

SMERNICE ZA INTEGRACIJO IN CENTRALIZACIJO

Povzetek smernic

Različica: 1.1

Ljubljana, januar 2022

Izvajalci:	Univerza v Ljubljani Fakulteta za elektrotehniko Ljubljana, Tržaška cesta 25
	Univerza v Ljubljani Fakulteta za računalništvo in informatiko Ljubljana, Večna pot 113
Podizvajalec:	IPMIT Institut za projektni management in informacijsko tehnologijo d.o.o. Ljubljana, Kotnikova 30
Naročnik:	Družba za avtoceste v Republiki Sloveniji (DARS d.d.) Celje, Ulica XIV. divizije 4
Številka pogodbe:	DARS št. 2019/2018
Številka naloge:	2.1.2
Naslov naloge:	Analiza stanja in priprava podlag za integracijo in centralizacijo sistemov za nadzor in vodenje prometa v NC DARS - 2. segment Smernice za integracijo in centralizacijo
Naslov dokumenta:	Povzetek smernic
Različica dokumenta:	1.0
Nosilec pogodbe izvajalca:	dr. Andrej Kos, univ. dipl. inž. el. (UL FE)
Predstavniki izvajalca:	dr. Andrej Kos, univ. dipl. inž. el. (UL FE) dr. Marko Bajec, univ. dipl. inž. rač. in inf. (UL FRI)
Predstavniki naročnika:	Božidar Volk, univ. dipl. gosp. inž. (DARS) Kristjan Cah, dipl. org. inf. (DARS)
Datum izdelave:	april 2021
Datum spremembe:	Januar 2022

- Soavtorji dokumentov (UL FE):
- dr. Janez Bešter, univ. dipl. inž. el.
 - dr. Andrej Kos, univ. dipl. inž. el.
 - dr. Matevž Pogačnik, univ. dipl. inž. el.
 - dr. Urban Sedlar, univ. dipl. inž. el.
 - dr. Andrej Štern, univ. dipl. inž. el.
 - mag. Roman Kotnik, univ. dipl. inž. el.
 - mag. Luka Koršič, univ. dipl. inž. el.
 - Jaka Cijan, univ. dipl. inž. el.
 - Klemen Pečnik, univ. dipl. inž. el.
- Soavtorji dokumentov (UL FRI):
- dr. Marko Bajec, univ. dipl. inž. rač. in inf.
 - dr. Slavko Žitnik, univ. dipl. inž. rač. in mat.
 - dr. Dejan Lavbič, univ. dipl. inž. rač. in inf.
- Soavtorji dokumentov (Ipmit):
- mag. Dejan Štrukelj, univ. dipl. ekon.
 - mag. Roman Tomažič, univ. dipl. inž. rač. in inf.
 - Aljaž Bratkovič, mag. posl. ved
- Soavtorji dokumentov (DARS):
- Kristjan Cah, dipl. org. inf.
 - Marko Kovačič, univ. dipl. inž. el.
 - Robert Kompan, univ. dipl. inž. tehnol. prom.
 - Aleš Rink, dipl. inž. rač.
 - Amir Mehadžič, dipl. inž. el.

Različice dokumenta

Različica	Datum	Spremembe
1.0	April 2021	Izdaja različice 1.0
1.1	Januar 2022	Spremenjena različica 1.1 brez točke 5 – Področje kadrov

Pomembno

Tehnološke smernice različice 1.1, povzete v tem dokumentu, predstavljajo prvi korak k zagotavljanju jasnih usmeritev z neposredno uporabno vrednostjo v postopkih integracije in centralizacije na področjih arhitekture vodenja prometa, komunikacijskih omrežnih storitev, informacijskih in aplikativnih rešitev, video nadzornega sistema ter področja kadrovskih kompetenc za obvladovanje visoko-tehnološke infrastrukture.

Bolj poglobljena obravnava presega okvir izvedenega projekta.

V okviru dokumenta Predstavitev projekta so nakazani nadaljnji koraki v smeri tehnično poglobljenih smernic in nujnost njihovega stalnega posodabljanja skladno z dinamiko sprememb na področju IKT ter prioritete družbe DARS.

Kazalo

Predstavitev dokumenta	1
1. Arhitektura sistemov upravljanja s prometom (<i>SIC-ARH</i>)	2
1.1. Organizacija nadzornih centrov (<i>SIC-ARH-ORG</i>)	2
1.2. Funkcije nadzornih centrov (<i>SIC-ARH-FUN</i>)	3
1.3. Prezemi funkcij med nadzornimi centri (<i>SIC-ARH-PRF</i>)	8
2. Komunikacijska omrežja (<i>SIC-OMR</i>)	10
2.1. Arhitektura komunikacijskega vozlišča in podatkovnega centra (<i>SIC-OMR-AKR</i>)	10
2.2. Arhitektura lokalnih in dostopovnih omrežij (<i>SIC-OMR-LOK</i>)	13
2.3. Zagotavljanje zanesljivosti in razpoložljivosti (<i>SIC-OMR-ZZR</i>)	15
2.4. Zagotavljanje varnosti na omrežnem nivoju (<i>SIC-OMR-VAR</i>)	17
2.5. Upravljanje in nadzor omrežij (<i>SIC-OMR-UNO</i>)	20
2.6. Višje nivojski komunikacijski protokoli (<i>SIC-OMR-PRO</i>)	23
2.7. Testiranje omrežij in omrežnih naprav (<i>SIC-OMR-TST</i>)	25
3. Aplikacijski nivo (<i>SIC-APL</i>)	27
3.1. Arhitektura aplikacijskega nivoja (<i>SIC-APL-AAN</i>)	27
3.2. Sistemske zahteve (<i>SIC-APL-SIS</i>)	38
3.3. Standardi in protokoli na aplikacijskem nivoju (<i>SIC-APL-STP</i>)	45
3.4. Hranjenje podatkov (<i>SIC-APL-HP</i>)	49
3.5. Testiranje aplikacij in testna okolja (<i>SIC-APL-TST</i>)	55
3.6. Zagotavljanje varnosti na aplikacijskem nivoju (<i>SIC-APL-VAR</i>)	61
3.7. Integracija z zunanjimi sistemi (<i>SIC-APL-INT</i>)	79
3.8. Podatkovni centri (<i>SIC-APL-PDC</i>)	81
3.9. Obravnava nepredvidenih dogodkov (<i>SIC-APL-OND</i>)	84
4. Video nadzorni sistem (<i>SIC-VID</i>)	87
4.1. Arhitektura sistema za video nadzor prometa (<i>SIC-VID-AVS</i>)	87
4.2. Povezljivost in omrežni nivo (<i>SIC-VID-PON</i>)	91
4.3. Kamere za video nadzor prometa (<i>SIC-VID-CAM</i>)	93
4.4. Sistemi za video detekcijo prometa (<i>SIC-VID-VDP</i>)	97
5. Zaključek	98

Predstavitev dokumenta

Dokument Povzetek smernic predstavlja strnjen skupek smernic iz posameznih področnih dokumentov različice 1.0:

- Arhitektura sistemov upravljanja s prometom (SIC-ARH)
- Komunikacijska omrežja (SIC-OMR)
- Aplikacijski nivo (SIC-APL)
- Video nadzorni sistem (SIC-VID)

Smernice so zapisane po poglavjih s kratkimi uvodi, ki uporabniku predstavijo namen podanih vsebin. V kolikor uporabniku dokumenta v strnjenem izvlečku povzeta smernica ne vsebuje dovolj informacij, lahko za dodatne razlage poseže po celovitih področnih dokumentih z vsebovanimi ustreznimi utemeljitvami.

Podrobna predstavitev metodologije priprave dokumentov in smernic, skupaj z načini njihove uporabe, je podrobno opisana v uvodnem dokumentu Predstavitev dokumenta.

V nadaljevanju so področni dokumenti predstavljeni po posameznih poglavjih z aktualnimi smernicami iz različice 1.0. Pričakovano je, da se bo vsaka sprememba v obliki dodajanja ali posodobitve smernic v področnih dokumentih odražala tudi na tem Povzetku smernic. Tako bo aktualna različica Povzetka smernic vedno odražala stanje celotnih usmeritev za integracijo in centralizacijo.

1. Arhitektura sistemov upravljanja s prometom (SIC-ARH)

V okviru arhitekture sistemov upravljanja s prometom so bile obravnavane hierarhična organizacija nadzornih centrov, zanesljivost arhitekture in opredeljenost delovnih mest nadzornikov prometa. Hkrati so bile obravnavane relacije med nadzornimi centri in funkcije, ki se v njih izvajajo. ter pogoji za uspešno prevzemanje samih funkcij med različnimi nadzornimi centri v primeru zaznanih težav v delovanju, izvajanja vzdrževalnih del in podobnih situacijah.

Na podlagi navedenih obravnav so bile pripravljene smernice, ki so namenjene optimalni organizaciji nadzornih centrov in so razdeljene v sledeča medsebojno vsebinsko povezana poglavja:

- Organizacija nadzornih centrov
- Funkcije nadzornih centrov
- Prevzemi funkcij med nadzornimi centri.

1.1. Organizacija nadzornih centrov (SIC-ARH-ORG)

Nadzorni centri DARS delujejo v režimu 24/7, njihov osnovni namen pa je upravljanje s kritično cestno prometno infrastrukturo. Sam sistem upravljanja s prometom je hierarhično razdeljen na več nivojev. Stopnja razvitosti nadzornih centrov na posameznem nivoju je različna. Posledično mora DARS ob vpeljevanju novih rešitev izvajati heterogene pristope, ki zahtevajo več napora in finančnih vložkov. Priporoča se postopna vpeljava in uporaba sistematičnega pristopa, s katerim se bo zagotovila osnova za izvajanje dolgoročne integracije.

Z namenom večanja zanesljivosti delovanja in omogočanja prevzemanja upravljanja iz oddaljene lokacije (npr. v času motenega delovanja določenega nadzornega centra) je treba določene elemente arhitekture (npr. procesorsko moč, algoritme, pravila in pomnilniške kapacitete) premakniti čim bolj k virom, saj so tako na razpolago za lokalno upravljanje tudi v primerih izpada komunikacijskih poti. Hkrati je treba poenotiti tudi opremo delovnih mest v nadzornih centrih. Vse navedeno je mogoče v določenem obsegu doseči tudi z uporabo IP-KVM sistema, katerega uporaba se predlaga v prehodnem obdobju, in sicer dokler ni zagotovljena enotna implementacija smernic aplikativnega nivoja. Poseben poudarek je zaradi razpršenosti lokacij, sistemov in večjega števila uporabnikov treba nameniti upravljanju uporabniških profilov. Uvesti je treba enotno prijavo.

SIC-ARH-ORG-010:

Pri vpeljavi novih rešitev ali posodobitvah sistemov in naprav upravljanja s prometom je treba zagotoviti skladnost s smernicami za integracijo in centralizacijo. V smernicah naj bodo opredeljena pravila, po katerih se izvajajo nadgradnje sistemov ali se nova oprema (programska in strojna) integrira v sistem.

SIC-ARH-ORG-020:

Za večanje zanesljivosti arhitekture je treba določene elemente arhitekture, kot so npr. procesorska moč, algoritmi, pravila in pomnilniške kapacitete, premakniti k virom.

SIC-ARH-ORG-030:

Organiziranost in opredeljenost delovnega mest nadzornika prometa mora biti poenotena na vseh nivojih nadzornih centrov. To velja predvsem za programsko opremo in uporabniške vmesnike. Hkrati mora biti v čim večji meri zagotovljena tudi enaka strojna oprema, kamor spada število in razporeditev monitorjev, tipkovnica, telefon in stenski prikazovalnik.

SIC-ARH-ORG-040:

Sistemi za nadzor in vodenje prometa morajo biti zasnovani na način, da je z njimi mogoče upravljati preko tehnologije IP-KVM.

SIC-ARH-ORG-050:

Upravljanje sistemov, npr. predorov, trase, ipd. iz LNC se v prehodnem obdobju lahko izvede tudi centralizirano in integrirano z uporabo tehnologije IP-KVM. Dolgoročna uporaba IP-KVM sistema se predlaga za tiste sisteme, ki ne bodo centralizirani, je pa pomembno, da so hitro dostopni.

SIC-ARH-ORG-060:

Nadzornikom prometa v nadzornem centru mora biti omogočena personalizirana enotna prijava v sistem ne glede na lokacijo. Po prijavi bo nadzornik prometa lahko izvajal le tiste funkcije, ki mu jih omogočajo dodeljene uporabniške pravice.

1.2. Funkcije nadzornih centrov (SIC-ARH-FUN)

V okviru nadzornih centrov se izvaja večje število funkcij (npr. upravljanje s prometom, zagotavljanje nadzora nad delovanjem opreme, načrtovanje upravljanja s prometom, obveščanje uporabnikov ipd.), pri čemer trenutno ni jasne ločnice, katere funkcije in na kakšen način se izvajajo na posameznem hierarhičnem nivoju nadzornih centrov. Posledično je treba vpeljati jasno delitev pristojnosti in odgovornosti, in sicer predvsem na relaciji med GNC in RNC. Prav tako je pomembno, da se funkcije enotno izvajajo v vseh nadzornih centrih. Prvi korak predstavlja delitev funkcij na strateške (namenjene so dolgoročnemu načrtovanju razvoja

upravljanja s prometom) in operativne (namenjene konkretnim akcijam upravljanja s prometom).

Pomembno je, da imajo nadzorniki prometa v nadzornih centrih v realnem času na razpolago pravilne in ažurne podatke, ki jim omogočajo izvajanje funkcij vodenja in nadzora prometa in so pravočasno opozorjeni na morebitne anomalije. Prav tako morajo biti vpeljane rešitve nadzornega sistema, ki omogočajo izvajanje nadzora nad pravilnim delovanjem posameznih komponent strojne in programske opreme nadzornega centra in nadzornega centra kot celote. K visoki učinkovitosti vodenja in nadzora prometa doprinese tudi vpeljava jasno definiranih pravil na segmentu koordinacije delovanja nadzornih centrov in obveščanja uporabnikov ali zunanjih entitet, in sicer v obliki ustreznih postopkovnikov. Poglavje je razdeljeno na naslednja področja:

- Splošni del
- Strateške funkcije
- Operativne funkcije

Splošni del

SIC-ARH-FUN-010:

V nadzornih centrih se mora na vseh nivojih zagotoviti poenoteno izvajanje funkcij, kot so upravljanje s prometom, obveščanje uporabnikov, zagotavljanje nadzora nad delovanjem opreme, načrtovanje upravljanja s prometom in podobne.

