır. Bu yaklaşım, hizmet sağlayıcının çalışanlarının emniyet sorunlarını ve tehlikeleri ceza alma korkusu olmadan rapor edebildikleri etkili bir emniyet raporlamasının yeşermesini ve sürdürülmesini hedeflemektedir. Dolayısıyla, hizmet sağlayıcı suçlama yapmadan ve yaptırım korkusu olmadan, tekrarlamasını önlemeye yardımcı olacak en iyi önlemleri almak üzere, olayı ve bu olaya yol açmış olabilecek örgütten kaynaklanan veya bireysel etkenleri analiz edebilecektir.

5. DÜZELTME ÖNLEMLERİ

[Devletin CAA'sı], hizmet sağlayıcının denetlenmesinden sorumlu denetleyici aracılığıyla, hizmet sağlayıcı tarafından önerilen düzeltme önlemlerini ve/veya ihlale neden olan olayın ele alınması için mevcut bulunan sistemleri değerlendirecektir. Önerilen düzeltme önlemlerinin uygun olduğu ve olayın tekrarlanmasını önleyebileceği ve gelecekte uyum sağlanmasına yardımcı olabileceği görülürse, ihlalin gözden geçirilmesi yaptırım olmadan tamamlanacaktır. Düzeltme önlemlerinin veya mevcut sistemlerin uygun görülmediği durumlarda, [Devletin CAA'sı] yaptırımı önleyecek tatmin edici bir çözüm bulmak için hizmet sağlayıcı ile etkileşim kurmayı sürdürecektir. Ancak, hizmet sağlayıcının olayı ele almayı ve etkili düzeltme önlemleri almayı reddettiği durumlarda, [Devletin CAA'sı] bir yaptırım veya sertifika ile ilgili bir idari ceza uygulamayı dikkate alacaktır.

6. YAPTIRIM PROSEDÜRLERİ

Havacılık düzenlemelerinin ihlali, düzenlemelerin gerçekten yanlış anlaşılmasından havacılık emniyetine önem vermemeye kadar çok farklı nedenlerle ortaya çıkabilir. [Devletin CAA'sı] farklı koşulların ışığı altında [ilgili Devlet Yasasına] göre emniyet yükümlülüklerini etkili bir şekilde ele almak için bir dizi yaptırım prosedürüne sahiptir. Bu prosedürler, aşağıdakiler gibi çeşitli eylemlerle sonuçlanabilirler:

a) danışmanlık;

b) düzeltmeye yönelik eğitim;

c) yetkilerin değiştirilmesi, askıya alınması veya iptal edilmesi.

7. YAPTIRIM EYLEMLERİNİN TARAFSIZLIĞI

Yaptırım kararları aşağıdakilerden etkilenmemelidir:

a) kişisel çatışma;

b) cinsiyet, ırk, din, politik görüş veya bağlılık gibi konular veya

c) dahil olan kişilerin kişisel, politik veya mali gücü.

8. MÜDAHALE ORANTISALLIĞI

Yaptırım kararları, aşağıdaki iki ilkeye göre, belirlenen ihlaller ve neden oldukları emniyet riskleri ile orantılı olmalıdır:

a) [Devletin CAA'sı] sürekli ve kasıtlı olarak Sivil Havacılık Düzenlemeleri dışında çalışanlara karşı yaptırımda bulunmalıdır ve

b) [Devletin CAA'sı] emniyet sorunlarının çözülmesi taahhüdünde bulunanların eğitilmesini, eğitimlerinin desteklenmesini veya gözetim altında tutulmalarını amaçlamalıdır.

9. ADİL YARGI VE HESAP VERME SORUMLULUĞU

Yaptırım kararları:

a) adil olmalıdır ve yasal prosedür izlenmelidir;

b) ilgili kişilere açık olmalıdır;

c)yaptırımda bulunmayı düşünürken olayın gerçekleştiği koşulları ve hizmet sağlayıcının tavrı/eylemleri hesaba katılmalıdır;

d) benzer/aynı koşullar için tutarlı eylemler/kararlar uygulanmalıdır ve

e) uygun dahili ve harici gözden geçirmelere konu olmalıdırlar.

10. İSTİSNALAR

10.1 Bu politika, uyumsuzluk durumunun gizlenmesi için kasıtlı çabanın kanıtı varsa geçerli değildir.

10.2 Bu politika, hizmet sağlayıcı tehlikelerin tanımlanması ve emniyet riski yönetimi araçları konusunda güven sağlayamadığında geçerli değildir.

10.3 Bu politika, hizmet sağlayıcı ihlalleri sürekli tekrarlıyorsa geçerli değildir. İhlallerin sürekli tekrarlanması, geçmişte aynı veya yakından ilgili ihlallerin yapılmış olmasıdır.

10.4 Bu tür durumlarda, yerleşik yaptırım prosedürlerindeki ceza matrisi (veya geçerli ölçü) geçerli olacaktır.

(İmza) _____
Devletin Sorumlu Müdürü

Bir SMS Ortamında Yaptırım Prosedürleri

1.GENEL

[Devletin] Devlet emniyet programına (SSP) göre, [Devletin CAA'sı] bir SMS ortamında çalışan sertifika sahiplerinin denetlenmesinden sorumludur. Yaptırım prosedürleri bir SMS ortamında çalışan hizmet sağlayıcıların denetiminden sorumlu olanlara, yaptırım eylemi uygulanırsa başarılı olacağından emin olmak için eylemlere veya eylemsizliklere gösterilmesi gereken uygun müdahaleler hakkında tavsiyelerde bulunarak, kılavuzluk sağlar. Yaptırım prosedürleri süreçte destekleyici bir işlev görür ve herhangi bir yaptırım konusu ile ilgili son karar Sorumlu Müdürünün sorumluluğundadır.

2. UYGULANABİLİRLİK

2.1 Bu prosedürler, etkinliklerini bir SMS'ye uygun olarak gerçekleştiren kişiler veya hizmet sağlayıcılar tarafından yapılan ihlaller için geçerlidir.

2.2 Bu prosedürler [tarihinden] itibaren geçerlidir. [Devletin Sivil Havacılık Düzenlemelerinde] belirtilen önceki prosedürlerin yerine geçerler ve bu prosedürleri geçersiz kılarlar.

2.3 Hizmet sağlayıcılar operasyonlarını bir SMS'ye uygun olarak gerçekleştirme konusundaki isteklerini gösterdiklerinde, SMS yaptırım prosedürleri henüz kabul edilen bir SMS'leri olmamasına karşın, SMS'nin bazı temel bileşenlerine sahip olan ve tam uygulama sürecinde olan hizmet sağlayıcılar tarafından gerçekleştirilen ihlallerde kullanılabilir.

2.4 [Devletin CAA'sı] SMS yaptırım prosedürlerini bir ihlalin incelenmesinin başlamasından sonra, keyfi olarak bir SMS geliştirme oldukları iddiasında bulunan hizmet sağlayıcılar için geçerli kabul etmeyecektir. Bu prosedürler, nihayetinde SMS düzenlemelerindeki gereksinimleri karşılayacak bir SMS'nin geliştirilmesinde gayretli bir şekilde çaba gösteren ve [Devletin CAA'sı] tarafından yayınlanan tavsiye materyali [AM-xxx] — SMS İçin Uygulama Prosedürleri Kılavuzu'nda çerçevesi çizilene benzeyen bir "aşamalı yaklaşımı" izleyen hizmet sağlayıcılar için kullanılacaktır.

2.5 Hizmet sağlayıcılar bir SMS ortamında çalıştıklarını gösteremediklerinde, yaptırım eylemleri 3. paragrafta açıklanan prosedürlerin avantajları olmadan uygulanacaktır.

3. PROSEDÜRLER

3.1 SMS yaptırım prosedürlerini kullanarak bir inceleme yapılması gerekip gerekmediğini belirlemek için, havacılık yaptırım denetleyicilerinin söz konusu hizmet sağlayıcının SMS uygulama durumunu belirlemesi gerekir. Bu belirleme, başlangıçta denetleyiciler ve incelenen hizmet sağlayıcının denetiminden ve sertifikasyonundan sorumlu olan baş denetleyici arasındaki ilişki aracılığıyla yapılmalıdır.

