

Implementacija sustava upravljanja sigurnošću na primjeru odobrene organizacije za osposobljavanje pilota

Dragović, Matej

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:119:378300>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-04-18**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Sveučilište u Zagrebu
Fakultet prometnih znanosti

Matej Dragović

IMPLEMENTACIJA SUSTAVA UPRAVLJANJA SIGURNOSTI
NA PRIMJERU ODOBRENE ORGANIZACIJE ZA
OSPOSOBLJAVANJE PILOTA

DIPLOMSKI RAD

Zagreb, 2019.

Zagreb, 5. travnja 2019.

Zavod: **Zavod za zračni promet**
Predmet: **Sigurnost zračnog prometa**

DIPLOMSKI ZADATAK br. 5316

Pristupnik: **Matej Dragović (0135228166)**
Studij: **Promet**
Smjer: **Zračni promet**

Zadatak: **Implementacija sustava upravljanja sigurnošću na primjeru odobrene organizacije za osposobljavanje pilota**

Opis zadatka:

Opisivanje predmeta istraživanja. Postavljanje svrhe i cilja istraživanja. Prezentacija strukture rada.
Opisati razvojnu kronologiju upravljanja sigurnošću zračnog prometa, analizirati razvojne faze i elaborirati teorije sigurnosti.
Detaljno opisati sustav upravljanja sigurnošću u zračnom prometu.
Analizirati metodologiju planiranja sustava upravljanja sigurnošću u zrakoplovnoj operativi.
Opisati faze i procese implementacije sustava upravljanja sigurnošću na primjeru odobrene organizacije za osposobljavanje pilota.
Sintetizirati rezultate istraživanja i zaključno rezimirati rad.
Specificirati korištenu literaturu i izvore.

Mentor:

Predsjednik povjerenstva za
diplomski ispit:

prof. dr. sc. Sanja Steiner

Sveučilište u Zagrebu
Fakultet prometnih znanosti

Diplomski rad

IMPLEMENTACIJA SUSTAVA UPRAVLJANJA SIGURNOSTI
NA PRIMJERU ODOBRENE ORGANIZACIJE ZA
OSPOSOBLJAVANJE PILOTA

IMPLEMENTATION OF SAFETY MANAGEMENT SYSTEM
ON SAMPLE OF AN APPROVED PILOT TRAINING
ORGANIZATION

Mentor: prof. dr. sc. Sanja Steiner

Student: Matej Dragović 0135228166

Zagreb, 2019

SAŽETAK

Zrakoplovstvo je složena i sigurnosno kritična industrija. Iako je zračni sustav onaj koji ne može uvijek biti u potpunosti bez opasnosti i rizika, krajnji je cilj uvijek eliminacija zrakoplovnih nesreća i ozbiljnih nezgoda. Iz razloga što ne postoji garancija da će ljudske aktivnosti ili sustavi izgrađeni od strane čovjeka biti potpuno oslobođeni operativnih grešaka i njihovih posljedica, sigurnost mora biti dinamična karakteristika zrakoplovnog sustava gdje se rizik sigurnosti mora neprestano umanjivati. Kako bi svaka organizacija koja pruža zrakoplovne usluge ili proizvode mogla upravljati sigurnošću, potrebno je implementirati sustav upravljanja sigurnošću. Takav sustav ima za funkciju da osigurava da svi sigurnosni rizici budu identificirani, procijenjeni i na zadovoljavajući način ublaženi ili ako je to moguće u potpunosti otklonjeni.

KLJUČNE RIJEČI: sigurnost, rizik, opasnosti, sustav upravljanja sigurnošću, implementacija.

Aviation is a complex and safety-critical industry. Although the aviation system is one that cannot be completely free of hazards and associated risks, the final goal is always the elimination of aircraft accidents and/or serious incidents. Because there are no guarantees that human activities or human-built systems will be completely free from operational errors and their consequences, safety has to be a dynamic characteristic of the aviation system where risks to safety need to be constantly mitigated. In order for any organization that provides air services or products to manage security, the implementation of a safety management system is needed. Safety management system has function of ensuring that all safety risks are identified, evaluated, and mitigated or if possible eliminated.

KEYWORDS: safety, risk, hazards, safety management system, implementation.

SADRŽAJ

1. UVOD	1
2. FUNDAMENTI UPRAVLJANJA SIGURNOSTI U ZRAČNOM PROMETU	3
2.1. Evolucija sigurnosti	4
2.2. Ljudi u sustavu organizacije	6
2.3. Model nastanka nesreće	9
2.4. Metode upravljanja sigurnošću	11
2.5. Pogreške i prekršaji.....	13
2.6. Sigurnosna kultura	15
3. SUSTAV UPRAVLJANJA SIGURNOSTI U ZRAČNOM PROMETU.....	20
3.1. Definicija sustava upravljanja sigurnošću	20
3.2. Regulatorni okvir sustava upravljanja sigurnošću	21
3.3. Sustav upravljanja sigurnošću za male organizacije.....	24
3.4. ICAO okvir sustava upravljanja sigurnošću	26
3.5. Politike i ciljevi sigurnosti	27
3.5.1. Opredijeljenost i odgovornost rukovodstva	28
3.5.2. Krajnja odgovornost za sigurnost	29
3.5.3. Imenovanje ključnog osoblja za sigurnost.....	29
3.5.4. Koordinacija planiranja postupaka u slučaju opasnosti	30
3.5.5. Dokumentacija sustava upravljanja sigurnošću	31
3.6. Upravljanje sigurnosnim rizicima.....	32
3.6.1. Identifikacija opasnosti	33
3.6.2. Procjena i ublažavanje sigurnosnih rizika.....	34
3.7. Osiguranje sigurnosti	35
3.7.1. Praćenje i mjerenje performansi sigurnosti.....	36
3.7.2. Upravljanje promjenama.....	36
3.7.3. Kontinuirano unaprjeđenje SMS-a	37
3.8. Promocija sigurnosti	37
3.8.1. Osposobljavanje.....	38
3.8.2. Komunikacija.....	39

4. METODOLOGIJA PLANIRANJA SUSTAVA UPRAVLJANJA SIGURNOSTU U ZRAKOPLOVNOJ OPERATIVI.....	40
4.1. Integracija sustava upravljanja.....	40
4.3. GAP analiza i plan implementacije sustava upravljanja sigurnošću.....	42
4.4. Fazni pristup implementaciji sustava upravljanja sigurnošću.....	43
4.4.1. Prva faza implementacije sustava upravljanja sigurnosti	44
4.4.2. Druga faza implementacije sustava upravljanja sigurnošću	45
4.4.3. Treća faza implementacije sustava upravljanja sigurnosti.....	46
4.4.4. Četvrta faza implementacije sustava upravljanja sigurnošću	47
5. IMPLEMENTACIJA SUSTAVA UPRAVLJANJA SIGURNOSTU NA PRIMJERU ODOBRENE ORGANIZACIJE ZA OSPOSABLJAVANJE PILOTA.....	48
5.1. Odobrena organizacija za osposobljavanje pilota	48
5.2. Sustav upravljanja sigurnošću na primjeru ATO-a	49
Politika sigurnosti odobrene organizacije za osposobljavanje pilota	49
5.2.3.Upravljanje sigurnosnim rizicima u odobrenoj organizaciji za osposobljavanje pilota	55
5.2.4. Osiguranje sigurnosti u odobrenoj organizaciji za osposobljavanje pilota.....	64
5.2.5. Promocija sigurnosti u HZNS-u.....	68
6. ZAKLJUČAK.....	73
LITERATURA	75
POPIS KRATICA.....	77
POPIS SLIKA	79
POPIS TABLICA	80

1.UVOD

Sustav Upravljanja sigurnošću (SMS) zračnog prometa je sustav kojeg je Međunarodna organizacija civilnog zrakoplovstva nametnula za implementaciju u svrhu proaktivnog upravljanja sigurnošću u zračnom prometu. Takav sustav temelji se na mjerenju, praćenju i optimiziranju pokazatelja performansi cjelokupnog sustava i odvijanja procesa unutar organizacije. Sustav upravljanja sigurnošću uspostavlja se na temelju Priručnika o upravljanja sigurnošću razvijenog od strane Međunarodne organizacije civilnog zrakoplovstva (ICAO Safety Management Manual).

Samim pristupanjem Republike Hrvatske Europskoj uniji dovelo je do usvajanja Nacionalnog programa sigurnosti (SSP) od strane Vlade Republike Hrvatske koji se odnosi na implementaciju sustava upravljanja sigurnosti u zrakoplovnu regulativu i operativu u nadležnosti Hrvatske agencije za civilno zrakoplovstvo (HACZ).

Obveza implementacije sustava upravljanja sigurnošću odnosi se na sve sudionike koji pružaju usluge u zračnom prometu pa je sukladno s time potrebno uspostaviti sustav sigurnosnih normativa i programa koji obuhvaćaju nadzor, provjere i kontinuirano unaprjeđenje sigurnosti.

Predmet rada je usmjeren na upravljanje sigurnošću u zračnom prometu s obzirom na povezanost razvoja tehnologije te informatizacije u smislu proaktivnog pristupa upravljanja sigurnosti.

Svrha diplomskog rada odnosi se na metodologiju implementacije sustava upravljanja sigurnošću kao sustava proaktivnog upravljanja sigurnosti u zrakoplovstvu. Proces implementacije prikazuje se kroz četiri faze u odobrenoj organizaciji za osposobljavanje pilota te je cilj dati primjer kako bi takav sustav trebao izgledati s obzirom na standarde i preporuke uspostave sustava upravljanja sigurnosti.

Diplomski rad sastoji se od šest poglavlja:

1. Uvod;

2. Fundamenti upravljanja sigurnošću zračnog prometa – poglavlje koje se odnosi na načine pristupa sigurnosti, evolucije sigurnosti te koncepcije i metode sigurnosti koje proaktivnim pristupom mogu pozitivnu utjecati na sigurnost.
3. Sustav upravljanja sigurnošću u zračnom prometu – poglavlje koje prikazuje integriranu organizaciju sigurnosnog upravljanja te implementaciju sigurnosnog djelovanja u svim procesima djelatnosti organizacije;
4. Metodologija planiranja sustava upravljanja sigurnošću – poglavlje prikazuje integraciju i fazni pristup implementacije sustava upravljanja sigurnošću;
5. Implementacija sustava upravljanja sigurnošću u odobrenoj organizaciji za osposobljavanje pilota – opisan je model upravljanja sigurnosti te elementi sigurnosti unutar same organizacije.
6. Zaključak

2. FUNDAMENTI UPRAVLJANJA SIGURNOSTI ZRAČNOG PROMETA

U samom kontekstu zrakoplovstva, sigurnost je stanje u kojem se rizici povezani sa zrakoplovnim aktivnostima ili u izravnoj potpori djelovanju zrakoplova smanjuju i kontroliraju na prihvatljivoj razini [1].

Zrakoplovna sigurnost je sama po sebi veoma dinamična. Nove sigurnosne opasnosti prijetnje i rizici stalno se pojavljuju s napretkom tehnologije i rastom zračnog prometa te se moraju ublažavati. Sve se dok sigurnosni rizici drže pod odgovarajućom razinom kontrole, sustav koji je otvoren i dinamičan kao zrakoplovstvo još uvijek može biti siguran. Veoma je važno napomenuti da prihvatljive sigurnosne performanse ovise ili su pod utjecajem domaćih i međunarodnih normi kulture [1].

Pojam zrakoplovne sigurnosti može imati različite konotacije poput:

- nulte stope nesreća ili ozbiljnih nezgoda;
- sloboda od opasnosti ili rizika, odnosno onih faktora koji uzrokuju ili bi mogli nanijeti štetu
- odnos prema nesigurnim radnjama i uvjetima zaposlenika (koji održavaju korporativnu kulturu)
- stupanj do kojeg su inherentni rizici u zrakoplovstvu „prihvatljivi“
- postupak prepoznavanja i upravljanja rizikom
- kontrola slučajnog gubitka (osoba i imovine) i
- kontrolu štete na okoliš [1].

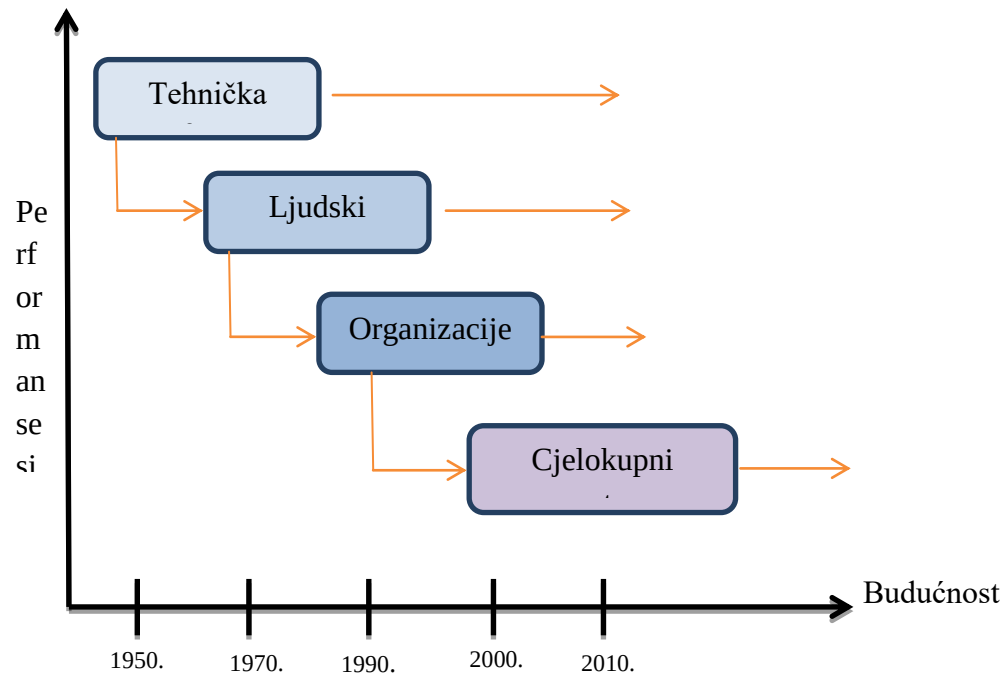
Za razumijevanje ekonomičnosti sigurnosti, potrebno je fundamentalno razumijevanje ukupnih troškova nesreće ili ozbiljnih nezgoda. Iako uklanjanje nesreća ili ozbiljnih nezgoda i dalje ostaje cilj u zrakoplovstvu, stopostotna stopa sigurnosti praktično je nedostižna jer će se pogreške pojaviti usprkos najboljim naporima da ih se izbjegne. Nijedna ljudska aktivnost ili sustav stvoren od čovjeka ne može jamčiti da su apsolutno sigurni ili bez rizika. Stoga je sigurnost relativni pojam u sigurnom sustavu [2].

2.1. Evolucija sigurnosti

Sami napredak u zrakoplovnoj sigurnosti može se opisati kroz četiri faze, koji su otprilike usklađeni s vremenima aktivnosti. Pristupi su navedeni u nastavku te su prikazani na Slici 1.

- a) Tehnička faza – od ranih 1900-ih do kraja 1960-ih zrakoplovstvo se razvija u smjeru masovnog prijevoza u kojem su identificirani sigurnosni nedostaci povezani s tehničkim faktorima i tehnološkim propustima. Stoga su se sigurnosni naponi usredotočili na istraživanje i poboljšanje tehničkih čimbenika odnosno samih zrakoplova i zrakoplovne infrastrukture. Do 1950-ih, tehnološka poboljšanja dovela su do postepenog opadanja u učestalosti nesreća, a sigurnosni procesi proširili su se na obuhvatnost regulatornog usklađivanja i nadzora.
- b) Faza ljudskih faktora – Do ranih 1970-ih učestalost zrakoplovnih nesreća znatno je opala zbog velikog tehnološkog napretka i poboljšanja sigurnosnih propisa. Zrakoplovstvo je postalo sigurniji način prijevoza, a žarište sigurnosnih nastajanja proširilo se i na ljudske čimbenike uključujući stvari poput „interakcije čovjek/stroj“. Unatoč ulaganju resursa u ublažavanje pogrešaka, ljudski se faktori navode kao ponavljajući faktor u nesrećama. Ljudski su se faktori uglavnom usredotočili na pojedinca, bez potpuno razmatranja operativnog i organizacijskog konteksta. Tek je početkom devedesetih bilo priznato da pojedinci posluju u kompleksnom okruženju koje je uključivalo više faktora koji mogu utjecati na ponašanje.
- c) Faza organizacije – Tijekom sredine 1990-ih, sigurnost se počela sagledavati iz systemske perspektive i počela je obuhvaćati organizacijske čimbenike, kao i ljudske i tehničke čimbenike. Pojam „organizirane nesreće“ je uveden. Ta perspektiva razmatrala je utjecaj takvih stvari kao organizacijska kultura i politike učinkovitosti kontrole sigurnosnih rizika. Uz to, rutinsko prikupljanje i analiza sigurnosnih podataka pomoću reaktivnih i proaktivnih metodologija omogućilo je organizacijama praćenje poznatih sigurnosnih rizika i otkrivanje novih trendova sigurnosti. Prethodno navedena poboljšanja osigurala su učenje i temelje koje vode to trenutnog pristupa upravljanja sigurnošću.

- d) Faza cjelokupnog sustava – Od početka 21. Stoljeća mnoge su države i pružatelji usluga prihvatili sigurnosne pristupe iz prošlosti i razvili se na višu razinu sigurnosne zrelosti. Oni su započeli s primjenom SSP-a¹ (State Safety Program) ili SMS-ova² (Safety Management System) i koriste sigurnosne prednosti. Međutim, sigurnosni sustavi do danas su se uglavnom usredotočili na sigurnosne performanse i lokalnu kontrolu, uz minimalni obzir na šiti kontekst cjelokupnog zrakoplovnog sustava. To je dovelo do sve većeg prepoznavanja složenosti zrakoplovnog sustava i različitih organizacija koje sve imaju ulogu u zrakoplovnoj sigurnosti [1].



Slika 1. Faze razvoja sustava upravljanja sigurnošću

Izvor: [1]

¹ State Safety Program

² Safety Management System

2.2. Ljudi u sustavu organizacije

Kako ljudi razmišljaju o svojim odgovornostima prema sigurnosti i kako se odnose s drugima kako bi ih obavljali svoje zadatke u radu značajno utječu na sigurnosne rezultate organizacije. Upravljanje sigurnošću mora se baviti načinom na koji ljudi, pozitivno i negativno doprinose organizacijskog sigurnosti. Ljudski su čimbenici: razumijevanje načina na koje ljudi komuniciraju sa svijetom, njihovih sposobnosti i ograničenja i utjecaj na ljudsku aktivnost radi poboljšanja načina na koji ljude rade svoj posao. Kao rezultat, razmatranje ljudskih čimbenika sastavni je dio upravljanja sigurnošću, neophodnog za razumijevanje, prepoznavanje i ublažavanje rizika kao i za optimizaciju ljudskog doprinosa organizacijskoj sigurnosti [1].

U nastavku su navedeni načini u kojima postupci upravljanja sigurnošću uzimaju u obzir ljudske čimbenike:

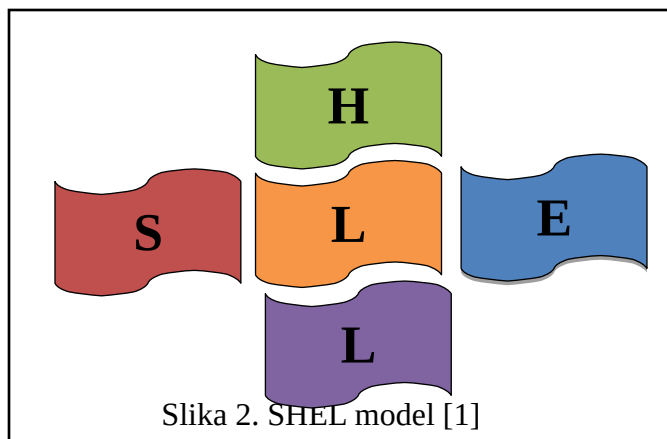
- a) posvećenost višeg rukovodstva stvaranju radnog okruženja koje optimizira radne performanse i ohrabruje osoblje da se aktivno uključe u svoj doprinos organizaciji i doprinosi procesu upravljanja sigurnošću;
- b) odgovornosti osoblja u pogledu upravljanja sigurnošću su razjašnjene kako bi se osiguralo zajedničko razumijevanje i očekivanja;
- c) osoblje pruža informacije od organizacije koja:
 - a. opisuje očekivano ponašanje na poslu u odnosu na organizacijske procese i postupke
 - b. opisuje koje će akcije poduzeti organizacija kao odgovor na pojedinačno ponašanje
- d) razine ljudskih resursa prate kako bi se osiguralo da postoji dovoljno ljudstva za potrebe organizacije;
- e) utvrđuju se politike, procesi i postupci za poticanje izvješćivanja o sigurnosti
- f) podaci o sigurnosti analiziraju se kako bi se omogućilo razmatranje onih rizika koji se odnose na promjene na ljudskog učinka i ograničenja;
- g) kontinuirano nadgledanje normalnih operacija uključuje procjenu jesu li procesi i postupci u skladu s pravilima i ako nisu, provode se istrage kako bi se utvrdio uzrok;

- h) sigurnosne istrage uključuju procjenu doprinosa ljudskih faktora, ne samo ispitivanje ponašanja već i razloga takvog ponašanja (kontekst) s razumijevanjem da u većini slučajeva ljudi daju sve od sebe kako bi dobili posao;
- i) upravljanje procesom promjena uključuje razmatranje evoluirajućih zadataka i uloga čovjeka u sustavu;
- j) osoblje je osposobljeno kako bi se osiguralo kompetentno za obavljanje svojih dužnosti, a i preispituje se učinkovitost obuke, a programi obuke prilagođavaju se promjenjivim potrebama [1].

Kroz povijest stvoren je niz modela pomoću kojih se izvodi procjena ljudskih čimbenika vezanih za sigurnosne performanse. Model SHELL stavlja naglasak na čovjeka i njegovu interakciju s ostalim komponentama i značajkama zrakoplovnog sustava te da se ljudski čimbenici razmatraju kao integrirani dio od SRM-a (*Safety Risk Management*). Prema SHELL modelu, nesreće zahtijevaju udruživanje više faktora gdje je svaki faktor važan ali propust vezan za jedan faktor neće uzrokovati propust u sustavu. Kvarovi opreme ili operativne pogreške nikad nisu uzrok kršenja sigurnosti sustava, već okidači. Kršenja sigurnosnih obrana su odgođena posljedica odluka donesenih na najvišim razinama sustava koji su pasivni dok se ne aktiviraju njihovi učinci ili njihov štetni potencijal zbog određenih operativnih okolnosti. Pod takvim specifičnim okolnostima ljudske greške ili propusti na operativnoj razini djeluju kao okidači latentnih uvjeta te pogoduju kršenju sigurnosti sustava [2].