SIC-ARH-FUN-020:

Uvede naj se kategorizacija funkcij na strateške in operativne funkcije. Strateške funkcije so namenjene pripravi dolgoročnega načrtovanja upravljanja s prometom in pripravi strategije razvoja tehnoloških sistemov. Operativne funkcije pa so namenjene upravljanju s prometom, upravljanju s podatki, zagotavljanju nadzora nad delovanjem opreme, koordinaciji med nadzornimi centri in ostalimi entitetami ter obveščanju uporabnikov in ostalih entitet.

Strateške funkcije

SIC-ARH-FUN-030:

Funkcije se morajo izvajati skladno z dolgoročnim načrtom upravljanja s prometom, v katerem je opredeljeno tudi enotno izvajanje funkcij v vseh nadzornih centrih po hierarhiji (GNC – RNC) in usklajene pristojnosti ter odgovornosti posameznih subjektov. Podrobno morajo biti opredeljeni tudi postopki sodelovanja med nadzornimi centri v primeru izvajanja ukrepov na območjih, kjer se stikajo pristojnosti različnih RNC. Vključiti je treba predorske in trasne NZiR.

SIC-ARH-FUN-040:

Za izmenjavo podatkov med nadzornimi centri, in sicer na relacija GNC-RNC in RNC-RNC, morajo biti usklajeni postopki izmenjave. Prav tako je treba zagotoviti jasne definicije, kateri podatki se izmenjujejo, v kakšni obliki in s kakšnim namenom.

Operativne funkcije

SIC-ARH-FUN-050:

Pripravi naj se strategija razvoja tehnoloških sistemov, iz katere bo razvidna jasno opredeljena smer nadaljnjega razvoja posameznega sistema oz. podsistema, uporabljenega v nadzornem centru. V strategiji se opredeli vizija bodočega razvoja, oblikuje strateške cilje za celoten nabor sistemov in podsistemov v nadzornih centrih in opredeli smer bodočega razvoja. Dokument strategije predstavlja osnovo za bodoče nadgradnje že vpeljanih sistemov in podsistemov ter vpeljavo novih.

SIC-ARH-FUN-060:

Nadzorniki prometa v nadzornih centrih morajo imeti v realnem času na razpolago podatke, ki jim omogočajo izvajanje funkcij vodenja in nadzora prometa na trasi in v predoru. Funkcije upravljanja s prometom se morajo v vseh nadzornih centrih izvajati na enoten način in z uporabo čim bolj enotnih rešitev oziroma čim bolj poenotenih uporabniških vmesnikov.

SIC-ARH-FUN-070:

Koordinacijo delovanja RNC v primeru dogodkov, ki presegajo pristojnosti posameznega RNC, glede na strateško in vsebinsko razdelitev prevzame GNC.

SIC-ARH-FUN-080:

V primeru nastopa izrednega dogodka morajo biti sistemi v čim večji meri sposobni samodejne zaznave in analize le-tega. Na podlagi zaznave tovrstnih dogodkov morajo biti avtomatsko proženi alarmi, ki na dogodek opozorijo nadzornika prometa v nadzornem centru. Nadzornik prometa se na dogodek odzove skladno s sprejetimi postopkovniki (predorskimi in trasnimi NZiR). Kjer je mogoče, naj bo zagotovljeno avtomatsko izvajanje ukrepov po vnaprej opredeljenih programih.

SIC-ARH-FUN-090:

Med odzivom na izredni dogodek oziroma reševanjem katere druge situacije je treba shraniti čim več podatkov o poteku akcije, npr. vodenje ustreznih dnevnikov, pri čemer tehnološka rešitev avtomatsko generira predlogo z vsemi relevantnimi podatki. Po odzivu na izredni dogodek se opravi pogovore z vsemi vpletenimi entitetami in preuči vse zbrane izkušnje. Po analizi je treba pripraviti predloge izboljšav in po potrebi ažurirati navodila za ukrepanje.

SIC-ARH-FUN-100:

Za potrebe ukrepanja v primeru predvidenih izrednih dogodkov morajo biti vnaprej pripravljeni in vzdrževani ustrezni postopkovniki. Nadzorniki prometa v nadzornem centru izvajajo ukrepe skladno s sprejetimi postopkovniki.

SIC-ARH-FUN-110:

Zajem in zbiranje podatkov naj bo pomaknjeno čim bolj k samim virom podatkov, da so podatki na razpolago za lokalno upravljanje tudi v primerih izpada komunikacijskih poti ali regionalnih nadzornih centrov.

SIC-ARH-FUN-120:

Zajem podatkov mora biti omogočen iz vseh nameščenih trasnih in predorskih podsistemov. Omogočen naj bo tudi zajem podatkov iz zunanjih sistemov. Zajem podatkov mora vsebinsko in tehnološko potekati na čim bolj enoten način in je v domeni RNC. Podatke iz tujine zajema GNC.

SIC-ARH-FUN-130:

Obdelava podatkov na nivoju RNC in GNC se mora vsebinsko in tehnološko izvajati na čim bolj enoten način in po vnaprej opredeljenih pravilih. Na nivoju RNC naj se obdelava podatkov izvaja za potrebe delovanja posameznega RNC, kompleksnejše analize in obdelave podatkov naj se izvajajo v okviru GNC. Podatki morajo biti transformirani v pravilno obliko, očiščeni, opremljeni s časovnim žigom in navedbo lokacije.

SIC-ARH-FUN-140:

Analiza podatkov mora biti pripravljena na način, da je mogoča izmenjava podatkov med različnimi sistemi in aplikacijami. Omogočen mora biti prenos podatkov med nadzornimi centri. V okviru RNC se analizirani podatki uporabljajo zgolj za potrebe upravljanja prometa na lokalni ravni, medtem ko se prenos podatkov preko GNC izvaja za potrebe upravljanja prometa na državni in meddržavni ravni. Kot naprednejšo obliko analize podatkov se priporoča uporaba mehanizma strojnega učenja.

SIC-ARH-FUN-150:

Zagotovljene morajo biti kontrole, kot je npr. protokol sinhronizacije, ali se podatki zbirajo, pravilno obdelujejo in pravilno prenašajo med posameznimi entitetami. Na morebitna odstopanja (nedelovanje naprave ali sistema) mora sistem avtomatsko opozoriti pristojni nadzorni center (RNC ali GNC).

SIC-ARH-FUN-160:

Hramba podatkov mora biti organizirana na način, da omogoča visoko stopnjo neprekinjenega poslovanja tudi v primeru izpadov delov sistemov.

SIC-ARH-FUN-170:

Vpeljane morajo biti rešitve nadzornega sistema, ki omogočajo izvajanje nadzora nad pravilnim delovanjem posameznih komponent strojne in programske opreme nadzornega centra in nadzornega centra kot celote. V okviru RNC mora biti omogočeno izvajanje samo-diagnostike in posredovanje napak oziroma odstopanj v delovanja direktno reševalcem. Nadzorni center naj bo v tem primeru samo obveščen o avtomatskem posredovanju.

SIC-ARH-FUN-180:

Uporaba sistemov za vodenje in nadzor prometa mora biti na vsakem hierarhičnem nivoju čim bolj poenotena, v smislu enakih funkcionalnosti in zmogljivosti sistema. Omogočeno mora biti prevzemanje funkcij med nadzornimi centri, ki se izvaja po vnaprej opredeljenih pogojih in protokolih.

SIC-ARH-FUN-190:

Koordinacijo med nadzornimi centri izvaja GNC. Operativno izvajanje samih aktivnosti na lokalni ali regionalni ravni ostaja v domeni posameznih RNC-jev.

SIC-ARH-FUN-200:

Opredeljeni morajo biti enotni protokoli za izvajanje koordinacije na lokalni ravni, ki je v pristojnosti RNC. Čezmejna koordinacija naj se po večini izvaja preko GNC (ohrani se obstoječe dobre prakse).

SIC-ARH-FUN-210:

Pri obveščanju uporabnikov mora biti zagotovljena točnost, konsistentnost in ažurnost obvestil na vseh uporabljenih komunikacijskih kanalih.

SIC-ARH-FUN-220:

Ne glede na komunikacijski kanal se mora obveščanje zunanjih entitet izvajati po vnaprej opredeljenih protokolih, ki jih je treba vključiti v postopkovnike. Izmenjava obvestil in podatkov na meddržavni ravni naj poteka po protokolu DATEX II.

1.3. Prevzemi funkcij med nadzornimi centri (SIC-ARH-PRF)

Za učinkovito upravljanje s prometom je ključno usklajeno delovanje nadzornih centrov na vseh hierarhičnih nivojih. V primeru izpadov delovanja posameznega centra (npr. zaradi okvar, vzdrževalnih del, ...) mora biti njihova vloga v procesu upravljanja s prometom ustrezno prevzeta s strani preostalih nadzornih centrov. Povezanost med nadzornimi centri mora biti zato vzpostavljena na način, da je omogočeno prevzemanje funkcij drugih nadzornih centrov v primeru izpadov v delovanju le-teh. Prevzemanje funkcij nadzornih centrov mora biti omogočeno na relacijah RNC - GNC, RNC - LNC, RNC - RNC in LNC - LNC.

Predpogoj za prevzemanje funkcij med nadzornimi centri na različnih nivojih je ustrezno zasnovana topologija prenosnih omrežij in postavitve ter zasnova strojne in programske. Prav tako morajo biti vzpostavljeni ustrezni varnostni mehanizmi na organizacijskem in aplikativnem nivoju, ki bodo omogočali zanesljiv in varen prenos funkcij. Po vzpostavitvi tehničnih in organizacijskih pogojev za prevzem funkcij med nadzornimi centri je treba opredeliti tudi jasna pravila in postopke po katerih se ti prenosi izvajajo, in sicer tako v smeri prevzema funkcij, kot kasnejše povrnitve v normalno stanje.

SIC-ARH-PRF-010:

Povezanost med nadzornimi centri mora biti vzpostavljena na način, da je omogočeno prevzemanje funkcij drugih nadzornih centrov v primeru izpadov v delovanju le-teh. Primer izpadov predstavljajo izvajanje vzdrževalnih del, okvare ali drugi podobni dogodki. Prevzemanje funkcij nadzornih centrov naj bo omogočeno med nivoji RNC – GNC in RNC - LNC ter znotraj posameznega nivoja RNC – RNC in LNC - LNC.

SIC-ARH-PRF-020:

Topologija prenosnih omrežij in postavitev ter zasnova strojne in programske opreme mora biti vzpostavljena na način, da omogoča prevzemanje funkcij med nadzornimi centri na različnih nivojih.

SIC-ARH-PRF-030:

Za prenos izvajanja funkcij med nadzornimi centri morajo biti vzpostavljeni varnostni mehanizmi na organizacijskem in aplikativnem nivoju, ki bodo omogočali zanesljiv in varen prenos funkcij.

SIC-ARH-PRF-040:

Postopkovniki morajo jasno opredeljevati postopke pod katerimi se izvajajo prenosi funkcij med nadzornimi centri v procesu prevzema in kasnejše povrnitve v normalno stanje.

2. Komunikacijska omrežja (*SIC-OMR*)

Dokument Komunikacijska omrežja obravnava arhitekturo komunikacijskih omrežij naročnika z vidikov zagotavljanja varnosti, zanesljivosti, razpoložljivosti in skladnosti z uveljavljenimi standardi ter dobrimi praksami. Rezultat dokumenta je strnjen v smernicah, kjer so usmeritve na posameznih področjih podane z različnimi stopnjami priporočil po nujnosti upoštevanja, od neobveznih do najvišjih zahtev po upoštevanju. Pregledna shema arhitekture omrežja s hrbteničnim, lokalnimi in dostopovnimi omrežji je v izvirnem dokumentu prikazana v uvodnem poglavju, tu prikazane smernice pa so razvrščene po naslednjih poglavjih:

- Arhitektura komunikacijskega vozlišča in podatkovnega centra
- Arhitektura lokalnih in dostopovnih omrežij
- Zagotavljanje zanesljivosti in razpoložljivosti
- Zagotavljanje varnosti na omrežnem nivoju
- Upravljanje in nadzor omrežij
- Višje nivojski komunikacijski protokoli
- Testiranje omrežij in omrežnih naprav

2.1. Arhitektura komunikacijskega vozlišča in podatkovnega centra (*SIC-OMR-AKR*)

Najvišje v arhitekturi omrežja se nahajajo glavni nadzorni center (GNC) ter druga komunikacijska vozlišča s podatkovnimi centri, ki predstavljajo stičišče in agregacijo podatkovnih tokov notranjih podsistemov. Tu se podatki shranjujejo, izmenjujejo, obdelujejo in prikazujejo v realnem času. Osnovne funkcije tega dela omrežja so tudi povezave z zunanjimi sistemi (npr. OKC in CORS) ter zagotavljanje izhodne točke v javni internet. GNC se s svojo logično nadzorno vlogo vodenja, ki je danes fizično prisotna v Dragomlju, prek hrbteničnih povezav omrežja DARS povezuje do geografsko ločenih RNC, ki s svojimi lokalnimi omrežji predstavljajo vir za dostop in priključevanje senzorskih podatkov. Smernice za arhitekturo krovnega in povezovalnega omrežja obravnavajo povezave, opremo, tehnologije, protokole in mehanizme, ki se odražajo po celotnem omrežju DARS. Poglavje Arhitektura komunikacijskega vozlišča in podatkovnega centra obravnava naslednja področja:

- Vpeljava omrežnih varnostnih con
- Podpora globalnemu usmerjanju in večdomnost
- Sekundarne lokacije nadzornih centrov
- Tunelski mehanizmi med nadzornimi centri
- Podpora za oddaljen dostop
- Smernice za razvoj omrežja za video promet
- Zagotavljanje kakovosti storitev
- Topologija povezav med nadzornimi centri
- Uporaba mobilnih tehnologij v omrežju DARS

Vpeljava omrežnih varnostnih con

SIC-OMR-AKR-010:

Po celotnem omrežju naročnika je potrebna vpeljava omrežnih varnostnih con. Naročnik s tem pridobi boljši pregled nad omrežjem ter bolj preprosto in sistematično nastavitve varnostnih politik.