3.2 Baş denetleyici, hizmet sağlayıcının SMS yaptırım prosedürleri için yukarıda belirtilen ölçütlere uygun olup olmadığını belirler. İlk değerlendirmeyi kolaylaştırmak için, [Devletin CAA'sı] SMS'nin geliştirilmesi ve uygulanması sürecini başlatan hizmet sağlayıcıların bir listesini oluşturmalıdır. Bu listenin havacılık yaptırımları için kullanılması, SMS yaptırımları prosedürlerinin kullanılması ile ilgili karar verirken denetleyicilere yardımcı olacaktır.

3.3 Hizmet sağlayıcının SMS'sinin "aşamalı yaklaşımı" sırasında, belirli koşulların yerine getirilmesi koşuluyla, [Devletin CAA'sı] SMS yaptırım prosedürlerini tamamen uygulanan bir SMS'ye sahip olmayan hizmet sağlayıcılara uygulayacaktır.

3.4 [Devletin CAA'sı] SMS yaptırımı prosedürlerinin uygulanmasından önce en azından aşağıdaki üç koşulun yerine getirilmesini gerektirir:

a) Hizmet sağlayıcı üst yönetim tarafından desteklenen, etkili bir dahili tehlike raporlama programına sahiptir;

b) Hizmet sağlayıcı operasyonlarının büyüklüğü ve karmaşıklığına uygun ve neden olan etkenlerin belirlenmesi ve düzeltici önlemlerin geliştirilmesi için yeterli bir proaktif olay analizi sürecine sahiptir;

c) 3. paragrafta atıfta bulunulan süreçten elde edilen, SDCPS'yi tehlikeye atmayacak şekilde korunan bilgiler istek üzerine söz konusu hizmet sağlayıcıya atanan baş denetleyiciye iletilmelidir.

İhlalin ilk bildirimi

3.5 Havacılık yaptırımı denetleyicileri, bir ihlalin tespit edilen veya olası bir ihlal hakkında bilgi alınan tüm olaylarda bir ön analiz gerçekleştirmelidir.

Ön analiz

3.6 Alınan bilgiler temelinde aşağıdaki sorular dikkate alınmalıdır:

a) Bir SMS'ye göre etkinlikte bulunan bir kişi veya örgütün bir ihlal gerçekleştirmiş olabileceğine inanmak için makul nedenler var mı?

b) Olay bir yaptırım eyleminin düşünülmesini gerektirecek kadar ciddi mi?

c) Yaptırım eylemi için saklanması gerekebilecek, kolay bozulan bir kanıt var mı?

Etkili destek sağlama

3.7 Bu üç soru olumlu olarak yanıtlandığında, baş denetleyici haberdar edilmelidir. Bilgiler olayı ve ihlali belirleyecektir.

3.8 İstendiğinde, havacılık yaptırımı denetleyicileri, yaptırım eylemi uygulanırsa başarılı olacağından emin olmak için ihlale gösterilmesi gereken uygun müdahaleler hakkında tavsiyelerde bulunarak, Sorumlu Müdüre etkili bir destek sağlar. Sorumlu Müdüre verilen destek bozulabilir kanıtların toplanması ve güvenceye alınmasını da içerir.

Bir yaptırım incelemesinin başlatılması

3.9 Bir yaptırım incelemesi, yaptırım denetleyicilerinin değil, sadece baş denetleyicinin isteğine bağlı olarak başlatılmalıdır.

Dokunulmazlık

3.10 Bir SMS altında oluşturulan bir SDCPS'den elde edilen hiçbir bilgi, yaptırım eyleminin temeli olarak kullanılmamalıdır.

Not— SMS yaptırım politikası ve ilgili prosedürler SMS düzenlemelerine göre çalışan, Uluslararası Sivil Havacılık Teşkilatı (ICAO) tarafından belirlenen kılavuz ilkeleri izleyen ve 3. paragraftaki koşulları yerine getiren yabancı havayolu operatörleri için de geçerli olabilir.

— — — — — — — — —

Bölüm 5 Ek 5

BİR SSP UYGULAMA PLANININ GELİŞTİRİLMESİ İLE İLGİLİ KILAVUZ BİLGİLER

1. ARKA PLAN

1.1 Bu ek bir SSP uygulama planının geliştirilmesinde Devletlere kılavuzluk sağlar. Bir SSP uygulama planı, bir Devletin sivil havacılıkta emniyetin yönetilmesi ile ilgili sorumluluklarını yerine getirmesini sağlayan süreçleri, prosedürleri ve araçları sırayla, ilkelere dayanan bir şekilde nasıl uygulamaya koyabileceğini açıklamaktadır.

1.2 Bir SSP'nin uygulanması, Devletin havacılık sisteminin büyüklüğü ve karmaşıklığına uygun olmalıdır ve Devlet içindeki sivil havacılık işlevlerinin bireysel unsurlarından sorumlu çok sayıda otorite arasında koordinasyon gerektirir. Bu kılavuz bilgiler referans amacıyla verilmiştir ve Devletlerin gereksinimlerine uyacak şekilde ayarlanması gerekebilir.

1.3 Bir SSP uygulama planının geliştirilmesi Devletlerin aşağıdakileri yapmasını sağlayacaktır:

a) Devlette emniyetin yönetilmesi için uygulanacak kapsamlı stratejinin formüle edilmesi;

b) SSP'ye göre farklı Devlet havacılık örgütleri tarafından gerçekleştirilen süreçlerin koordine edilmesi;

c) Hizmet sağlayıcının emniyet yönetimi sisteminin (SMS) nasıl çalışacağını belirleyen kontrollerin oluşturulması;

d) hizmet sağlayıcının SMS'sinin işletilmesinin yerleşik kontrollere uygun şekilde gerçekleştirildiğinden emin olunması ve

e) SSP ile hizmet sağlayıcının SMS'sinin işletilmesi arasındaki etkileşimin desteklenmesi.

1.4 Devlet belirli hizmetlerin (örneğin havaalanı hizmetleri, hava navigasyonu hizmetleri) sağlanmasından sorumlu olduğunda, hizmeti veren örgüt bir SMS geliştirmeli ve uygulamalıdır (Bölüm 10 Ek 2'deki SMS uygulama planına bakınız).

Not - Bu ek bağlamında, "hizmet sağlayıcı" havacılık hizmeti sunan tüm örgütleri ifade etmektedir. Bu terim hizmetlerinin sunulması sırasında emniyet risklerine maruz kalan onaylı eğitim örgütlerini, uçak operatörlerini, onaylı bakım örgütlerini, uçak tip tasarımı ve/veya üretiminden sorumlu örgütleri, hava trafik hizmeti sağlayıcılarını ve sertifikalı havaalanlarını kapsar.

2. SSP BOŞLUK ANALİZİ

2.1 Bir SSP uygulama planı geliştirmek için, ICAO SSP çerçevesine göre Devlet içinde mevcut bulunan yapıların ve süreçlerin analizi yapılmalıdır. Bu, Devletin, SSP'nin unsurlarının Devlet içinde bulunup bulunmadıklarını ve olgunluk durumlarını değerlendirmesini sağlayacaktır. Boşluk analizi tamamlandığında ve belgelendiğinde, eksik veya hatalı oldukları belirlenen bileşenler/unsurlar, mevcut olanlarla birlikte SSP uygulama planının temelini oluşturacaktır.