Slika 2. Prikazuje odnos između čovjeka (u središtu modelu) i radnog mjesta komponente. Model SHELL sadrži satelitske komponente:

- a) *Software* (S) - sadrži postupke, obuku, podršku;
- b) *Hardware* (H) - odnosi se na strojeve i opremu;
- c) *Environment* (E) - radno okruženje u kojem ostatak L-H-S sustava mora funkcionirati;
- d) *Liveware* (L) - odnosi se na čovjeka u radnom mjestu.



Izvor: [1]

U samom središtu modela nalazi se operativno osoblje. Međutim, od svih dimenzija u modelu ova je najmanje predvidljiva i najosjetljivija na učinke unutarnjih (glad, umor, motivacija i sl.) i vanjskih (temperatura, svjetlost, buka). Iako su ljudi veoma prilagodljivi, podložni su znatnim varijacijama u izvedbi. Ljudi nisu standardizirani u istoj mjeri kao *hardware* tako da ni rubovi blokova prikazanih na slici 2. nisu jednostavni i ravni. Ostale komponente modela potrebno je uskladiti s osobljem kako bi se izbjegao stres na radnom mjestu. Model SHELL koristan je za vizualizaciju sljedećih sučelja između različitih komponenti zrakoplovnog sustava:

- a) L–H (*Liveware – Hardware*) – sučelje se odnosi na odnos između ljudskih i fizičkih svojstava opreme, strojeva i objekata. To uzima u obzir ergonomiju rada opreme od strane osoblja, kako se prikazuju sigurnosni podaci i kako se označavaju i funkcioniraju prekidači i ručice za rukovanje tako da su logične i intuitivne za rad
- b) L-S (*Liveware – Software*) – ovo sučelje odnosi se na odnos između čovjeka i sustava podrške na radnom mjestu kao što su propisi, priručnici, kontrolni propisi, publikacije, procese i postupke te računalni softver. Uključuje pitanja kao što su nedavna iskustva, točnost, format i prezentacija, vokabular, jasnoća i upotreba simbola. L-S razmatra procese i postupke odnosno koliko ih je lako slijediti njihovo razumijevanje
- c) L-L (*Liveware - Liveware*) – Navedeno sučelje je odnos i interakcija između ljudi u radnom okruženju. Neke od tih interakcija su unutar organizacije (kolege, nadređeni, menadžeri), a mnoge interakcije su između pojedinaca iz različitih organizacija (kontrolori zračnog prometa s pilotima, piloti s inženjerima itd.). Unutar tih interakcija važnost komunikacije i međuljudskih vještina, kao i grupne dinamike određuje kvalitetu izvedbe [1].

2.3. Model nastanka nesreće

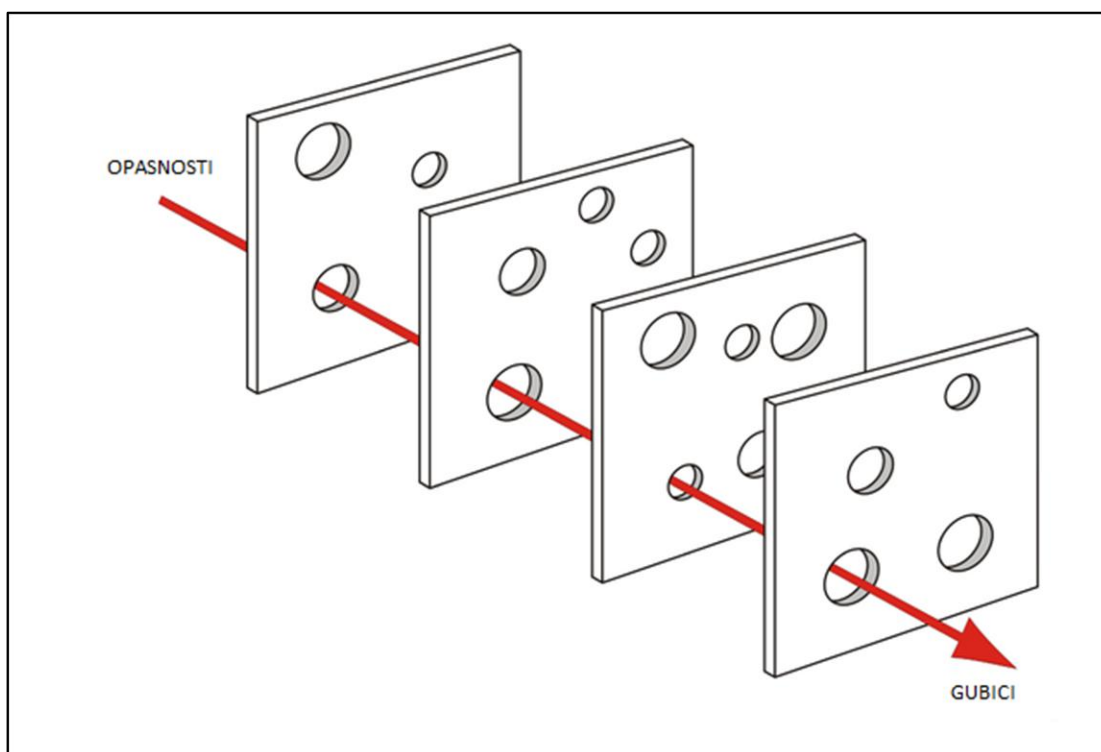
Model „švicarskog sira“ razvijen od strane Jamesa Reasona dobro je poznat u zrakoplovnoj industriji i taj model ilustrira nastanak nesreće kao posljedicu uzastopnih probijanja sustava sigurnosti. Probijanja sustava sigurnosti mogu biti potaknuti nizom faktora kao što su kvarovi opreme ili operativne greške. Model švicarskog sira govori da su složeni sustavi poput zrakoplovstva izuzetno dobro zaštićeni slojevima obrane. Neuspjeh u jednoj djelu sustava rijetko je posljedičan. Probijanja sigurnosnih obrana mogu biti odgođena posljedica odluka donesenih na višim razinama organizacije koje mogu ostati u stanju mirovanja dok se njihovi štetni učinci ne aktiviraju od strane operativnih uvjeta (poznati kao latentni uvjeti). U takvih specifičnim okolnostima, ljudske greške na operativnoj razini djeluju na probijanje završnih slojeva sigurnosne obrane. Reasonov model predlaže da sve nesreće uključuju kombinaciju aktivnih kvarova i latentnih uvjeta.

Aktivni su radnje odnosno zanemarivanja, uključujući pogreške i kršenja pravila, koji imaju neposredan štetni učinak. Aktivni kvarovi povezani su s osobljem koji djeluju u zrakoplovnoj operativi (piloti, kontrolori zračnog prometa, inženjeri za održavanje zrakoplova itd.) i mogu dovesti do šetnog ishoda.

Latentni uvjeti mogu postojati u sustavu i prije šetnog ishoda. Posljedice latentnih uvjeta mogu dugo vremena ostati u mirovanju. U početku se ovi latentni uvjeti ne prikazuju kao šetni ali pod određenim uvjetima mogu postati jasni kada se zaštite obrambenog nivoa probiju. Latentni uvjeti u sustavu mogu uključivati one uvjete koju je stvorila sigurnosna kultura kao što su izbor opreme ili organizacijski plan, nesložnost oko ciljeva organizacije neispravne odluke menadžmenta.

Pojam „organizacijske nesreće“ pomaže identificiranjem ovih latentnih uvjeta na razini cijelog sustava u odnosu na lokalizirane napore u svrhu da se minimiziraju aktivni neuspjesi od strane pojedinaca. Organizacijski donositelji odluka često uravnotežuju ograničene resurse i potencijalne konflikte prioriteta i troškova. Odluke koje svakodnevno donose u velikim organizacijama, u određenim okolnostima mogu nenamjerno dovesti do šetnog ishoda [1].

Slika 3. prikazuje kako Reasonov model „švicarskog sira“ pomaže u razumijevanju interakcija organizacijskih i upravljačkih čimbenika u uzrokovanju nesreća. U zrakoplovni sustav ugrađeno je više obrambenih slojeva radi zaštite od varijacija u ljudskim performansama ili odlukama na svim razinama organizacije. Ali svaki sloj obično ima slabosti prikazane u rupicama „švicarskog sira“. Ponekada se sve slabosti poredaju (na slici prikazane kao rupice) što dovodi do probijanja koji prodire sve sigurnosne barijere i može rezultirati katastrofalnim ishodom [1].



Slika 3. Koncept nastanka nesreće [5]

Izvor: [5]

Model „švicarskog sira“ može se koristiti kao vodič za analizu država i pružatelja usluga ako se pojedinci uključeni u incident ili identificirani rizik omogućili da se ta situacija manifestira. Isto tako, može se primijeniti za vrijeme SRM-a³ (*Safety Risk Management*), sigurnosnog nadzora interne auditi, promjene rukovodstva i istrage sigurnosti. U svakom se slučaju model može koristiti za razmatranje koje su organizacijske obrane sustava efektivne, koje mogu biti probijene o gdje bi sustav mogao imati koristi od dodatnih obrana. Kad se slabosti

³ Safety Risk Management

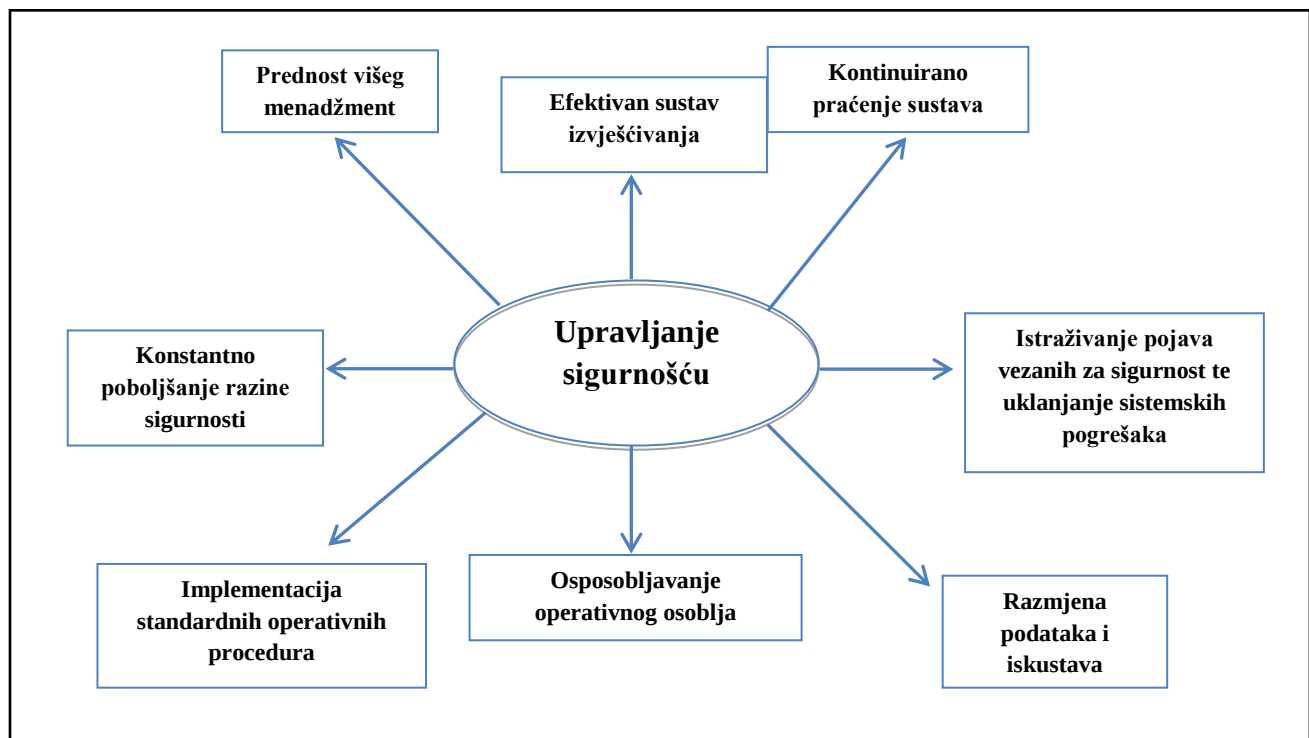
identificiraju one mogu biti pojačane dodatnim mjerama u slučaju prevencije potencijalnih budućih incidenata [1].

2.4. Metode upravljanja sigurnošću

Pojam upravljanja sigurnošću u zrakoplovnoj operativi sastoji se od tradicionalnih i modernih pristupa upravljanja sigurnošću. Postoje tri vrste metoda upravljanja sigurnošću, reaktivna, proaktivna i prediktivna metoda prikazane na Slici 5.

Slika 4. prikazuje elemente upravljanja sigurnošću koji se odnose na organizacijsku strukturu, sustav odgovornosti, politiku i procedure organizacije. Elementi upravljanja sigurnošću su: efektivan sustav izvješćivanja, kontinuirano praćenje sustava, istraživanje pojava vezanih za sigurnost te uklanjanje sistemskih pogrešaka, razmjena podataka i iskustava, osposobljavanje operativnog osoblja, implementacija standardnih operativnih procedura, konstantno poboljšanje razine sigurnosti i prednost višeg menadžmenta.

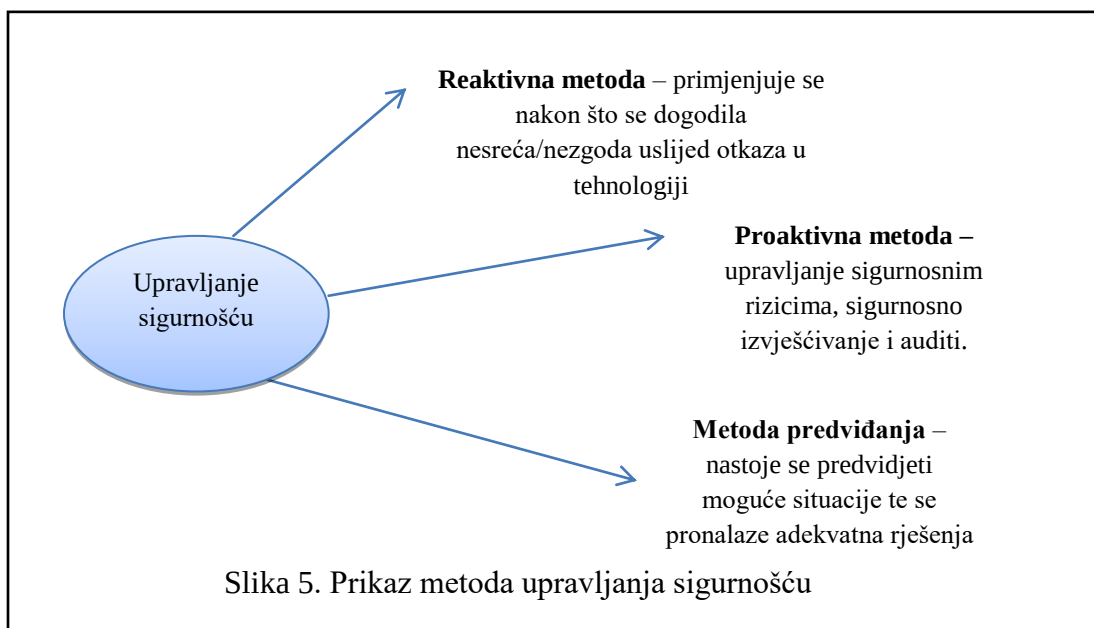
Reaktivni ili tradicionalni pristup odnosi se na događaje uzrokovane tehnološkim kvarovima ili neobičnim događajima. Svojstva koja opisuju tradicionalni pristup upravljanju sigurnošću su udovoljavanje minimalnih sigurnosnih zahtjeva; razina sigurnosti temelji se na prijavljenim sigurnosnim pojavama zajedno s inherentnim ograničenjima, kao što su ispitivanje aktualnih kvarova, nedostatak podataka kako bi se utvrdili sigurnosni trendovi, nedostatak uvida o lancu uzročnih i posljedičnih događaja, te postojanju i ulozi latentnih stanja [3].



Slika 4. Elementi upravljanja sigurnošću

Izvor: [4]

Krajem sedamdesetih godina prošlog stoljeća, kada se broj operacija smanjio do mjere da daljnji napredak poboljšanja nije bio moguć, reaktivni sustav prestao je zadovoljavati. Tada su vodeći operateri pronalazili načine za daljnje poboljšanje sigurnosti koje se temelji na proaktivnom djelovanju. Proaktivna metoda temelji se na strategijama upravljanja sigurnosnim rizicima koji uključuju identifikaciju opasnosti i poduzimanje potrebnih radnji za smanjene sigurnosnih rizika. Strategija proaktivne metode sastoji se od nedvosmislene politike višeg menadžmenta, identifikacije opasnosti i procjenu rizika korištenjem *state-of-the art* metode procjene rizika, sigurnosni sustavi izvješćivanja koji se koriste za prikupljanje, analizu, razmjenu operativnih sigurnosno povezanih podataka, nadležno istraživanje sigurnosnih pojava u svrhu identifikacije sustavnih sigurnosnih nedostataka, sigurnosni nadzor i cilj nadzora te eliminacija problematičnih područja, sigurnosna obuka osoblja, distribucija i razmjena najbolje prakse između operatera i pružatelja usluga, izgradnja korporativne sigurnosne kulture koja potiče dobre sigurnosne prakse i komunikacije. Metoda predviđanja temelji se na sustavnom predviđanju moguće problematike bilježenjem performansi sustava u stvarnom vremenu kroz svakodnevno poslovanje organizacije [4].



Izvor: [4]

2.5. Pogreške i prekršaji

Pogreška se definira kao djelovanje ili neaktivnost operativne osobe koja dovodi do odstupanja od namjera ili očekivanja organizacije. U kontekstu SMS-a, država i pružatelj usluga moraju razumjeti da će ljudi počinuti pogreške bez obzira na razinu korištene tehnologije, razine obrazovanja ili postojećih propisa procesa i postupaka. Iz tog razloga važan cilj je uspostaviti i održavati sustav obrane kako bi se smanjila vjerojatnost pogreške i što je još važnije kako bi smanjio negativni utjecaj pogreške kada se one dogode. Da bi učinkovito izvršili taj zadatak, pogreške moraju biti identificirane, prijavljene i analizirane tako da se mogu poduzeti odgovarajuće korektivne mjere. Pogreške se mogu podijeliti u dvije sljedeće kategorije:

- a) Omaške i propusti su pogreške u izvršavanju namjeravane radnje. Omaške su radnje koje ne idu onako kako smo planirali, a propusti su pogreške nastale zbog zaboravnosti.
- b) Greške su propusti u planu djelovanja što znači da ukoliko je izvršenje plana bilo točno samo izvršenje plana ne bi imalo pozitivan ishod [5].

Sigurnosne strategije moraju biti uspostavljene u svrhu kontrole i otklanjanja pogrešaka. Strategije za kontrolu pogrešaka koriste osnovnu obranu unutar zrakoplovnog sustava a to uključuje sljedeće:

- Strategije redukcije – pružaju izravnu intervenciju za smanjenje ili uklanjanje faktora koji pridonose pogrešci. Primjeri strategije redukcije uključuju poboljšanje ergonomske faktora i smanjenje ometanja okoliša.
- Strategije hvatanja - pretpostavljaju da će doći do pogreške. Namjera je “uhvatiti” pogrešku prije nego što se osjete bilo kakve štetne posljedice pogreške. Strategije hvatanja razlikuju se od strategija redukcije po tome što koriste kontrolne liste i druge proceduralne intervencije, a ne izravno uklanjanje grešaka.
- Strategije tolerancije – odnose se na sposobnost sustava da prihvati pogrešku ali bez doživljavanja ozbiljnih posljedica. Uključivanje suvišnih sustava ili višestruki inspekcijski postupci primjeri su mjera koje povećavaju toleranciju sustava na pogreške.

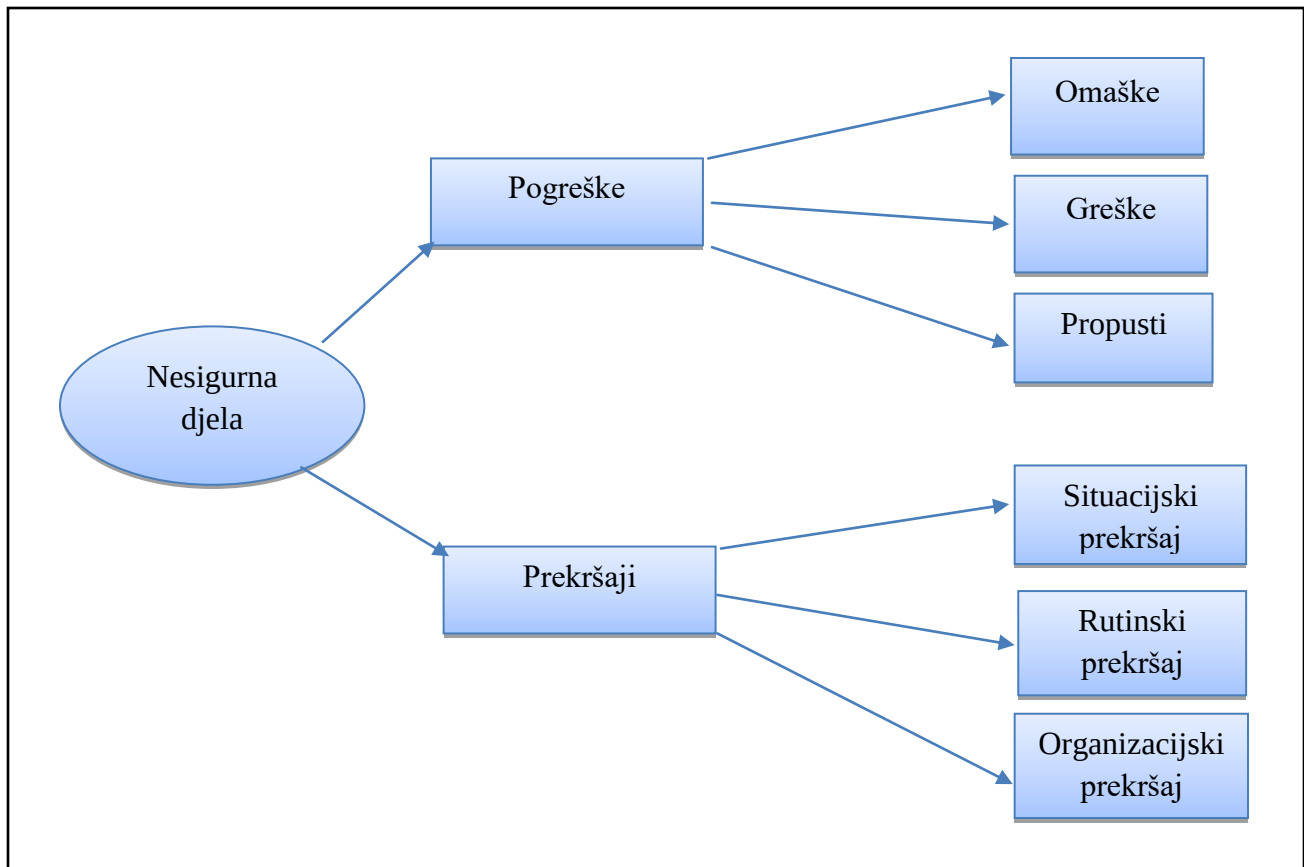
Budući da na rad osoblja općenito utječu organizacijski, regulatorni i okolišni čimbenici, upravljanja rizikom sigurnosti mora uključivati razmatranje organizacijskih politika, procesa i postupaka koji se odnose na komunikaciju, raspoređivanje osoblja, raspodjelu resursa i ograničenja proračuna koja to mogu pridonijeti učestalosti pogrešaka [5].