Podpora globalnemu usmerjanju in večdomnost

SIC-OMR-AKR-020:

Iz omrežja naročnika naj bo omogočena vzpostavitev večdomnih povezav proti vsaj dvema ponudnikoma internetnih storitev. Večdomna povezava mora biti vzpostavljena s pomočjo protokola BGP prek enega ali dveh robnih usmerjevalnikov v avtonomnem sistemu naročnika na ločenih lokacijah, saj to omogoča vzpostavitev redundantnih povezav proti internetu.

Sekundarne lokacije nadzornih centrov

SIC-OMR-AKR-030:

V primeru izpada določenega nadzornega centra je potrebno njegovo funkcijsko vlogo prevzeti na sekundarni lokaciji. Z rezervno lokacijo ali več njih je potrebno pokriti izpade nadzornih centrov vseh nivojev v hierarhiji. Hrbtenično omrežje in lokalna omrežja nadzornih centrov morajo biti načrtovani na način, da preslikana lokacija v kateremkoli trenutku ne presega omrežnih kapacitet.

Tunelski mehanizmi med nadzornimi centri

SIC-OMR-AKR-040:

Za zagotavljanje kibernetske varnosti se na povezavah med nadzornimi centri predvidi uporaba tunelskih povezav z mehanizmi avtentikacije, enkripcije in integritete podatkovnih tokov. Varnostni prehodi na lokacijah nadzornih centrov morajo podpirati protokol IPsec, ki mora biti obvezno uporabljen v primeru vzpostavitve tunelskih povezav čez javni internet in opsijsko na povezavah MPLS VPN, saj slednji ne omogoča mehanizmov za zagotavljanje varnosti na omrežnem nivoju (npr. šifriranje prometa IP).

Podpora za oddaljen dostop

SIC-OMR-AKR-050:

V javnem internetu lociranim uporabnikom omrežja DARS in oddaljenim lokacijam je potrebno zagotoviti varen in zanesljiv dostop do notranjih virov omrežja prek navideznih zasebnih omrežij. Za vzpostavitev povezav VPN med lokacijama je potrebno namestiti ustrezno na pravo tj. požarno pregrado, usmerjevalnik ali L3 stikalo na rob omrežja in na pripadajočo oddaljeno lokacijo. Prav tako je potrebno terminalno opremo, tj. računalnik, tablico ali pametni telefon, opremiti z ustrezno programsko opremo za vzpostavljanje tunelov glede na pravila in varnostno politiko oddaljenega dostopa do notranjega poslovnega omrežja naročnika.

Smernice za razvoj omrežja za video promet

SIC-OMR-AKR-060:

Omrežje za prenos videa mora biti izvedeno ločeno od drugega podatkovnega prometa v lokalnem delu omrežja naročnika do LNC ali RNC, kar zahteva vpeljavo nove opreme in vzpostavitev novih povezav po celotnem omrežju naročnika. V ločenem omrežju za video je potrebno zagotoviti nadzor in ločeno upravljanje omrežja. V hrbteničnem omrežju se ti dve omrežji združita na isti fizični povezavi z virtualno ločitvijo na VRF in VLAN. V ločenem omrežju za prenos video prometa naj se na omrežnem nivoju izključi QoS, jumbo pakete in flow control ter se uporabi stikala, ki podpirajo IEEE 802.1BA/Q/AS. Za upravljanje multicast prometa naj se uporabi IGMPv3 ter usmerjevalni protokol PIM.

Zagotavljanje kakovosti storitev

SIC-OMR-AKR-070:

Omrežne naprave v omrežju naročnika morajo podpirati mehanizme za zagotavljanje kakovosti storitev. Vpeljani koncepti QoS morajo naročniku omogočati ustrezno obravnavo različnih podatkovnih tokov, kjer se ob omrežnih zamašitvah bolj pomembnim tokovom zagotovi manjše zakasnitve ter manjšo verjetnost izgube paketov.

Topologija povezav med nadzornimi centri

SIC-OMR-AKR-080:

Med nadzornimi centri morajo biti vzpostavljene redundantne povezave. Stremeti je potrebno proti topologiji zanke in se izogibati topologiji zvezde. Uporaba najetih vodov za sekundarne povezave se priporoča v primerih, kjer so ti speljani po ločenih geografskih poteh glede na primarne povezave. Za potrebe zagotavljanja sekundarnih ali terciarnih redundantnih povezav med nadzornimi centri je potrebno upoštevati možnosti uporabe mobilnih tehnologij.

Uporaba mobilnih tehnologij v omrežju DARS

SIC-OMR-AKR-090:

Za doseganje visokih stopenj zanesljivosti, redundance, varnosti in fleksibilnosti v omrežju naročnika je potrebno vključevanje sodobnih mobilnih tehnologij. Pri uvajanju konceptov IoT z velikim številom senzorskih naprav se za zagotavljanje zmogljivosti, garancije QoS in povečano varnost uporabijo napredni namenski mehanizmi in protokoli mobilnih omrežij.

2.2. Arhitektura lokalnih in dostopovnih omrežij (SIC-OMR-LOK)

Poudarki pri omrežni arhitekturi narekujejo izvedbo topologije lokalnih omrežij v obliki zank (angl. mesh), kjer se obroč topološko smatra kot najnižja oblika redundantne izvedbe povezav. Dopusča se možnost povezovanja nižje ležečih nadzornih centrov neposredno na hrbtenico. Potrebno je zagotoviti podporo za IPv6 protokol za omrežne in končne naprave, ki se priključujejo v omrežje naročnika. Zagotoviti je potrebno segmentacijo vsakega senzorskega sistema v svoj VLAN, kjer logično zasnovani naslovni shemi IPv4 in IPv6 zagotavljata možnosti sledljivosti in hitrega geolociranja posamezne naprave v omrežju. Zaradi specifik se naj prenos video prometa izvaja v ločenem omrežju od ostalih podatkovnih virov. Po celotnem komunikacijskem omrežju se mora podpreti uporabo konceptov QoS, ki naročniku omogočajo pretok kritičnih podatkov v primeru zamašitev.

Poglavje Arhitektura lokalnih in dostopovnih omrežij obravnava naslednja področja:

- Topologija lokalnih omrežij
- Vpeljava IPv6 protokola v omrežje DARS
- Segmentacija podsistemov DARS s pomočjo tehnologij VLAN
- Segmentacija in dodeljevanje naslovov IPv4
- Segmentacija in dodeljevanje naslovov IPv6
- Izmenjava podatkov med podsistemi
- Priključevanje in nadzor novih senzorskih podsistemov

Topologija lokalnih omrežij

SIC-OMR-LOK-010:

Topologija povezav v lokalnih omrežjih naročnika mora biti zasnovana kot dvonivojska zanka topologija. Zanka prvega nivoja naj povezuje agregatorje prometa na nivoju predorov ali regionalnega nadzornega centra. Zanke drugih nivojev naj povezujejo na topologijo obroča več dostopovnih vozlišč, ki predstavljajo točke priklopa za senzorske podsisteme. Glede na obstoječe stanje lokalnih povezav, se za vzpostavitev redundantnih povezav med LNC in vozlišči proti RNC lahko uporabi tudi redundantno hrbtenično omrežje.

Vpeljava IPv6 protokola v omrežje DARS

SIC-OMR-LOK-020:

Vsi prihodnji senzorski sistemi, strežniška infrastruktura, uporabniške ter omrežne naprave v omrežju naročnika morajo podpirati dvojni protokolni sklad IPv4/IPv6.

Segmentacija podsistemov DARS s pomočjo tehnologij VLAN

SIC-OMR-LOK-030:

Vsak senzorski podsistem v omrežju naročnika mora biti nameščen v svoje virtualno lokalno omrežje VLAN. S segmentacijo in uporabo VLAN lahko naročnik zagotovi izolacijo prometa na določen senzorski podsistem ne glede na fizično lokacijo posamezne naprave v omrežju. Na ta način sta pregled in upravljanje omrežnih segmentov lažja, enostavnejša pa je tudi implementacija varnostne politike.

Segmentacija in dodeljevanje naslovov IPv4

SIC-OMR-LOK-040:

Naslovna shema segmentacije celotnega IPv4 naslovnega prostora v omrežju naročnika mora biti zasnova smiselno z možnostjo prepoznavne geolokacije ter podsistema, kateremu končna naprava pripada. Tovrstna razdelitev IP naslovnega prostora zagotavlja naročniku logično in optimalno vključevanje novih naprav ali podsistemov v omrežje. Ob tem je možna tudi vzpostavitev optimalnega usmerjanja prometa glede na lokacijo posameznega podomrežja oz. gradnjo povzetkov poti pri uporabi usmerjevalnih protokolov.

Segmentacija in dodeljevanje naslovov IPv6

SIC-OMR-LOK-050:

Interna politika določanja IPv6 naslovov v omrežju naročnika mora zagotoviti način zapisa naslova, iz katerega je logično prepoznaven storitveni segment ter geolokacija naprave. IPv6 naslovi so dolgi, zato je potrebno izbrati dober kompromis med preglednostjo in ohranjanjem zadostne količine informacij. Za enkratne entitete v omrežju DARS je priporočljivo, da imajo najkrajšo možno obliko zapisa. Med te naprave se uvrščajo strežniki ter omrežna oprema. Pri množici končnih naprav želi naročnik pridobiti sledljivost in hitro geolokacijsko prepoznavo že iz zapisa samega.

Izmenjava podatkov med podsistemi

SIC-OMR-LOK-060:

Izmenjava podatkov med podsistemi omrežja naročnika mora biti izvedena na enotni požarni pregradi, ki je nameščena na lokaciji lokalnega ali regionalnega nadzornega centra. Predvidi se, da ima požarna pregrada na lokaciji lokalnega nadzornega centra nameščeno redundantno požarno pregrado, ki s primarno komunicira prek protokolov za zagotavljanje visoke razpoložljivosti. Na ta način se zagotovi enotna točka upravljanja in nadzora za vse senzorske podsisteme, ki se v omrežje priključujejo pod okriljem določenega RNC. Pisanje pravil na požarni pregradi je tako preprostejše in bolj pregledno ter omogoča hitrejšo integracijo novih podsistemov v omrežje naročnika. Požarna pregrada mora biti v upravljanju DARS ali s strani DARS specializiranega pooblaščenega zunanjega izvajalca.

Priključevanje in nadzor novih senzorskih podsistemov

SIC-OMR-LOK-070:

Vsi senzorski podsistemi, ki se povezujejo v omrežje, se morajo držati jasnih in enotnih pravil priključevanja. Politika integracije in komunikacija med podsistemi je definirana s strani omrežne administracije naročnika, ki opravlja tudi popoln nadzor in upravljanje nad vsemi podsistemi. V primeru vzdrževanj, odpovedi ali napak na opremi podsistemov mora imeti naročnik vpogled v vse dnevniške zapise naprav.

2.3. Zagotavljanje zanesljivosti in razpoložljivosti (SIC-OMR-ZZR)

V omrežju naročnika je potrebno vzpostaviti geografsko redundantno lokacijo z vso kritično infrastrukturo. V lokalnih omrežjih se vzpostavi delovanje protokolov za preprečevanje zank ter protokolov za zagotavljanje visoke razpoložljivosti. Izmenjava podatkov med podsistemi se izvaja na požarni pregradi, ki ima zagotovljeno redundantno postavitev. Nastavitve požarnih pregrad v lokalnih omrežjih se določi na način, kjer so najbolj kritični sistemi vedno dosegljivi, delujoči in centralno upravljani. Za vse regionalne nadzorne centre se predvidi sekundarne lokacije v primeru izpada. Nadzorni centri so med seboj povezani prek varnih povezav VPN. Redundanca povezav se izvede po topologiji zank. Predvidi se nadgradnjo povezav s pomočjo mobilnih tehnologij 5G.

Poglavje Zagotavljanje zanesljivosti in razpoložljivosti obravnava naslednja področja:

- Zagotavljanje redundance med agregacijskimi vozlišči
- Georedundanca kritične strežniške in omrežne infrastrukture
- Protokoli za preprečevanje zank na nivoju L2
- Združevanje vmesnikov v navidezni kanal
- Protokoli za zagotavljanje visoke razpoložljivosti na omrežnem nivoju

Zagotavljanje redundance med agregacijskimi vozlišči

SIC-OMR-ZZR-010:

Topologija povezav med agregacijskimi vozlišči lokalnih omrežij naročnika mora biti izvedena redundantno. Redundanco zagotovimo s popolno zanko ali s topologijo obroča s prostorsko fizično ločenimi povezavami. V kolikor popolne zanke ali takega obroča ni mogoče zagotoviti, so lahko agregacijska vozlišča neposredno povezana tudi prek hrbteničnega omrežja, katerega topologija je redundantna.

Georedundanca kritične strežniške in omrežne infrastrukture

SIC-OMR-ZZR-020:

V omrežju naročnika je potrebno vzpostaviti geografsko redundantno sekundarno lokacijo z vso kritično omrežno in strežniško infrastrukturo. Zagotoviti je potrebno zadostno razdaljo med lokacijama, da se izravna tveganje večine okoljskih in tehničnih dejavnikov, ki lahko vplivajo na delovanje celotnega sistema.

Protokoli za preprečevanje zank na nivoju L2

SIC-OMR-ZZR-030:

V omrežju naročnika se na vseh segmentih zančnih topologij med stikali zahteva uporabo zaščitnih mehanizmov za preprečevanje zank STP, RSTP in MSTP ter hitrih preklopov na redundantne povezave v primeru izpadov. Izhodišča za izbor protokolov za preprečevanja zank so časovne zahteve naprav in aplikacij, ki jih uporablja naročnik.

Združevanje vmesnikov v navidezni kanal

SIC-OMR-ZZR-040:

V omrežju naročnika se za povečanje prepustnosti in večje razpoložljivosti med segmenti LAN priporoča vzpostavitev kanalov z združevanjem vmesnikov. Uporaba tovrstnih kanalov je smiselna, kjer to omogoča omrežna infrastruktura, sicer se predvidi nadgradnja fizičnih povezav in zamenjava vmesnikov oz. celotnih stikal.