2.2 Gereken SSP bileşenlerinin/unsurlarının geliştirilmesi için, Devletin düzenlemeler, politikalar veya prosedürler oluşturması veya değiştirmesi gerekip gerekmediğinin belirlenmesi için her bir bileşen/unsur değerlendirilmelidir. SSP uygulama planının geliştirilmesinin temelini oluşturan ICAO SSP çerçevesi, aşağıdaki gibi dört bileşen ve on bir unsur içerir:

1. Devletin emniyet politikası ve hedefleri

    1.1 Devlet emniyet mevzuatı çerçevesi
    1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları
    1.3 Kaza ve olay incelemeleri
    1.4 Yaptırım politikası

2. Devletin emniyet riski yönetimi

    2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri
    2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

3. Devlet tarafından emniyetin güvence altına alınması

    3.1 Emniyet denetimi
    3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi
    3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

4. Devlet tarafından emniyetin teşvik edilmesi

    4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.
    4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

3. SSP UYGULAMA PLANI

3.1 SSP uygulama planı, SSP'nin nasıl geliştirileceği ve Devlet emniyet yönetimi etkinliklerine nasıl entegre edileceğini gösteren bir taslaktır. Çabanın potansiyel büyüklüğü düşünüldüğünde, SSP'nin geliştirilmesi ve uygulanmasının altında yatan etkinliklerle ilgili iş yükünün doğru şekilde yönetilmesi önemlidir. ICAO SSP çerçevesinin dört bileşeni ve on bir unsurunun, belirli teslim edilebilen parçaların tamamlanmasını sağlayan sıralı bir şekilde uygulanması önerilir. Sıralı yöntem boşluk analizine ve her bir Devletteki havacılık sisteminin karmaşıklığına ve kapsamına bağlıdır.

3.2 Bir SSP'nin özel amaçlarından biri hizmet sağlayıcılar tarafından SMS'nin uygulanmasını destekleyen bir bağlam oluşturmaktır. Bu nedenle, SSP etkinlikleri kapsamı içinde, dört belirli adım hizmet sağlayıcılar tarafından SMS'nin uygulanmasını destekler. Bunlar Bölüm 11'de ele alınan dört adımdır.

1.DEVLETİN EMNİYET POLİTİKASI VE HEDEFLERİ

1.1 Devlet emniyet mevzuatı çerçevesi

a) Uluslararası ve ulusal standartlara uygun şekilde, Devletin hakimiyet alanı içinde emniyetin yönetimini nasıl sağlayacağını tanımlayan ulusal bir emniyet mevzuatı çerçevesini ve özel düzenlemelerin gözden geçirilmesi, geliştirilmesi ve gerektiğinde yayınlanması.

b) Devletin havacılık örgütlerinin Devlet içindeki emniyetin yönetilmesi ile ilgili belirli etkinliklere koordineli bir şekilde katılmasını ve bu örgütlerin rollerinin, sorumluluklarının ve ilişkilerinin oluşturulmasını sağlamak için Devlet için bir kurul, komite v.s. şeklinde ulusal düzeyde bir grup oluşturulması.

c) Devletle uyumlu ve ilgili kalmalarını sağlamak için, emniyet mevzuatını ve özel düzenlemelerin periyodik olarak gözden geçirilecekleri bir zaman aralığı oluşturulması.

1.2 Devletin emniyet sorumlulukları ve hesap verme sorumlulukları

a) SSP'nin oluşturulması ve sürdürülmesi ile ilgili gereklilikleri, sorumlulukları ve hesap verme sorumlulukların belirlenmesi, tanımlanması ve belgelenmesi. Bu, SSP'nin Devletin emniyet hedeflerini karşılayacak şekilde planlanması, organize edilmesi, geliştirilmesi, sürdürülmesi, kontrolü ve sürekli olarak iyileştirilmesi için yönergeleri de içerir. SSP'nin uygulanması için gereken kaynakların sağlanması hakkında açık bir ifade de içermelidir.

b) Devlet SSP'sinin, *diğerlerinin yanında*, aşağıdaki özelliklere de sahip olması gereken Sorumlu Müdürünün belirlenmesi ve atanması:

1) Devlet adına, SSP'nin uygulanması ve sürdürülmesi için nihai sorumluluk ve hesap verme sorumluluğu;

2) SSP'nin yerini tutması için atanmış Devlet havacılık örgütüyle ilgili insan kaynakları konularında tam yetki;

3) SSP'nin yerini tutması için atanmış Devlet havacılık örgütüyle ilgili önemli mali konularda tam yetki;

4) Hizmet sağlayıcının sertifika yönetimiyle ilgili konularda ilgili nihai yetki ve

5) Devletin havacılıkla ilgili tüm emniyet sorunlarının çözülmesinde nihai sorumluluk.

c) SSP uygulama takımının oluşturulması.

d) Devlet havacılık örgütlerinin farklı yönetim seviyeleri arasında SSP'nin uygulanması ile ilgili her bir görev için gereken zamanın atanması.

e) Tüm personele SSP'ye katılımlarına uygun bir seviyede SSP konseptlerinin tanımlanması.

f) Aşağıdakileri içeren, ama bunlarla sınırlı kalmayan bir Devlet emniyet politikasının geliştirilmesi ve uygulanması:

1) Denetim altındaki tüm havacılık etkinliklerinin en yüksek emniyet performansı seviyesine ulaşmasını sağlamak için stratejiler ve süreçler geliştirmeye ve uygulama taahhüdü;

2) Devlet içinde emniyetin yönetimi için ulusal emniyet mevzuatı çerçevesinin ve geçerli operasyonel düzenlemelerin geliştirilmesi ve yayınlanması.

3) hem emniyetle hem de diğer konularla ilgili olarak, personelinin sorumluluklarını yerine getirmesini sağlamak için Devlet havacılık örgütlerine gerekli kaynakların ayrılması taahhüdü;

4) etkili bir tehlike raporlaması ve iletişimi sistemi aracılığıyla Devlet içinde emniyetin yönetilmesinin teşvik edilmesi;

5) emniyet verileri toplama ve işleme sistemlerinin (SDCPS) korunması için gerekli önlemlerin alınması;

6) emniyet sorunlarının çözülmesinde hizmet sağlayıcılarla etkili bir şekilde etkileşim kurma taahhüdü;

7) Devlet emniyet politikasının açıkça onaylanmış şekilde tüm personele iletilmesi taahhüdü ve

8) bir SMS ortamında hizmet sağlayıcının operasyonlarını yansıtan bir yaptırım politikası.

g) Devlet emniyet politikasının, Devlet havacılık örgütlerinin tüm seviyelerinde anlaşılmasını, uygulanmasını ve dikkate alınmasını sağlamak için gerekli koşulların oluşturulması.

1.3 Kaza ve olay incelemeleri

a) Devlet içinde emniyetin yönetilmesinin teşvik edilmesi amacıyla, tek amacı kazaların ve olayların önlenmesi olan ve suçlama veya yükümlülüklerin dağıtılması olmayan bağımsız bir kaza ve olay inceleme süreci bulunmasını sağlayan mekanizmaların geliştirilmesi ve oluşturulması.

b) Devlet kaza ve olay inceleme kurumunun diğer Devlet havacılık örgütlerinden bağımsızlığını korumak için gerekli düzenlemelerin geliştirilmesi ve oluşturulması.

1.4 Yaptırım politikası

a) Hizmet sağlayıcıların belirli emniyet sapmalarını içeren eylemlerin, dahili olarak, hizmet sağlayıcının emniyet yönetimi sistemi (SMS) bağlamı içinde ve uygun Devlet kurumunu tatmin edecek şekilde ele almasına ve çözmesine izin verilen koşulları ve şartları belirleyen bir yaptırım politikasının geliştirilmesi ve yayınlanması. Yaptırım politikası aynı zamanda, emniyet sapmalarının yerleşik yaptırım prosedürleri aracılığıyla ele alınabileceği koşulları ve şartları da belirlemelidir.

b) Bu politika aynı zamanda, bir SMS altında oluşturulan bir dahili tehlike raporlama sistemi veya uçuş verileri izleme sisteminden elde edilen bilgilerin yaptırım için kullanılmamasını da sağlamalıdır.