Prekršaji se definiraju kao “namjerna čin svjesnog kršenja zakona ili propusta koji rezultira odstupanjem od utvrđenih propisa, postupaka, normi ili praksi”. Unatoč tome, neusklađenost nije nužno i rezultat kršenja jer odstupanja od regulatornih zahtjeva ili operativnih postupaka mogu biti rezultat pogreške. Da biste dodatno zakomplicirali problem, iako su kršenja namjerna odnosno svjesna djela, oni nisu uvijek djela zlonamjere. Pojedinci mogu svjesno odstupiti od normi, u uvjerenju da kršenje olakšava ostvarenje zadataka bez stvaranja štetne posljedice. Ovakve povrede predstavljaju pogreške u prosudbi i ne mogu automatski rezultirati disciplinskim mjerama ovisno o važećim politikama. Kršenja ovakve vrste mogu se kategorizirati na sljedeći način:

- Situacijski prekršaji - počinjena su kao odgovor na čimbenike u određenom kontekstu kao što su vremenski pritisak ili veliko radno opterećenje.
- Rutinski prekršaji – ova vrsta prekršaja postaju običajan način poslovanja unutar radne grupe. Takvi prekršaji počinjena su kao odgovor na situacije u kojima ispunjavanje utvrđenih postupaka čine završetak zadataka teškim. To se može dogoditi zbog pitanja

praktičnosti, nedostataka radnih sposobnosti i drugih pitanja zbog kojih osobe usvajaju “uobičajene postupke”, koji s vremenom postaju rutina. U nekim slučajevima rutinske prekršaji su dobro utemeljeni i mogu rezultirati uklapanjem rutine kršenja kao prihvaćeni postupak nakon što je provedena odgovarajuća sigurnosna procjena i ako se pokaže da sigurnost nije ugrožena.

- Organizacijski potaknuti prekršaji – mogu se smatrati produženjem rutinskih prekršaja. Ova vrsta prekršaja obično se događa kada organizacija pokušava udovoljiti povećanim zahtjevima zanemarivanjem i ignoriranjem svojih stanjem sigurnosnih sustava obrane [5].



Slika 6. Klasifikacija nesigurnih djela

Izvor: [1]

2.6. Sigurnosna kultura

Sigurnosna kultura je prirodna posljedica postojanja ljudi u zračnom sustavu. Sigurnosna kultura opisana je kao “kako se ljudi ponašaju u odnosu na rizik kada ih nitko ne gleda“. To je

izraz kako menadžment i zaposlenici u organizaciji shvaćaju, vrednuju i daju prednost sigurnosti, a odražava se u mjeri u kojoj su pojedinci i djelatnost:

- a) svjesni rizika i poznatih opasnosti s kojima se suočava organizacija i njezine aktivnosti;
- b) neprestano odnose prema očuvanju i poboljšanju sigurnosti;
- c) mogućnosti pristupu resursima potrebnim za sigurne operacije;
- d) spremnosti i sposobnosti prilagođavanja kad se suoče s pitanjima sigurnosti;
- e) spremnost na komunikaciju o pitanjima sigurnosti;
- f) dosljedno ocjenjivanje sigurnosnih ponašanja u cijeloj organizaciji [1].

Kultura karakterizira uvjerenja, vrijednosti, pristranosti i njihovo rezultirajuće ponašanje koje dijele članovi društva, grupe ili organizacije. Za upravljanje sigurnošću važno je razumijevanje ovih kulturnih komponenti i interakcija među njima. Tri najutjecajnije vrste kultura su organizacijska, profesionalna i nacionalna kultura. Kultura izvještavanja ključna je sastavnica ovih različitih kultura. Spoj kulturnih komponenti mogu značajno varirati između organizacija i mogu negativno utjecati na učinkovito izvještavanje o opasnostima, analize uzroka događaja i smanjenje rizika. Stalno poboljšanje sigurnosnih performansi moguće je kada sigurnost postaje vrijednost unutar organizacije kao i prioritet na nacionalnoj ili profesionalnoj razini. U nastavku su pojašnjena tri različita oblika kulture pa slijedi:

- Organizacijska kultura odnosi se na karakteristike i percepciju sigurnosti među članovima koji međusobno djeluju unutar određenog entiteta. Organizacijski sustavi vrijednosti uključuju politike prioriteta ili uravnoteženja u odnosu na kvalitetu, sigurnosti u odnosu na učinkovitost, financijske radnje naspram tehničkih.
- Profesionalna kultura razlikuje karakteristike određenih profesionalnih skupina. Kroz odabir osoblja, obrazovanje, obuku, iskustvo na radnom mjestu i pritisak vršnjaka i sl. profesionalci imaju tendenciju da usvoje sustav vrijednosti i razvijaju obrasce ponašanja u skladu sa svojim vršnjacima i prethodnicima. Učinkovita profesionalna kultura odražava sposobnost profesionalnih skupina da razlikuju pitanja sigurnosti u radu od ugovornih i ili industrijskih pitanja. Zdrava profesionalna kultura može se okarakterizirati

kao sposobnost svih profesionalnih grupa unutar organizacije za zajedničko rješavanje problema sigurnosti.

- Nacionalna kultura razlikuje karakteristike pojedinih naroda, uključujući ulogu pojedinaca unutar društva, način raspodjele vlasti i nacionalni prioriteti u pogledu resursa, odgovornosti, morala, ciljeva i različitih pravnih sustava. Iz perspektive upravljanja sigurnošću, na nacionalnoj razini kultura igra značajnu ulogu u određivanju politike provedbe propisa, uključujući odnos između osoblja regulatornog tijela i osoblja u industriji i stupanja zaštite podataka u vezi sa sigurnošću [5].

Uspjeh sustava izvješćivanja u potpunosti ovisi o neprekidnom protoku informacija od organizacija i pojedinaca kao i o njihovim povratnim informacijama. Zaštita sigurnosnih podataka i povezani izvori ključna je za osiguravanje stalne dostupnosti informacija. Na primjer, u dobrovoljnim sustavima prijavljivanja sigurnosti to se može realizirati putem povjerljivog sustava u svrhu održavanja ili poboljšanja sigurnosti. Prednosti su dvostruke. Često je osoblje najbliže sigurnosnim opasnostima pa dobrovoljni sustav prijavljivanja omogućava njihovo aktivno prepoznavanje tih opasnosti i predlaganje mogućih rješenja. Istovremeno, uprava može prikupiti važne sigurnosne informacije i graditi povjerenje s organizacijama ili operativnim osobljem koje informacije prijavljuju [1].

Jesu li organizacije ili pojedinci unutar iste spremni prijaviti svoje iskustvo i pogreške u velikoj mjeri ovisi o uočenim prednostima i nedostacima povezanim s izvještavanjem. Sustavi izvješćivanja o sigurnosti mogu biti anonimni ili povjerljivi. U anonimnom sustavu prijavljivanja osoba koja prijavljuje ne odaje svoje identitet. Zbog takve vrste prijave ne postoji mogućnosti za dodatna pojašnjenja sadržaja izvješća niti mogućnosti davanja povratnih informacija. U povjerljivom sustavu prijavljivanja, svi identifikacijski podaci osobe koja je prijavila događaj poznati su samo imenovanoj osobi. Ako su organizacije i pojedinci koji prijavljuju sigurnosna pitanja zaštićeni i postupaju na pošten i dosljedan način, vjerojatnije je da će prijavljivati takve informacije i surađivati s upravom radi učinkovitog upravljanja sigurnosnim rizikom [1].

Od država se očekuje da usvoje zakone koji će se pridržavati odredbu Dodatka 19 za zaštitu sigurnosnih podataka. U slučaju dobrovoljnog sustava izvješćivanja, treba osigurati povjerljivost i sustav izvješćivanja mora raditi u skladu sa zakonima o sigurnosti. Nadalje, organizacije trebaju imati odgovarajuću disciplinsku politiku koja je dostupna svima i široko

razumljiva. Disciplinska politika trebala bi jasno naznačiti koja se ponašanja smatraju neprihvatljivima i kako će organizacija reagirati u takvim slučajevima. Disciplinsku politiku treba primjenjivati pravedno, razumno i dosljedno. Organizacije i pojedinci moraju vjerovati da će im biti pružena podrška u izvješćivanju interesa sigurnosti. Povećanje povjerljivih izvještaja i smanjenje anonimnih izvještaja obično ukazuje na napredak organizacije ka pozitivnoj sigurnosnoj kulturi [1].

Način na koji se sigurnosne vrijednosti uključuju u praksu menadžmenta i osoblja izravno utječu na to koliko su ključni uspostava i održavanje elemenata SSP-a i SMS-a. Kao posljedica toga, sigurnosna kultura ima izravan utjecaj na sigurnosne performanse. Ako netko vjeruje da sigurnost nije toliko bitna, tada nesigurne odluke, nestručnost, zabušavanje mogu biti rezultat, posebno kada se rizik percipira kao nizak i nema očigledne posljedice ili opasnosti. Sigurnosna kultura organizacije značajno utječe na to kako se njihov SSP i SMS razvija i koliko postaje učinkovit. Kultura sigurnosti je vjerojatno najznačajniji utjecaj na upravljanje sigurnošću. Ako je organizacija postavila sve zahtjeve upravljanja sigurnošću ali pri tome nema pozitivne kulture sigurnosti velika je vjerojatnost da će organizacija podbaciti [1].

Pozitivna kultura temelji se na visokom stupnju povjerenja i poštovanja između osoblja i uprave. Potrebno je uložiti trud i vrijeme da se izgradi pozitivna kultura sigurnosti koja se lako može oštetiti odlukama rukovodstva. Kad rukovodstvo aktivno podupire sigurne prakse, to postaje normalan način postupanja. Idealna situacija je potpuno implementiran i učinkovit SSP/SMS i pozitivna sigurnosna kultura. Stoga se sigurnosna kultura organizacije često gleda kao odraz zrelosti SSP-a/SMS-a. Učinkovito upravljanje sigurnošću omogućava pozitivnu sigurnosnu kulturu i pozitivna kultura sigurnosti omogućava učinkovito upravljanje sigurnošću.

Pozitivna sigurnosna kultura ima sljedeće značajke:

- a) menadžeri i zaposlenici, pojedinačno i zajedno žele donositi odluke i poduzimati takve radnje koje promoviraju sigurnost;
- b) pojedinci i skupine kontinuirano kritiziraju svoje ponašanje i procese i pozdravljaju kritiku drugih kako se mijenja njihovo okruženje;
- c) uprava i osoblje dijele zajedničku svijest o opasnostima i rizicima s kojima se organizacija suočava te o potrebi upravljanja rizika;

- d) pojedinci djeluju i donose odluke u skladu s uvjerenjem da je sigurnost dio njihovog načina na koji posluju;
- e) pojedinci cijene informiranost i informiranje drugih o sigurnosti;
- f) pojedinci vjeruju svojim kolegama i menadžerima s informacijama i iskustvima, a izvještavanje o pogreškama ih potiče kako bi se poboljšala sigurnost [1].

3. SUSTAV UPRAVLJANJA SIGURNOSTU U ZRAČNOM PROMETU

3.1. Definicija sustava upravljanja sigurnošću

Sustav upravljanja sigurnošću predstavlja integriranu organizaciju sigurnosnog upravljanja te implementaciju sigurnosnog djelovanja u svim procesima djelatnosti organizacije. Za potrebe suvremenog upravljanja sigurnošću prihvaćena je definicija Međunarodne organizacije civilnog zrakoplovstva (ICAO)⁴.

Sustav upravljanja sigurnošću je sustavan pristup upravljanja sigurnošću, koji uključuje odgovarajuću organizacijske strukture, sustav odgovornosti, politike i postupke [6].

Sustav upravljanja sigurnošću je sustav kojom se osigurava siguran rad zrakoplova kroz učinkovito upravljanja sigurnosnim rizicima. Takav sustav je dizajniran za kontinuirano poboljšavanje sigurnosti prepoznavanjem opasnosti, prikupljanjem i analizom podataka i kontinuiranom procjenom sigurnosnih rizika. SMS želi proaktivno obuzdati ili ublažiti rizike prije nego što oni dovedu do zrakoplovnih nesreća ili incidenata [5].

Prema definiciji ESARR⁵, sustav upravljanja sigurnošću je sustav koji osigurava formalizirani, eksplicitni i proaktivni pristup sustavnom upravljanju sigurnošću radi ispunjavanja sigurnosnih odgovornosti u okviru pružanja usluge [7].

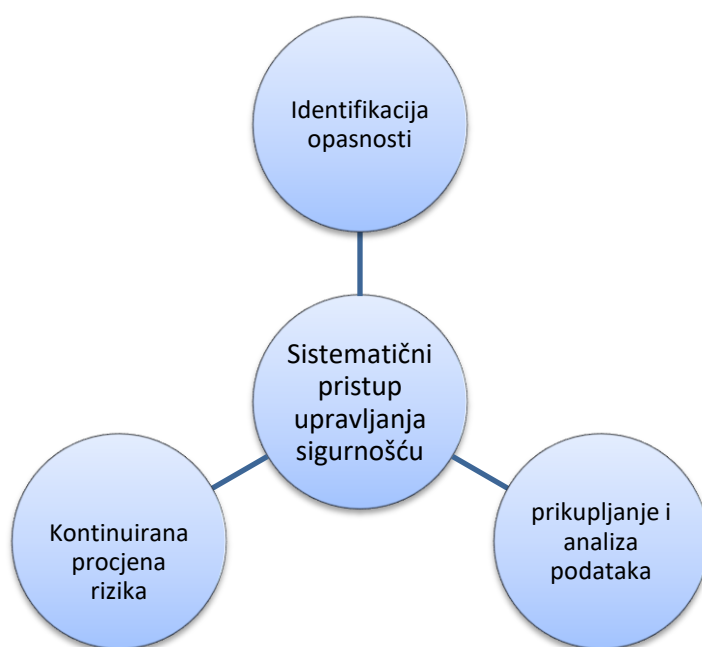
Sustav upravljanja sigurnošću potreban je zrakoplovnim organizacijama da prepozna opasnosti i kako upravljati rizicima tijekom isporuke svojih usluga ili proizvoda. SMS sadrži ključne elemente koji su bitni za prepoznavanje opasnosti i upravljanje sigurnosnim rizikom osiguravajući da:

- a) da su potrebne informacije dostupne;
- b) da su dostupni odgovarajući alati za uporabu organizacije;
- c) da alati odgovaraju određenom zadatku
- d) da su alati razmjerni potrebama i ograničenjima organizacije; i
- e) da se odluke donose na temelju potpunog razmatranja sigurnosnog rizika [5].

⁴ International Civil Aviation Organization

⁵ EUROCONTROL Safety Regulatory Requirement

Svrha SMS-a je pružateljima usluga pružiti sistematični pristup upravljanju sigurnošću (Slika 7.). Osmišljen je za kontinuirano poboljšavanje sigurnosnih performansi kroz identifikaciju opasnosti, prikupljanje i analizu podataka, te kontinuiranu procjenu sigurnosnih rizika. SMS želi proaktivno ublažiti sigurnosne rizike prije nego što rezultiraju zrakoplovnim nesrećama ili nezgodama. Također, omogućuje pružateljima usluga učinkovito upravljanje svojim aktivnostima, sigurnosnim performansama i resursima, istodobno stječući bolje razumijevanje njihovog doprinosa zrakoplovnoj sigurnosti. Učinkovit SMS državama pruža mogućnost pružatelja usluga za upravljanje sigurnosnim rizicima i osigurava učinkovito upravljanje sigurnošću na državnoj razini.



Slika 7. Sistematični pristup upravljanja sigurnošću

Izvor: [1]

3.2. Regulatorni okvir sustava upravljanja sigurnošću

Konvencijom o međunarodnom civilnom zrakoplovstvu (Čikaška konvencija) osnovana je Međunarodna organizacija civilnog zrakoplovstva koja koordinira i regulira međunarodne zračne plovidbe.

Prilozi (*Annex*) Međunarodne organizacija za civilno zrakoplovstvo pružaju standarde i preporučene prakse (SARP)⁶ koje primjenjuju ili usvajaju nacionalna zrakoplovna tijela države kao propise ili najbolje prakse u civilnom zrakoplovstvu. Iako su države potpisnice dužne regulirati zrakoplovstvo u skladu s ICAO SARP-ovima za civilno zrakoplovstvo, vojne zrakoplovne vlasti također usklađuju svoje propise. ICAO Dodatak 19, prvi put je objavljen u srpnju 2013. posvećen je upravljanju sigurnošću i održavanju Nacionalnog plana sigurnosti (SSP) od strane država, kao i za pružanje sustava upravljanja sigurnošću (SMS) od strane odgovarajućih pružatelja usluga koji su uključeni u razne usluge i industrije u zračnom prometu. Odredbe prvog izdanja Dodatka 19. razvijene su u skladu s preporukama koje je dao generalni direktor konferencije civilnog zrakoplovstva o Globalnoj strategiji za sigurnost zrakoplovstva (Montreal, 2006.) i na Konferenciji o sigurnosti (Montreal, 2010.) u vezi s potrebom Dodatka 19. posvećenom upravljanju sigurnošću. ICAO prepoznaje da je učinkovita primjena SMS-a od strane pružatelja usluga postupan proces i ovisi o složenosti zračnog prometa i stupnju zrelosti nadzora svake države. Stupanj i način provedbe ICAO Dodatka 19 razlikuju je u svakoj državi. U skladu s ICAO-ovim Dodatkom 19., države su dužne osigurati da sljedeći pružatelji usluga u zračnom prometu implementiraju SMS unutar svojih organizacija:

- a) odobrene organizacije za obuku koje djeluju u skladu s Dodatkom 1.
- b) operateri zrakoplova ili helikoptera ovlaštene za obavljanje međunarodnog komercijalnog zračnog prometa u skladu s Dodatkom 6.
- c) odobrene organizacije za održavanje koje pružaju usluge operatorima aviona ili helikoptera koji sudjeluju u međunarodnom prometu u skladu s Dodatkom 6.
- d) organizacije odgovorne za projektiranje ili proizvodnju zrakoplova, motora ili propelera u skladu s Dodatkom 8.
- e) pružatelji usluga zračnog prometa (ATS)⁷ u skladu s Dodatkom 11.
- f) operatori certificiranih aerodroma u skladu s Dodatkom 14 [8].

Na području Europe djeluje EASA⁸, agencija koja je osnovana 2002.-e godine uredbom Europskog parlamenta i Vijeća. Preuzela je odgovornost od Zajedničkih zrakoplovnih vlasti,

⁶ Standards and Recommended Practices

⁷ Air Traffic Services

⁸ European Aviation Safety Agency

JAA⁹ 2009. godine, a cilj joj je osiguranje visoke razine sigurnosti u civilnom zrakoplovstvu provođenjem zajedničkih sigurnosnih pravila i mjera [9].

Europski program za sigurnost u zračnom prometu (EASP)¹⁰ sastoji se od integriranog skupa pravila na razini Unije, zajedno s aktivnostima i postupcima za zajedničko upravljanje sigurnošću civilnog zrakoplovstva na europskoj razini. Potrebno je naglasiti kako to nije plan aktivnosti, nego na razini EU-a funkcionalno odgovara nacionalnom programu sigurnosti kako je opisan u Dodatku 19. Čikaškoj konvenciji. U dokumentu o Europskom programu za sigurnost u zračnom prometu objašnjava se kako se upravlja sigurnošću u EU-u i njegovim državama članicama, uključujući upravljanje pomoću zakonodavstva Unije kao i drugih politika, praksi i aktivnosti. [10]

Svrha dokumenta o Europskom programu za sigurnost u zračnom prometu nije zamjena dokumenata o programima sigurnosti država članica, nego njihova dopuna. Budući da se mnogo pravila i aktivnosti povezanih sa sigurnošću u zračnom prometu donosi i koordinira na razini EU-a, države članice trebale bi se u svojim dokumentima o nacionalnim programima sigurnosti pozivati na dokument o Europskom programu za sigurnost u zračnom prometu kako bi potpuno objasnile kako se unutar njihovih državnih područja upravlja sigurnošću u zračnom prometu, kako se od njih zahtijeva Čikaškom konvencijom. Naime, budući da je EU¹¹ donio propise u mnogim područjima sigurnosti u zračnom prometu, države članice ne mogu opisati kako upravljaju sigurnošću, a da ne obuhvate i dimenziju EU-a. [10]

EASA i zrakoplovna industrija usko surađuju u procesu upravljanja sigurnosnim rizicima, odnosno identifikaciji rizika, procjeni rizika i odlučivanju o najboljem načinu djelovanja kako bi se ublažili ti rizici. Na temelju toga razvijen je Europski plan sigurnost zračnog prometa. (EPAS)¹² [11]

Peto izdanje EPASA-a obuhvaća petogodišnje razdoblje između 2016. i 2020. Godine i sada je sastavni dio programskih aktivnosti EASA-e. To znači da se sigurnosnim prioritetima utvrđenim u EPAS-u adresiraju posebnim radnjama u programima promicanja propisa ili

⁹ Joint Aviation Authorities

¹⁰ European Aviation Safety Programme

¹¹ European Union

¹² European Plan for Aviation Safety

promocije sigurnosti EASE-e, posebnim radnjama vezanim za program nacionalne sigurnosti (SSP). Također, pojačan je naglasak na korištenje promocije sigurnosti i usmjerenje nadzornih aktivnosti za ublažavanje sigurnosnih rizika. [11]

Glavni cilj EPAS-a je stvoriti zajednički fokus na europska pitanja zrakoplovne sigurnosti kao što su nastavak na radu povećanja zrakoplovne sigurnosti te izjednačavanje s ICAO standardima. Navedeni pristup poboljšava posvećenost trenutačnim inicijativama i istovremeno doprinosi izbjegavanju preklapanju sigurnosnih inicijativa. [11]

3.3. Sustav upravljanja sigurnošću za male organizacije

SMS je organizirani pristup upravljanja sigurnošću koji uključuje odgovarajuću organizacijsku strukturu, sustav odgovornosti, politiku i procedure.