Protokoli za zagotavljanje visoke razpoložljivosti na omrežnem nivoju

SIC-OMR-ZZR-050:

V omrežju naročnika se na segmentih lokalnih omrežij, v katerih so nameščene končne ali senzorske naprave za podporo kritičnim sistemom, zahteva uporabo virtualnih nadomestnih usmerjevalnih protokolov. Z uporabo VRRP ali po funkcionalnosti enakovrednih protokolov je omogočen aktivni preklon prometa prek redundantne naprave v najkrajšem možnem času.

2.4. Zagotavljanje varnosti na omrežnem nivoju (SIC-OMR-VAR)

Nastavitve omrežnih varnostnih politik morajo po celotnem omrežju naročnika privzeto blokirati vse dohodne in odhodne podatkovne prometne tokove proti in iz vseh kritičnih podsistemov. Za omrežje naročnika se priporoča razdelitev na večje število varnostnih con. Podprto je potrebno imeti večdomno BGP povezavo proti internetu. Zunanjim deležnikom se omogoči povezavo do omrežja DARS prek oddaljenega dostopa ali varne povezave oddaljene lokacije. Uporaba sistema za upravljanje varnostnih informacij in dogodkov je nujna zaradi statusa kritičnosti infrastrukture. Zagotoviti je potrebno robustne avtentikacijske mehanizme ter, v primeru varnostnih incidentov, skladnost odzivnih procesov z varnostno politiko podjetja. Potrebno je izvesti integracijo sistemov za detekcijo in preprečevanje vdorov. Prav tako morajo biti fizično zaščitene pred zunanjimi dejavniki tudi naprave v omrežju naročnika, kjer je potrebno izvesti izklop nerabljenih storitev in zahtevati avtentikacijo priklopa končnih naprav.

Poglavje Zagotavljanje varnosti na omrežnem nivoju obravnava naslednja področja:

- Fizična zaščita naprav
- Izklop neuporabljenih storitev na omrežni opremi
- Omejevanje in avtentikacija priklopa končnih naprav
- Zaščitni mehanizmi za ohranjanje topologije zank
- Zagotavljanje varnosti protokola IP na omrežni opremi
- Integracija sistemov za detekcijo in preprečevanje vdorov
- Uporaba sodobne varnostne platforme
- Delovanje požarnih pregrad v lokalnih omrežjih
- Nastavitve omrežnih varnostnih politik
- Avtentikacijski mehanizmi in uporaba močnih gesel
- Sistemi za upravljanje varnostnih informacij in dogodkov
- Vzpostavitev odzivnega procesa v primeru incidentov

Fizična zaščita naprav

SIC-OMR-VAR-010:

Omrežne in senzorske naprave v naročnikovem omrežju morajo biti ustrezno fizično zaščitene pred okoljskimi nevarnostmi in pred človeškimi faktorji. Vsi fizični posegi in dostopi do opreme morajo biti odobreni in zabeleženi z dnevniško sledjo. Uvede naj se uporaba dvofaktorske avtentikacije in uporaba biometrije tam, kjer so najbolj kritični segmenti.

Izklop neuporabljenih storitev na omrežni opremi

SIC-OMR-VAR-020:

Po celotnem omrežju naročnika se zahteva izklop vseh nerabljenih protokolov, storitev in vmesnikov na vseh omrežnih napravah, s čimer se močno zmanjša površina za kibernetске napade.

Omejevanje in avtentikacija priklopa končnih naprav

SIC-OMR-VAR-030:

V omrežju naročnika se povsod, kjer je to mogoče, zahteva uporaba protokolov za omejevanje števila končnih naprav na dostopovnih stikalih, avtentikacije, implementacije varnostne politike ter centralnega nadzora priključenih končnih naprav 802.1x. Uvajanje naprav, ki ne podpirajo 802.1x, je možno samo z odobritvijo naročnika.

Zaščitni mehanizmi za ohranjanje topologije zank

SIC-OMR-VAR-040:

V zankastih topologijah segmentov LAN omrežja naročnika je potrebno zaščititi topologije na L2 pred morebitnimi nepooblaščenimi spremembami ter odpraviti možnost morebitnega izpada ali napada, ki je posledica priključevanja naprav na stikalo. S tem se nepooblaščenim osebam onemogoči, da bi lahko v omrežje priključile svoje korensko stikalo, ki bi predstavljalo stično točko vsega podatkovnega prometa.

Zagotavljanje varnosti protokola IP na omrežni opremi

SIC-OMR-VAR-050:

Za stikala v omrežju naročnika, kjer ni implementirana centralna avtentikacija končnih naprav, se zahteva uporaba mehanizmov DHCP snooping, Dynamic ARP Inspection ter IP Source Guard ali po funkcionalnosti enakovrednih zaščitnih mehanizmov.

Integracija sistemov za detekcijo in preprečevanje vdorov

SIC-OMR-VAR-060:

V omrežju naročnika mora biti nameščen in pravilno konfiguriran sistem za detekcijo in preprečevanje vdorov v realnem času.

Uporaba sodobne varnostne platforme

SIC-OMR-VAR-070:

Omrežje naročnika mora imeti integrirano varnostno platformo naslednje generacije, ki skrbi za filtracijo prometa ter vsebuje napredne mehanizme sodobnih požarnih pregrad kot so prepoznavanje aplikacij na L7, prepoznavanje uporabnikov, zaščita proti zlonamerni programski kodi ter možnost pregledovanja kriptiranega prometa. Zagotovljena mora biti možnost enotnega upravljanja in nadzora skupine vseh požarnih pregrad iz centralne lokacije ter tudi možnost lokalnega upravljanja vsake požarne pregrade posebej.

Delovanje požarnih pregrad v lokalnih omrežjih

SIC-OMR-VAR-080:

V primeru odpovedi RNC ali ključne omrežne opreme ali povezave iz RNC proti LNC centrom mora vsak LNC delovati kot samostojna omrežna entiteta in zagotavljati implementacije varnostnih politik za vse senzorske podsisteme. V primeru odpovedi LNC mora njegovo funkcijsko vlogo prevzeti RNC ali drug LNC. V času normalnega obratovanja RNC in vseh povezav na nivoju lokalnega omrežja pa je požarna pregrada v LNC lahko v aktivnem ali pasivnem načinu delovanja. Način delovanja določa implementacija logik varnostnih nastavitev, ki je pogojena z naborom funkcionalnosti požarne pregrade.

Nastavitve omrežnih varnostnih politik

SIC-OMR-VAR-090:

Omrežna varnostna politika mora po celotnem omrežju naročnika privzeto blokirati vse dohodne in odhodne podatkovne prometne tokove proti in iz vseh kritičnih podsistemov v omrežju.

Avtentikacijski mehanizmi in uporaba močnih gesel

SIC-OMR-VAR-100:

Robustni avtentikacijski mehanizmi predstavljajo pomemben aspekt informacijske in komunikacijske varnosti. Kjer je mogoče, se na omrežni in strežniški infrastrukturi predvidi uporaba javnih in zasebnih ključev ter strojnih ključev. Kjer je edina možnost uporaba gesla, mora to biti dovolj kompleksno in imeti omejen rok trajanja. Za kritične storitve, dostopne z javnega interneta, priporočamo uporabo dvofaktorske avtentikacije. Z gesli je potrebno ravnati pazljivo in jih v primeru kompromitiranja nemudoma spremeniti. Naročnik mora vse zahteve, povezane z življenjskim ciklom in uporabo gesel, zbrati v obliki celovite varnostne politike podjetja.

Sistemi za upravljanje varnostnih informacij in dogodkov

SIC-OMR-VAR-110:

Glede na kritičnost operacij je v omrežju naročnika nujna uporaba sistema SIEM za zbiranje in korelacijo dnevniških zapisov in varnostnih dogodkov, kar omogoča skrajšanje časa, potrebnega za detekcijo varnostnega incidenta.

Vzpostavitev odzivnega procesa v primeru incidentov

SIC-OMR-VAR-120:

V omrežju naročnika mora biti vzpostavljen odzivnik v primeru kibernetkega napada, tehnične ali človeške napake, ki ogrozi normalno delovanje omrežja in naprav. Z učinkovitim odzivnim procesom naročnik pridobi ustaljene postopke ter tehnične in netehnične prijeme, ki zmanjšajo potreben čas do ponovno delujočega stanja sistema ali omrežja.

2.5. Upravljanje in nadzor omrežij (SIC-OMR-UNO)

Smernice za upravljanje in nadzor omrežij DARS se osredotočajo na omrežne, senzorske in končne naprave, povezave ter na omrežje kot celoto. Učinkovit nadzor nad omrežjem in napravami samimi omogoča upravljalcem omrežja hitrejšo detekcijo morebitnih napak v omrežju ter ponovno vzpostavitev normalno delujočega stanja omrežja v čim krajšem možnem času. Dobre prakse na tem področju pripomorejo k lažji integraciji novih storitev v obstoječe omrežje ter vzpostavitev enotnih točk upravljanja omrežja s sodobnimi orodji in koncepti.

Z vpeljavo sistema za spremljanje sprememb v omrežju z revizijsko sledjo pri nadgradnjah se naročniku zagotovi povrnitev vseh predhodno delujočih stanj omrežja. Vpeljava testnega okolja predvidi izvedbe testnih scenarijev ob nadgradnjah v omrežju. Uvedba naprednega sistema za

nadzor storitev in alarmiranje kvarnih dogodkov omogočata naročniku nadzor nad storitvami in napravami ter zmanjšata potreben čas do ponovne povrnitve sistema v delujoče stanje.

Poglavje Upravljanje in nadzor omrežij obravnava naslednja področja:

- Centralni nadzor omrežja DARS
- Centralno upravljanje omrežja DARS
- Sistem za spremljanje sprememb v omrežju z revizijsko sledjo
- Vpeljava testnega okolja
- Mehanizem za povrnitev omrežja na stabilno različico
- Sistem za nadzor storitev
- Sistem za alarmiranje
- Uvedba konzolnega dostopa do vseh naprav v omrežju

Centralni nadzor omrežja DARS

SIC-OMR-UNO-010:

V omrežju naročnika je potrebno vzpostaviti platformo za centralni nadzor omrežja, povezav ter ključnih omrežnih in končnih naprav.

Centralno upravljanje omrežja DARS

SIC-OMR-UNO-020:

V omrežju naročnika je potrebno vzpostaviti platformo in uporabiti orodja za centralno upravljanje omrežnih naprav.

Sistem za spremljanje sprememb v omrežju z revizijsko sledjo

SIC-OMR-UNO-030:

V omrežju naročnika mora biti vzpostavljen sistem za spremljanje sprememb nastavitev vseh omrežnih naprav z revizijsko sledjo. Naročniku je na ta način omogočena povrnitev predhodno delujoče stanja naprav v primeru morebitnih napak. Naročnik naj za sledljivost operacij v omrežju uvede tudi ticketing sistem.

Vpeljava testnega okolja

SIC-OMR-UNO-040:

V omrežju naročnika je nujna vzpostavitev testnega okolja in testnih scenarijev ob nadgradnjah programske opreme, operacijskih sistemov ali sprememb v nastavitvah naprav. Izvedba tovrstnega testiranja v testnem okolju se za naročnika prevede ob nadgradnjah obstoječih in integraciji novih naprav ali storitev.

Mehanizem za povrnitev omrežja na stabilno različico

SIC-OMR-UNO-050:

V omrežju naročnika se mora zagotoviti sisteme za sledenje in povrnitev celotnega ali dela omrežja na katerokoli prejšnjo stabilno različico programske opreme, operacijskega sistema ali nastavitvene datoteke.

Sistem za nadzor storitev

SIC-OMR-UNO-060:

V omrežju naročnika naj bo omogočena vzpostavitev sistema za nadzor delovanja storitev neodvisno od nadzora omrežnih naprav.

Sistem za alarmiranje

SIC-OMR-UNO-070:

V omrežju naročnika mora biti vzpostavljen centralni sistem za alarmiranje v primeru odpovedi omrežnih povezav, naprav ali storitev. Uporabljati se mora tudi kanal za obveščanje o alarmih, katerega delovanje ni odvisno od internetne povezave.

Uvedba konzolnega dostopa do vseh naprav v omrežju

SIC-OMR-UNO-080:

Administratorji naročnikovega omrežja morajo vedno imeti omogočen konzolni dostop do vseh fizičnih in virtualnih naprav v omrežju. Naročniku je tako omogočena možnost spreminjanja nastavitve omrežnih in strežniških naprav tudi v primeru internetnega izpada.

2.6. Višje nivojski komunikacijski protokoli (SIC-OMR-PRO)

Obravnava višjenivojskih protokolov mora biti prilagojena posameznim aplikacijam in storitvam. Stremeti je potrebno k uporabi manjšega števila protokolov, ki so širše poznani in standardizirani. Po dogovoru z naročnikom se lahko uporablja tudi lastniške protokole, kjer mora vpeljava potekati po postopkih, ki veljajo za razvoj standardiziranih (od razvoja do testiranj). Pri vrednotenju protokolov je potrebno upoštevati vsaj naslednje kriterije: dokumentiranost, učinkovitost, robustnost, varnost, razširjenost in izbran podatkovni model. Z obravnavanimi koraki in vidiki (tudi avtomatiziranega) testiranja dobi naročnik zagotovilo, da je uporabljen protokol primeren za uporabo in zadošča zahtevam aplikacije. Za poenotenje komunikacijske ravni se priporoča postopno uvajanje poenotene arhitekture OPC UA. Zato naj vse nove namestitve naprav ali sistemov že omogočajo priključitev v OPC UA, za starejše sisteme pa se predvideva uvedba namenskih protokolnih prehodov.

Poglavje Višje nivojski komunikacijski protokoli obravnava naslednja področja:

- Standardizacija protokolov
- Izbira protokolov
- Testiranje protokolov
- Vpeljava poenotene odprte arhitekture OPC UA

Standardizacija protokolov

SIC-OMR-PRO-010:

Določitev protokolov mora biti izvedena za vsako posamezno aplikacijo in storitev. Za aplikacije s podobnimi zahtevami je možna uporaba istih protokolov, a le v primeru predhodno potrjene skladnosti z zahtevami. S tem se zagotovijo najvišje stopnje varne in učinkovite rabe protokolov za posamezne aplikacije.

SIC-OMR-PRO-020:

Za lažje obvladovanje uporabljenih protokolov je nujna uporaba čim manjšega nabora standardiziranih protokolov. Prednostno se naj izbirajo protokoli, ki so poznani evropskemu prostoru in pripadajo priznanim standardizacijskim telesom, kar omogoča lažjo vpeljavo opreme in izvedbo postopkov integracije.