1.5 SSP dokümantasyonu

a) SSP'nin oluşturulması ve sürdürülmesi ile ilgili gereklilikleri, sorumlulukları ve hesap verme sorumlulukları belgeleyen bir Devlet emniyet kütüphanesinin geliştirilmesi ve oluşturulması. Emniyet kütüphanesi, gerektiğinde, ulusal emniyet mevzuatı çerçevesi, Devlet emniyet politikası ve hedefleri, SSP gereklilikleri, SSP süreçleri ve prosedürleri, süreçler ve prosedürler için hesap verme sorumlulukları, sorumluluklar ve yetkiler ve SSP ile ilgili olarak Devletin kabul edilebilir emniyet seviyesi (ALoS) ile ilgili SSP dokümantasyonunu korur ve günceller.

Teslim edilebilen parçalar

1. Devlet emniyet mevzuatı çerçevesinin yayınlanması.

2. Devletin emniyetle ilgili sorumlulukları ve hesap verme sorumluluklarının belirlenmesi, belgelenmesi ve yayınlanması.

3. Devlet emniyet ve yaptırım politikalarının Sorumlu Müdür tarafından imzalanması.

4. Devlet emniyet ve yaptırım politikalarının, Devlet havacılık örgütleri içinde denetim altındaki hizmet sağlayıcılar arasında dağıtılması.

5. Bağımsız kaza ve olay inceleme sürecinin mevcut olması.

6. SSP örgüt yapısının mevcut olması.

Kilometre taşları

1. Sorumlu Müdürün belirlenmesi.

2. Önerilen emniyet politikasının taslağının hazırlanması.

3. Emniyetle ilgili sorumluluk ve hesap verme sorumluluğu sıralarının oluşturulması.

4. Önerilen SSP örgüt yapısının onaylanması.

5. SSP süreçleri için bütçenin onaylanması.

Not — Bu ekte önerilen teslim edilebilir parçalar ve kilometre taşları sadece örnektir ve havacılık etkinliklerinde farklı bir kapsam ve karmaşıklık bulunan Devletlerdeki SSP çerçevesinin bileşenlerinin uygulanmasında öngörülebilecek diğer teslim edebilir parçalarla sınırlanmamalıdır.

2. DEVLETİN EMNİYET RİSKİ YÖNETİMİ

2.1 Hizmet sağlayıcının SMS'si için emniyet gereklilikleri

a) Hizmet sağlayıcıların tehlikeleri nasıl tanımlayacağını ve emniyet risklerini nasıl yöneteceğini ve kontrol edeceğini belirleyen kontroller olarak hizmet sağlayıcının SMS'si için gerekliliklerin, özel operasyonel düzenlemelerin ve uygulama politikalarının (SMS düzenleyici çerçevesi, tavsiye niteliğindeki genelgeler v.s.) oluşturulması.

b) Bu gereklilikler hakkında hizmet sağlayıcılara danışmak için bir zaman aralığı oluşturulması.

c) Hizmet sağlayıcılarla uyumlu ve ilgili kalmalarını sağlamak için, gerekliliklerin ve özel düzenlemelerin periyodik olarak gözden geçirilecekleri bir zaman aralığı oluşturulması.

2.2 Hizmet sağlayıcının emniyet performansı üzerinde uzlaşma.

a) Aşağıdakiler temelinde bir hizmet sağlayıcının SMS'nin emniyet performansı üzerinde uzlaşmaya varmak için bir prosedür geliştirilmesi ve oluşturulması:

1) emniyet performansı göstergesi değerleri;

2) emniyet performansı hedef değerleri ve

3) eylem planları.

b) Üzerinde uzlaşılan prosedüre hizmet sağlayıcının emniyet performansını aşağıdakilere uygun olacağının eklenmesi:

1) hizmet sağlayıcının özel operasyonel bağlamların karmaşıklığı ve

2) hizmet sağlayıcının emniyet risklerini ele almak için sahip olduğu kaynakların mevcudiyeti.

c) Emniyet performansı göstergeleri ve emniyet performansı hedeflerinin hizmet sağlayıcıya uygun ve ilgili kalmasını sağlamak için, SMS'nin üzerinde uzlaşılan emniyet performansının periyodik olarak gözden geçirilmesiyle hizmet sağlayıcının SMS'nin emniyet performansının ölçülmesi.

d) Daha düşük seviyeli sonuçların ve farklı hizmet sağlayıcılar arasında en sık karşılaşılan süreçlerin değerlendirilmesi bir yöntem geliştirilmesi.

e) Farklı SMS'ler içinde ölçülebilir performans sonuçlarının belirlenmesi.

Teslim edilebilen parçalar

1. SMS düzenlemelerinin yayınlanması.

2. Hizmet sağlayıcılara dağıtılan SMS uygulama planı ile ilgili kılavuz materyal.

3. Hizmet sağlayıcıların üzerinde uzlaşılan emniyet performansının ilk yıllık değerlendirilmesi.

Kilometre taşları

1. SMS düzenlemelerin hizmet sağlayıcılara gözden geçirmeleri için dağıtılması.

2. SMS kılavuz materyalinin hizmet sağlayıcılara gözden geçirmeleri için dağıtılması.

3. Devlet teknik personelinin tehlikelerin tanımlanması ve emniyet riski yönetimi konularında eğitiminin tamamlanması.

4. Hizmet sağlayıcıların emniyet performansı hakkında uzlaşma prosedürünün tamamlanması.

3. DEVLET EMNİYET GÜVENCESİ

3.1 Emniyet denetimi

a) Hizmet sağlayıcılar tarafından tehlikelerin tanımlanmasının ve emniyet risklerinin yönetilmesinin yerleşik düzenleyici kontrollere göre yapılmasını sağlayacak mekanizmalarının oluşturulması.

b) Emniyet riski kontrollerinin hizmet sağlayıcının SMS'sine entegre edilmesini sağlayan mekanizmaların oluşturulması.

c) Dahili bir SSP denetiminin geliştirilmesi.

3.2 Emniyet verilerinin toplanması, analiz edilmesi ve alışverişi

a) Tehlikelerin ve emniyet risklerinin devlet seviyesinde toplanması, analiz edilmesi ve saklanması için bir yöntem geliştirilmesi ve oluşturulması.

1) zorunlu bir tehlike raporlama sisteminin oluşturulması;

2) gizli bir tehlike raporlama sisteminin oluşturulması;

3) bir Devlet tehlike veritabanı geliştirilmesi;

4) saklanan verilerden bilgi elde etmek için bir mekanizma oluşturulması;

5) tehlikelerin hem toplu olarak Devlet seviyesinde hem de bireysel olarak hizmet sağlayıcılar seviyesinde toplanması için bir yöntem oluşturulması ve

6) Düzeltme eylemi planlarını uygulamak için bir yöntem oluşturulması.

b) Hizmet sağlayıcının tehlikelerin tanımlanması ve emniyet riski yönetimi süreçlerinin yerleşik düzenleme gerekliliklerine uygun olmasının ve emniyet riski kontrollerinin aşağıdakiler dahil olmak, ama bunlarla sınırlı olmamak üzere hizmet sağlayıcının SMS'sine uygun bir şekilde entegre edilmesinin sağlanması:

1) incelemeler;

2) denetimler ve

3) araştırmalar.

c) Uygulama için aşağıdaki sıranın izlenmesi:

1) hizmet sağlayıcının SMS'sine entegre edilen düzenleyici emniyet riski kontrolleri;

2) Hizmet sağlayıcının tehlikelerin tanımlanması ve emniyet riski yönetimi süreçlerinin yerleşik düzenleme gerekliliklerine uygun olmasını sağlayan denetim etkinlikleri ve

3) emniyet riski kontrollerinin hizmet sağlayıcılar tarafından uygulandığının doğrulanmasını sağlayan denetim etkinlikleri.

d) Emniyet ölçümü ile emniyet performansı ölçümünün bir kombinasyonunu bir araya getirerek, kabul edilebilir emniyet seviyesinin (ALoS) oluşturulması:

1) Emniyet ölçümü kaza ve ciddi olay oranları ve düzenlemelere uyum gibi yüksek seviyeli, yüksek sonuçlu olayların veya yüksek seviyeli Devlet işlevlerinin sonuçlarının nicelleştirilmesini içerir.