Važno je prepoznati da je SMS sustav koji se uspostavlja „od vrha prema dolje“, što znači da je rukovoditelj organizacije odgovoran za implementaciju i kontinuirano udovoljavanje zahtjevima SMS-a. SMS neće biti efektivan bez pune potpore odgovornog rukovoditelja. Ne postoji jedan SMS model koji pristaje svim tipovima i veličinama organizacija pružatelja usluga. Složeni SMS sustavi u većini slučajeva nisu odgovarajući za male pružatelje usluga, te bi takve organizacije trebale prilagoditi SMS veličini, prirodi i kompleksnosti svojih aktivnosti i u skladu s tim osigurati potrebne resurse [12].

Uvođenje sustava za upravljanje sigurnošću u zrakoplovstvu donosi posebne izazove za male organizacije. Određene male organizacije mogu imati percepciju da je implementacija sustava upravljanja sigurnošću presložena ili preskupa. Pod pojmom male organizacije smatra se organizacija koja ima od pet do dvadeset zaposlenika, a organizacije s manje od pet zaposlenih smatraju se vrlo malim organizacijama iako nadležne vlasti neće definirati takve organizacije na taj način. SMS se može svesti na vrlo jednostavan koncept:

- aktivno traženje sigurnosnih problema u operacijama, proizvoda ili usluga ovisno o vrsti organizacije;
- razvijanje popravkih radnji za smanjivanje rizika koji predstavljaju ti sigurnosni problemi i;
- nadgledanje kontrole rizika [13].

Veličina organizacije nije jedina stavka prema kojoj joj njezina složenost već se u obzir uzima rizik i složenost aktivnosti kojima se sama organizacija bavi odnosno sudjeluje. Nadalje, složenost organizacije se prikazuje prema:

- operativnom okruženju (planinski teren, arktičke operacije, prekomorske operacije, itd.);
- tip operacija (putnički prijevoz, prijevoz robe, radovi iz zraka, hitne medicinske usluge, itd.);
- kompleksnost flote odnosno broj i vrste zrakoplova;
- broj mjesta s kojih se vrše operacije;
- organizacije za održavanje (broj ovlaštenja, vrste ovlaštenja za proizvod), specijalizirani poslovi i sl.);
- vrste proizvoda i dijelova koji se dizajniraju ili proizvode;
- broj operacija zrakoplova (aerodromi i pružatelji usluga u zračnoj plovidbi);
- okolni teren i razine opremljenosti aerodroma;
- gustoća i složenost prometa za pružatelje usluga u zračnoj plovidbi;
- opseg ugovorenih aktivnosti; i
- broj uzletno-sletnih staza i staza za voženje na aerodromima.[13]

Proces implementacije sustava upravljanja sigurnošću u maloj organizaciji može se izvoditi uz pomoć vodiča izrađenog od strane SM ICG-a¹³. Vodič se sastoji od četiri koraka a oni su: analiza nedostataka, dizajn i razvoj, uvod i pokretanje i poboljšanje i mjerenje učinkovitosti [13].

Prvi korak je vidjeti kako izgleda idealni SMS, a zato to treba gledati kroz organizaciju u kojoj se provodi implementacija i razmotriti kako to primijeniti. Veoma je važno proučavanje smjernica za implementaciju te analizu nedostataka organizacije ako je ona dostupna. Pomoću navedene analize potrebno je identificirati koje elemente sustava organizacija već ima uspostavljene te koje elemente je potrebno uspostaviti. Nadležno tijelo države u kojoj se uspostavlja sustav upravljanja sigurnošću može pružiti primjer analize nedostataka [13].

Drugi korak se odnosi dizajn i razvoj odnosno potrebno je osmisliti plan implementacije SMS-a. Nakon što je prethodno napravljena analiza nedostataka potrebno je elemente koji su

¹³ Safety Management International Collaboration Group

usklađeni ili nedostaju istaknuti u implementacijskom planu. Dokumentacije sustav upravljanja sigurnošću je bitna stavka ovog koraka te je potrebno dokumentirati procese i aktivnosti koje se provode, i one koje organizacija planira uvesti. Razuman pristup je dodati SMS procese i aktivnosti u dokumentaciju koju organizacije već ima, kao što je to operativni priručnik [13].

Korak tri odnosi se na uvod i pokretanje SMS-a te uključivanje zaposlenika u svrhu izrađivanja što boljeg sustava. Potrebno je osigurati da je osoblje uključeno i da razumije što nadležna osoba za implementaciju želi postići. Jasna politika sigurnosti i opredijeljenost uprave ka sigurnosti najbolji je način za početak. Dobra kultura sigurnosti se razvija i njeguje otvorenim razgovorom odgovorne osobe sa zaposlenicima. Čak i za male organizacije potrebno je određeno vrijeme da se SMS uvede i neko vrijeme postane efektivan iz tog razloga potrebno je osigurati dovoljno vremena za implementaciju [13].

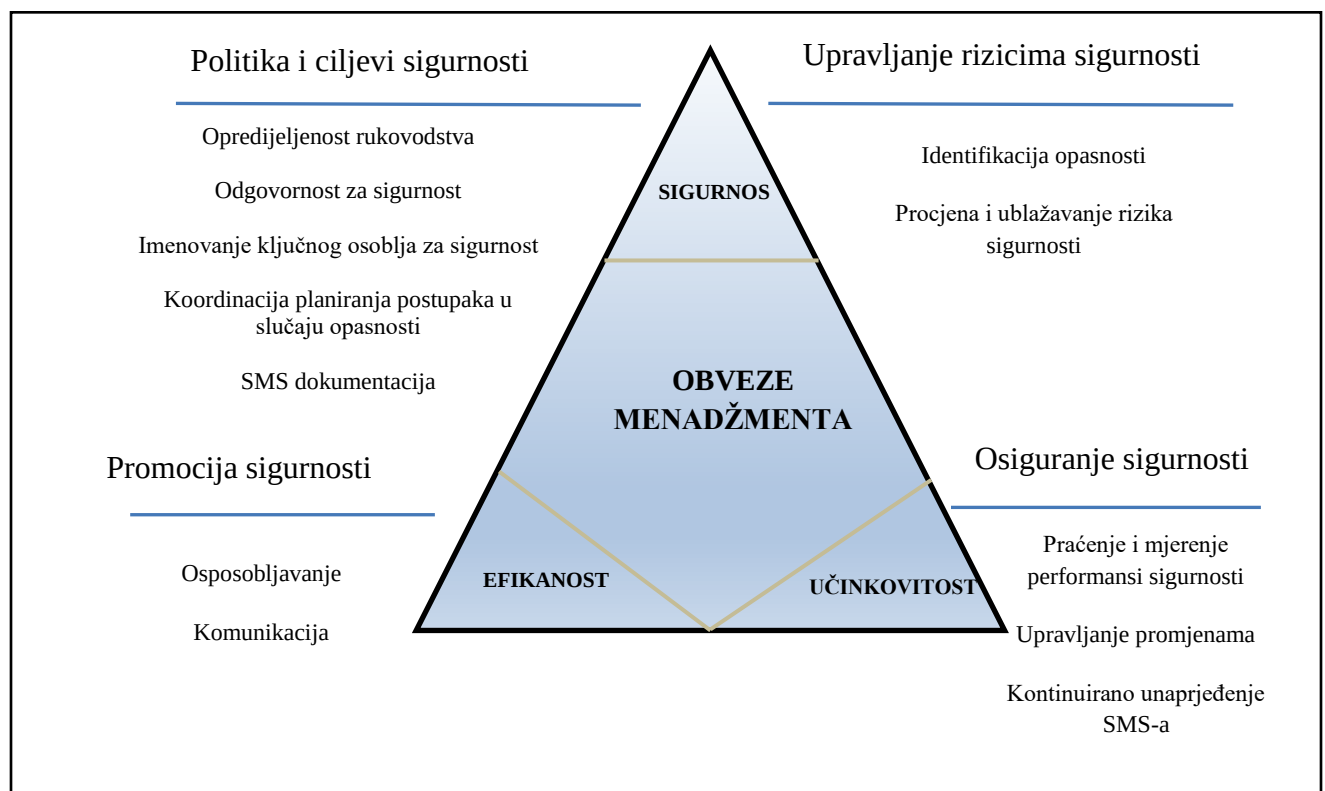
U četvrtom koraku težište je na poboljšavanju i mjerenju učinkovitosti sada implementiranog sustava. Savjetuje se da se izradi procjena funkcioniranja SMS-a svakih šest mjeseci nakon iniciranja. Kako bi organizacija dobila bolju perspektivu stanja sustava potrebno je dobiti povratne informacije u odnosu na početno stanje kroz audite početne analize nedostataka te razgovora sa zaposlenicima. Također, savjetuje se procjena i povratna informacija od nadležnog tijela države u kojoj organizacija djeluje. Mjerenje učinkovitosti može se provesti kroz analizu broja značajnih događaja povezanih sa sigurnošću koje organizacija imala, broj zaprimljenih dobrovoljnih izvješća ili broja sastanaka u vezi sigurnosti. Prethodni koraci trebali bi organizacije dati indikaciju o tome što treba poboljšati. Redefiniranje i poboljšavanje SMS-a nikad ne prestaje što znači da je implementacija potpuna tek kad je uključenost sustava vidljiva u svakodnevnim operacijama i na taj način djeluje neko vrijeme [13].

3.4. ICAO okvir sustava upravljanja sigurnošću

ICAO je dokumentom ICAO Doc 9859 (SMM) – Sustav upravljanja sigurnošću uključuje 4 komponente (12 elemenata) navedenih u daljnjem tekstu te na Slici 8.

1. Politika i ciljevi sigurnosti
 - 1.1. Opredijeljenost rukovodstva
 - 1.2. Dužnosti i krajnja odgovornost za sigurnost
 - 1.3. Imenovanje ključnog osoblja za sigurnost

- 1.4. Koordinacija planiranja postupaka u slučaju opasnosti
- 1.5. SMS dokumentacija
2. Upravljanje sigurnosnim rizicima
 - 2.1. Identifikacija opasnosti
 - 2.2. Procjena i ublažavanje sigurnosnih rizika
3. Osiguranje sigurnosti
 - 3.1. Praćenje i mjerenje performansi sigurnosti
 - 3.2. Upravljanje promjenama
 - 3.3. Kontinuirano unapređenje SMS
4. Promocija sigurnosti
 - 4.1. Osposobljavanje
 - 4.2. Komunikacija [12].



Slika 8. ICAO okvir sustava upravljanja sigurnošću

3.5. Politike i ciljevi sigurnosti

Prva komponenta okvira SMS usredotočena je na stvaranje okruženja u kojem upravljanje sigurnošću može biti učinkovito. Temelji se na sigurnosnoj politici i ciljevima koji postavljaju opredjeljenje rukovodstva za sigurnost, njegove ciljeve i potpunu organizacijsku strukturu. [1]

Opredjeljenje rukovodstva i vodstvo u sigurnosti ključno je za implementaciju učinkovitog SMS i utvrđivanjem sigurnosnih ciljeva. Opredjeljenje rukovodstva je predstavljeno upravljačkim odlukama i raspodjelom resursa. Navedene odluke i radnje trebale bi uvijek biti u skladu sa sigurnosnom politikom i ciljevima njegovanja pozitivne sigurnosne kulture [1].

Sigurnosnu politiku trebalo bi izraditi i odobriti rukovodstvo, potpisat će je odgovorna vlast. Pri razvoju sigurnosne politike i sigurnosnih ciljeva potrebno je savjetovati s ključnim sigurnosnim osobljem, i kad je to potrebno, predstavničkim tijelima osoblja (forum radnika, sindikati) radi promicanja osjećaja zajedničke odgovornosti [1].

3.5.1. Opredijeljenost i odgovornost rukovodstva

Sigurnosnu politiku trebali bi značajno podržavati više rukovodstvo i odgovorna izvršna vlast. „Vidljivo odobrenje“ odnosi se na to da aktivna podrška menadžmenta o politici sigurnosti postaje vidljiva ostatku organizacije. To se može učiniti na bilo koji način komunikacije i putem usklađivanja aktivnosti sa sigurnosnom politikom [1].

Odgovornost je uprave da komunicira o sigurnosnim politikama u cijeloj organizaciji kako bi osigurala da sve osoblje bolje razumije i radi u skladu s sigurnosnom politikom. Kako bi se odrazilo opredjeljenje organizacije za sigurnost, politika sigurnosti trebala bi uključivati i obvezu da:

- a) kontinuirano poboljšava razinu sigurnosnih performansi;
- b) promovira i održava pozitivnu sigurnosnu kulturu unutar organizacije;
- c) udovoljavanje svim primjenjivim regulatornim zahtjevima;
- d) osigurati potrebne resurse za isporuku sigurnog proizvoda ili usluge;
- e) osiguravanje sigurnosti primarna je odgovornost svih rukovoditelja
- f) osigurati da je politika razumljiva, provodljiva i održavana na svim razinama

Politika Sigurnosti također bi se trebala pozivati na sustav izvješćivanja radi poticanja izvješćivanja sigurnosnih pitanja i informirati osoblje o disciplinskog politici koja se primjenjuje u slučaju sigurnosnih događaja ili sigurnosnih pitanja koja se prijavljuju. Disciplinska politika koristi se za utvrđivanje je li došlo do pogreške ili kršenja pravila tako da organizacija može utvrditi treba li poduzeti bilo kakve disciplinske mjere. Da bi se osigurao pravedan tretman osoba koje su uključene, neophodno je da oni koji su odgovorni za to odlučivanje posjeduju potrebnu tehničku stručnost kako bi se kontekst događaja mogao u potpunosti razmotriti [1].

3.5.2. Krajnja odgovornost za sigurnost

Pružatelj usluga mora imenovati odgovornog rukovoditelja, koji bez obzira na ostale funkcije, ima krajnju odgovornost i nadležnost za implementaciju i održavanje SMS-a. Pružatelj usluga, također, mora identificirati odgovornosti svih članova višeg rukovodnog osoblja za pitanja sigurnosti, bez obzira na njihove druge funkcije. Odgovornosti za sigurnost i ovlasti moraju biti dokumentirane i priopćene cijeloj organizaciji. [12]

3.5.3. Imenovanje ključnog osoblja za sigurnost

Imenovanje kompetentne osobe ili osoba koje će obavljati ulogu voditelja sigurnosti od presudnog je značaja za učinkovito implementirani i funkcionirajući SMS. Osoba koja obavlja funkciju voditelja sigurnosti odgovorna je izvršnom organu za provedbu SMS-a i za isporuku sigurnosnih usluga ostalim odjelima u organizaciji [1].

Voditelj sigurnosti savjetuje odgovorne izvršne rukovoditelje o pitanjima upravljanja sigurnošću i odgovoran je za koordinaciju i komuniciranje o pitanjima sigurnosti unutar organizacije kao i s vanjskim članovima zrakoplovne zajednice. Funkcije upravitelja sigurnosti uključuju, ali nisu ograničene na:

- a) upravljanje planom implementacije SMS-a u ime odgovorne izvršne vlasti;
- b) provesti te olakšati identifikaciju opasnosti i analizu sigurnosnog rizika;
- c) pratiti korektivne radnje i ocjenjivanje njihovih rezultata;
- d) pružati periodična izvješća o sigurnosnim performansama organizacije;
- e) održavanje SMS dokumentacije i zapisa;
- f) planirati i olakšati obuku o sigurnosti osoblja;

- g) davanje neovisnih savjeta o sigurnosnim pitanjima;
- h) nadziranje pitanja sigurnosti u zrakoplovnoj industriji i njihov uočeni utjecaj na organizaciju operacija usmjerenih na isporuku proizvoda i usluga; i
- i) koordiniranje i komunikacija s nadležnim zrakoplovnim vlastima po potrebi o pitanjima koja se odnose na sigurnost [1].

U slučajevima kada je funkcija dodijeljena grupi (npr. Kada pružatelji usluga proširuju svoje SMS-ove kroz više aktivnosti) jedna osoba trebala bi biti određena kao voditelj sigurnosti, kako bi održala izravnu i nedvosmisleni liniju izvještavanja odgovornoj izvršnoj vlasti. Nadalje, nadležnosti voditelja sigurnosti trebaju uključivati, ali se ne trebaju ograničavati na sljedeće:

- a) iskustvo upravljanja sigurnošću/kvalitetom;
- b) operativno iskustvo vezano za proizvod ili uslugu koju pruža organizacija;
- c) tehnička pozadina za razumijevanje sustava koji podržavaju operacije ili proizvod/uslugu koju organizacija pruža;
- d) međuljudske vještine;
- e) analitičke vještine i vještine u rješavanju problema;
- f) vještine upravljanja projektima;
- g) vještine usmene i pismene komunikacije; i
- h) razumijevanje ljudskih čimbenika [1].

3.5.4. Koordinacija planiranja postupaka u slučaju opasnosti

Koordinacija planiranja za reagiranje u izvanrednim situacijama odnosi se na planiranje aktivnosti koje se odvijaju u ograničenom vremenskom razdoblju tijekom operativne izvanredne situacije u zrakoplovstvu. Plan postupanja u slučaju opasnosti (ERP)¹⁴ sastavni je dio procesa sustava upravljanja rizikom (SRM) za rješavanje izvanrednih situacija, kriza ili događaja povezanih sa zrakoplovstvom. ERP se treba baviti predvidljivim kriznim situacijama koje su utvrđene SMS-om i uključuju ublažavajuće radnje, procese i kontrole za učinkovito upravljanje u slučajevima opasnosti [1].

Plan postupanja u slučajevima opasnosti treba osigurati: ERP mora osigurati:

¹⁴ Emergency Response Plan

- a) pravovremen, uređen i efikasan prijelaz iz normalnih operacija u operacije u slučaju opasnosti;
- b) određivanje nadležnosti u slučaju opasnosti;
- c) Određivanje odgovornosti u slučaju opasnosti;
- d) Ovlasti ključnog osoblja za provedbu radnji sadržanih u planu;
- e) Koordinaciju aktivnosti u cilju uklanjanja opasnosti;
- f) Siguran nastavak operacija ili povratak na normalne operacije, što je prije moguće. [12]

3.5.5. Dokumentacija sustava upravljanja sigurnošću

SMS dokumentacija treba sadržavati SMS priručnik koji opisuje usluge sustava upravljanja sigurnošću, procese i postupke pružatelja usluga kako bi se olakšala unutarnja administracija, komunikacija i održavanje SMS-a. To bi trebalo pomoći osoblju da shvate kako funkcionira SMS u organizaciji i kako ispuniti politika i ciljevi sigurnosti. Dokumentacija treba sadržavati opis sustava koji pruža granice SMS-a. To bi također trebalo pojasniti odnos između različitih politika, procesa, postupaka i praksi te definirati na koji se način povezuju sa sigurnosnim pravilima i ciljevima pružatelja usluga. Dokumentacija bi trebala biti prilagođena i napisana kako bi se bavila svakodnevnim aktivnostima upravljanja sigurnošću koje će osoblje u cijelog organizaciji lako razumjeti. Priručnik za upravljanje sustava sigurnošću može biti samostalni dokument ili se može integrirati s drugim organizacijskim dokumentima koje održava pružatelj usluge [1].

SMS priručnik treba sadržavati detaljan opis pravila, postupaka i procesa pružatelja usluga koji uključuju:

- a) upravljanje dokumentacijom i zapisima;
- b) regulatorni SMS zahtjevi;
- c) okvir i područje primjene SMS-a;
- d) politika i ciljevi sigurnosti;
- e) odgovornosti za sigurnost i ključno osoblje;
- f) sustav izvješćivanja;
- g) procesi identifikacije opasnosti i upravljanje rizicima;
- h) indikatori performanse sigurnosti;

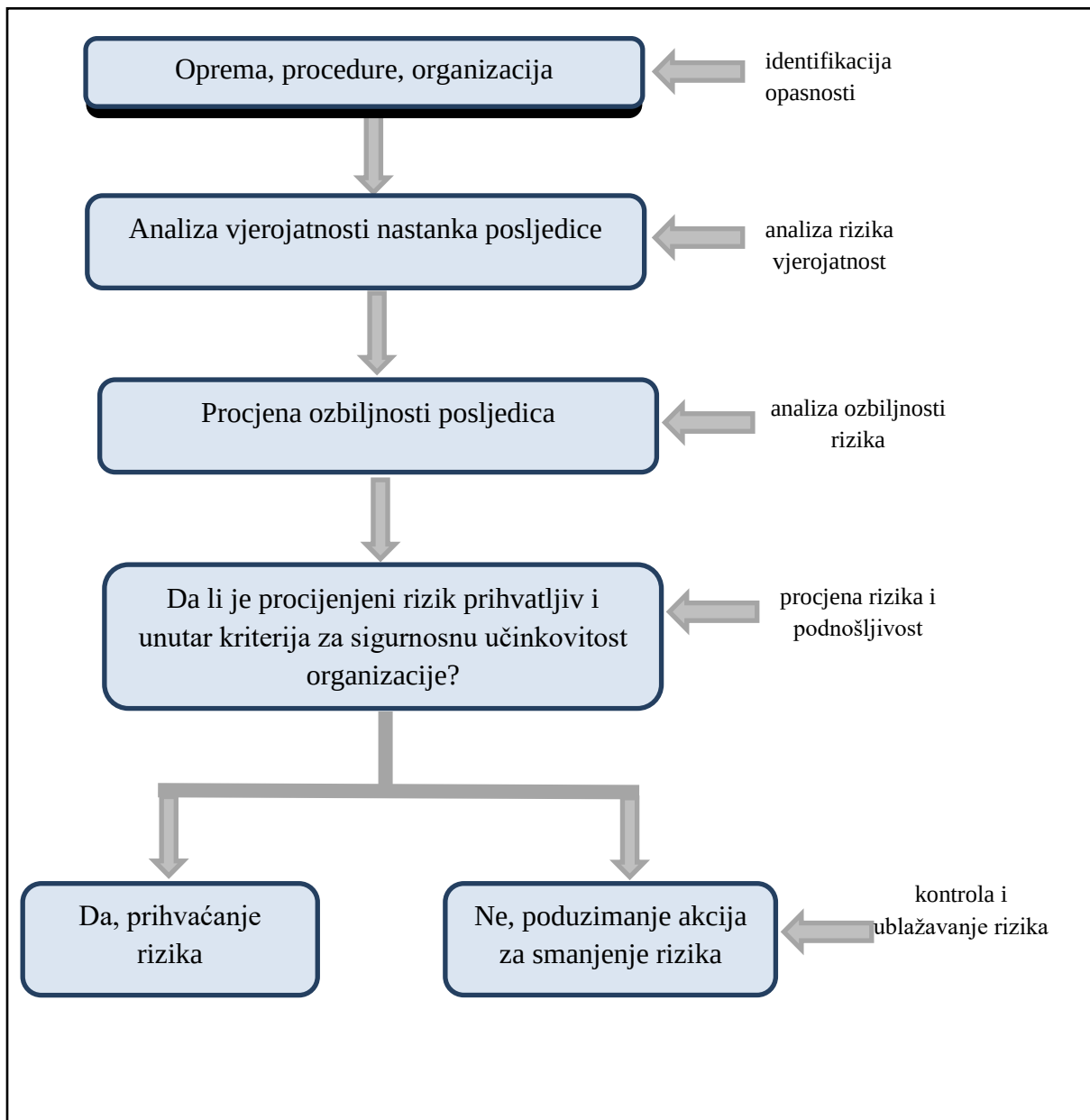
- i) osposobljavanje i komunikacija vezana uz sigurnost;
- j) upravljanje promjenama;
- k) kontinuirano poboljšanje i auditiranje sigurnosti;
- l) planiranje postupaka u slučaju opasnosti; i
- m) promocija sigurnosti [12].