SIC-OMR-PRO-030:

Lastniške ali lastno dopolnjene protokole se lahko, po dogovoru z naročnikom, vpelje samo v primerih, kjer standardizirani protokoli zahtevam aplikacije ne ustrezajo. Vpeljava mora potekati po postopkih, ki veljajo za standardizacijo (nedvoumen opis, formalna specifikacija, verifikacija) in razvoj protokolov (faze specifikacije, načrtovanja, implementacije, testiranja). Na tak način bodo lastniški protokoli po lastnostih lahko primerljivi s standardiziranimi.

Izbira protokolov

SIC-OMR-PRO-040:

Kriteriji za izbiro protokolov se določijo na osnovi zahtev aplikacij. Za primerjavo protokolov in njihovo izbiro je potrebno vrednotiti vsaj naslednje kriterije: dokumentiranost, učinkovitost, robustnost, varnost, razširjenost in izbran podatkovni model. Z izpolnjevanjem teh kriterijev bo izbran protokol optimalna rešitev za določeno aplikacijo.

Testiranje protokolov

SIC-OMR-PRO-050:

Preden se izbrani protokol vključi v uporabo, ga je potrebno testirati. Testiranje protokolov naj vključuje vsaj preverjanje skladnosti, funkcionalno preverjanje, preverjanje skalabilnosti, učinkovitosti, združljivosti in negativno testiranje.

SIC-OMR-PRO-060:

Testiranje protokolov mora zagotoviti izvajalec storitve oz. aplikacije. Izvaja naj se po korakih: analiza protokolnih zahtev, priprava načrta testiranja, priprava testnih scenarijev, izvedba testov in priprava dokumentacije. Naročnik bo s tem dobil zagotovilo, da je uporabljen protokol primeren za uporabo in zadošča zahtevam aplikacije.

SIC-OMR-PRO-070:

Za učinkovito pripravo testnih scenarijev naj se uporabi pristop z uporabo standardiziranega testnega jezika, npr. TTCN-3, kar omogoči avtomatsko ustvarjanje testnih primerov in zaznavanje morebitnih napak.

Vpeljava poenotene odprte arhitekture OPC UA

SIC-OMR-OPC-010:

Problem razdrobljenosti sistemov in težav z različnimi vmesniki za vsak podsistem je potrebno rešiti s poenoteno platformo. Po vzoru industrije 4.0, interneta stvari in dobrih praks v tujini naj naročnik stremi k vpeljavi enotne arhitekture OPC UA.

SIC-OMR-OPC-020:

Vse nove namestitve in nadgradnje naprav (lokalne postaje, podsistemi, strežniki) in aplikacij naj imajo podporo za OPC UA, kar zagotovi postopno vključevanje v napredno, zmogljivo, zanesljivo in varno komunikacijsko arhitekturo med podsistemi, lokalnimi postajami in aplikacijami.

SIC-OMR-OPC-030:

Za prilagoditev protokolov obstoječih komunikacijskih vmesnikov in starejših naprav na arhitekturo OPC UA je potrebno uporabiti protokolne prehode. Za prehod se lahko uporabijo rešitve uveljavljenih proizvajalcev, v primeru lastniških rešitev pa se zahteva implementacija strežnika OPC UA.

SIC-OMR-OPC-040:

Zagon arhitekture OPC UA naj bo postopen, z vključevanjem najprej omejenega števila naprav in aplikacij ter postopno širitvijo na širši nabor, vključno s protokolnimi prehodi za starejše sisteme.

2.7. Testiranje omrežij in omrežnih naprav (SIC-OMR-TST)

Visoko kakovost komunikacijskega omrežja je možno doseči z učinkovitim testiranjem omrežij in omrežnih naprav. Pri testiranju omrežij je potrebno dobro razumeti zastavljene cilje, testiran sistem in testne postopke, kar je možno s postopno izvedbo testiranja po korakih. Izvajalci testiranj morajo pred samo izvedbo pripraviti strukturiran opis testnih scenarijev v namenskem dokumentu, ki vključuje vse potrebne informacije o načrtovanih testih. Po izvedbi testiranja se pripravi poročilo, ki mora vsebovati vsaj razširjene podatke o testiranju, ugotovljena neskladja in druga relevantna opažanja ter končne rezultate testiranja z oceno uspešnosti. Pred vključevanjem nove omrežne naprave v produkcijsko omrežje se priporoča tudi preizkus zmogljivosti. Poglavje Testiranje omrežij in omrežnih naprav obravnava naslednja področja:

- Testiranje omrežij
- Testiranja zmogljivosti omrežnih naprav

Testiranje omrežij

SIC-OMR-TST-010:

Vzdrževanje omrežja se izvaja s testiranjem omrežja po korakih in v sodelovanju z naročnikom. Pred izvedbo testiranja mora vzdrževalec zagotoviti, da so cilji in načrt testiranja razumljivi in dogovorjeni. Priporoča se petstopenjski sistemski pristop k testiranju: priprava, načrtovanje, namestitve, izvedba in priprava rezultatov testiranja.

SIC-OMR-TST-020:

Pred izvedbo testiranja mora izvajalec pripraviti preprost in strukturiran opis testnih scenarijev v namenskem dokumentu, ki vključuje vsaj naslednje informacije o načrtovanih testih: unikatno identifikacijo, seznam uporabljene testne in testirane opreme, kratek opis z navedbo cilja, potrebne konfiguracije strojne in programske opreme, korake izvajanja in pričakovane rezultate.

SIC-OMR-TST-030:

Po izvedbi testiranja izvajalec pripravi poročilo, ki mora vsebovati vsaj: dopolnjene splošne podatke o testiranju (npr. seznam strojne opreme, verzije programske opreme, konfiguracijo strojne in programske opreme, pripadajočo dokumentacijo kot podlago za testiranje, seznam izvajalcev testiranja, datumsko opredelitev), ugotovljena neskladja in druga relevantna opažanja (oceno poslovno ustreznih in neustreznih rešitev, pregled ugotovljenih napak) in končne rezultate testiranja (kratek opis rezultatov, vrednosti izmerjenih parametrov testiranja, oceno uspešnosti).

Testiranja zmogljivosti omrežnih naprav

SIC-OMR-TST-040:

Pred vključevanjem nove omrežne naprave v produkcijsko omrežje se priporoča preizkus zmogljivosti. Testiranje naj poteka po ustaljenih metodologijah z upoštevanjem standardov in priporočil. Za izbiro najbolj primerne omrežne opreme iz razpoložljivega nabora se priporoča testiranje pri zunanjem neodvisnem izvajalcu.

SIC-OMR-TST-050:

Izvajalec mora pred vključitvijo omrežne naprave v omrežje naročnika opraviti zmogljivostno testiranje in podati poročilo o testiranju, ki vsebuje specifikacijo testne opreme, opis zahtev, ki so potrebne, da oprema zadosti razpisnim pogojem, testne scenarije s konfiguracijo naprave in rezultate testiranja.

3. Aplikacijski nivo (*SIC-APL*)

Smernice aplikacijskega nivoja (SIC-APL) predstavljajo jasno usmeritev za nadaljnji razvoj arhitekture informacijskega sistema za vodenje in nadzor prometa na avtocestnem omrežju. Vključujejo arhitekturne principe, skupne arhitekturne gradnike in ciljno aplikacijsko arhitekturo sistema in podsistemov. Priporočila in ugotovitve glede sistemskih zahtev se nanašajo na upravljanje nadzornega sistema in poslovnega dela naročnikovega okolja. Ugotovljeno je bilo, da je potrebno vzpostaviti proces upravljanja s spremembami za vse kritične sisteme, kot tudi urediti dokumentacijo za kritične sisteme, predvsem glede aplikacijske in strojne opreme naročnika. Pomembno je sledenje uveljavljenim standardom in protokolom, hranjenje in prenos podatkov mora biti poenoteno. Poleg integracije internih sistemov, ki jih je potrebno izdelati šibko sklopljene, je potrebno zunanje sisteme obravnavati ločeno, z dodatnimi zahtevami. Poglavji Podatkovni centri in Obravnava nepredvidenih dogodkov se dotikata še gradnje in vzdrževanja infrastrukture podatkovnih centrov, ki zagotavljajo nemoteno delovanje sistemov. Smernice v tem razdelku sestojijo iz devetih ločenih poglavij:

- Arhitektura aplikacijskega nivoja
- Sistemske zahteve
- Standardi in protokoli na aplikacijskem nivoju
- Hranjenje podatkov
- Testiranje aplikacij in testna okolja
- Zagotavljanje varnosti na aplikacijskem nivoju
- Integracija z zunanjimi sistemi
- Podatkovni centri
- Obravnava nepredvidenih dogodkov

Smernice aplikacijskega nivoja nastopajo v odvisnosti od ostalih poglavij, predvsem glede celostne arhitekture in kadrov. Slednji so še posebej pomembni, saj morajo zagotoviti spremljanje, nadzor, dokumentacijo in upravljanje predlaganih postopkov. Prav tako je potrebno nad predlaganimi smernicami imeti pregled in jih kontinuirano posodabljati.

3.1. Arhitektura aplikacijskega nivoja (*SIC-APL-AAN*)

Aplikacijske smernice in principi predstavljajo jasno usmeritev za nadaljnji razvoj arhitekture informacijskega sistema za vodenje in nadzor prometa na avtocestnem omrežju. Vključujejo arhitekturne principe, skupne arhitekturne gradnike in ciljno aplikacijsko arhitekturo sistema in podsistemov. Ključna za izvajanje arhitekturnih principov in smernic je vzpostavitev ustreznih zmogljivosti v okviru DARSa (z notranjimi kadri ali v povezavi z zunanjimi), ki bodo omogočile uveljavitev smernic, preverjanje njihovega izvajanja in nadaljnji razvoj ter prilagajanje. Za vzpostavitev zmogljivosti za obvladovanje kompleksne poslovno informacijske arhitekture je treba določiti organizacijo, procese, znanja in orodja (primeri procesov: upravljanja arhitekture, upravljanje IT, strateško načrtovanje, upravljanje razvojnega cikla, upravljanje kakovosti

programske opreme). Potrebno je upoštevati uporabo dobre prakse in okvirjev, kot npr. ITIL, COBIT, TOGAF. Poglavlje obravnava naslednja področja:

- Ključne zmogljivosti DARS
- Aplikacijski arhitekturni principi
- Principi okolja in virov
- Princip zagotavljanja kakovosti
- Principi o varnosti
- Ciljna krovna aplikacijska arhitektura

Ključne zmogljivosti DARS

SIC-APL-AAN-010:

Arhitekturni principi veljajo za vse oddelke, izvajalce in zunanje izvajalce, ki sodelujejo pri razvoju aplikacij in sistemov za spremljanje in nadzor prometa.

SIC-APL-AAN-020:

Za uveljavljanje principov in njihovo spreminjanje oziroma nadgrajevanje skrbijo arhitekti informacijskega sistema, ki jih določi DARS. Arhitekti potrjujejo, objavljajo in uveljavljajo vedno veljavno zadnjo verzijo principov.

SIC-APL-AAN-030:

Za uveljavljanje aplikacijske arhitekture in njeno spreminjanje skrbijo arhitekti informacijskega sistema. Arhitekti potrjujejo, objavljajo in uveljavljajo vedno veljavno zadnjo verzijo arhitekture. Razvoj sistema mora slediti ciljni krovni aplikacijski arhitekturi, ki jo predlagajo in potrjujejo arhitekti.

SIC-APL-AAN-040:

Arhitekti sistema za nadzor in vodenje prometa redno spremljajo ter ocenjujejo tveganja, ki jih lahko povzročijo spremembe v arhitekturi sistema (npr. z uvedbo nove komponente, vmesnika). Na podlagi ocenjenih tveganj sprejmejo ustrezne ukrepe za preprečitev izpada sistema, varnostnega tveganja ali druge neskladnosti delovanja.

SIC-APL-AAN-050:

Aplikacijske rešitve oz. aplikacijske arhitekture, ki odstopajo od ciljne arhitekture praviloma niso dovoljene. Za morebitne izjeme je potreben širši konsenz skupine arhitektov ter načrt odprave neskladja v prihodnje.

SIC-APL-AAN-060:

Pri načrtovanju novih standardnih aplikacijskih rešitev, menjavi ali nadgradnji imajo praviloma prednost že izdelane standarde rešitve na trgu, ki ustrezajo poslovnim potrebam (npr. integracijske platforme, upravljanje identitet in dostopov, monitoring sistem, ipd.)

SIC-APL-AAN-070:

Dostavljene rešitve morajo biti implementirane in dostavljene na način, da ne pogojujejo odvisnosti naročnika od trenutnega dobavitelja (ang. »vendor lock-in«)

SIC-APL-AAN-080:

Aplikacijske rešitve in sistemi morajo biti zasnovani na način, ki omogoča enostavno prilagajanje sistema v smislu novih uporabnikov, novih delovnih postaj, dodajanje strojnih in sistemskih zmogljivosti, dodajanja nove opreme in naprav na trasah in v predorih, kakor tudi dodajanja novih podatkovnih tipov (skalabilnost). Enako velja za zmanjševanje.

SIC-APL-AAN-090:

Pri nakupu ali razvoju rešitev se vedno preveri možnost uporabe preizkušenih in uveljavljenih odprtokodnih rešitev ali komponent pri čemer imajo prednost tiste, ki jih podpirajo lokalni dobavitelji, lokalni integratorji in podjetja za razvoj programske opreme. Ključni kriteriji pri izbire odprtokodnih rešitev: preizkušnost, upoštevani varnostni standardi, standardni protokoli, lokalna podpora.

SIC-APL-AAN-100:

Aplikacijske rešitve in celotna arhitektura morajo zagotavljati semantično in tehnično interoperabilnost na podlagi odprtih, širše sprejetih in neodvisnih standardov.

SIC-APL-AAN-110:

Informacijski sistem mora uporabljati uveljavljene, preizkušene in sodobne standarde na področju varnosti, izmenjave podatkov, integracij, API vmesnikov, komunikacij ter specifičnih EU standardov na področju sistemov za upravljanja prometa. Primer: OPC UA za izmenjavo podatkov in kontrol do obcestnih naprav, DATEX II za izmenjavo podatkov z drugimi sistemi ITS.