2) Emniyet performansı ölçümü, kaza oranları ve/veya düzenlemelere uyumun ötesinde bir SSP'nin gerçekçi olarak uygulanıp uygulanmadığının ölçülmesini sağlayan düşük seviyeli, düşük sonuçlu süreçlerin nicelleştirilmesini içerir.

3.3 Daha büyük öneme veya gereksinime sahip alanların denetiminin emniyet verileri temelinde hedeflenmesi

a) Tehlikelerin ve emniyet risklerinin analizi temelinde, incelemelerin, denetimlerin ve araştırmaların önceliklerinin belirlenmesi için prosedürlerin oluşturulması.

Teslim edilebilen parçalar

1. Devlet zorunlu ve gizli tehlike raporlama sisteminin mevcut olması.
2. Emniyet politikası ve hedeflerinin ilk yıllık gözden geçirmesinin yapılması.
3. Yaptırım politikasının ilk yıllık gözden geçirmesinin yapılması.
4. ALoS'un oluşturulması.

Kilometre taşları

1. Verilerin depolanması ve tehlikelerin ve emniyet risklerinin işlenmesinin Devlet seviyesinde gerçekleştirilmesi.
2. Tehlikeler ve emniyet riskleri hakkında bilgilerin hem toplu olarak Devlet seviyesinde hem de bireysel olarak hizmet sağlayıcılar seviyesinde toplanması.

4. DEVLET TARAFINDAN EMNİYETİN TEŞVİK EDİLMESİ

4.1 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması.

a) Dahili eğitim gerekliliklerinin belirlenmesi.

b) Tüm personel için genel eğitimin geliştirilmesi ve verilmesi.

c) Personel için SSP ve SMS'nin önemli bileşenleri hakkında aşağıdakileri içeren bir eğitim programının geliştirilmesi:

   1) işe alma eğitimi/ilk emniyet eğitimi;

   2) Görev başında (OJT) emniyet eğitimi;

   3) tekrarlanan emniyet eğitimi.

d) Eğitimin etkililiğini ölçen bir yöntem geliştirilmesi.

e) Aşağıdakileri içerecek şekilde, emniyetle ilgili konuların dahili olarak iletilmesi için bir yöntem geliştirilmesi:

   1) emniyet politikaları ve prosedürler;

   2) haberler;

   3) bültenler ve

   4) bir web sitesi.

4.2 Harici eğitim, iletişim ve emniyet bilgilerinin dağıtılması

a) Küçük operatörler dahil olmak üzere hizmet sağlayıcılar arasında SMS'nin uygulanmasını desteklemek için iki yönlü bir iletişim olanağının sağlanması.

b) Hizmet sağlayıcılar için SMS uygulama planı ile eğitimin ve kılavuz bilgilerin geliştirilmesi.

c) Aşağıdakileri içerecek şekilde, emniyetle ilgili konuların harici olarak iletilmesi için bir

yöntem geliştirilmesi:

1) emniyet politikaları ve prosedürler;

2) haberler;

3) bültenler ve

4) bir web sitesi.

Teslim edilebilen parçalar

1. Personel için genel emniyet eğitiminin ilk döngüsünün tamamlanması.

2. Teknik personel ve destek personeli için SSP ve SMS'nin önemli bileşenleri ile ilgili eğitim programının tamamlanması.

3. Küçük operatörler dahil olmak üzere hizmet sağlayıcılara dağıtılan SMS kılavuz materyali.

4. Hizmet sağlayıcılar için SMS'nin uygulanması ile ilgili eğitimin ilk döngüsünün tamamlanması.

5. Emniyetle ilgili bilgilerin dahili ve harici olarak iletilmesinin olanaklarının sağlanması.

Kilometre taşları

1. Emniyet denetimi işlevlerini gerçekleştiren teknik personel için minimum bilgi ve deneyim gerekliliklerinin belirlenmesi.

2. SMS ile ilgili kılavuz materyallerinin geliştirilmesi ve yayınlanması.

3. Devlet havacılık örgütleri ve hizmet sağlayıcılar için SMS eğitim programlarının geliştirilmesi.

4. Devlet haber bülteninin geliştirilmesi.

İLAVE A

ICAO KAZA/OLAY VERİLERİ RAPORLAMA (ADREP) SİSTEMİ

Annex 13, *Uçak Kazaları ve Olayları İncelemesi*, belgesine uygun olarak, Devletler 2250 kg'nin üzerinde onaylı maksimum kalkış kütlesine sahip bir uçağın karıştığı uçak kazaları hakkında ICAO'ya bilgi verirler. ICAO ayrıca 5700 kg'nin üzerindeki uçakların karıştığı uçak kazaları hakkında bilgi toplar. Bu raporlama sistemi ADREP olarak bilinir. Devletler belirli verileri önceden belirlenmiş (ve kodlanmış) biçimde ICAO'ya gönderirler. Devletlerden ADREP raporları alındığında, bilgiler kontrol edilir ve elektronik olarak saklanır, böylece dünya çapında olayların bir veri bankası oluşturulur.

CİDDİ OLAY ÖRNEKLERİ LİSTESİ

"Ciddi olay" terimi Annex 13, Bölüm 1'de aşağıdaki şekilde tanımlanmıştır:

Ciddi olay. Neredeyse bir kazanın oluşacağını gösteren koşulları içeren bir olay.

Aşağıda listelenen olaylar, ciddi olay olma olasılığı yüksek olaylardır. Bu liste tüm olayları kapsamamaktadır ve sadece ciddi olay tanımına yardımcı olma amacını taşımaktadır.

- Bir çarpışmayı ve veya güvensiz bir durumu önlemek için kaçınma manevrası gerektiren veya bir kaçınma eyleminin uygun olacağı çarpışmaya yakın durumlar.
- Arazide kontrollü uçuşun çok az farkla önlenmesi.
- Kapalı veya dolu bir pistte, bir taksi yolunda[1] veya atanmamış bir pistte iptal edilen kalkışlar.
- Kapalı veya dolu bir pistten, bir taksi yolundan[1] veya atanmamış bir pistten kalkışlar.
- Kapalı veya dolu bir piste, bir taksi yoluna[1] veya atanmamış bir piste inişler veya iniş denemeleri.
- Kalkış veya ilk tırmanış sırasında beklenen performansının elde edilmemesine neden olan büyük arızalar.
- Yangın söndürme malzemeleri yardımıyla söndürülseler de, yolcu bölmesinde, kargo bölmelerinde yangın ve duman ve motorun alev alması.
- Uçuş ekibinin acil durumda oksijen kullanmasını gerektiren olaylar.
- Yapısal uçak arızaları veya kaza olarak sınıflandırılmayan motorun ayrılması olayları.

1. Onaylı helikopter operasyonları dışında.

— Bir veya daha çok uçak sisteminde uçağın çalışmasını ciddi olarak etkileyen çok sayıda arıza.

— Uçuş sırasında uçuş ekibinin bilincini kaybetmesi.

— Pilot tarafından acil durum bildirimi gerektiren yakıt miktarı.

— A ciddiyet seviyesinde sınıflandırılan piste girişler. *Piste Girişlerin Önlenmesi El Kitabı* (Doc 9870) ciddiyet sınıflandırmaları hakkında bilgi içermektedir.

— Kalkış veya iniş olayları. Kalkış sırasında yeniden piste değerek havalanma, pistin kısa kalması veya pistin yanlarından ilerleme.

— Sistem arızaları, hava durumu olayları, onaylı uçuş süresi dışındaki operasyonlar ve uçağın kontrol edilmesini zorlaştırabilecek diğer olaylar.

— Uçuş kılavuzu veya navigasyonu için zorunlu olarak yedek bulunan bir sistemde birden fazla sistemin arızası.