3.6. Upravljanje sigurnosnim rizicima

Sigurnost je stanje u kojem je rizik od nanošenja štete osobama ili imovini ograničen i održavan na prihvatljivoj razini, kroz kontinuirani postupak identifikacije opasnosti i upravljanja rizikom. Proces koji vodi od identifikacije opasnosti prema procjeni rizika i ublažavanju rizika je proces upravljanja rizicima.

Pružatelji usluga trebali bi osigurati upravljanje njihovim rizicima sigurnosti. Taj postupak je upravljanje sigurnosnim rizikom (SRM), koji uključuje identifikaciju opasnosti, procjenu sigurnosnog rizika i ublažavanje sigurnosnog rizika. SRM sustavno prepoznaje opasnosti koje postoje u kontekstu isporuke proizvoda ili usluge. Opasnosti mogu biti posljedica sustava koji su manjkavi u svoj dizajnu, tehničkoj funkciji, ljudskim čimbenicima ili interakciji s drugim procesima i sustavima. Pažljiva analiza ovih čimbenika često može prepoznati potencijalne opasnosti u bilo kojem trenutku u životnom ciklusu operacije ili aktivnosti.

Razumijevanje sustava i radnog okruženja ključno je za postizanje visokih sigurnosnih performansi. Opasnosti se mogu prepoznati tijekom operativnog životnog ciklusa iz unutarnjih i vanjskih izvora. Procjene sigurnosti i ublažavanje sigurnosnih rizika potrebno je kontinuirano razmatrati kako bi se osiguralo da isti ostanu učinkoviti. Slika 9. prikazuje postupak prepoznavanja i upravljanja sigurnosnim rizikom za pružatelja usluga.



Slika 9. Postupak prepoznavanja i upravljanja sigurnosnim rizikom

Izvor: [5]

3.6.1. Identifikacija opasnosti

Identifikacija opasnosti prvi je korak u SRM procesu. Pružatelj usluga trebao bi razviti i održavati formalni postupak za prepoznavanje opasnosti koje bi mogle utjecati na zrakoplovnu sigurnost u svim područjima rada i aktivnosti. To uključuje opremu, uređaje i sustave. Bilo koja

opasnost koja može ugroziti zrakoplovnu sigurnost, a koja je pri tome identificirana i kontrolirana korisna je za sigurnost operacije. [1]

Opasnosti ili događaji povezani sa sigurnošću mogu biti pod kontrolom jedino ako je poznato da oni postoje. Temeljni problemi koji potencijalno ugrožavaju sigurnost operacija zrakoplova mogu biti identificirani kroz sustav izvješćivanja. Sustav izvješćivanja može biti reaktivan (iz događaja koji se dogodio) ili proaktivan (iz potencijalno nesigurnih stanja koje je identificirano). Izvješćivanje o manje značajnim nezgodama, koje ne moraju biti predmetom obveznog izvješćivanja, trebalo bi aktivno poticati. Ono pruža bolje razumijevanje o onome što se događa i omogućuje praćenje organizacijskih performansi, sigurnosti i pomoći u prepoznavanju razvoja trendova sigurnosti [13].

Dobrovoljni sustavi izvješćivanja o sigurnosti trebaju biti povjerljivi i zahtijevaju da bilo koji identifikacijski podaci o izvjestitelju budu poznati samo nekolicini pojedinaca (voditelja sigurnosti, i osoblje uključeno u sigurnosnu istragu) kako bi se omogućile daljnje aktivnosti. Održavanje povjerljivosti pomoći će olakšavanju otkrivanja opasnosti koje vode ljudskim pogreškama. Izvješća o dobrovoljnoj sigurnosti mogu se ukloniti o arhivirati nakon što se poduzmu potrebne radnje. Takva izvješća mogu poduprijeti buduće trendovske analize radi praćenja učinkovitosti ublažavanja rizika i prepoznavanja nastalih opasnosti [1].

3.6.2. Procjena i ublažavanje sigurnosnih rizika

Pružatelj usluga mora razviti model procjene sigurnosnog rizika i postupke koje će omogućiti dosljedan i sustavan pristup za procjenu sigurnosnih rizika. To bi trebalo uključivati metodu koja će pomoći utvrditi koji su sigurnosni rizici prihvatljivi ili neprihvatljivi i odrediti prioritete za postupke koje slijede [1].

SRM alate koji se mogu povremeno pregledavati i prilagođavati kako bi se osigurao da su prikladni za operativno okruženje pružatelja usluga. Pružatelj usluga može pronaći sofisticiraniji pristup koji bolje odgovara potrebama njihovog rada sa sazrijevanjem SMS-a. Pružatelj usluga i nadležna vlast (npr. CCAA)¹⁵ trebaju se dogovoriti kakva će se metodologija provoditi [1].

¹⁵ Croatian Civil Aviation Agency

Postupak procjene sigurnosnog rizika treba koristiti sve dostupne podatke o sigurnosti i sigurnosne informacije. Nakon procjene sigurnosnih rizika, pružatelj usluga uključit će se u proces odlučivanja na temelju podataka radi utvrđivanja kakva kontrola sigurnosnih rizika je potrebna. Odluka o tome kako pružatelji usluga prioritiziraju procjene sigurnosnog rizika i prihvaćaju kontrole sigurnosnog rizika njihov je odabir. Pružatelj usluga bi trebao pronaći postupak prioriteta na temelju:

- a) ocjene i kontrole najvećeg sigurnosnog rizika;
- b) raspodjele resursa za najveće sigurnosne rizike;
- c) učinkovito održavanje ili poboljšavanje sigurnosti
- d) ostvarenja navedenih i dogovorenih sigurnosnih ciljeva i SPT-a¹⁶; i
- e) udovoljavanju zahtjeva državnih propisa u vezi kontrole sigurnosnih rizika [1].

Nakon procjene sigurnosnih rizika moguće je provoditi odgovarajuće kontrole sigurnosnih rizika. Važno je uključiti i krajnje korisnike usluga ili proizvoda i stručnjake iz struke u određivanju odgovarajuće kontrole sigurnosnih rizika. Kada je dogovorena i provedena kontrola, sigurnosni učinak potrebno je nadzirati kako bi se osigurala učinkovitost kontrole sigurnosnog rizika. To je potrebno za provjeru integriteta, učinkovitosti i djelotvornosti novih kontrola sigurnosnih rizika u operativnim uvjetima. Rezultate SRM-a potrebno je dokumentirati i ta dokumentacija trebala bi uključivati opasnosti i sve posljedice, procjenu sigurnosnog rizika i sve poduzimanje radnje u vezi kontrole rizika. Navedena dokumentacija postaje povijesni izvor organizacijskog znanja o sigurnosti te se ono može koristiti za daljnje donošenje sigurnosnih odluka i za razmjenu podataka o sigurnosti. Ovo sigurnosno znanje isto tako pruža materijal za analizu trendova sigurnosti i sigurnosnu obuku i komunikaciju. Također, dokumentacija je veoma bitna za unutarnju audite organizacije kod procjene jesu li kontrole i radnje sigurnosnih mjera primijenjene i jesu li iste učinkovite [1].

3.7. Osiguranje sigurnosti

Osiguranje sigurnosti sastoji se od procesa i aktivnosti poduzetih kako bi se utvrdilo radi li SMS prema očekivanjima i zahtjevima. To uključuje kontinuirano nadgledanje njegovih procesa kao i radnog okruženja radi otkrivanja promjena ili odstupanja koja mogu predstaviti

¹⁶ Safety performance Target

nove sigurnosne rizike ili degradaciju postojeće kontrole sigurnosnih rizika. Takve promjene rizika mogu se tada rješavati kroz postupak SRM-a [5].

Aktivnosti osiguranja sigurnosti trebale bi uključivati razvoj i implementaciju aktivnosti kao odgovor na bilo koja pitanja koja imaju potencijalni sigurnosni utjecaj. Ove radnje kontinuirano poboljšavaju performanse SMS-a pružatelja usluga [1].

3.7.1. Praćenje i mjerenje performansi sigurnosti

Pružatelj usluga mora razviti, uspostaviti i održavati načine utvrđivanja (verifikacije) performanse sigurnosti prema ciljevima i politici sigurnosti organizacije, te validirati efektivnost metode kontrole rizika sigurnosti. Procedure izvješćivanja vezane uz performanse sigurnosti i praćenje moraju jasno definirati vrste prihvatljivog ili neprihvatljivog operativnog ponašanja, te jasno naznačiti uvjet pod kojima se osigurava imunitet od disciplinskih mjera. Proces praćenja i mjerenja performansi sigurnosti bi trebao uključiti:

- a) Izvješćivanje o sigurnosti;
- b) Studije o sigurnosti;
- c) Procjena stanja sigurnosti i praćenje trenda;
- d) Auditi sigurnosti; i
- e) Istrage (analize) [12].

3.7.2. Upravljanje promjenama

Promjena može utjecati na prikladnosti ili učinkovitost postojećih strategija ublažavanja sigurnosnog rizika. Pored toga, nove opasnosti i povezani rizici mogu se nenamjerno pojaviti uslijed događaja određene promjene. Takve opasnosti trebale bi biti identificirane tako da omogućuju procjenu i kontrolu svih povezanih sigurnosnih rizika [1].

Tipične promjene koje mogu utjecati na sigurnost:

- organizacijske promjene (novi direktor, odlazak iskusnog osoblja, organizacijsko restrukturiranje);
- operativne promjene (novi tip zrakoplova , novi ugovor, novi sustavi, nove operativne procedure); i

- fizičke promjene (uselj enje u novi objekt, uspostava nove baze, promjene na aerodromu).

Procjena rizika ključni je dio procesa, pa je potrebno odlučiti se za promjenu te započeti s procjenom ukupnog rizika koja ta promjena nosi. Nakon što je napravljen osnovni plan procesa procjene rizika potrebno je krenuti s identificiranjem i upravljanjem rizika. Treba uzeti u obzir da uvođenje novih procedura, operacija, i opreme vjerojatno nosi nove probleme vezane za sigurnost [13].

Procjenu rizika potrebno je provesti za svaki problem vezan uz sigurnost kako bi se poduzeli potrebni koraci u svrhu minimiziranja rizika i mogućih posljedica. Također, potrebno je dokumentirati plan i detaljno razraditi poduzimanje radnji po koracima. To će organizaciji pružiti uvid o ono što je dobro odrađeno, što nije. Isto tako organizacija će dobiti podatke za praćenje zašto su poduzete određene radnje u nekom razdoblju dok organizacije raste, razvija i širi svoje operacije [13].

3.7.3. Kontinuirano unaprjeđenje SMS-a

Pružatelj usluga mora pratiti i procjenjivati efektivnost uspostavljenih SMS procesa kako bi se osiguralo kontinuirano unaprjeđenje sveukupnih performansa SMS sustava. Kontinuirano unaprjeđenje mora: utvrditi neposredne uzroke zbog kojih su performanse ispod definiranih standarda i njihove implikacije na operacije SMS-a i popraviti situaciju u kojoj su performanse ispod definiranih standarda identificiranu kroz aktivnosti osiguranja sigurnosti. Kontinuirano unaprjeđenje bi se trebalo postići putem:

- a) evaluacije objekata, opreme, dokumentacije i procedura putem audita sigurnosti i istraga;
- b) evaluacije rada zaposlenika kako bi se utvrdila provedba njihovih odgovornosti;
- c) praćenja efektivnosti sustava kontrole i umanjenja rizika;
- d) praćenja organizacijskih promjena kako bi se utvrdilo da su te promjene efektivne [13]

3.8. Promocija sigurnosti

Promocija sigurnosti potiče izravnu sigurnosnu kulturu i pomaže u postizanju sigurnosnih ciljeva pružatelja usluga kombinacijom tehničke osposobljenosti koja se kontinuirano poboljšava

obukom i obrazovanjem, učinkovitom komunikacijom i razmjenom informacija. Rukovodstvo osigurava vodstvo za promicanje sigurnosne kulture u cijeloj organizaciji [1].

Učinkovito upravljanja sigurnošću ne može se postići samo strogim pridržavanjem politika i postupaka. Promocija sigurnosti utječe na pojedinačno i organizacijsko ponašanje i nadopunjava politike, postupke i procese organizacije, pružajući sustav vrijednosti koje podržavaju sigurnosne napore. Pružatelj usluga trebao bi uspostaviti i provoditi procese i postupke koji olakšavaju učinkoviti dvosmjernu komunikaciju na svim razinama organizacije. To bi trebalo uključivati jasan strateški pravac s vrha organizacije i omogućavanje komunikacije „odozgo prema gore“ koja potiče otvorene i konstruktivne povratne informacije od cijelog osoblja unutar organizacije[1].

3.8.1. Osposobljavanje

Dodatak 19. zahtijeva da pružatelj usluga razvije i održi program obuke o sigurnosti koji osigurava da osoblje je osposobljeno i kompetentno za obavljanje svojih dužnosti putem SMS-a. Također zahtijeva da opseg programa obuke o sigurnosti odgovara primjeru svakog pojedinca koji sudjeluje u SMS-u. Upravitelj sigurnosti je odgovoran da osigura prikladan program obuke sigurnosti. To uključuje pružanje odgovarajućih sigurnosnih informacija relevantnih za odredba sigurnosna pitanja s kojima se susreće organizacija. Osoblje koje je osposobljeno i kompetentno za obavljanje svojih SMS dužnosti, bez obzira na razinu u organizaciji, pokazatelj je opredjeljenja uprave za učinkovit SMS. Program obuke trebao bi sadržavati standarde za inicijalnu obuku i obuku obnove znanja. Inicijalna obuka sigurnosti trebala bi u obzir uzeti najmanje sljedeće:

- a) organizacijske politike sigurnosti i ciljeve;
- b) organizacijske uloge i odgovornosti vezane za sigurnost;
- c) osnovne principe SRM-a;
- d) sustave izvještavanja o sigurnosti;
- e) SMS procese i procedure organizacije; i
- f) ljudske faktore [1].

Opseg obuke za područje sigurnosti ovisit će o uključenosti pojedinca u SMS.

Obuka operativnog osoblja za područje sigurnosti treba uputiti na odgovornosti za sigurnost, sve operativne procedure i procedure sigurnosti, te značaj prepoznavanja i izvješćivanja o opasnostima. Ciljevi obuke trebaju biti poznavanje politike sigurnosti organizacije i osnova SMS.

Rukovodioci i nadzornici – Rukovodioci i nadzornici trebaju poznavati i razumjeti procese sigurnosti, identifikaciju opasnosti, upravljanje i ublažavanje rizika i upravljanje promjenama. Uz sadržaj specificiran za operativno osoblje, sadržaj obuke za rukovoditelje i nadzornike treba uključiti i analizu podataka o sigurnosti.

Više rukovodno osoblje – Obuka višeg rukovodnog osoblja za područje sigurnosti treba uključiti odgovornosti za sigurnost, usklađenost s regulatornim zahtjevima sigurnosti, osiguranje resursa, osiguranje efektivne među-odjelne komunikacije i aktivna promocija SMS-a. Uz sadržaj specificiran za prethodne dvije grupe, sadržaj obuke za više rukovodno osoblje treba uključiti i osiguranje sigurnosti, dužnosti i odgovornosti u području sigurnosti i uspostavu prihvatljivih razina sigurnosti.

Odgovorni rukovoditelj – Odgovorni rukovoditelj treba biti upoznat sa svojom ulogom i odgovornostima u SMS -u, politikom sigurnosti, SMS standardima i osiguranjem sigurnosti [12].

3.8.2. Komunikacija

Pružatelj usluga mora razviti, uspostaviti i održavati formalni način komuniciranja o pitanjima sigurnosti kojim se osigurava da je sve osoblje u potpunosti upoznato sa SMS-om, kojim pružatelj usluga prikuplja kritične informacije o sigurnosti i objašnjava zbog čega su poduzete aktivnosti iz područja sigurnosti, kao i zbog čega su donesene ili izmijenjene procedure o sigurnosti. Komunikacija o sigurnosti je temelj za razvoj i održavanje adekvatne kulture sigurnosti. Modeli komuniciranja uključuju distribuciju informacija putem:

- a) SMS priručnika;
- b) promocije politike sigurnosti;
- c) informacija o sigurnosti i biltena
- d) web stranice, elektronske pošte itd. [12].

4. METODOLOGIJA PLANIRANJA SUSTAVA UPRAVLJANJA SIGURNOŠĆU U ZRAKOPLOVNOJ OPERATIVI

SMS je sustav upravljanja koji mora biti u potpunosti integriran u svakodnevne operacije određene organizacije. Iz toga proizlazi da se SMS ne odobrava od strane regulatora (HACZ)¹⁷ kao samostalni proces, već se evaluira kroz proces certificiranja/nadzora organizacije. Pružatelj usluga zadovoljava inicijalnim zahtjevima nakon što HACZ zaprimi dokaze da su:

- nadležnosti i odgovornosti rukovodstva jasno definirane;
- politika sigurnosti je dokumentirana i potpisana od strane odgovornog rukovoditelja;
- SMS analiza nedostataka je provedena (analiza nedostataka); te
- dokumentirani rezultati.

Pružatelj usluga mora provesti analizu razlike kako bi prepoznao elemente i postupke potrebne za implementaciju i održavanje SMS-a te organizacije [4].

4.1. Integracija sustava upravljanja

Ovisno o organizacijskom, operativnom i regulatornom kontekstu, pružatelj usluga može implementirati integrirani SMS. Takva integracija može pružiti sinergiju upravljanjem sigurnosnim rizicima u više područja zrakoplovnih aktivnosti. Kao primjer, pružatelj usluga može implementirati jedan SMS za svoju organizaciju dizajniranja zrakoplova, organizaciju proizvodnje zrakoplova i sl. Isto tako mogu postojati situacije kada je pojedinačni SMS za svaku vrstu zrakoplovne aktivnosti više prikladan. Organizacije mogu definirati različite načine integriranja ili segregacije SMS-a kako najbolje odgovara njihovom poslovnom ili organizacijskom modelu, pod uvjetom da se usluge pravilno izvršavaju u skladu s propisima [5].

Pružatelji zrakoplovnih usluga obično primjenjuju sustave upravljanja za cijelu organizaciju. Učinkovitost organizacije ovisi o učinkovitosti integracije ovih sustava kako bi kvalitetno obavljali isporuku svojih proizvoda i usluga. U kontekstu SMS-a najvažniji aspekt integracije je sustav upravljanja kvalitetom (QMS)¹⁸. QMS se općenito definira kao

¹⁷ Hrvatska Agencija za Civilno Zrakoplovstvo

¹⁸ Quality Management

organizacijska struktura i povezana odgovornost potrebnih resursa, procesa i postupaka za uspostavljanja sustava kontinuiranog osiguranja i poboljšanja kvalitete usluge ili proizvoda. [5]

QMS i SMS su komplementarni sustavi. Naime, QMS je usmjeren na poštivanje datih propisa i zahtjeva za ispunjavanje očekivanja potrošača i ugovornih obveza, a SMS je usmjeren na sigurnosne performanse. Ciljevi SMS-u prepoznavanje opasnosti koje se odnose na sigurnost, procjenu povezanog rizika i provedbu učinkovite kontrole rizika. Suprotno tome, QMS je fokusiran na isporuku proizvoda i usluga koji zadovoljavaju relevantne specifikacije [5] .

S obzirom na komplementarne aspekte SMS-a i QMS-a, moguće je uspostaviti sinergijski odnos između dva sustava koja se mogu sažeti na sljedeći način:

- a) SMS podržava QMS procese poput audita, inspekcije, istrage, analize uzroka, oblikovanja procesa i preventivnih mjera;
- b) QMS može predvidjeti sigurnosna pitanja koja postoje usprkos organizacijskoj usklađenosti sa standardima i specifikacijama; i
- c) načela, politike i prakse kvalitete povezane su s ciljevima upravljanja sigurnošću. [5]

Odnos između QMS-a i SMS-a dovodi do komplementarnih doprinosa sustava u postizanju ciljeva sigurnosti i kvalitete organizacije. Usporedba ovih sustava dana je u Tablici 1. [5]

Tablica 1. Usporedba QMS-a i SMS-a

QMS	SMS
kvaliteta	sigurnost
osiguranje kvalitete	osiguranje sigurnosti
kontrola kvalitete	identifikacija opasnosti i kontrola rizika
kultura kvalitete	kultura sigurnosti
usklađenost sa zahtjevima	prihvatljiva razina sigurnosnih performansi
perspektiva	na temelju rezultata
standardi i specifikacije	organizacijski i ljudski čimbenici
reaktivno > proaktivno	proaktivno > reaktivno

Izvor: [5]

4.3. GAP analiza i plan implementacije sustava upravljanja sigurnošću

Analiza nedostataka (GAP analiza) uspoređuje postojeće procese i postupke upravljanja sigurnošću pružatelja usluga sa zahtjevima sadržanima u okviru SMS-a. Pružatelji usluga obično provode različite SMS funkcije zbog bolje usklađenosti s nacionalnim propisima ili ubog usvajanja najboljih praksi u industriji. Razvoj SMS-a trebao bi se temeljiti na postojećim organizacijskim strukturama i sustavima kontrole. Analiza nedostataka olakšava razvoj plana provedbe SMS-a identificiranjem nedostataka koje je potrebno otkloniti kako bi se SMS u potpunosti implementirao. Nakon što se analiza nedostataka dovrši i u potpunosti dokumentira, resursi i procesi koji su identificirani kao nedostajući ili neadekvatni činit će osnovu plana za implementaciju SMS-a. [5] Primjer obrasca analize razlike prikazan je na Slici 10.

Plan implementacije SMS-a trebao bi pružiti jasni prikaz resursa, zadataka i procesa potrebnih za implementaciju sustava. Vremenski okvir i redoslijed plana provedbe može ovisiti o raznim čimbenicima koji će biti specifični za svaku organizaciju, kao što su:

- a) regulatorni, potrošački i zakonski zahtjevi;
- b) više certifikata (s mogućim različitim datumima provedbe propisa);
- c) u kojoj se mjeri SMS može nadograditi na postojeće strukture i procese;
- d) dostupnost resursa i budžeta;
- e) međuovisnost između različitih koraka; i
- f) postojeće sigurnosne kulture [1].