SIC-APL-AAN-120:

Vse rešitve, komponente, vmesniki, aplikacije, storitve, podatkovne baze, komunikacije in naprave, ki jih dobavljajo ali implementirajo zunanji izvajalci, morajo biti dokumentirane na enoten način. Dokumentacija naj bo redno osveževana in uvrščena v DARS repozitorij sistemske dokumentacije. Dokumentacija o rešitvi mora vsebovati najmanj:

- 1. Seznam celotne dokumentacije s kratkim opisom vsebine, navedbo celotnega imena datoteke, verzijo, lokacijo datoteke v imeniški strukturi in skupino v katero se dokumentacija uvršča.*
- 2. Uporabniško dokumentacijo – navodila za uporabo za vse nivoje uporabnikov.*
- 3. Načrt testiranja, testni postopki in testni podatki ter poročila o testiranju.*
- 4. Seznam zunanjih orodij, ki niso del sistema in so potrebna za upravljanje in/ali razvoj sistema.*
- 5. Dokumentacijo izvedene analize rešitve (t.i. sistemska analiza).*
- 6. Dokumentacijo o arhitekturi in zasnovi sistema.*
- 7. Podrobno tehnično dokumentacijo, ki praviloma zajema:*
 - 7.1. standardno dokumentacijo izvirne kode,*
 - 7.2. dokumentacijo shem XML,*
 - 7.3. dokumentacijo vmesnikov spletnih storitev,*
 - 7.4. dokumentacijo programskih vmesnikov,*
 - 7.5. dokumentacijo uporabljenih lastnih ali tujih programskih komponent,*
 - 7.6. dokumentacijo postopkov in algoritmov, kar vključuje delovne tokove in vgrajena poslovna pravila,*
 - 7.7. splošno namestitveno shemo in navodila za namestitev v ciljno okolje za vsa podprta okolja,*
 - 7.8. diagram odvisnosti med programskimi vmesniki in sistemi.*
- 8. Dokumentacijo o sistemskih nastavitvah za vse elemente sistema (podatkovna baza, aplikacijski strežnik, idr.) z opisom razlogov za spremembo privzete nastavitve.*

SIC-APL-AAN-130:

Kritični deli arhitekture sistema, kot so kritične aplikacije, skupni aplikacijski gradniki, integracije, podatki in tudi fizične lokacije za vodenje in nadzor prometa morajo biti zasnovani na način, ki omogoča redundantnost. Kritične zmogljivosti (funkcije) naj imajo možnost delovanja/preklopa v redundantnem načinu (npr. prevzem nadzora in vodenja prometa iz rezervne lokacije).

SIC-APL-AAN-140:

Zunanji izvajalci za razvite in predane rešitve pripravijo zahtevano dokumentacijo ter prenesejo potrebno znanje za razumevanje delovanja in upravljanje rešitev na strokovnjake DARS.

Aplikacijski arhitekturni principi

SIC-APL-AAN-150:

Sistemi za spremljanje in nadzor prometa morajo temeljiti na tri in več nivojski arhitekturi, kjer se ločujejo najmanj podatki od poslovne logike in uporabniški vmesniki od poslovne logike. Prednostno se uporablja storitvena arhitektura.

SIC-APL-AAN-160:

Aplikacijske komponente in vmesniki morajo biti grajeni modularno in dokumentirani na način, ki omogoča enostavno ponovno uporabo. Ponovna uporaba gradnikov ima prednost pred nakupom ali razvojem novih komponent istih ali podobnih zmogljivosti (funkcionalnosti).

SIC-APL-AAN-170:

Integracije notranjih in zunanjih sistemov ter aplikacij morajo temeljiti na enotni integracijski platformi z enotnimi integracijskimi protokoli, vmesniki in pravili (npr. za WEB servise, message broker). Hkrati morajo integracije zagotavljati preverjeno varno integracijo, obvladljivo, upravljano ter spremljano (logirano). Primer: WSO2 API Management platforma. Praviloma se za integracijo naprav in trasnih ter predorskih podsistemov uporablja ločena platforma za integracijo od platforme za integracijo s »front-end« aplikacijami, nujenjem storitev in zunanjimi sistemi.

SIC-APL-AAN-180:

Pri uvajanju novih zmogljivosti in re-inženiringu ima razvoj novih aplikacijskih storitev (API), ki jih lahko vključijo (kličejo) standardne oz. enotne uporabniške aplikacije, prednost pred razvojem aplikacij z lastnimi uporabniškimi vmesniki. Princip »API first«.

SIC-APL-AAN-190:

Vmesniki (API) morajo biti dokumentirani na enoten način (specifikacija OpenAPI, zadnja verzija 3.0). Dokumentacija se redno posodablja. Tehnična dokumentacija mora biti na voljo razvijalcem in vzdrževalcem sistema, ki imajo za to ustrezne pravice in pooblastila.

SIC-APL-AAN-200:

Aplikacije morajo biti enostavne za uporabo, zadoščati uporabniškim zahtevam, biti intuitivne ter zagotavljati dobro uporabniško izkušnjo. Uporabniški vmesniki so poenoteni in morajo upoštevati naslednja načela: preprostost uporabe (hitro učenje), preglednost gradnikov, konsistentna uporaba gradnikov (isti element, isti pomen, na istem mestu), prepoznavnost uporabljenih gradnikov (npr. gumb za akcijo ima vedno enak izgled), vizualna hierarhija (uporabnik vedno ve kje se nahaja), učinkovitost uporabe (uporabnih do ključnih akcij trenutnega pogleda pride v kliku ali dveh), odzivnost (hiter odziv na uporabnikove akcije). Testiranje uporabniške izkušnje in vključevanje končnih uporabnikov v testiranje mora biti del uvajanja novih rešitev. Test uporabniške izkušnje s strani naročnika potrjuje ustreznost uporabniškega vmesnika. V primeru neskladnosti uporabniškega vmesnika bo naročnik zahteval presojo uporabniške izkušnje s strani neodvisnega svetovalca ali presojo po standardu ISO 9241-210.

SIC-APL-AAN-210:

Uporabniške aplikacije in uporabniški vmesniki so praviloma implementirani v spletnih tehnologijah in dostopni preko spletnih brskalnikov širokega nabora. Pri tem se uporabljajo najnovejše različice in posodobitve brskalnikov. Aplikacije morajo biti posodabljanе da delujejo na novih različicah spletnih brskalnikov.

SIC-APL-AAN-220:

Vsi uporabniki in aplikacije morajo uporabljati enoten DARS sistem za upravljanje identitet in avtorizacij ter s tem povezane in sprejete standarde, protokole in nosilce (npr. DARS kartica).

SIC-APL-AAN-230:

Pri načrtovanju rešitev in gradnikov arhitekture je potrebno upoštevati, da se funkcije nadzora in vodenja prometa za določeno traso ali predor izvajajo centralno (GNC, RNC, LNC), pri čemer se podatki distribuirajo (replicirajo) na več fizičnih lokacij nadzornih centrov. Kdo, kaj upravlja in s katerimi podatki ter kje, pa se določa na podlagi vloge uporabnika/nadzornika.

SIC-APL-AAN-240:

Razvijalci novih rešitev in storitev sistema morajo pri implementaciji, uvajanju in delovanju uporabljati dogovorjene skupne arhitekturne gradnike DARS. Vsako odstopanje ali morebitno začasno podvajanje funkcionalnosti izven skupnih gradnikov zahteva odobritev s strani arhitektov. Zahteva se priprava takojšnjega načrta poenotenja v kratkoročnem obdobju. Skupni arhitekturni gradniki imajo svoj življenjski cikel in se razvijajo ter posodablajo vzporedno z ostalimi aplikacijskimi rešitvami.

SIC-APL-AAN-250:

Aplikacijske rešitve morajo omogočati spreminjanje pogostejših parametrov delovanja brez posega v programsko kodo. Pravice za spreminjanje parametrov ima praviloma administrator.

SIC-APL-AAN-260:

Kritične aplikacije in komponente sistema za nadzor in vodenje prometa morajo zagotavljati revizijske sledi, ki ustrezajo standardom in dobri praksi na tem področju in lahko prestanejo revizijski pregled brez ugotovljenih nepravilnosti s strani revizorja informacijskega sistema. Zahteve za revizijsko sled določi DARS za vsako aplikacijo, komponento ali podsistem ločeno. Npr. za najbolj kritične aplikacije se »audit trail« določi na nivoju podatkov in za vse operacije CRUD, za manj kritične pa predvsem: kdo, kdaj in kaj uporablja. Dostop za branje revizijskih sledi imajo samo pooblaščen osebe, dostopi do revizijskih sledi pa se ravno tako beležijo.

Principi okolja in virov

SIC-APL-AAN-270:

Uvajanje novih aplikacijskih tehnologij, programskih platform in okolij mora potekati nadzorovano, njihovo število naj bo čim manjše in obvladovano. Pred uvedbo novih tehnologij, okolij in platform je potrebno soglasje skupine arhitektov DARS.

SIC-APL-AAN-280:

Razvojno, testno in produkcijsko okolje so tri ločena okolja, ki jih mora zagotavljati tako DARS, kot zunanji izvajalci, ki sodelujejo pri razvoju. Razvojna okolja so praviloma vzpostavljena pri razvijalcih, razvojne hiše, ki imajo praviloma tudi svoje testno okolje. Testno okolje vzpostavi tudi DARS in je osnova za izvedbo in potrditev testov pred produkcijo. Za kritične dele arhitekture se zahteva tudi »stage« okolje (pre-deployment), ki je vzpostavljeno in upravljano pri naročniku.

SIC-APL-AAN-290:

Uporabniške aplikacije in komponente (nove namestitve, posodobitve) se na delovne postaje nadzornikov nameščajo centralno, iz centralne lokacije, iz nadzorovanega in varnega vira, ki je prestal zahtevano testiranje.

SIC-APL-AAN-300:

Razvijalci rešitev, storitev in aplikacij znotraj sistema za nadzor in vodenje prometa morajo stremeti k racionalni uporabi računalniških virov (pomnilniške kapacitete, procesorski viri, komunikacije). DARS zahteva optimalno utilizacijo strežniških virov, kar v praksi pomeni sobivanje več aplikacij, komponent ali podatkovnih baz sistema na istem strežniku (fizičnem ali virtualnem) do meje, ki pomeni še sprejemljivo zanesljivost, varnost in odzivnost sistema, upoštevajoč varnostni faktor.

SIC-APL-AAN-310:

Vse aplikacije, komponente in programski moduli morajo biti zasnovani na način, ki omogoča enostavno vključitev v sistem za centralno spremljanje delovanja in diagnostiko sistemov DARS (monitoring in diagnostika).

Princip zagotavljanja kakovosti

SIC-APL-AAN-320:

Planiranje testiranja in testiranje na različnih nivojih (Unit, Performance, Security, User) mora biti del vsake spremembe, nadgradnje ali razvoja aplikacijskih rešitev. Vsako testiranje mora spremljati obvezna dokumentacija. Upravljanje sprememb in testiranje mora potekati preko sistema za upravljanje sprememb in testiranje, sam proces pa vodijo skrbnik sistema, tehničnih skrbnik in vsebinski skrbnik. Po uveljavitvi dobre prakse testiranja sledi naslednja stopnja zagotavljanja kakovosti, ki vključuje celoten življenjski cikel programske opreme kritične infrastrukture.

Principi o varnosti

SIC-APL-AAN-330:

Varnost podatkov in transakcij je ključnega pomena za zanesljivo in varno delovanje sistema. Načrtovanje, preverjanje in testiranje varnosti programske kode, podatkov, transakcij in integracij mora biti del vsake nadgradnje sistema.

SIC-APL-AAN-340:

Izvajalci morajo upoštevati varnostne standarde in priporočila (npr. ISO/IEC 27001, EU ENISA priporočila za ICS SCADA za kritično infrastrukturo). Izvajalci morajo predati poročila o varnostnem testiranju predanih rešitev.

SIC-APL-AAN-350:

DARS izvaja redne varnostne preglede informacijskega sistema, interno in s pomočjo revizorja informacijskega sistema.

Ciljna krovna aplikacijska arhitektura

SIC-APL-AAN-360:

Ciljna aplikacijska arhitektura, potrjena s strani DARS arhitektov, predstavlja smer postopnega razvoja arhitekture. Predstavlja osnovno za načrtovanje in razvoj/nakup novih rešitev in komponent znotraj sistema za nadzor in vodenje prometa, kakor tudi za prilagajanje in usmerjanje razvoja obstoječih rešitev. Uporabljajo jo tako interni strokovnjaki kot načrtovalci, predstavniki zunanjih izvajalcev.

SIC-APL-AAN-370:

Skupni gradniki arhitekture so potrjeni s strani DARS arhitektov in predstavljajo smer postopnega razvoja arhitekture. Predstavlja osnovno za načrtovanje in razvoj/nakup novih rešitev in komponent znotraj sistema za nadzor in vodenje.

SIC-APL-AAN-380:

Enotna storitvena platforma API management mora biti uporabljena za objavo, dostop, zagotavljanje varnosti in upravljanje vmesnikov, web servisov, mikrostoritev, sporočilnih vrst in drugih storitvenih tipov. Vsi izvajalci, razvijalci uporabljajo eno API management platformo. Izpostavljene vmesnike na API management platformi uporabljajo tako interne aplikacije kot zunanji sistemi. Razvoj mora slediti smeri kjer se prednostno razvijajo vmesniki in storitve, kot pa posamezne namenske aplikacije. Primer dobre prakse (WSO2 API Management – open source, TIBCO API management).

SIC-APL-AAN-390:

Uporablja se enoten GIS sistem in podatkovna baza, s skupnimi sloji in podatki za vse ostale podsisteme in komponente, ki potrebujejo GIS podatke (npr. SKADA). Uporablja se za geolociranje in geokodiranje vseh gradnikov, naprav in objektov sistema, ki to zahtevajo (npr. lokacija določenega senzorja, lokacija strežnika v pogonski centrali)

SIC-APL-AAN-400:

Statični model sistema NKS/SNVP (tudi t.i. „asset“ management) in sistem za modeliranje predstavljajo osrednjo komponento, ki omogoča opis vsake naprave, senzorja ali opreme, ki je del sistema SNVP/NKS. Opis določa karakteristike naprave, tip naprave, podatke o napravi, podatkovno strukturo s katero naprava operira, protokol, standard, geolokacijo naprave in druge podatke (npr. skrbnik, leto namestitve, vzdrževalni posegi). Vsaka nova naprava je določenega tipa, ki že v naprej določi njeno delovanje in karakteristike (semantična interoperabilnost). Na ta način se nove naprave in načini delovanja hitreje vključijo v produkcijsko delovanje, na enem mestu se spreminjajo lastnosti določenega tipa naprave, ki se distribuirajo do komponent sistema, ki to potrebujejo za svoje delovanje.