İLAVE B

ACİL MÜDAHALE PLANLAMASI

1. GİRİŞ

1.1 Belki havacılık kazaları nadir olaylar olduklarından, çok az örgüt bir kaza olmasına hazırdır. Pek çok örgüt bir acil durum veya kriz sırasında veya sonrasında olayları yönetmek için etkili planlara sahip değildir. Bir örgütün bir kazanın veya başka bir acil durumun sonrasında nasıl yol alacağı, önemli bir emniyet olayı sonrasındaki ilk birkaç saat ve günde işleri nasıl idare edeceğine bağlıdır. Bir acil müdahale planlaması bir kaza sonrasında hangi eylemlerin yapılması gerektiğini ve her bir eylemden kimin sorumlu olduğunu yazılı olarak ortaya koyar. Havaalanı operasyonlarında, bu acil müdahale planlamasına havaalanı acil durum planı (AEP) denir. Bu el kitabında, genel terim olan acil müdahale planlaması (ERP) kullanılmıştır.

1.2 Genellikle bir uçak kazasının sonucunda, acil müdahale planlamasını uçak ve havaalanı operasyonları ile ilgili olarak düşünmek normal olsa da, bu kavram diğer hizmet sağlayıcılara da aynı şekilde uygulanabilir. ATS sağlayıcılar söz konusu olduğunda, buna önemli bir güç kesilmesi veya radar, iletişim veya diğer önemli tesislerin kaybı dahil olabilir. Bir bakım örgütü için, hangar yangını veya önemli bir yakıt dökülmesini içerebilir. Bu bağlamda, bir acil durum bir örgüte önemli bir zarar veya rahatsızlık veren bir olay olarak görülebilir.

1.3 İlk bakışta, acil durum planlamasının emniyet yönetimi ile pek ilgisi olmadığı düşünülebilir. Ancak, etkili acil müdahale hasar veya yaralanmaların en aza indirilmesini amaçlayan emniyet derslerinin alınmasını ve uygulanmasını sağlar.

1.4 Bir acil duruma başarılı bir müdahale etkili planlamayla başlar. Bir acil müdahale planı (ERP) önemli bir planlanmayan olaydan, en kötü durumda bir kazadan sonra örgütün işlerinin yönetilmesine sistematik bir yaklaşımın temelini oluşturur.

1.5 Bir acil müdahale planının amacı aşağıdakileri sağlamaktır:

a) normal operasyonlardan acil durum operasyonlarına düzenli ve etkin bir şekilde geçiş;

b) acil durum yetkisinin dağıtılması;

c) acil durum sorumluluklarının atanması;

d) kritik personelin planda bulunan eylemler için yetkilendirilmesi;

e) acil durumla başa çıkma çabalarının koordinasyonu ve

f) operasyonlara emniyetli bir şekilde devam edilmesi veya normal operasyonlara en kısa zamanda dönülmesi.

2. ICAO GEREKLİLİKLERİ

2.1 Uçuş operasyonlarını gerçekleştiren veya destekleyen tüm örgütler bir acil müdahale planına sahip olmalıdır. Örneğin:

a) Annex 14 — *Havaalanları* belgesinde, bir havaalanında uçak operasyonları ve bir havaalanında gerçekleştirilen diğer etkinliklere uygun bir havaalanı acil durum planı oluşturulması gerektiği belirtilir. Plan bir havaalanında veya yakınlarında ortaya çıkan bir acil durum sırasında alınması gereken önlemlerin koordinasyonunu sağlamalıdır.

b) *Bir Operasyon El Kitabının Hazırlanması* (Doc 9376) belgesinde, bir şirketin operasyonlar el kitabında bir kazadan sonra personelin görevleri ve yükümlülükleri hakkında talimatlar ve kılavuz bilgiler bulunması gerektiği belirtilir. El kitabı, kriz yönetiminin odak noktası olan merkezi bir kaza/acil müdahale merkezinin kurulması ve işletilmesi ile ilgili kılavuz bilgileri içermelidir. Şirket uçağının yer aldığı kazalar hakkında kılavuz bilgilere ek olarak, şirketin hizmet acentesi olduğu uçaklardaki (örneğin kod paylaşımı anlaşmaları ve sözleşmeli hizmetler aracılığıyla) kazalar için de kılavuz bilgiler sağlanmalıdır. Daha büyük şirketler, tüm bu acil durum planlama bilgilerini operasyon el kitaplarının ayrı bir cildinde bir araya getirmeyi tercih edebilirler.

c) *Havaalanı Hizmetleri El Kitabı* (Doc 9137), Kısım 7 — *Havaalanı Acil Durum Planlaması* belgesinde, hem havaalanı hem de uçak operatörlerine acil durumlar için önceden planlama yapma ve operatör de dahil olmak üzere farklı havaalanı kuruluşları arasında koordinasyon sağlama konusunda kılavuz bilgiler sunulur.

2.2 Etkili olması için, bir ERP:

a) kaza sırasında görevde olması muhtemel kişiler için ilgili ve yararlı olmalıdır;

b) ilgili personel için kontrol listelerini ve hızlı başvuru için iletişim bilgilerini içerir;

c) tatbikatlarla düzenli olarak test edilmelidir

ve

d) ayrıntılar değiştiğinde güncellenmelidir.

3. ERP İÇERİĞİ

Bir acil müdahale planı (ERP) normal olarak bir el kitabı formatında belgelenir. Acil durumlarla başa çıkmak için çeşitli kuruluşların ve personelin sorumlulukları, rolleri ve eylemlerini belirtmelidir. Bir ERP aşağıdaki gibi konuları hesaba katmalıdır:

a) ***Yürürlükteki politikalar.*** ERP acil durumlara müdahale için, incelemelerle ilgili yürürlükteki yasalar ve düzenlemeler, yerel yetkililerle anlaşmalar, şirket politikaları ve öncelikleriyle olduğu gibi yönlendirme sağlamalıdır.

b) ***Örgüt.*** ERP aşağıdakiler aracılığıyla müdahale eden örgütlere göre yönetimin amaçlarını ifade etmelidir:

1) müdahale eden takımlara kimin atanacağını ve kimin bu takımları yöneteceğini belirleyerek;

2) müdahale takımlarına atanan personelin rollerini ve sorumluluklarını tanımlayarak;

3) raporlama yetkisi sıralarını açıklığa kavuşturarak;

4) bir kriz yönetimi merkezi (CMC) kurarak;

5) özellikle önemli bir kazadan sonraki ilk birkaç gün boyunca, çok sayıda bilgi isteği almak için prosedürleri oluşturarak;

6) medyayla başa çıkmak için kurumsal sözcüyü belirleyerek;

7) acil etkinlikler için mali yetkiler dahil olmak üzere, hangi kaynakların mevcut olacağının tanımlanması;

8) Devlet yetkilileri tarafından başlatılan formel incelemeler için şirket temsilcisinin belirlenmesi; ve

9) Kritik personel için bir çağırma planı tanımlamak v.s.

Örgüt işlevlerini ve iletişim ilişkilerini göstermek için bir örgüt çizelgesi kullanılabilir.

c) ***Bildirimler.*** Plan örgüt içinde kimin bir acil durum konusunda bilgilendirileceğini, harici bildirimleri kimin, ne şekilde yapacağını belirtmelidir. Aşağıdakilerle ilgili bildirim gereksinimleri dikkate alınmalıdır:

1) yönetim;

2) Devlet yetkilileri (arama kurtarma, düzenleyici kurum, kaza inceleme kurulu v.s.);

3) yerel acil müdahale hizmetleri (havaalanı yetkilileri, itfaiye, polis, ambulanslar, tıp kurumları v.s.);

4) kurbanların yakınları (pek çok eyalette polis tarafından üstlenilen hassas bir konudur);

5) şirket personeli;

6) medya ve

7) hukuk, muhasebe birimleri, sigorta kurumları v.s.

d) ***İlk müdahale.*** Koşullara bağlı olarak, yerel kaynakların arttırılması ve örgütün çıkarlarının gözetilmesi için kaza alanına bir ilk müdahale takımı gönderilebilir. Bu tür bir takım için dikkate alınması gereken etkenler şunlardır:

1) İlk müdahale takımını kim yönetmelidir?

2) İlk müdahale takımına kimler katılmalıdır?

3) Kaza alanında örgüt adına kim konuşmalıdır?