Potrebno je izraditi plan provedbe SMS-a uz konzultiranje s izvršnim predstavnikom i rukovodstvom organizacije te odabrati odgovornog za radnje sukladno vremenskim rokovima. Plan bi se trebao odnositi na koordinaciju s vanjskim organizacijama ili izvođačima ako je isto primjenjivo. Plan implementacije SMS-a može se dokumentirati u različitim oblicima, varirajući od jednostavnog lista papira do specijaliziranog softvera za upravljanje projektima. Plan treba redovito nadzirati i po potrebi ažurirati. [1]

I država i pružatelj usluga trebaju biti svjesni da za postizanje učinkovitog SMS-a može trebati nekoliko godina. Pružatelji usluga trebali bi se pozivati na svoju državu jer mogu postojati zahtjevi za postupnim pristupom implementaciji SMS-a. [1]

ICAO reference	Aspects to be analyzed or question to be answered	Answer	Status of implementation
Component 1 – SAFETY POLICY AND OBJECTIVES			
Element 1.1 – Management commitment and responsibility			
SMM (Doc 9859) Chapter 8	Is there a safety policy in place?	☐ Yes ☐ No	
SMM (Doc 9859) Chapters 3 and 8	Does the safety policy reflect organizational commitments regarding safety management?	☐ Yes ☐ No	
SMM (Doc 9859) Chapters 3 and 8	Does the safety policy include a clear statement about the provision of the necessary resources for the implementation of the safety policy;	☐ Yes ☐ No	
SMM (Doc 9859) Chapters 3 and 8	Does the safety policy include the safety reporting procedures?	☐ Yes ☐ No	

Slika 10. Primjer analize nedostataka (GAP analiza)

Izvor: [13]

4.4.Fazni pristup implementaciji sustava upravljanja sigurnošću

Implementacija sustava upravljanja sigurnošću sustavni je proces. Unatoč tome, ovaj postupak veoma je izazovan zadatak s obzirom na čimbenike kao što su dostupnost vođača i resursa za implementaciju, kao i prethodno poznavanje pružatelja usluga o samim procedurama i postupcima SMS-a.

Razlozi faznog pristupa primjeni SMS-a uključuju:

- pružanje niz upravljivih koraka u implementaciji SMS-a, uključujući raspodjelu resursa;
- potrebu da se omogući implementacija okvira elemenata SMS-a u raznim redoslijedima, ovisno o rezultatima analize razlike svakog pružatelja usluga;
- početna dostupnost podataka i analitičkih procesa koji podržavaju reaktivne, proaktivne i prediktivne prakse upravljanja sigurnošću; i

- d) potrebu za metodičkim postupkom koji bi osigurao učinkovitu i održivu implementaciju SMS-a.[5]

Fazni pristup prepoznaje da je implementacija potpuno zrelog SMS-a. višegodišnji proces. Fazni pristup implementaciji omogućuje SMS-u da postane snažniji kako se završi svaka faza implementacije. Temeljni procesi upravljanja sigurnošću dovršeni su prije prelaska na sljedeće faze koje uključuju procese veće složenosti. [5]

Predložene su četiri faze provedbe SMS-a, a svaka faza povezana je s raznim elementima prema ICAO SMS okviru. Države i pružatelji usluga mogu se odlučiti za prilagođavanje ako isto smatraju prikladno njihovim okolnostima. [5]

4.4.1. Prva faza implementacije sustava upravljanja sigurnosti

Cilj prve faze implementacije SMS je pružanje plana kako zahtjevi za SMS-om trebaju biti zadovoljeni i integrirani u kontrolne sustave organizacije, kao i okvir odgovornosti za provedbu samog sustava.

Tijekom prve faze utvrđuje se osnovno planiranje i dodjela odgovornosti za što je potrebna analiza nedostataka (GAP analiza). Iz analize razlike organizacija može odrediti status svojih postojećih procesa upravljanja sigurnošću i može započeti s planiranjem razvoja daljnjih procesa upravljanja sigurnošću. [5]

Aktivnosti koje se provode po završetku prve faze implementacije moraju biti dovršene na način da zadovoljavaju očekivanja tijela za nadzor civilnog zrakoplovstva kako su navedena u relevantnim zahtjevima i uputama.

Aktivnosti koje se provode kroz prvu fazu su:

- Predanost i odgovornost rukovodstva – određivanje odgovorne osobe kao sigurnosnog rukovoditelja, uspostavljanje tima za implementaciju, razvoj plana implementacije, osiguravanje odgovarajuće SMS obuke i tehničke stručnosti tima ,praćenje i izvještavanje o napretku implementacije, definiranje opsega aktivnosti organizacije i provedba analize razlike;
- Razvijanje plana implementacije SMS-a;

- Imenovanje ključnog osoblja za sigurnost – identificirati ključnu osobu SMS-a, uspostavljanje ureda za sigurnost;
- Obuka i obrazovanje – provedba analize potrebe za obukom, organizacija i uspostava rasporeda obuke svih djelatnika prema njihovoj odgovornosti i sudjelovanje u SMS-u, prepoznavanje potrebnih troškova za obuku, razvijanje postupka vrednovanja, i uspostavljanje sustava evidencije obuke sigurnosti; i
- Sigurnosna komunikacija – pokretanje mehanizma za sigurnosnu komunikaciju i uspostavljanje načina prenošenja podataka putem sigurnosnih biltena, web stranice ili elektroničke pošte. [5]

4.4.2. Druga faza implementacije sustava upravljanja sigurnošću

Druga faza implementacije sustava upravljanja sigurnošću odnosi se na provedbu osnovnih postupaka upravljanja sigurnošću te ispravljanje potencijalnih nedostataka u postojećim procesima sustava upravljanja sigurnošću. Većina organizacija ima neke osnovne aktivnosti upravljanja sigurnošću na različitim razinama provedbe stoga ova faza ima za cilj konsolidaciju postojećih aktivnosti i razvijanje onih koji još ne postoje. Druga faza implementacije vremenski traje otprilike do dvanaest mjeseci kao i kod prve faze implementacije. [5]

Aktivnosti koje se provode u drugoj fazi implementacije:

- Predanost i odgovornost rukovodstva – razvijanje politike sigurnosti i potpisivanje politike sigurnosti od strane odgovorne osobe, priopćavanje sigurnosnih politika cijeloj organizaciji, uspostavljanje rasporeda pregleda sigurnosnih politika kako bi se osiguralo da politika ostane relevantna i primjerena organizaciji, utvrđivanje ciljeva za SMS-a razvijanjem sigurnosnih standarda učinkovitosti kroz pokazatelje sigurnosnih performansi i planova akcije;
- Sigurnosna odgovornost – definiranje sigurnosne odgovornosti i komunikacija istih kroz organizaciju, uspostavljanje SAG-a¹⁹, uspostavljanje odbora za sigurnost, uspostavljanje komunikacijske veze između ureda za sigurnost, odgovornog izvršnog tijela i SAG-a,

¹⁹ Safety Action Group

imenovanje odgovornog izvršitelja kao predsjednika odgovornog za sigurnost i SMS koordinaciju te izrada rasporeda sastanka ureda za sigurnost;

- koordinacija planiranja ERP-a – pregled ERP-a u vezi s delegiranjem ovlasti i dodjelom odgovornosti za izvanredna stanja, uspostavljanje postupaka koordinacije za djelovanja ključnog osoblja u slučaju izvanrednog događaja, identifikacija vanjskih subjekata koja će pomoći u komunikaciji s organizacijom u slučaju izvanredne situacije, uspostavljanje koordinacije između različitih ERP-ova, inkorporirati informacije o koordinaciji između različitih ERP-ova u dokumentaciju organizacije;
- SMS dokumentacija – izrada SMS priručnika, uspostavljanje sustava prijavljivanja sigurnosti. [5]

4.4.3. Treća faza implementacije sustava upravljanja sigurnosti

Cilj treće faze je uspostaviti procese upravljanja sigurnosnim rizicima. Pred kraj treće faze, organizacija će biti spremna za prikupljanje podataka o sigurnosti i provođenje sigurnosnih analiza na temelju podataka dobivenih putem sustava izvještavanja. Ova faza vremenski traje okvirnih osamnaest mjeseci iako sama vremenski period ovisi o veličini organizacije koja implementira sustav upravljanja sigurnosti. [5]

Aktivnosti koje se provede u ovoj fazi su sljedeće:

- Identifikacija opasnosti – uspostavljanje dobrovoljnog sustava izvještavanja, uspostavljanje programa za sustavni pregled svih zrakoplovnih sigurnosnih pitanja i procesa i uspostavljanje postupaka za određivanje prioriteta i dodjeljivanje utvrđenih opasnosti u cilju ublažavanja rizika;
- Procjena i ublažavanje sigurnosnog rizika – uspostavljanje postupka upravljanja sigurnosnim rizikom, razvijanje i usvajanje matrice sigurnosnih rizika relevantnih za rad organizacije u organizacijske materijale za obuku;
- Nadzor i mjerenje sigurnosnih performansi – uspostavljanje internog postupka prijavljivanja istrage događaja, prikupljanje podataka o sigurnosti te analiza i obrada podataka s visokim posljedicama;
- Upravljanje promjenama – postupak u kojem je potrebno uspostaviti upravljanje promjenama koje uključuju procjenu sigurnosnih rizika;

- Kontinuirano unaprjeđenje SMS-a – uspostavljanje programa za unutarnju i vanjske audite kvalitete. [5]

4.4.4. Četvrta faza implementacije sustava upravljanja sigurnošću

Posljednja faza implementacije uključuje provedbu upravljanja sigurnosnim rizicima i osiguranje sigurnosti. U ovoj fazi se osigurava operativna sigurnost primjenom periodičnog praćenja, povratnih informacija i kontinuiranih korektivnih radnji za održavanje učinkovitosti kontrole sigurnosnih rizika. [5]

Aktivnosti i procesi koji se provode u posljednjoj fazi implementacije su sljedeći:

- predanosti i odgovornosti rukovodstva – poboljšavanje postojeće disciplinske politike uz dužno razmatranje nenamjernih pogrešaka, namjernih pogrešaka ili prekršaja.
- identifikacija opasnosti – integrirati opasnosti dobivenih od istraženih izvješća sa sistemom dobrovoljnog sustava izvješćivanja opasnosti i omogućiti identifikaciju opasnosti i postupke upravljanja rizikom s kooperantovim SMS-om;
- sigurnosno praćenje i mjerenje performansi – poboljšanje sustava prikupljanja i obrade podataka o sigurnosti radi uključivanja događaja s nižim posljedicama, uspostavljanje pokazatelja sigurnosti s nadzorom razine cilja.
- kontinuirano unapređenje SMS-a – uspostavljanje audita SMS-a ili drugih operativnih pregleda/anketa SMS-a ako je to potrebno;
- obuka - osigurati da je SMS program obuke proveden za sve relevantno osoblje;
- sigurnosna komunikacija – uspostavljanje mehanizama za promicanje razmjene sigurnosnih informacija. [5]

5. IMPLEMENTACIJA SUSTAVA UPRAVLJANJA SIGURNOSTI NA PRIMJERU ODOBRENE ORGANIZACIJE ZA OSPOSABLJAVANJE PILOTA

5.1. Odobrena organizacija za osposobljavanje pilota

Hrvatsko zrakoplovno nastavno središte (HZNS/CATC)²⁰ neovisna je jedinica uspostavljena u svrhu praktične obuke pilota unutar Zavoda za aeronautiku Fakulteta Prometnih Znanosti (FPZ/FFTS)²¹ Sveučilišta u Zagrebu. Kao takva, HZNS je bila prva i najveća organizacija koja je obavljala certificiranu letačku obuku prema JAR-FCL²² zahtjevima i standardima unutar Republike Hrvatske. Navedena organizacija u današnje vrijeme je certificirana kao odobrena organizacija za obuku (ATO)²³ od strane Hrvatske agencije za civilno zrakoplovstvo (CCAA). Također, potrebno je navesti da HZNS ima iskusno osoblje letačkih instruktora koji su u potpunosti posvećeni prenošenju i dijeljenju znanja i iskustva koje posjeduju na buduće pilote koji se školuju unutar organizacije.

Kako je HZNS organizacija koja provodi osposobljavanje civilnih pilota, odnosno ATO (Approved Training Organisation), ista posjeduje flotu od pet zrakoplova: dva Cessna C172, jedan Cessna 172N, jedan Diamond DV 20, jedan Piper PA44-180 te je u posjedu simulatora FNPTII/MCC Elite S923. [14]

HZNS certificirana je organizacija za provođenje sljedećih tečajeva:

- Integrirano ATP(A) osposobljavanje za CPL(A)/ ME/IR dozvolu pilota,
- Seminar obnove znanja FI(A)/IRI(A),
- MCC(A) modularni program obuke,
- MEP(A) modularni program obuke,
- Program obnove znanja za klasu zrakoplova MEP(A),
- Program obnove znanja za klasu zrakoplova SEP(A),
- Program obnove znanja za instrumentalno ovlaštenje IR(A),
- PPL (A) program obuke,

²⁰ Hrvatsko zrakoplovno nastavno središte/ Croatian aviation training centre

²¹ Fakultet Prometnih Znanosti/ Faculty of Transport and Traffic Sciences

²² Join Aviation Requirements Flight Crew License

²³ Approved Training Organization

- Program obuke letenja noću (NR),
- LAPL (A) program obuke. [14]

U potrebi za kontroliranim i sigurnim održavanjem zrakoplovne flote, HZNS je ujedno i organizacija za održavanje zrakoplova koja posjeduje certifikat EASA Part-145 (AMO)²⁴ te je također i CAMO²⁵ za zrakoplove unutar svoje flote kao i za zrakoplove treće strane[14].

5.2. Sustav upravljanja sigurnošću na primjeru ATO-a

Politika sigurnosti odobrene organizacije za osposobljavanje pilota

Prema HZNS Operativnom priručniku navedena organizacija obavezuje se implementirati, razvijati te kontinuirano poboljšavati strategije, sustave upravljanja te procese u svrhu osiguranja da aktivnosti koje organizacija provodi (ATO, FTSD, Part-M, i Part-145) budu na najvišoj razini sigurnosti prema sigurnosnim standardima. Također organizacija se obvezuje da će udovoljavati nacionalnim i međunarodnim važećim zakonima i sigurnosnim standardima te sukladno time pružati maksimalno moguću razinu usluge.

Pristup rada HZNS-a je stvaranje i održavanje organizacije koja je proaktivna, sigurna i koja se kontinuirano fokusira na sigurnost i poslovanje. Samim time, imperativ organizacije je da svi zaposlenici imaju mogućnost prijavljivanja nesreća, nezgoda i događaja putem razvijenog sustava izvješćivanja. Rukovodstvo organizacije ohrabruje zaposlenike u smislu pismenog ili usmenog izvješćivanja o bilo kojoj pojavi koja bi mogla utjecati na sigurnost. Takva vrsta politike organizacije prikazuje da je svrha sustava izvješćivanja i internih istraga poboljšavanje sigurnosti, a ne prebacivanje krivice na pojedince. Kao takva, sigurnost HZNS-a treba bi biti briga svih zaposlenih na svim razinama organizacije iako primarna odgovornost za sigurnost leži na rukovodstvu [15].

HZNS se isto tako obvezuje da će osigurati stalno unaprjeđenje proaktivnog i sustavnog upravljanja, svih operativnih performansi i radnih procesa uključujući upravljanje sigurnošću i nadzora usklađenosti sustava. Kao organizacija, HZNS je odgovoran osigurati dostupnost

²⁴ Approved Maintenance Organization

²⁵ Continuing Airworthiness Management Organization

odgovarajućih i potrebnih ljudskih i financijskih resursa za provedbu strategije i politike upravljanja sigurnošću.

Vizija HZNS-a je stvaranje sigurnijeg Europskog neba kroz visoke standarde kvalitete u obuci pilota te održavanju zrakoplova. Kao misiju HZNS navodi promociju usklađivanja i standardizaciju osposobljavanja pilota u Hrvatskoj kroz suradnju, dijeljenje stečenih znanja, vještina i resursa između članova i drugih sudionika.

Strateški ciljevi organizacije su:

- razvijanje mreže izvrsnosti obuke pilota i održavanja zrakoplova u zrakoplovnoj industriji u Hrvatskoj;
- biti glas Europskih organizacija za osposobljavanje,
- promicanje poštivanja nacionalnih i međunarodnih standarda;
- promicanje suradnje između članova Europske unije i
- razvijanje i provedba postupaka i smjernica za zrakoplovnu obuku. [15]

5.2.1.1. Dužnosti i krajnja odgovornost za sigurnost odobrene organizacije za osposobljavanje pilota

Odgovorni rukovoditelj (AM)²⁶ snosi ukupnu odgovornost za sve aktivnosti HZNS-a kao što su nadzor usklađivanja prema propisima, planiranje postupanja u slučaju opasnosti (ERP) te njegovu implementaciju te strukturu i opseg funkcioniranja unutarnjeg sustava praćenja usklađenosti. AM pismeno definira i potvrđuje odgovornosti, ovlaštenja i međusobne radne odnose zaposlenika koji upravljaju, izvode i potvrđuju radnje vezane uz poštivanje propisa [15].

Odgovorni rukovoditelj je odgovorna osoba za:

- uspostavljanje praćenja poštivanja politike sigurnosti ZNS-a;
- upravljanje učinkovitim sustavom upravljanja;
- vođenje svih operacija u skladu s primjenjivim zahtjevima;

²⁶ Accountable Manager

- osiguravanje resursa potrebnih za implementaciju i rad sustava upravljanja kao i obavljanje korektivnih radnji. Navedeni resursi uključuju kvalificirano radno osoblje, infrastrukturu, opremu, financije te informatičku podršku u smislu sustava i opreme;
- uz pomoć rukovoditelja za praćenje usklađenosti, osiguranje da su sve primijenjene korektivne akcije provedene, i da se aktivnosti organizacije provode u skladu s propisima;
- koordinacija između različitih odjela organizacije [15].

AM može povjeriti dužnosti prema potrebi kako bi se osiguralo nesmetano i učinkovito funkcioniranje organizacije, ali ne može povjeriti svoj vlastite odgovornosti.

Dužnosti i odgovornosti AM-a, rukovoditelja odjela su:

- raspodjela odgovornosti i dužnosti te izdavanje instrukcija pojedincima u svrhu provedbe politika i postavljanje sigurnosnih standarda u njihovom području djelovanja;
- provedba neposredne akcije na sigurnosni problem odnosno mjera koje prepisuje CCAA i/ili sve relevantne obvezne sigurnosne informacije koje izdaju CCAA ili EASA, uključujući direktive o plovidbenosti;
- provedba usklađenosti s regulatornim zahtjevima, ograničenjima certifikata i internim politikama i procedurama;
- nadgledanje sigurnosnih standarda, uključujući nadgledanje pridržavanja zaposlenika standardima pomoću audita i inspekcija;
- procjena pokazatelja sigurnosnih učinaka u njihovom području djelovanja;
- evaluacija sigurnosnih zapisa kako bi se izbjegla pojava nepoželjnih događaja;
- evidentiranje i analiza odstupanja od specifičnih standarda HZNS-a i osiguranje korektivnih akcija te preventivno djelovanje unutar organizacijske jedinice;
- sastavljanje periodičnih evaluacija podataka;
- promicanje korporativne kulture sigurnosti, kvalitete, politika i općeg standarda rada i svijesti o riziku;
- osiguranje sveobuhvatnog upravljanja dokumentima, njihovo pohranjivanje te povezivanje s CCAA u pogledu administracije i koordinacije;

- osiguravanje da svi podređeni ispunjavaju kvalifikacijske uvjete za aktivnosti koje obnašaju, upravljanje i planiranje kontinuiranog obrazovanja i razvoja karijere;
- osiguranje da su svi podređeni upoznati te da se pridržavaju svih propisa, ograničenja certifikata te internih politika i procedura;
- odgovornost za upravljanje učinkovitim sustavom upravljanja [15].

5.2.1.2. Imenovanje ključnog osoblja za sigurnost odobrene organizacije za osposobljavanje pilota

Rukovoditelj sigurnosti (SM)²⁷ je osoba koja je imenovana od strane odgovornog rukovoditelja (AM) u svrhu postizanja potrebnog stupnja ovlasti u radu sa sigurnosnim pitanjima. U HZNS-u, SM je osoba koja se smatra središnjom točkom za razvoj, administraciju i održavanje učinkovitog sustava upravljanja sigurnošću. Ukoliko je potrebno, SM-u će biti dostupno dodatno osoblje u svrhu obavljanja zadataka povezanih s upravljanjem sigurnošću.

SM unutar organizacija obavljanja najmanje sljedeće funkcije:

- upravljanje planom implementacije sustava upravljanja sigurnošću u ime AM-a;
- upravljanje rizicima koji uključuje identifikaciju opasnosti, procjenu i ublažavanje rizika;
- nadgledanje provedbe postupka bilo kojih radnji vezanih za ublažavanje rizika kako bi se osiguralo izvršavanje sigurnosnog akcijskog plana;
- provođenje periodičnih izvješća o sigurnosnim performansama;
- vođenje SMS dokumentacije;
- organizacija obuke zaposlenika vezano za upravljanja sigurnošću;
- savjetovanje AM-a i voditelja zrakoplovnog odjela o sigurnosnim pitanjima;
- pomaže odgovornim rukovoditeljima;
- nadzor sustava upravljanja sigurnošću;
- pokreće interne istrage određenih događaja ili nesreće te provodi daljnje postupke vezane za isto [15].

²⁷ Safety Manager

5.2.1.3. Koordinacija planiranja postupaka u slučaju opasnosti

ERP unutar HZNS-a je osmišljen s ciljem da pomogne u upravljanju s izvanrednim događajima u zrakoplovstvu kao što su nesreće, ozbiljne nezgode ili bilo koji drugi događaji za koje je potrebno uspostavljanje skupine za izvanredne događaje. Navedeni plan pruža određene procese i smjernice osoblju koje obavlja ključne zadatke u svrhu osiguravanja sigurnog rada te postupanja u slučajevima opasnosti kako bi se organizacija što prije oporavila od mogućih posljedica.

Sljedeći događaji mogu rezultirati krizom i aktivirati Plan za hitne slučajeve:

- zrakoplovna nesreća ili ozbiljna nezgoda;
- katastrofa u radnim prostorijama: požar, eksplozija, zagađenje, poplava
- gubitak radnog resursa: radionica, hangar, zrakoplov;
- posljedice katastrofe u blizini prostorija HZNS-a;
- više žrtava povezanih s katastrofom, bolešću ili zarazom;
- unutarnja ili vanjska prijetnja: terorizam, prijetnje, sabotaza;
- gubitak energije: struja, plin
- gubitak komunikacije: internet, fiksna ili mobilna linija [15].