SIC-APL-AAN-410:

Skupni šifranti že samo po sebi predstavljajo skupni gradnik in se morajo uporabljati v vseh aplikacijskih rešitvah ter se posodabljati na enem mestu in po potrebi distribuirati na različne lokacije oz. podatkovne baze. So eden ključnih elementov za enotnost prihodnjih aplikacijskih rešitev in njihove enotne uporabe.

SIC-APL-AAN-420:

Zaradi velikega števila predvidljivih situacij oz. predvidljivega zahtevanega ravnanja v določenih prometnih situacijah se predlaga skupni gradnik (Konfigurator pravil za procesiranje dogodkov in podatkovnih tokov), ki bo namenjen določanju (definiranju, modeliranju) pravil in njihovemu obvladovanju (npr. Scenarij, Prometni program). V skupnem gradniku bo možno definirati zaporedje akcij na določenih napravah ob pojavu določenega dogodka ali na zahtevo nadzornika. Obstajati mora možnost določanja kompleksnih pravil, izračunov, priklic podatkov iz baze, logičnih pogojev in podobno. Omogočati mora distribucijo (namestitvev) potrjenih pravil do ciljnih naprav npr. "edge computing", GNC, RNC, kjer pravila izvajajo programske komponente, kot t.i. "rule engine". Gre za centralni repozitorij pravil oz. prometnih programv.

SIC-APL-AAN-430:

V arhitekturi predvidevamo enotno platformo za integracijo in dve pomembni mesti integracije. Prva je integracija zalednih sistemov in zalednih sistemov do uporabniškega vmesnika (SCADA), ki naj med seboj komunicirajo preko storitev in enotnega API managementa. Druga je integracija zalednih sistemov do obcestnih in predorskih naprav kjer se enako zahteva enotna platforma za integracijo in dogovorjeni protokoli izmenjave podatkov.

SIC-APL-AAN-440:

Nadzornik mora imeti enoten vmesnik za nadzor tras in predorov ter upravljanje prometa. Predlaga se uporabniški vmesnik spletne tehnologije. Uporabniški vmesnik naj dostopa do funkcij zalednega sistema za nadzor in vodenje prometa preko vmesnikov/storitev in API management platforme. To omogoča enostavno in enotno integracijo različnih zmogljivosti in različnih proizvajalcev programske opreme v skupni uporabniški vmesnik nadzornika. Vsak nadzornik preko uporabniškega vmesnika lahko dostopa le do tistih podatkov, trase, funkcionalnosti, ki mu bodo dodeljena na podlagi uporabniške vloge.

SIC-APL-AAN-450:

"Edge computing" agent je programska komponenta, ki je nameščena na lokalnih procesnih enotah ali napravah samih na trasah in v predorih. Omogoča sprejemanje ukazov od t.i. "rule engine" za izvajanje različnih operacij, predvsem kompleksnih. Na ta način se lahko zagotovi enotno komuniciranje do vseh naprav in lokalnih procesnih enot kljub različnim proizvajalcem opreme in različnim starostim opreme, hkrati se poenostavi komuniciranje in obogati zmogljivost (npr. Iz RNC "rule engine" se pošlje 1 kompleksen ukaz do naprave, ki ga naprava sama ne bi razumela, agent s svojo procesno logiko prevede v razumljive ukaze napravi in vzporedno izvede dodatno procesiranje).

SIC-APL-AAN-460:

„Rule engine“ za procesiranje dogodkov je programska komponenta, ki izvaja več zaporednih ali vzporednih korakov na podlagi določenih pravil (npr. Prometni program). Pravila so določena v skupnem gradniku „Konfigurator pravil“ in so distribuirana do „Rule engine“ v izvajanje. Proženje posameznih skupin pravil ali scenarijev se izvede na zahtevo nadzornika ali samodejno na podlagi dogodka, ki proži določeno verigo pravil ali scenarij. Skupna komponenta „Rule engine“ je nameščena v podatkovnem centru za RNC in GNC aplikacijske komponente in „lažja“ različica v lokalnih procesnih enotah („edge computing“).

SIC-APL-AAN-470:

Lokalne procesorske zmogljivosti (LP, LNC) naj se postopoma nadgrajuje v smeri, da bodo sposobne: izvajati kompleksnejše algoritme, sprejemati odločitve na podlagi lokalnih dogodkov ali dogodkov v bližini, izvajati analitiko podatkov v realnem času, delovati avtonomno v kritičnih situacijah ali v primeru izpadov povezav do RNC, GNC. Hkrati morajo lokalne enote omogočati sprejemanje novih pravil, algoritmov ali protokolov, ki jih distribuira in posodablja RNC ali GNC.

SIC-APL-AAN-480:

Operativni podatki o nadzoru in vodenju prometa se zbirajo in obdelujejo v operativnem sistemu za vodenje in nadzor prometa, izvajajo se nujno potrebne analize nad podatki, ki so potrebne za hitro ukrepanje. Nadaljnja analitika, poročila, trendi, statistike ter odkrivanje zakonitosti v podatkih se mora izvajati na ločenem sistemu za analitiko.

SIC-APL-AAN-490:

Dvojno vnašanje istih podatkov, prepisovanje in ročno kopiranje podatkov v uporabniških vmesnikih znotraj sistema za vodenje in nadzor prometa niso zaželeni. Zahteva se stalna optimizacija in avtomatizacija pretoka podatkov in uporaba vmesnikov (API) za izmenjavo podatkov med sistemi.

3.2. Sistemske zahteve (SIC-APL-SIS)

Priporočila in ugotovitve glede sistemskih zahtev se nanašajo na upravljanje nadzornega sistema in poslovnega dela naročnikovega okolja. Ugotovljeno je bilo, da je potrebno vzpostaviti proces upravljanja s spremembami za vse kritične sisteme, kot tudi urediti dokumentacijo za kritične sisteme, predvsem glede aplikacijske in strojne opreme naročnika. Predlagane so bile zahteve glede redundance in aktivnosti glede nadzora dostopov ter nastavitev uporabniških pravic. Ugotovljeno je bilo tudi, da se mora programska oprema v okolju naročnika poenotiti,

podana so priporočila glede virtualizacije strežnikov. Priporočila se nanašajo tudi na nameščanje nove ali posodobljanje programske opreme skladno glede na vzpostavljen SLA. Predpisani so tipi dokumentov za dokumentacijo ter potrebe po vzpostavljanju različnih okolij v sistemu naročnika - testno, učno, produkcijsko. Poglavje obravnava naslednja področja:

- Nadzorni sistem
- Poslovni del
- Redundanca
- Prinzip "Zero Trust"
- Virtualizacija
- Upravljanje z nadgradnjami in novimi namestitvami
- Dokumentacija
- Okolja

Nadzorni sistem

SIC-APL-SIS-010:

Za upravljanje s kritičnimi sistemi se za DARS predvidi vloge poslovnega lastnika, systemskega lastnika in lastnika za odziv in obnovo.

SIC-APL-SIS-020:

Na voljo mora biti ažurna in verodostojna dokumentacija za kritične sisteme, pri čemer mora zajemati aplikacijsko ter strojno opremo ter podporno dokumentacijo.

SIC-APL-SIS-030:

Vsak kritični sistem mora imeti definirane izhodiščne metrike za normalno delovanje sistema. Njegovo delovanje je potrebno redno spremljati in ob preseženih definiranih metrikah za normalno delovanje prožiti alarme.

SIC-APL-SIS-040:

Za vse kritične sisteme naročnika je opredeljen proces upravljanja s spremembami, ki najprej poteka na testnem okolju, ki je čimbolj podobno produkcijskemu okolju, nato pa poteka v za to namenjenem času na produkcijskem okolju. Prav tako so zabeležene vse spremembe in zgodovina vzdrževalnih posegov, hkrati pa je zagotovljena tudi dokumentacija o posodobljeni dokumentaciji po implementaciji sprememb. Dokumentacija vsebuje tudi dokumentacijo glede težav s katerimi se je soočilo v procesu spreminjanja ter kdo in kdaj je naredil spremembe na sistemu.

SIC-APL-SIS-050:

Za vse kritične sisteme naročnika je zagotovljena podpora, ki predvideva:

- *Podporo na samem kraju (on-site support) v opredeljenem času*
- *Dosegljivost v opredeljenem delovnem času za zagotavljanje podpore preko vnaprej dogovorjenih kanalov komunikacije (telefon, HelpDesk rešitev, elektronska pošta,...)*
- *Zadostno strokovno znanje podpornih služb za zagotavljanje učinkovite podpore.*

SIC-APL-SIS-060:

Za vse kritične sisteme naročnika mora obstajati proces upravljanja z večjimi incidenti, kjer je potrebno zagotoviti definicijo postopka eskalacije večjega incidenta ter obstoj enotne vstopne točke za incidente. Dobra praksa na tem področju narekuje tudi beleženje vseh incidentov in hranjenje zgodovine ter oceno stopnje ob prijavi incidenta kritičnega sistema.

Poslovni del

SIC-APL-SIS-070:

Poslovni del informacijskega sistema naročnika mora zagotavljati pregled nad vzdrževanjem in servisnimi posegi na strojni in sistemski programski opremi, zagotoviti mora spremljanje področnih projektov, analizo delovanja teh sistemov in zagotavljati predloge za izboljšave.

Redundanca

SIC-APL-SIS-080:

Izbira redundance naj bo odvisna od namena in zahtev. Za vsako funkcionalno zaključeno enoto informacijskega sistema je potrebno posebej določiti tip redundance:

- *Kritični izračuni, trenutne napake niso sprejemljive: uporabi se pasivna ali hibridna redundanca. (poslovni del)*
- *Visoka razpoložljivost, dolga življenjska doba, hitra obnovitev sistema: aktivna redundanca. (VNP, VDP)*
- *Zelo kritični programi, najvišja zanesljivost: hibridna redundanca. (Senzorika, Kažipot, detekcija vožnje v nasprotni smeri, NKS)*

Princip Zero Trust

SIC-APL-SIS-090:

Informacijski sistem naročnika mora delovati po modelu ZeroTrust, ki predvideva stalno preverjanje pravic dostopa naprav, uporabnikov in aplikacij. (Princip "nikoli zaupaj, vedno preveri"). Predvideva, da so naprave, uporabniki in aplikacije vedno zunaj omrežja naročnika.

SIC-APL-SIS-100:

Za zaščito pred zlonamernimi programi mora informacijska rešitev predvideti sledeče aktivnosti:

- *Takoj po izdaji namestiti kritične varnostne popravke operacijskih sistemov.*
- *Takoj po izdaji namestiti kritične varnostne popravke nameščenih aplikacij.*
- *Uporabljati uporabniške račune z minimalnim naborom pravic, s katerimi še lahko opravimo zahtevano delo. (Prepovedano je uporabljati administratorskih oz. root računov za redno delo).*
- *Ne sme se prenašati neznanih datotek in nameščati neznanih programov.*
- *Posebna previdnost mora biti posvečena priponkam v elektronski pošti. Priponk, ki se jih ne pričakuje v dopetje, ne odpiramo.*
- *Omejiti je potrebno uporabo skupnih datotek.*
- *Uporabnike je potrebno ustrezno izobraziti.*
- *Za delovne postaje moramo uporabljati centralizirano upravljane anti-malware (anti virusne) programe.*

Virtualizacija

SIC-APL-SIS-110:

Odločitev za namestitev izbranega hipervizerja neposredno na fizično strojno opremo ali na že nameščen operacijski sistem je potrebno utemeljiti z upoštevanjem prednosti in slabosti obeh načinov.

SIC-APL-SIS-120:

Programska oprema za virtualizacijo naj bo poenotena v celotnem IS naročnika.

SIC-APL-SIS-130:

Pred virtualizacijo strežnikov je potrebno narediti analizo porabe virov posameznega strežnika, ki bo virtualiziran ter mu dodeliti ustrezni del procesorske moči in hitrega pomnilnika.

SIC-APL-SIS-140:

Testna in razvojna okolja za posamezne aplikacije naj bodo nameščena na virtualnih strežnikih.

SIC-APL-SIS-150:

Virtualizacijo obstoječih strežnikov morajo izvesti visoko usposobljeni strokovnjaki. Predhodno se mora preveriti primernost sistema za virtualizacijo.

SIC-APL-SIS-160:

Pred virtualizacijo strežnika z obstoječo licenčno programsko opremo je potrebno preveriti, če je proizvajalec zagotovil delovanje licenčne programske opreme tudi na virtualiziranem okolju. Za novo licenčno opremo in nadgrajeno opremo mora dobavitelj zagotoviti, da jo je mogoče uporabiti v virtualiziranem okolju.

SIC-APL-SIS-170:

Pred virtualizacijo strežnika s programsko opremo, ki obdeluje podatke v realnem času, je potrebno preveriti primernost virtualizacije.

Upravljanje z nadgradnjami in novimi namestitvami

SIC-APL-SIS-180:

Vse nadgradnje programske opreme naročnika je potrebno preučiti v smislu vpliva na delovanje obstoječih sistemov DARS.

SIC-APL-SIS-190:

Vzpostaviti je potrebno centralni repozitorij za vso programsko opremo.

SIC-APL-SIS-200:

Nameščanje in nadgradnje programske opreme mora biti dovoljeno samo iz repozitorija.

SIC-APL-SIS-210:

Nameščanje in nadgradnje programske opreme lahko opravi samo strokovno osebje naročnika glede na pisna navodila proizvajalca aplikacij ali pooblaščen ponudnik storitev glede na SLA – Service-level agreement. Pisna navodila morajo biti v obliki, da to omogočajo.