4) Özel donanım, giysi, dokümantasyon, nakliye, barınma v.s. bakımlarından neler gerekecektir?

e) ***Ek yardım.*** Uygun eğitim ve deneyime sahip çalışanlar bir örgütün ERP'sinin hazırlanması, uygulanması ve güncellenmesi sırasında yararlı destekler sağlayabilirler. Uzmanlıkları aşağıdakiler gibi görevlerin planlanması ve yürütülmesinde yararlı olabilir:

1) çarpışma tatbikatlarında yolcu rolü oynamak;

2) kazadan kurtulanlarla ilgilenmek;

3) yakın akrabalarla ilgilenmek v.s.

f) ***Kriz yönetim merkezi (CMC).*** Etkinleştirme ölçütleri yerine getirildiğinde, örgüt genel merkezinde bir CMC oluşturulmalıdır. Ek olarak, kaza alanında veya yakınında bir komuta merkezi (CP) oluşturulabilir. ERP aşağıdaki gerekliliklerinin nasıl yerine getirileceğini dikkate almalıdır:

1) personel sayısının belirlenmesi (ilk müdahale dönemi sırasında belki 7 gün 24 saat, haftada 7 gün);

2) iletişim donanımı (telefon, faks, internet v.s.);

3) dokümantasyon gereklilikleri, acil etkinlik kayıtlarının tutulması;

4) ilgili şirket kayıtlarının toplanması;

5) ofis mobilyaları ve sarf malzemeleri
ve

6) referans belgeleri (acil müdahale kontrol listeleri ve prosedürler, şirket el kitapları, havaalanı acil durum planları ve telefon listeleri gibi).

Kriz merkezi hizmetleri için, şirket merkezinden uzaktaki bir krizde operatörün çıkarlarının korunması için bir havayolu veya uzman bir örgütten sözleşmeyle hizmet alınabilir. Şirket personeli normalde bu tür bir sözleşmeli merkeze en kısa zamanda takviye yapacaktır.

g) ***Kayıtlar.*** Örgütün olay ve etkinliklerin kayıtlarını tutması gereksinimine ek olarak, örgütün herhangi bir Devlet inceleme takımına istedikleri bilgileri vermesi de gerekmektedir. ERP araştırmacılara aşağıdaki bilgi türlerini vermelidir:

1) uçak, uçuş ekibi ve operasyon hakkında tüm gerekli bilgiler;

2) iletişim kurulacak noktalar ve olayla ilgisi olan personelin listeleri;

3) olayla ilgili tüm kişilerle yapılan görüşmelere (ve beyanlara) ait notlar.

4) fotoğraf veya diğer kanıtlar.

h) ***Kaza alanı.*** Önemli bir kazadan sonra, örneğin ölümcül durumlarla ilgilenmek için polis, itfaiye, tıbbi yardım personeli, havaalanı yetkilileri, tıbbi tetkikçiler (tıbbi muayene sorumluları) ve Devlet kaza denetleyicileri, Kızıl Haç gibi yardım kuruluşları ve hatta medya gibi pek çok farklı yetki alanından temsilciler alana girmek için haklı sebeplere sahip olacaktır. Bu ilgili tarafların etkinliklerinin koordinasyonu, polisin ve/veya incelemede bulunan kurumun sorumluluğunda olsa da, uçak operatörü kaza alanındaki aşağıdaki etkinlik konularını açıklığa kavuşturmalıdır:

1) aşağıdaki durumlarda bir üst düzey şirket temsilcisi atamak:

— merkezde;
— merkezden uzakta;
— açık denizde veya yabancı bir Devlette.

2) hayatta kalan yolcuların yönetimi;

3) kurbanların yakınlarının gereksinimleri;

4) enkazın emniyeti;

5) cesetlerin ve ölenlerin kişisel eşyalarının taşınması;

6) kanıtların korunması;

7) inceleme yapan yetkililere (gereken şekilde) yardım edilmesi;

8) enkazın temizlenmesi ve atılması v.s.

i) ***Medya.*** Şirketin medyaya nasıl tepki gösterdiği, olaydan ne şekilde çıkacağını etkileyebilir. Açık yönlendirme gereklidir. Örneğin:

1) yasalara göre korunması gereken bilgiler (FDR verileri, CVR ve ATC kayıtları, tanık ifadeleri v.s.);

2) genel merkezde ve kaza alanında üst örgüt adına kimin konuşabileceği (halkla ilişkiler yöneticisi, icra kurulu başkanı veya diğer bir üst yönetici, yönetici, şirket sahibi);

3) medyanın sorularına hemen yanıt verilmesi için hazırlanmış bir ifadeyle ilgili yönlendirme;

4) hangi bilgilerin açıklanabileceği (hangilerinin açıklanmasından kaçınılması gerektiği);

5) şirketin ilk açıklamasının zamanlaması ve içeriği;

6) medya için düzenli güncelleme sağlanması için ayrılan olanaklar.

j) ***Resmi incelemeler.*** Devlet kaza inceleme sorumluları ve polisle karşı karşıya olduklarında ne yapmaları gerektiği konusunda şirket personeli için kılavuz bilgiler sağlanmalıdır.

k) ***Ailelere destek.*** EPR kurbanların (ekip ve yolcular) ailelerine destek olma konusunda örgütün yaklaşımı hakkında da kılavuz bilgiler içermelidir. Bu kılavuz bilgiler aşağıdakileri içerebilir:

1) Aile desteği hizmetlerinin sağlanması konusunda devlet tarafından zorunlu tutulan gereklilikler;

2) kaza yerini veya hayatta kalanları ziyaret etmek için yolculuk ve konaklama düzenlemeleri;

3) her bir aile için program koordinatörü ve iletişim kurulacak nokta(lar);

4) güncel bilgilerin sağlanması;

5) yas danışmanlığı v.s.;

6) kurbanlar ve aileleri için acil mali destek;

7) anma hizmetleri v.s.

Bazı devletler bir operatör tarafından sağlanacak destek tiplerini tanımlamıştır.

l) ***Kritik bir olay sonrası stres danışmanlığı.*** Stresli koşullarda çalışan personel için, ERP kılavuzluk hizmetlerinin, görev sınırlarının belirlenmesini ve olay sonrası stres danışmanlığını içerebilir.

m) ***Olay sonrası gözden geçirme.*** Acil durumdan sonra, kritik personelin tam bir sorgulama yapması ve ERP ve ilgili kontrol listelerinde düzeltmeler yapılmasına neden olabilecek, olay sonrasında alınan önemli dersleri kaydetmesini sağlamak için yönlendirme sağlanmalıdır.

4. UÇAK OPERATÖRÜNÜN SORUMLULUKLARI

4.1 Uçak operatörünün acil müdahale planı (ERP), operatörün personelinin havaalanının hangi sorumlulukları alacağını ve operatörden nasıl bir tepki beklendiğini bilmesi için havaalanı acil durum planı (AEP) ile koordine edilmelidir. Acil müdahale planlamasının bir parçası olarak, havaalanı operatörü ile birlikte uçak operatörlerinden aşağıdakiler beklenir:

a) personeli acil durumlara hazırlamak için eğitim sağlamak;

b) acil durumla ilgili olarak gelen telefonlarla ilgilenilmesi için düzenlemeler yapmak;

c) yaralanmamış kişiler için uygun bir bekleme alanı belirlemek ("karşılama hizmetleri");

d) şirket personelinin görevleri için bir tanım yapmak (örneğin işin başındaki kişi, bekleme alanlarında yolcuları kabul etmek için karşılayıcılar);

e) önemli yolcu bilgilerinin toplanması ve yolcuların gereksinimlerinin karşılanması;

f) acil durum sırasında iki yönlü destek sağlamak için diğer operatörler ve kuruluşlarla düzenlemeler yapmak;

g) aşağıdakileri içeren bir acil durum kiti hazırlamak ve hazır durumda tutmak:

1) gerekii idari sarf malzemeleri (formlar, kağıt, isim etiketleri, bilgisayarlar v.s.) ve

2) kritik telefon numaraları (doktorlar, yerel oteller, dilbilimciler, yemek şirketleri, havayolu taşıma şirketleri v.s.).