ERM²⁸ ili njegov zamjenik odgovorna je osoba i on odlučuje je li potrebno za određeni događaj aktivirati ERP. Koncept plana u izvanrednim situacijama osmišljen je kako bi ispunio sljedeće ciljeve:

- osiguravanje urednog i sigurnog prijelaza iz normalnih u izvanredne operacije i povratak u normalne operacije;
- nacrt plana komunikacije i obavještavanja, uključujući komunikaciju obavještavanja nadležnih vlasti i skupine za upravljanje izvanrednim događajima;
- definiranje sustava, uloga i podataka za kontakt skupine za upravljanje u izvanrednim događajima;
- pružanje smjernica i početnih postupaka reakcije za članove skupine kako bi se početni zadaci mogli pravilno izvršavati;

²⁸ Emergency Response Manager

- osiguranje dobrobiti zaposlenika, instruktora i studenta.

Zbog veličine organizacije, HZNS ima ograničene mogućnosti u vezi s izvanrednim događajima i sve aktivnosti ukoliko dođe do pojave potencijalnog ili stvarnog događaja biti će usmjerene na provedbu odgovarajućeg plana u slučaju opasnosti kako bi se umanjili štetni učinci na osoblje i imovinu [15].

5.2.1.4. SMS dokumentacija odobrene organizacije za osposobljavanje pilota

Glavna svrha upravljanja dokumentima je osigurati da su svi potrebni, ispravi i ažurirani dokumenti dostupni onim korisnicima koji ih trebaju i kada im trebaju.

HZNS je razvio sustav koji pruža:

- distribuciju relevantne dokumentacije i priručnika koju osigurava CMM²⁹ putem web stranice HZNS-a;
- distribuciju i kontrolu dokumenta koje HZNS ne izrađuje;
- identifikaciju i uklanjanje zastarjele i nevaljane dokumentacije;
- skladištenje i distribuciju dokumenta dobivenih od vanjskih izvora, nadležnih zrakoplovnih vlasti te proizvođača opreme i sredstva za rad.

HZNS distribuira dokumente u elektroničkoj verziji putem službene internet stranice HZNS-a. Jedina iznimka distribucije dokumenata mogu biti za:

- arhiva – svi originalni dokumenti čuvaju se u uredu CMM-a u papirnatom i elektroničkom obliku;
- dokumenti o zrakoplovu;
- dokumenti CCAA [15].

²⁹ Compliance Monitoring Manager

5.2.3.Upravljanje sigurnosnim rizicima u odobrenoj organizaciji za osposobljavanje pilota

U svrhu bolje provedbe sigurnosnih politika i postupaka, HZNS je osnovao odbor s nazivom Odbor za audite sigurnosti (SRB), čiji je glavni posao razmatranje pitanja strateških sigurnosnih aktivnosti kao podrška sigurnosti kao vrstu podrške odgovornom rukovoditelju.

AM predsjedava SRB-om, a njega čine:

- voditelj obuke, tj Šef školstva (HT);
- FSTD rukovoditelj;
- MM rukovoditelj za održavanje zrakoplova;
- CAMO rukovoditelj;
- CMM rukovoditelj za usklađenost;
- SM rukovoditelj za sigurnost [15].

Svaki član SRB-a može predložiti poziv bilo kojoj relevantnoj osobi koja opet može doprinijeti pružanjem relevantnih informacija odgovornom rukovoditelju kako bi se omogućilo donošenje odluka na temelju podataka o sigurnosti. Navedeni odbor osigurava da su na raspolaganju odgovarajuća sredstva za postizanje, održavanje utvrđenih sigurnosnih učinaka te pružanje strateškog smjera.

SRM kontrolira:

- da aktivnosti izvođenja sigurnosti ne budu u sukobu s politikom sigurnosti i ciljevima,
- pravovremenost poduzimanja korektivnih i ublažavajućih radnji;
- efikasnost HZNS-ovih procesa upravljanja sigurnošću;
- proces procjene rizika;
- istraživanja i osvrti studija sigurnosti;
- upravljanje promjenama;
- sigurnosne postupke istrage [15].

Sustav upravljanja sigurnošću bavi se opasnostima kroz pet koraka ili faza:

1. procesi identifikacije opasnosti;
2. analiza događaja;
3. procjena rizika;
4. ublažavanje rizika;
5. nadzorne aktivnosti [15].

5.2.3.1. Identifikacija opasnosti

Opasnost je svaka situacija ili stanje koje može izazvati štetne posljedice, na primjer, ozljede ili gubitak života, imovine ili oštećenja okoliša. Identifikacija opasnosti je identifikacija svake situacije ili stanja (opasnosti) koja može izazvati štetne posljedice.

Procesi prepoznavanja opasnosti opisani su u HZNS-u kroz procese prikupljanja, analiziranja, bilježenja i stvaranja povratnih informacija o opasnostima i povezanim opasnostima koji mogu utjecati na sigurnost.

Svi zaposlenici HZNS-a odgovorni su za otkrivanje i prijavljivanje opasnosti putem obrasca za identifikaciju opasnosti uključujući i dobrovoljno izvještavanje. Obrazac za identifikaciju opasnosti prikazan je na Slici 11.

HZNS koristi reaktivne i proaktivne metode prepoznavanja opasnosti. Reaktivne metode sadrže podatke o nesrećama, nezgodama i informacijama o sustavima izvještavanja. Proaktivne metode uključuju sustave za izvješćivanje o otvorenim ili aktivnim opasnostima te praćenje podataka o letu i ankete sigurnosti [15].



HAZARD IDENTIFICATION FORM

HI-XX

1

FPZ-HZNS employees and students may use this form to report hazard(s). Safety Manager will investigate the hazard(s) to determine if mitigation is needed. Form can be submitted confidentially (anonymously) if desired. Employees are advised that reporting is under the non-punitive policy, in accordance with HZNS Safety Policy.

EMPLOYEE'S/ STUDENT'S NAME:

(optional)

DIVISION:

(optional)

PHONE/E-MAIL:

(optional)

UNSAFE CONDITION OR PRACTICE (HAZARD)

LOCATION

CAUSE(S) OF UNSAFE CONDITION OR PRACTICE (HAZARD)

SUGGESTION FOR POSSIBLE MITIGATION OF UNSAFE CONDITION OR PRACTICE (HAZARD)

Has this matter been reported to your supervisor?

YES

NO

Date:

Signature:

FORWARD THIS FORM TO SAFETY MANAGER OR IN SAFETY MAILBOX OR TO E-MAIL: sdovhanj@fpz.hr

TO BE FILLED BY SAFETY MANAGER (SM):

Acceptance date:

Further actions:

YES

NO

Comment:

Close date:

Signature:

HZNS-FRM-5

Date: 18.03.2016

Rev. 3

Slika 11 Obrazac identifikacije opasnosti

Izvor: [15]

Okvir opasnosti je širok i HZNS razmatra sljedeća područja za postupak identifikacije opasnosti:

- čimbenici dizajna, uključujući opremu i dizajn zadatka;
- ljudski čimbenici, uključujući postupak odlučivanja;
- postupci i radne prakse, uključujući njihovu dokumentaciju i popise provjera;
- komunikacije, uključujući najprikladniji medij, terminologiju;
- kadrovske čimbenike kao što su politike zapošljavanja i obuke;
- organizacijski čimbenici kao što su kompatibilnosti proizvodnih i sigurnosnih ciljeva, raspodjele resursa, radni pritisci, učinkovitosti interne komunikacije i sigurnosne kulture organizacije;
- čimbenici radne sredine kao što su buka vibracija, temperatura, osvjetljenje i dostupnost zaštitne opreme i odjeće;
- čimbenici regulatornog nadzora, uključujući primjenjivost i provedbu propisa, certificiranje opreme, osoblja i procedura te adekvatnost nadzornih audita,
- vrste obrane koje uključuju takve čimbenike kao što su dostupnost odgovarajućih sustava identificiranja, upozoravanja, tolerancija pogreške opreme i opseg otpornosti sustava na neuspjeh [15].

Svaka od navedenih skupina pažljivo je obrađena kroz matrice procjene sigurnosnog rizika HZNS-a definiranje ozbiljnosti i procjenom vjerojatnosti povezanih rizika. Korištenjem navedene matrice lako je procijeniti rizika stoga HZNS može lako definirati preventivne mjere koje povećavaju operativnu sigurnost rada u HZNS-u [15].

5.2.3.2. Procjena i ublažavanje sigurnosnih rizika u odobrenoj organizaciji za osposobljavanje pilota

Za postupak analize sigurnosti odgovoran je SM. Veoma je važno da se pregledaju sve prijavljene opasnosti i događaji te da se donese odluka o tome kakve će se analize sigurnosti provoditi i na koji način.

SM odlučuje o potrebi sigurnosne analize i o članovima skupine koja će ih provoditi ukoliko je to potrebno. SM uvijek je član takve skupine.

Postupak analize sigurnosti sastoji se od sljedećih koraka:

- obavijesti o pojavi i procjeni opasnosti;
- prikupljanju dostupnih dokumenata, informacija i intervju;
- rekonstrukcija logičkog napredovanja događaja;
- integrirane istrage;
- ako su potrebne daljnje akcije, provođenje procjenu rizika i utvrđivanje razinu prihvatljivosti rizika;
- sigurnosni komunikacijski postupak [15].

Prema navedenom, proces analize za cilj ima povećanje sigurnosti. Stoga bi se analize trebale usredotočiti na incidente i događaje, a ne na nesreće.

Opseg analize ovisi o stvarnim ili potencijalnim posljedicama pojave opasnosti. Izvješća o opasnostima i incidentima koji ukazuju na potencijalni rizik analizirat će se u većoj dubini od onih s niskim potencijalom rizika. Dubina i detaljnost analize provesti će se tako da se jasno i temeljno identificiraju i potvrde opasnosti.

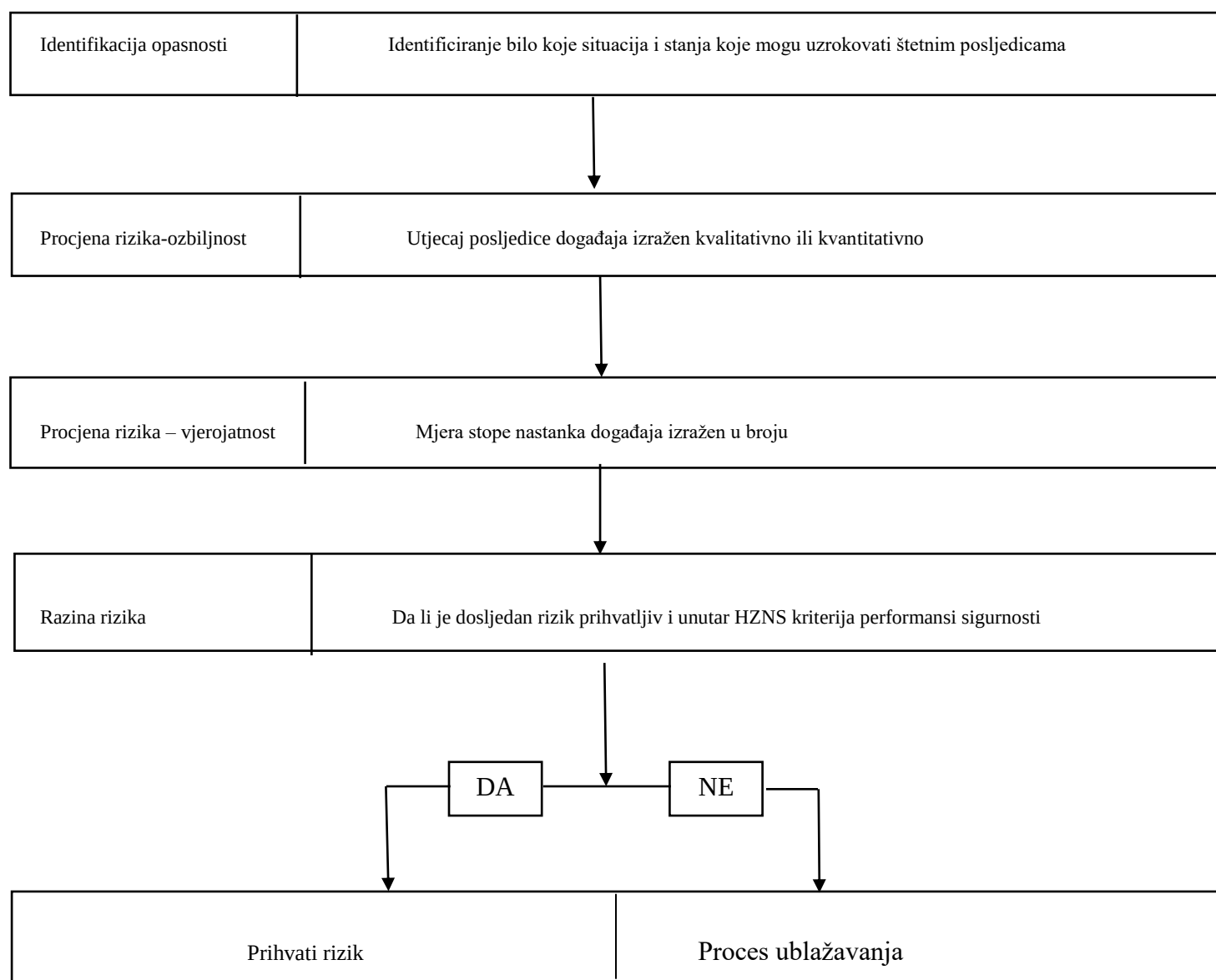
Da bi razvio razumijevanje nesigurnih uvjeta, istražitelj će primijeniti opisani sistemski pristup opisan u priručniku. Izvori informacija potrebni za analizu sigurnosti uključuju:

- dokumentaciju;
- praćenje operativnih podataka;
- intervju;
- simulacije;
- sigurnosne baza podataka [15].

Procjena rizika uključuje razmatranje i vjerojatnosti i težine potencijalnih posljedica. Prilikom procjene rizika važno je razlikovati opasnosti (potencijalno nanošenje štete) i rizika (vjerojatnost i ozbiljnost te štete ostvarene u određenom razdoblju). Procjena rizika može se razmatrati na dva načina:

- vjerojatnost koja uzrokuje štetne posljedice,
- ozbiljnost mogućih štetnih posljedica.

Kombinacija ozbiljnosti i vjerojatnosti definirana je kao razina rizika (podnošljivosti). Odluka o intervenciji donosi se na temelju razine rizika. Voditelj odjela ovlašten je donositi odluke o razini rizika. Ako rizik utječe na više odjela, AM ima ovlasti donositi konačnu odluku . [15].



Slika 12 Analiza opasnosti i proces procjene rizika

Izvor: [15]

Proces procjene rizika pokreće SM u suradnji s rukovoditeljem odjela, SRB-om i prikladnim stručnjakom prije donošenja završne odluke. Završnu odluku kreira SRB, predstavlja je AC-u i predstavlja kroz HZNS [15].

Procesi procjene i ublažavanja rizika analiziraju, uklanjaju i ublažavaju potencijalno opasne rizike do prihvatljive razine. Matrica procjene rizika alat je za određivanje prioriteta po rizicima u svrhu određivanja razine rizika. Matrica rizika prikazana je na Slici 13. te je iz nje vidljivo da vjerojatnost pojave rizika može biti prikazana kao učestala, povremena, rijetka, neznatna i izuzetno neznatna. Također označena je brojevima od 1 do 5 što označava vjerojatnost pojave gdje broj 1 prikazuje izuzetno neznatnu, a broj 5 učestalu vjerojatnost. Ozbiljnost rizika prema matrici može biti neznatna, mala, znatna, opasna i katastrofalna. Prikazuju se u matrici slovima A, B, C, D i E te označavaju ozbiljnost rizika[15].

RISK PROBABILITY	RISK SEVERITY				
	CATASTROPHIC (A)	HAZARDOUS (B)	MAJOR (C)	MINOR (D)	NEGLIGIBLE (E)
FREQUENT (5)	5 A	5 B	5 C	5 D	5 E
OCCASIONAL (4)	4 A	4 B	4 C	4 D	4 E
REMOTE (3)	3 A	3 B	3 C	3 D	3 E
IMPROBABLE (2)	2 A	2 B	2 C	2 D	2 E
EXTREMELY IMPROBABLE (1)	1 A	1 B	1 C	1 D	1 E

Slika 13 Matrica procjene rizika

Izvor: [13]

Procjena rizika izrađuje se na način da se rizik klasificira na tri razine kako je prikazano na Slici 14. Predloženi kriteriji procjene mogu biti nedopustivo područje, tolerantno područje i prihvatljivo područje. Indeks procjene rizika prikazuje vjerojatnost i ozbiljnost potencijalnog rizika te se označavaju kodom (broj i slovo). Kao povratne informacije o procijenjenom riziku

prikazani su predloženi kriteriji koji mogu biti neprihvatljivi u postojećim okolnostima, prihvatljivo temeljeno na smanjenju rizika i prihvatljivo [15].

SUGGESTED CRITERIA	ASSESSMENT RISK INDEX	SUGGESTED CRITERIA
INTOLERABLE REGION	5A, 5B, 5C, 4A, 4B, 3A,	Unacceptable under the existing circumstances
TOLERABLE REGION	5D,5E 4C,4D,4E 3B,3C,3D 2A, 2B,2C	Acceptable based on risk mitigation. It may require management decision
ACCEPTABLE REGION	4A 3A,3B 2A,2B,2C 1A,1B,1C,1D, 1E	Acceptable

Slika 14 Procjena rizika

Izvor: [15]

Za bolje razumijevanje matrice sigurnosnog rizika koriste se tablice vjerojatnosti i ozbiljnosti sigurnosnih rizika.

Tablica 2 Vjerojatnost sigurnosnog rizika

Vjerojatnost rizika	Objašnjenje	Vrijednost
Učestalo	Mogućnost pojave događaja više puta (> 3 puta godišnje)	5
Povremeno	Mogućnost pojave događaja ponekad (< 3 puta godišnje)	4
Rijetko	Mogućnost pojave događaja rijetka (barem jednom u kompaniji a redovno u zrakoplovnoj industriji)	3
Neznatno	Mogućnost pojave neznatna (nije poznata pojava u kompaniji ali barem jednom u zrakoplovnoj industriji)	2
Izuzetno neznatno	Mogućnost pojave izuzetno neznatna (nikada se nije dogodio u zrakoplovnoj industriji)	1

Izvor: [15]

Tablica 3 Ozbiljnost sigurnosnog rizika

Opasnost od pojave	Osoblje	Okoliš	Šteta [kn]	Utjecaj na ugled	Vrijednost
Katastrofalna	Višestruki smrtni slučajevi	Veliki učinak na zagađenje	Šteta>1M	Međunarodni utjecaj	A
Opasna	Ljudske žrtve	Učinci teški za popravak	Šteta<1M	Nacionalni utjecaj	B
Značajna	Ozbiljne ozljede	Učinci na lokalnoj razini	Šteta< 250.000	Značajan utjecaj	C
Mala	Lagane ozljede	Mali učinci	Šteta< 50.000	Ograničen utjecaj	D
Neznatna	Neznatne ili bez ozljeda	Neznatno ili bez učinka	Šteta< 5000	Mali ili bez učinka	E

Izvor: [15]

5.2.4. Osiguranje sigurnosti u odobrenoj organizaciji za osposobljavanje pilota

Osiguranje sigurnosti temelji se na principu kontinuiranog ciklusa poboljšanja. Kontinuirano poboljšanje postiže se internim evaluacijama, unutarnjim i vanjskim auditima i inspekcijama, a odnosi se na:

- proaktivno i reaktivno vrednovanje objekata, opreme, dokumentacije i postupaka audita, inspekcija i anketa vezanih za sigurnost;
- proaktivna procjena učinka pojedinca radi provjere ispunjavanja njegovih sigurnosnih obveza kao što su periodične provjere sposobnosti (evaluacija);
- reaktivne procjene kako bi se provjerila učinkovitost sustava za kontrolu i ublažavanje sigurnosti [15].

5.2.4.1. Praćenje i mjerenje performansi sigurnosti

Nadzor i mjerenje sigurnosnih performansi postupak je kojim se provjerava sigurnosna učinkovitost HZNS-a u odnosu na organizacijsku politiku sigurnosti i ciljeve koji su definirani u Priručniku upravljanja HZNS-a.

Mjerenje sigurnosnih performansi je aktivnost koja uključuje neprekidno nadgledanje i mjerenje odabranih pokazatelja sigurnosne učinkovitosti. Pokazatelji sigurnosne učinkovitosti imaju izravan utjecaj na sigurnosnu učinkovitost HZNS-a, povezane ciljeve i procese za koje su odgovorni rukovoditelji odjela. Voditelj odjela odgovoran je za praćenje i mjerenje performansi i rezultata procesa iz područja za koje je odgovoran. Aktivnosti odjela za sigurnost uključuju praćenje tih pokazatelja.

Ciljevi sigurnosnih performansi povezani su s pokazateljima sigurnosne učinkovitosti i postavljaju se na godišnjoj osnovi. Ovisno o pokazatelju, cilj se može smanjiti (broj pojava događaja) ili povećati u odnosu s sadašnjim statusom.

Proces praćenja sigurnosti uključuje:

- izvješćivanje o sigurnosti – podaci prikupljeni pomoću prikupljenih izvješća o sigurnosti predstavljaju vrijedan izvor informacija u vezi sa događajima i trendovima koji se odnose na sigurnost;
- studije sigurnosti – u slučaju kada nedostatak sigurnosti zahtijeva veliku promjenu, a ne identificiranje pojedinih opasnosti; studije sigurnosti uključivat će široka pitanja sigurnosti za analizu sličnih događaja; studije sigurnosti provode se tijekom sastanka SRB-a.
- sigurnosni pregledi – uključuju pregled sigurnosnih podataka od strane SM-a i mogu se odvijati za vrijeme SRB-a sastanaka
- sigurnosne audita usredotočene su na integritet sustava upravljanja HZNS-om i periodično ocjenjuju status ublažavanja sigurnosnog rizika;
- sigurnosna ispitivanja – ispitati određene elemente ili postupke kao što su problematična područja u svakodnevnim operacijama, percepcije i mišljenja operativnog osoblja i područja neslaganja ili zbunjenosti [15].

Mogući negativni trendovi i nedostaci mogu se utvrditi tijekom postupka. U takvim slučajevima koristi se postupak adekvatne audite. Svi relevantni podaci moraju se prikazati u procjeni upravljanja.

Auditi i inspekcije sigurnosti predstavljaju sustavni, neovisni i dokumentirani postupak prikupljanja dokaza i njihove objektivne procjene kako bi se utvrdilo u kojoj mjeri HZNS ispunjava i je li u skladu sa zahtjevima i internim postupcima koji se odnose na upravljanje sigurnošću. Planirani auditi sigurnosti i inspekcije u HZNS-u provode kvalificirani revizori organizacije. Audit sigurnosti i inspekcije usredotočene su na integritet sustava upravljanja i povremeno ocjenjuju stanje mjera ublažavanja sigurnosti.

Opseg audita i inspekcija sigurnosti:

- okviri audita ili inspekcije;
- proces upravljanja rizikom i povezane mjere ublažavanja rizika;
- ljudski resurs;
- izvedba;

- razina kompetencije i osposobljenosti za rukovanje opremom i objektima te održavanje njihove razine performansi [15].

Auditi i inspekcije sigurnosti mogu biti prema određenom rasporedu ili u slučaju događaja. Provode se s kontrolnom listom sigurnosti koja se dobiva iz relevantnih dokumenata o sigurnosnim propisima, priručnika i internih sigurnosnih propisa.

Ankete o sigurnosti provode se interno a inicirani su od SM-a ili kvalificiranog HZNS revizora. Ciljevi anketa su procijeniti čimbenike koji utječu na sigurnost, značajne aktivnosti i sigurnosne procese te olakšati prepoznavanje opasnosti i rizika.

Ako se promatra aktivnost prilikom anketiranja, posebno tijekom istraživanja leta i/ili simulatora koji će dovesti do pronalaska pojave koja može utjecati na sigurnost, mogu se zatražiti daljnji dokazi kako bi se moglo objektivno odrediti. Osobe koje provode ankete poziva se da ne upotrebljavaju niti jedan događaj da bi donijeli odluku. Događaji otkriveni tijekom ankete svakako moraju dovesti do daljnjih istraga i mogu dovesti do pronalaska. Stoga je bitno da situacija koja je opažena samo jednom ne mora nužno biti pokazatelj sustavnog nedostatka. Sigurnosne ankete uključuju upotrebu kontrolnih lista, upitima ili povjerljivih intervjua. Anketa se može zakazati i provesti kao:

1. samostalna aktivnost;
2. aktivnost potaknuta određenim događajem;
3. dio sigurnosne auditi ili inspekcije radi prikupljanja dokaza o provedbi [15].

5.2.4.2. Upravljanje promjenama u odobrenoj organizaciji za osposobljavanje pilota

Upravljanje promjenama je formalni postupak koji identificira vanjske i unutarnje promjene koje mogu utjecati na operacije HZNS-a i sigurnosne performanse. Upravljanje promjenama koristi postojeći postupak upravljanja sigurnošću HZNS-a za prepoznavanje potencijalnog rizika koji omogućava da nema štetnog utjecaja na sigurnost operacija. Promjene mogu uvesti nove opasnosti koje bi mogle utjecati na učinkovitost već postojećih postupaka ublažavanja rizika. Upravljanje promjenama može se odvijati tijekom sastanka SRB-a gdje SM vodi evidenciju zapisa.

Rezultat procesa upravljanja promjenama uključuje plan provedbe koji definira potrebne resurse, odgovornosti, rokove i daljnju komunikaciju i distribuciju informacija. Obavezna proaktivna identifikacija opasnosti, procjena i ublažavanje rizika primjenjuju se za slučajeve koji uključuju, ali se ne ograničavaju na:

- porast sigurnosnih događaja ili sigurnosnih kršenja;
- operativne promjene, uključujući ali ne ograničavajući se na: promjenu rukovodstva, zaposlenika, novih ruta, novih promjena obuke, tipa zrakoplova, primjena novih alata itd.;
- HZNS-ove strukturne promjene uključujući ali ne ograničavajući se na: brz rast ili smanjenje, pružatelje usluga, promjenu vlasništva;
- promjenama u propisima [15].

5.2.4.3. Kontinuirano unapređenje SMS-a u odobrenoj organizaciji za osposobljavanje pilota

HZNS kontinuirano nastoji poboljšati sigurnosne performanse i sustav upravljanja sigurnošću. Prvi korak za poboljšanje je upravljanje procesom. Procesom se ne može upravljati ako proces nije mjerljiv. Kontinuirano poboljšavanje potrebno pažljivo uzeti s postupkom mjerenja i praćenja učinka.

Svi izvori podataka konstantno se prate i postoji spremnost na uvođenje potrebnih promjena kako bi se sustav upravljanja osvježio i snažno usredotočio na kontinuirano poboljšavanje sigurnosnih performansi. To se postiže:

- planiranim i neplaniranim praćenjem (auditi i inspekcije) sustava upravljanja kao programa praćenja sigurnosti i usklađenosti;
- redovit pregled pokazatelja sigurnosne učinkovitosti i rezultata praćenja od strane SRB-a radi provjere sigurnosnih performansi HZNS-a;
- redovita analiza neispravnosti ili ispod-standardnih operativnih rezultata;
- utvrđivanje uzroka nestandardnih performansi;
- upravljanje rizikom;
- ublažavanje i eliminiranje uzroka nestandardnih performansi;

- periodične pregledavanje politike u svrhu osiguranja trajne važnosti za operacije HZNS-a;
- periodično pregledavanje priručnika i postupaka kako bi se osigurala kontinuirana usklađenost s propisima (najmanje jednom godišnje).

Zaključno, kontinuirano poboljšavanje može se provoditi sve dok HZNS pokazuje stalnu predostrožnost obzirom na učinkovitost svojih operacija i ublažavajućih radnji. Sukladno navedenom, svi procesi u HZNS-u odvijati će se najmanje jednom godišnje [15].

5.2.5. Promocija sigurnosti u HZNS-u

Osoblje HZNS-a dužno je proći obuku koja je sukladna odgovornostima koje to osoblje pruža unutar organizacije. Takva obuka vezna za sigurnost je integrirana kroz module školovanja. Osoblje HZNS-a prisustvuje nekim ili svim predavanjima modula ovisno o njihovoj poziciji, odjelu i budućem angažmanu u sigurnosnim aktivnostima. SM i CMM vode evidenciju o zaposlenicima koji su prošli obuku.

Nastavni plan modula predstavlja minimalne predmete koji će se obraditi tijekom osposobljavanja. a. Osposobljavanje može biti kao obuka u učionici ili kao samostalna obuka ovjerena od strane SM-a ili CMM-a.

SM ili CMM odlučuju o temi osposobljavanja i vode evidenciju o sposobnostima za sve iskorištene instruktore. Osposobljavanje će se provoditi u prvih šest mjeseci radnog odnosa ili uvođenjem modul školovanja. SM i CMM vode evidenciju o izvedbi obuke opisane u ovom poglavlju [15].

5.2.5.1. Osposobljavanje djelatnika za sigurnost

Osoblje uključeno u aktivnosti HZNS-a moraju proći odgovarajuću obuku o svojim odgovornostima u okviru HZNS-a. Obuka vezana uz nadzor sigurnosti i usklađenost sustava integriran je putem modula obuke. Djelatnici HZNS-a nazočiti će nekim ili svim modulima ovisno o njihovom položaju, odjelu i budućem sudjelovanju u aktivnostima praćenja sigurnosti i poštivanja propisa.

Nastavni plan modula za obuku predstavlja minimalne predmete kojima će se baviti tijekom obuke. Sama obuka može se provoditi u obliku učionice, samostalnim učenjem. Obuka

će se provoditi nakon zaposlenja ili nakon uvođenja sustava modula obuke. Obuka za rukovodeće osoblje sastoji se od početne obuke (moduli 1, 2, 3, 4 i 5) i dodatne obuke (moduli 6, 7, 8, 9 i 10). Revizori moraju proći početnu i dodatnu obuku. Obnova znanja se provodi svake tri godine.

Modul 1 odnosi se na prikazivanje i upoznavanje: HZNS-a, odnose s drugim organizacijama s kojima je HZNS u stalnoj interakciji, organizacijske strukture, odgovorno osoblje i sl. Osposobljavanje za Modul 1 traje 2 sata (30min za obnovu znanja), a obuku moraju proći svi zaposlenici organizacije.

Modul 2 se odnosi na prikazivanje opće svjesnosti o tome što je sigurnost uključujući: regulatorni okvir, koncepciju, elemente, procese, troškove i koristi sustava upravljanja sigurnošću. Osposobljavanje traje 4 sata (obnova znanja 1 sat) te obuku moraju proći svi zaposlenici.

Modul 3 obuhvaća kontinuirano poboljšanje organizacije. Obukom navedenog modula pruža se shvaćanje svrhe kontinuiranog praćenja, korektivnih i preventivnih mjera te sustava obuke. Osposobljavanje traje 2 sata za sve zaposlenike i 4 sata za AM-a, SM-a, CMM-a, auditore te druge zaposlenike sigurnosti.

Modul 4 pruža pregled i svijest o konceptu i aktivnostima sustava sigurnosti u HZNS-u, a to uključuje sigurnosnu politiku, strategije i sigurnosne ciljeve, regulatorni okvir SMS-a, integrirani pristup, SRB, SMS, te upravljanje promjenama. Vrijeme trajanja obuke je 3 sata (obnova znanja 45min), a obuku moraju proći svi zaposlenici.

Modul 5 pruža znanje i informacije o upravljanju dokumentacijom primjenjivom na HZNS operacije. To će uključivati pregled dokumentacije HZNS-a, postavljanje općih standarda dokumentacije, identifikacije i ručno označavanje, HZNS registar dokumenata, audit sustava priručnika te sustav raspodjele dokumentacije FPZ-HZNS. Trajanje obuke potrajati će 3 sata (30 min za obnovu znanja) te ju moraju proći svi zaposlenici [15].

Modul 6 odnosi se na pružanje svijesti o postojećim i primjenjivim propisima i njihovoj provedbi uključujući: nacionalno i međunarodno zakonodavstvo, propise koji se odnose na interakciju

FPZ-HZNS. Obuka traje 4 sata (1 sat za obnovu znanja) te ju trebaju proći AM, zaposlenici sigurnosti, CMM, rukovoditelji odjela i auditori.

Modul 7 ima za cilj dati pregled ERP elemenata i pojedinačnih dužnosti i dokumentacije, treninga diskusija. Trajanje ove obuke traje 2 sata (30 minuta za obnovu znanja) te obuku moraju proći AM, zaposlenici sigurnosti, rukovoditelji odjela, CMM i auditori.

Modul 8 odnosi se na pružanje praktičnog znanja i svijesti o upravljanju rizika, identifikaciji opasnosti, procjeni rizika te prednostima korištenja istih. Trajanje ove obuke traje 8 sata (2 sata za obnovu znanja) te obuku moraju proći AM, zaposlenici sigurnosti, rukovoditelji odjela, CMM.

Modul 9 pruža praktično znanje i svjesnost o razlozima mjerenja sigurnosnih učinaka, indikatorima performansi, reakcijama na uzbune, postavljanja razine ciljeva te prihvatljive razine sigurnosti. Trajanje ove obuke traje 4 sata (1 sata za obnovu znanja) te obuku moraju proći AM, zaposlenici sigurnosti, rukovoditelji odjela, CMM i auditori.

Modul 10 obuhvaća ugovorne aktivnosti. Cilj je osigurati praktično znanje i svijest o ugovornim aktivnostima HZNS-a i procesima praćenja. Trajanje ove obuke traje 4 sata (1 sata za obnovu znanja) te obuku moraju proći AM, zaposlenici sigurnosti, rukovoditelji odjela, CMM i auditori.

Modul 11 za cilj ima pripremiti buduće auditore za provođenje provjere kvalitete i provjere sigurnosti pomoću predavanja teorije i praktične obuke kroz auditi. Ova obuka je kompleksna te uključuje raspored audita, odgovornosti, pripremu, objavu, pronalazke, kontrolu i izvješća. Vrijeme trajanja obuke je 16 sat uključujući praksu, dok je samo ponavljanje gradiva 4 sata. Obuku moraju proći auditori koji su završili prva tri modula. [15].

Svrha kontinuiranog usavršavanja i HZNS-u je osigurati da organizacija i svi zaposlenici poboljšavaju i standarde performansi u pogledu svih aspekata, filozofija, politika i postupaka sustava upravljanja. Sustav obuke rukovodstva ponavlja se najmanje svake 3 godine ili svaki put nakon zabilježenih ozbiljnih odstupanja tijekom praćenja aktivnosti HZNS-a. Odgovornost SM i CMM je da organizira i vodi evidenciju o obuci rukovodstva [15].

5.2.5.2. Distribucija i komunikacija informacija i podataka vezanih za sigurnost u odobrenoj organizaciji za osposobljavanje pilota

Sigurnosna komunikacija izrazito je bitna za razvoj i održavanje odgovarajuće sigurnosne kulture u HZNS-u. Sigurnosna komunikacija sastoji se postupka procjene prikladnosti komunikacije o sigurnosti i o utjecaju na HZNS. Načini komunikacije uključuju:

- sigurnosne postupke i politiku;
- distribuciju dokumentacije HZNS-a;
- obavijestima o sigurnosti;
- redoviti sastanci između osoblja i AM-a radi informacijama o trenutnim radnjama i postupcima [15].

Sigurnosna komunikacija u HZNS-u osigurava:

- da su svi zaposlenici svjesni aktivnosti upravljanja sigurnošću i sigurnosne kulture HZNS-a;
- distribucije kritičnih sigurnosnih informacija posebno u vezi s procijenjenim rizicima i analiziranim opasnostima;
- objašnjenje zašto se poduzimaju pojedine radnje;
- objašnjenje zašto se sigurnosni postupci uvode ili mijenjaju;
- dopunjavanje i unapređivanje sigurnosne kulture HZNS-a [15].

SM odgovoran je za adekvatnu i pravovremenu komunikaciju o sigurnosti. Obavijesti o sigurnosti glavni su način sigurnosne komunikacije u HZNS-u te se objavljuju po potrebi.

Sustav internog prijavljivanja događaja vezanih za sigurnost jedan je od načina kvalitetne razmjene i distribucije sigurnosnih podataka te mu je primarna svrha poboljšanje razine sigurnosnih performansi organizacije a pri tome ne pripisivati krivicu. Dužnost svakog zaposlenika HZNS-a je da prijavi sve informacije koje mogu biti prethodnica nesrećama ili nezgodama. Cilj sustava prijavljivanja događaja je:

- omogućiti procjenu sigurnosnih postupaka posljedica svakog relevantnog incidenta i nesreće uključujući i prethodne slične pojave;

- osigurati široko znanje o relevantnim incidentima i nezgodama kako bi iz njih mogli naučiti;

Dužnost svakog zaposlenika HZNS-a je da prijavi sve informacije koje mogu biti prethodnica nesrećema ili nezgodama. [15].

6. ZAKLJUČAK

Sustav upravljanja sigurnošću je sustav kojom se osigurava siguran rad zrakoplova kroz učinkovito upravljanja sigurnosnim rizicima. Takav sustav je dizajniran za kontinuirano poboljšavanje sigurnosti prepoznavanjem opasnosti, prikupljanjem i analizom podataka i kontinuiranom procjenom sigurnosnih rizika. Iz razloga što ne postoji garancija da će ljudske aktivnosti ili sustavi izgrađeni od strane čovjeka biti potpuno oslobođeni operativnih grešaka i njihovih posljedica, sigurnost mora biti dinamična karakteristika zrakoplovnog sustava gdje se rizik sigurnosti mora neprestano umanjivati.

Sustav upravljanja sigurnošću potreban je zrakoplovnim organizacijama da prepozna opasnosti i kako upravljati rizicima tijekom isporuke svojih usluga ili proizvoda. SMS sadrži ključne elemente koji su bitni za prepoznavanje opasnosti i upravljanje sigurnosnim rizikom.

Kao pomoć državama u procesu implementacije sustava upravljanja sigurnošću u zrakoplovnim organizacijama izdan je Dodatak 19 koji sadrži SARP-ove za upravljanje sigurnosnim rizicima. Isto tako, ICAO je izdao Safety Management Manual (SMM) namijenjen pružanju smjernicama državama i zrakoplovnim organizacijama razvoju i primjeni sustava upravljanja sigurnošću koji je u skladu s međunarodnim standardima i preporučenim praksama.

Hrvatsko zrakoplovno nastavno središte neovisna je jedinica uspostavljena u svrhu praktičnog osposobljavanja pilota. Kao takva organizacija dužna je implementirati sustav upravljanja sigurnošću. Kako bi se sustav upravljanja sigurnosti implementirao potrebno je izraditi plan implementacije kroz koji je potrebno definirati rokove, akcije i način pristupa navedenom procesu. Potrebno je navesti da je sam proces implementacije fazni proces u četiri faze što omogućuje da sustav upravljanja sigurnošću postaje snažniji kako se završi svaka faza implementacije.

Unutar operativnog organizacijskog priručnika HZNS definira sustav upravljanja sigurnošću sukladno djelatnosti koju provodu. Priručnik (OOM) se sastoji od dvanaest dijelova unutar kojih su opisani politike i ciljevi organizacije, dokumentacija, struktura, obveze i dužnosti, sustav upravljanja, procesi kontinuiranog praćenja sigurnosti, evaluacije rukovodstva, sustava izvješćivanja, ERP-a, sustava obuke, obuke putem simulacija.

Cilj implementacije sustava upravljanja sigurnošću je uvođenje proaktivne politike sigurnosti u smislu utemeljenja sigurnosne kulture, dobrovoljnog sustava izvješćivanja, pripravnosti za opasnosti i rizike, kontinuiranog praćenja i drugih sigurnosnih elemenata. HZNS je kroz dugogodišnju implementaciju SMS unutar svoje organizacije postigao zavidnu razinu sigurnosti te potvrđuje činjenicu da SMS, ako je pravilno vođen smanjuje rizike od štetnih učinaka.

LITERATURA

1. International Civil Aviation Organization: Safety Management Manual, Doc 9859, AN/474, Fourth Edition, Montreal, Kanada, 2018.;
2. Chee Kin, R., The Impact of Safety Management Systems on Safety Performance: Commercial Aviation Operations; Thesis, Griffith University, Griffith, 2015;
3. Vuković, R., Implementacija sustava upravljanja sigurnošću u generalnoj avijaciji na primjeru operatera Geofoto, Diplomski rad, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2014.;
4. Steiner, S., Elementi sigurnosti zračnog prometa, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 1998.;
5. International Civil Aviation Organization: Safety Management Manual, Doc 9859, AN/474, Third Edition, Montreal, Kanada, 2013.;
6. International Civil Aviation Organization, International Standards and Recommended Practices, Annex 19 to the Convention on International Civil Aviation, Safety Management, First Edition, 2013.;
7. Use of Safety Management Systems by ATM Service Providers, ESSAR 3, 2000.;
8. Batuwangala, E., Silva, J., Wild, G., The Regulatory Framework for Safety Management Systems in Airworthiness Organisations; RMIT University, Melbourne, 2018.;
9. Steiner, S., Materijali za nastavu kolegija: „Sigurnost zračnog prometa“, Fakultet prometnih znanosti, Zagreb, 2014.;
10. The European Aviation Safety Programme, The European Aviation Safety Programme Document, 2nd edition, Report to the European Parliament and the Council, European Commission, Brussels, 7.12.2015.;
11. European Aviation Safety Agency, European Plan for Aviation Safety 2016.-2020. Final, 25.1.2016.;
12. Hrvatska agencija za civilno zrakoplovstvo, Naredba o zrakoplovnoj sigurnosti, Sigurnosna direktiva, ASO-2010-004, Implementacija sustava upravljanja sigurnošću, Zagreb, 2013.;

13. Safety Management International Collaboration Group, SMS for Small Organizations, Guidance to Small Organizations on Implementing SMS, 2015.;
14. Hrvatsko zrakoplovno nastavno središte: <https://www.fpz.unizg.hr/zan/?tag=hzns> (kolovoz, 2019.)
15. Croatian Aviation Training Center (HZNS), Organization's Management Manual, Faculty of Transport and Traffic Sciences, Zagreb 2017.

POPIS KRATICA

AM (Accountable Manager) Odgovorni rukovoditelj

AMO (Approved Maintenance Organization) Odobrena organizacija za održavanje zrakoplova

ATO (Approved Training Organization) Odobrena organizacija za osposobljavanje

ATS (Air Traffic Services) Usluge u zračnom prometu

CAMO (Continuing Airworthiness Management Organization)

CCAA (Croatian Civil Aviation Agency) Hrvatska agencija za civilno zrakoplovstvo

CMM (Compliance Monitoring Manager) Rukovoditelj nadzora usklađenosti

EASA (European Aviation Safety Agency) Europska agencija za zrakoplovnu sigurnost

EASP (European Aviation Safety Programme/European Aviation Safety Policy) Europski program zrakoplovne sigurnosti/Europska politika zrakoplovne sigurnosti

EPAS (European Plan for Aviation Safety) Europski plan za zrakoplovnu sigurnost

ERP (Emergency Response Plan) Interventni plan

ESARR EUROCONTROL Safety Regulatory Requirement) EUROCONTROL-ovi regulatorni sigurnosni zahtjev

EU (European Union) Europska Unija

FTTS/FPZ (Faculty of transport and Traffic Sciences) Fakultet Prometnih Znanosti

HZNS/CATC (Croatian Aviation Training Centre) Hrvatsko Znanstveno Nastavno Središte

ICAO (International Civil Aviation Organization) Međunarodna organizacija za civilno zrakoplovstvo

JAA (Joint Aviation Authorities) Zajedničke zrakoplovne vlasti

JAR-FCL (Join Aviation Requirements Flight Crew License) Zajedničke zrakoplovne vlasti - certifikat letećeg osoblja

QM (Quality Management) Upravljanje kvalitetom

SAG (Safety Action Group) Sigurnosne grupe

SARP (Standards and Recommended Practices) Standardi i preporučene prakse

SM ICG (Safety Management International Collaboration Group) Međunarodna grupa za suradnju upravljanja sigurnošću

SMM (Safety Management Manual) Priručnik upravljanja sigurnošću

SMS (Safety Management System) Sustav upravljanja sigurnošću

SSP (State Safety Program) Nacionalni program sigurnosti zračnog prometa

POPIS SLIKA

Slika 1. Faze razvoja sustava upravljanja sigurnošću	5
Slika 2. SHEL model	8
Slika 3. Koncept nastanka nesreće.....	10
Slika 4. Elementi upravljanja sigurnošću.....	12
Slika 5. Prikaz metoda upravljanja sigurnošću	13
Slika 6. Klasifikacija nesigurnih djela	15
Slika 7. Sistematični pristup upravljanja sigurnošću	21
Slika 8. ICAO okvir sustava upravljanja sigurnošću	27
Slika 9. Postupak prepoznavanja i upravljanja sigurnosnim rizikom	33
Slika 10. Primjer analize nedostataka (GAP analiza)	43
Slika 11. Obrazac identifikacije opasnosti	57
Slika 12. Analiza opasnosti i proces procjene rizika	60
Slika 13. Matrica procjene rizika	61
Slika 14. Procjena rizika	62

POPIS TABLICA

Tablica 1. Usporedba QMS-a i SMS-a	41
Tablica 2 Vjerojatnost sigurnosnog rizika	63
Tablica 3 Ozbiljnost sigurnosnog rizika	63



Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj _____ diplomski rad
isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na
objavljenju literaturu što pokazuju korištene bilješke i bibliografija.
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz
necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj
visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu _____ diplomskog rada
pod naslovom **Implementacija sustava upravljanja sigurnošću na primjeru**
odobrene organizacije za osposobljavanje pilota
na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom
repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 11.9.2019 _____

Student/ica: _____
(potpis)