4.2 Havaalanında veya yakınında bir kaza durumunda, operatörlerden aşağıdakiler gibi önlemler almaları beklenecektir:

a) uçak operatörünün etkinliklerini koordine etmek için havaalanı komuta merkezine rapor vermek;

b) yerinde destek ve kara kutuların kurtarılması;

c) araştırma görevlilerine uçak parçalarının tanımlanmasında ve tehlikeli parçaların emniyetli hale getirilmesinde yardımcı olmak;

d) yolcular, uçuş ekibi ve uçakta bulunabilecek tehlikeli maddeler hakkında bilgi sağlamak;

e) yaralanmamış kişileri belirlenen bekleme alanı taşımak;

f) yaralanmamış kişilerden yolculuğa devam etmek isteyenler veya konaklama veya başka bir desteğe ihtiyacı olanlar için düzenlemeler yapmak;

g) havaalanı halkla ilişkiler sorumlusu ve polisle koordinasyon halinde medyaya bilgi vermek; ve

h) inceleme kurumunun onayı ardından uçağı (ve/veya enkazı) kaldırmak.

Bu paragraf bir uçak kazasına yönelik olsa da, bazı konseptler havaalanı operatörleri ve hava trafik hizmeti sağlayıcılar tarafından yapılan acil durum planlamaları için de geçerlidir.

5. KONTROL LİSTELERİ

Önemli bir uçak kazasına ilk müdahalede yer alan herkes, bir dereceye kadar sarsıntı yaşayacaktır. Bu nedenle, acil müdahale süreci kontrol listelerinin kullanılmasına dayanır. Bu kontrol listeleri, şirketin operasyon el kitabı veya acil müdahale el kitabının ayrılmaz bir parçasını oluşturabilir. Etkili olmaları için, kontrol listeleri düzenli olarak:

a) gözden geçirilmeli ve güncellenmelidir (örneğin arama listelerinin ve iletişim bilgilerinin geçerliliği) ve

b) gerçekçi tatbikatlarla test edilmelidir.

6. EĞİTİM VE TATBİKATLAR

Bir acil müdahale planı yazılı bir niyet göstergesidir. Umulan, ERP'nin önemli bir kısmının asla gerçek koşullar altında test edilmemesidir. Bu niyetlerin operasyonel kapasiteler ile desteklenmesini sağlamak için eğitim gerekir. Eğitimin "raf ömrü" kısa olduğundan, düzenli denemeler ve tatbikatlar yapılması önerilir. Arama ve iletişim planı gibi ERP'nin bazı kısımları "masaüstü" tatbikatlarıyla test edilebilir. Diğer kuruluşların katılımını içeren "yerinde" etkinlikler gibi diğer konuların düzenli olarak tatbikatının yapılması gerekir. Bu tatbikatlar, plandaki sorunları gösterme avantajına sahiptir, böylece plan gerçek bir acil durumdan önce düzeltilebilir.

İLAVE C

İLGİLİ ICAO KILAVUZ MATERYALLERİ

El Kitapları

Gelişmiş Yüzey Hareketi Yönlendirme ve Kontrol Sistemleri (A-SMGCS) El Kitabı (Doc 9830)

Havaalanı Tasarımı El Kitabı (Doc 9157)

Havaalanı Hizmetleri El Kitabı (Doc 9137)

Uçuşa Elverişlilik El Kitabı (Doc 9760)

Küresel Hava Navigasyonu Planı (Doc 9750)

Küresel Hava Trafik Yönetimi İşletme Konsepti (Doc 9854)

Uçak Bakımı İçin İnsani Etkenler Kılavuz Bilgileri El Kitabı (Doc 9824)

Hava Trafik Yönetimi (ATM) Sistemleri İçin İnsan Faktörleri Kılavuz Bilgileri (Doc 9758)

Emniyet Denetimleri İçin İnsan Faktörleri Kılavuz Bilgileri El Kitabı (Doc 9806)

İnsan Faktörleri Eğitim El Kitabı (Doc 9683)

Hat Operasyonları Emniyet Denetimi (LOSA) (Doc 9803)

Sivil Uçakların Önlenmesi El Kitabı (Doc 9433)

Sivil Uçak Operasyonları İçin Potansiyel Olarak Tehlikeli Olabilecek Askeri Etkinliklerle İlgili Emniyet Önlemleri El Kitabı (Doc 9554)

Uçak Kazaları ve Olayları İnceleme El Kitabı (Doc 9756)
Kısım I — *Örgüt ve Planlama*
Kısım III — *İnceleme*[1]
Kısım IV — *Raporlama*

Buzlanmayı Giderici/Önleyici Operasyonları El Kitabı (Doc 9640)

Tüm Hava Koşullarında Operasyonlar El Kitabı (Doc 9365)

Sivil Havacılık Tıbbı El Kitabı (Doc 8984)

---

1. Hazırlanmaktadır

Operasyonların İncelenmesi, Onaylanması ve Sürekli Gözetimi İçin Prosedürler El Kitabı (Doc 8335)

Telsiz Telefon El Kitabı (Doc 9432)

Minimum Ayrım Mesafesinin Belirlenmesi İçin Hava Alanı Planlaması El Kitabı (Doc 9689)

Hava Trafik Yönetim Sistemi Gereklilikleri El Kitabı (Doc 9882)

Havaalanlarının Sertifikasyonu El Kitabı (Doc 9774)

Hava Navigasyon Sistemin Küresel Performansı El Kitabı (Doc 9883)

ICAO Kuş Çarpması Bilgi Sistemleri (IBIS) El Kitabı (Doc 9332)

FL 290 ve FL 410 Arasında Bu Değerler Dahil Olmak Üzere 300 m (1 000 ft) Azaltılmış Dikey Ayrım Minimumunun Uygulanması El Kitabı (Doc 9574)

Zorunlu İletişim Performansı (RCP) El Kitabı (Doc 9869)

Paralel veya Paralele Yakın Aletli Pistlerde Simultane Operasyonlar (SOIR) El Kitabı (Doc 9643)

Yüzey Hareketi Yönlendirme ve Kontrol Sistemleri (SMGCS) El Kitabı (Doc 9476)

Normal Operasyonlar Emniyet Araştırması (NOSS) (Doc 9910)

Performans Temelli Navigasyon El Kitabı (Doc 9613)

Bir Operasyonlar El Kitabının Hazırlanması (Doc 9376)

Emniyet Denetimi El Kitabı (Doc 9735)

Emniyet Gözetimi El Kitabı (Doc 9734)

SİRKÜLERLER

Hava Trafik Hizmetlerinin Desteklenmesi İçin ADS-B'nin Değerlendirilmesi ve Uygulama İçin Kılavuz Bilgiler (Cir 311)[1]

Hava Alanı Planlama Metodolojisinin Daha Fazla Uygulama İle Desteklenmesi İçin Çarpışma Risk Modellemesi İçin Birleştirilmiş Çerçeve (Cir 319)[1]

Uçak Kazası Kurbanları ve Ailelerine Destek Kılavuz Bilgileri (Cir 285)

Uçak Kazası Alanlarındaki Tehlikeler (Cir 315)

İnsan Faktörleri Derleme No 15 — Kabin Emniyetindeki İnsan Faktörleri (Cir 300)

İnsan Faktörleri Derleme No 16 — Havacılık Emniyetindeki Kültürler Arası Faktörler (Cir 302)

1. Hazırlanmaktadır

İnsan Faktörleri Derleme No 17 — Hava Trafik Kontrolünde Tehdit ve Hata Yönetimi (TEM) (Cir 314)

Yeni Büyük Uçakların Mevcut Havaalanlarında Kullanılması (Cir 305)

Uçak Kazası İncelemeleri İçin Eğitim Kılavuz Bilgileri (Cir 298)

ÇEŞİTLİ

ADREP raporlama (http://www.icao.int/anb/aig/Reporting.html)

— SON —