SIC-APL-SIS-220:

Nameščanja in nadgradnje namenskih aplikacij se opravi po protokolu, ki ga predpiše naročnik. Del protokola je tudi dokument z navodili za vrnitev sistemov v stanje pred nameščanjem in nadgrajevanjem ter dokument popisa vpliva nadgrajenja na ostale sisteme naročnika.

SIC-APL-SIS-230:

Nameščanja in nadgradnje strežniške programske opreme se opravi po navodilih proizvajalca in protokolu, ki ga predpiše naročnik.

Dokumentacija

SIC-APL-SIS-240:

Naročnik vzpostavi repozitorij ali dokumentni sistem za vso dokumentacijo v zvezi s strojno in programsko opremo.

SIC-APL-SIS-250:

Naročnik zahteva, da se ob predaji uporabniške programske opreme preda tudi sledeča dokumentacija:

- *krovni dokument uporabniške programske opreme,*
- *uporabniška dokumentacija za vse nivoje uporabnikov,*
- *načrt testiranja,*
- *seznam uporabljenih zunanjih orodij,*
- *dokumentacija izvedene analize rešitve,*
- *dokumentacija o arhitekturi in zasnovi sistema in*
- *podrobna tehnična dokumentacija.*

Naročnik lahko v posameznih primerih določi izjeme pri predaji dokumentacije.

SIC-APL-SIS-260:

Dobavitelj sistemske programske opreme mora naročniku zagotoviti:

- *Brezplačen dostop do baz znanja proizvajalca in spremljanje odprtih problemov preko spleta.*
- *Brezplačen spletni dostop do popravkov in nadgradenj (gonilniki, firmware) pri proizvajalcu opreme.*
- *Brezplačne storitve nadgradnje sistemske programske opreme v času garancije opreme v primeru funkcionalnih težav ali v primeru odstopanj od deklariranih lastnosti ponujene opreme.*
- *Dostop do tehnične podpore pri dobavitelju ali proizvajalcu.*
- *Pomoč pri reševanju tehničnih problemov v zvezi z nameščeno opremo v rednem delovnem času (v obdobju garancije).*

Naročnik lahko v posameznih primerih določi izjeme pri zahtevah.

SIC-APL-SIS-270:

Naročnik predpiše posebne pogoje, ki jih mora zagotoviti dobavitelj sistemske programske opreme.

Okolja

SIC-APL-SIS-280:

Sistem mora omogočiti da se, glede na pisna navodila proizvajalca ali dobavitelja opreme, na infrastrukturi naročnika vzpostavi testno, staging in šolsko okolje.

SIC-APL-SIS-290:

Za potrebe nadaljnega razvoja in upravljanja prometne infrastrukture je priporočljiva izdelava digitalnega dvojčka celotne prometne infrastrukture.

SIC-APL-SIS-300:

Za potrebe testiranja dopolnitev, popravkov ali novih informacijskih sistemov, mora arhitektura rešitve predvideti vzpostavitev testnega okolja ali integracijo v že obstoječe testno okolje pri naročniku.

SIC-APL-SIS-310:

Za potrebe testiranja dopolnitev, popravkov ali novih informacijskih sistemov, mora arhitektura rešitve predvideti vzpostavitev staging okolja ali integracijo v že obstoječe staging okolje pri naročniku.

SIC-APL-SIS-320:

Za potrebe uvajanja in šolanja uporabnikov za delo z informacijskimi sistemi, lahko arhitektura rešitve predvideva vzpostavitev šolskega (uvajalnega) okolja ali integracijo v že obstoječe šolsko (uvajalno) okolje pri naročniku.

3.3. Standardi in protokoli na aplikacijskem nivoju (SIC-APL-STP)

Standardi in protokoli na aplikacijskem nivoju naslavljajo predvsem modeliranje podatkovnih tipov, način izmenjave podatkov, protokole namenjene temu in standardizirane formate, ki morajo zagotavljati interoperabilnost. Poleg zahtevane dokumentacije se ob vsaki spremembi predlaga vnovičen pregled področja in standardov za izmenjavo podatkov. V primeru razvoja lastnega protokola je treba zagotoviti njegovo odprtost vsaj naročniku in zagotoviti jasno dokumentacijo, da lahko protokol implementira kdorkoli. Poleg modeliranja podatkov v izmenjavi ali hrambah je potrebno odjemalcem nuditi vse potrebne podatke brez podvajanj in brez potrebe, da bi se na odjemalcih morala izvajati dodatna poslovna logika. Najbolj uporabljena formata za izmenjavo sta XML in JSON, za katera so definirana tudi standardna sporočila za izmenjavo podatkov. Poleg vseh nujnih pravil se predlaga uporaba platforme za upravljanje z aplikacijskimi vmesniki, ki bi že sama po sebi (angl. »by design«) zagotovila doslednost pri uporabi shem in protokolov. Poglavje obravnava naslednja področja:

- Zahteve za podatkovno povezljivost
- Komunikacija na aplikacijskem nivoju
- Formati in standardi zapisa
- Platforme za upravljanje z vmesniki

SIC-APL-STP-010:

Vsi sistemi v okolju DARS morajo biti upravljani preko dokumentiranih in standardiziranih ali ustrezno prilagojenih aplikacijskih programskih vmesnikov. Sistemi morajo biti dostopni na način, da je možno nadzorovati in upravljati promet iz poljubne lokacije znotraj omrežij nadzornih centrov z lahkimi odjemalci, pri čemer se predvideva, da odjemalci ne izvajajo poslovne logike (t.j. sistemi morajo sami zagotavljati varno izvajanje akcij).

SIC-APL-STP-020:

Vsi sistemi, ki nadzorujejo ali upravljajo promet (npr. odjemalske aplikacije) in sporočajo stanja ali neposredno upravljajo z infrastrukturo (npr. lokalne postaje, lokalni nadzorni centri), morajo preko definiranih vmesnikov komunicirati s primarnim sistemom za nadzor in upravljanje cest (npr. SNVP/NKS). V primeru izpada primarnega sistema se morajo sistemi avtomatsko povezati z alternativnim sistemom (npr. v drugem nadzornem centru), ki predstavlja kopijo izpadlega sistema, s čimer se omogoči, da nadzor in upravljanje prometa nemoteno poteka dalje.

SIC-APL-STP-030:

Pri implementaciji novega sistema je potrebno slediti izbrani metodologiji razvoja. Znotraj te pa je potrebno pri razvoju ali posodobitvi programskih vmesnikov slediti naslednjim korakom:

(A) Pregled novosti in standardov pri izmenjavi podatkov na zadevnem področju.

(B) Pregled zadevnih obstoječih vmesnikov za integracijo in njihove posodobitve: Izvajalec mora izdelati načrt aplikacijskih vmesnikov, ki vsebuje (a) protokol komunikacije, (b) tip in shemo sporočil, (c) zaloge vrednosti in stanja v primeru napak ter (d) opis funkcionalnosti vmesnika. Pri tem je potrebno opraviti pregled obstoječih vmesnikov (iz obstoječega kataloga DARS) in izbrati standardizirane protokole/sheme podatkov ter zagotoviti skladnost z obstoječimi tehnologijami oz. vizijo DARS.

(C) Definicija in uskladitev vseh shem podatkov za izmenjavo med naročnikom in izvajalcem.

(D) Potrditev s strani naročnika: DARS mora pred začetkom implementacije načrt izvajalca potrditi, prav tako to velja za morebitne spremembe v času implementacije.

Zahteve za podatkovno povezljivost

SIC-APL-STP-040:

Pri izgradnjah ali nadgradnji novih sistemov naj se pri implementaciji programskih vmesnikov uporablja pristop s pomočjo fasade vmesnikov (angl. API facade pattern) v kombinaciji z načrtovanjem poenotenega vmesnika (angl. Standards committee approach). Naročnik in izvajalec morata biti glede lastnosti novih vmesnikov usklajena.

SIC-APL-STP-050:

Za vse programske vmesnike sistemov v nadzornih centrih DARS mora biti izdelana in sproti ažurirana knjižnica vmesnikov. Poleg osnovnega opisa vmesnikov, mora vsebovati tudi njihove lastnosti (npr. shema sporočil, naslavljanje, vračanje napak, dostopne pravice, točke implementacij vmesnika, omejevanje hitrosti in druge omejitve).

SIC-APL-STP-060:

Zaledni sistemi morajo preko aplikacijskih vmesnikov nuditi prilagojene podatke brez nepotrebnih podvajanj (tudi v primeru nadzora - pošiljanje le sprememb stanja in signala "heart-beat" v primeru enakosti). Podatki morajo biti že ustrezno obdelani za neposredno nadaljnjo uporabo s strani uporabniška vmesnika (npr. odjemalske aplikacije) - bolj natančno: odjemalci morajo uporabljati "lahke" tehnologije in s strani zalednega sistema pridobiti predprocesirane podatke brez odvečnih podvojenih podatkov skozi čas, da je lahko učinkovitost čim večja.

Komunikacija na aplikacijskem nivoju

SIC-APL-STP-070:

Vsaka komunikacija preko programskih vmesnikov, ki je kritična glede upravljanja in nadzora prometa, mora zagotavljati oz. implementirati potrjevanje prejema podatkov. Pri vzpostavljanju povezav do aplikacijskih programskih vmesnikov je potrebno zagotoviti varno povezavo (npr. preko SSL), skladno s smernicami o varnosti na aplikacijskem nivoju.

SIC-APL-STP-080:

Vsi implementirani sistemi morajo preko aplikacijskih programskih vmesnikov zagotavljati dovolj hitro pošiljanje in prejemanje podatkov, vključno z upoštevanjem morebitne transformacije in kompresije podatkov. Dovolj hitro pomeni, da sistem omogoča ustrezno delovanje vodenja in nadzora prometa. V primeru, da začne posamezen odjemalec prekomerno obremenjevati sistem, je potrebno njegovo komunikacijo omejevati (angl. rate limiting).

SIC-APL-STP-090:

Aplikacijski programski vmesniki morajo biti zaščiteni s sistemom za avtentikacijo in avtorizacijo, pri čemer je potrebno beležiti tudi komunikacijo preko njih zaradi zagotavljanja revizijskih sledi. Sistem za avtentikacijo mora podpirati različne nivoje dostopa (npr. administrator, nadzornik, vodja izmene) in dovoljenja, pri čemer morajo biti za vse vmesnike določene pravice dostopa.

SIC-APL-STP-100:

Organizacija URL shem oz. dostopne točke do vmesnikov morajo podpirati verzioniranje programskih vmesnikov (npr. /v2/admin, /v3/control). Posamezne verzije in razlike med njimi morajo biti dokumentirane v dokumentaciji z opisom aplikacijskih programskih vmesnikov.

SIC-APL-STP-110:

Komunikacija med posameznimi sistemi (npr. SCADA sistemi, LP in LNC/RNC) naj poteka preko ustreznega industrijskega protokola (npr. OPC UA ali določenega s strani naročnika), ki lahko zagotavlja potrebne lastnosti za izgradnjo sistema s pomočjo jasnih aplikacijskih programskih vmesnikov. Del komunikacije z odjemalskimi sistemi in zunanjimi sistemi se lahko implementira s pomočjo splošno-namenskih protokolov.

Formati in standardi zapisa

SIC-APL-STP-120:

Pri prenosu podatkov preko aplikacijskih programskih vmesnikov se zahteva uporaba standardiziranih formatov, kot so JSON in XML. Implementacija lastnih formatov je dovoljena le v izrednih primerih, pri čemer mora izvajalec naročniku utemeljiti, zakaj je lasten format potreben, kar mora naročnik potrditi, izvajalec pa rešitev in celoten protokol natančno dokumentirati. V primeru zagotavljanja hitrejših in še bolj kompaktnih prenosov se uporablja transformacija podatkov v binarne formate (npr. protobuf).

SIC-APL-STP-130:

Obstaja več aktualnih shem sporočil v pripravljalni fazi ali že uveljavljenih (de-facto) standardov, ki jih je potrebno spremljati in voditi register primernih shem, za njihovo področje. Priporoča se vključevanje v čim več standardizacijskih aktivnosti na področju nadzora in upravljanja prometa. Izvajalci morajo znati implementirati aktualne standarde na tem področju.

SIC-APL-STP-140:

Pri pripravi javnega naročila za uvedbo novega ali nadgradnjo obstoječega sistema je potrebno pregledati aktualne standarde na področju predstavitve podatkov in zahtevati upoštevanje shem v okviru aplikacijskih programskih vmesnikov in tudi drugje (npr. podatkovni modeli za podatkovne baze). Upoštevanje specifičnih standardov se določi v okviru javnega naročila ali se glede tega uskladi skupaj z izvajalcem.

Platforme za upravljanje z vmesniki

SIC-APL-STP-150:

Sistem za upravljanje z aplikacijskimi programskimi vmesniki lahko med seboj povezuje vse aplikacijske sisteme v okolju DARS. Takšen sistem hkrati predstavlja dokumentacijo dostopov do vseh sistemov in na pregleden način vpeljuje nove sisteme, ugaša stare, izvaja nadgradnje določenih delov, ipd. Ob izbiri sistema je potrebno zagotoviti, da bo sistem prilagodljiv na nove tehnologije, saj potem takšen sistem predstavlja krovno tehnologijo, ki jo bo zamenjati težje kot katerikoli drug sistem v okolju. Prav tako je potrebno zagotoviti ustrezen kader, ki bo s platformo upravljal in jo nadzoroval.

3.4. Hranjenje podatkov (SIC-APL-HP)

V sistemih za nadzor in vodenje prometa se podatki hranijo na več nivojih - od lokalnih postaj do glavnega nadzornega centra. Glede na podatkovno intenzivnost in trenutne potrebe se predlaga poenotenje shem in izbiro istih tipov podatkovnih baz na vseh nivojih. Relacijske podatkovne baze so dovolj zmogljive za vse zahtevane naloge, pri čemer bo v primeru vključevanja množice senzorjev ali uvedbe podatkovnega skladišča potrebno vpeljati tudi podatkovne baze NoSQL. Večji poudarek v poglavju hranjenja podatkov je namenjen načrtovanju podatkovnih baz, saj je pomembno, da je shema skladna s standardi, poenotena med nadzornimi centri in da zaradi nerazumevanja ne prihaja do podvajanja podatkov. Nekatere manjše podatkovne baze, ki jih potrebujejo vsi nadzorni centri v Sloveniji, bi morale biti sinhronizirane. Trenutne zahteve ne kažejo potreb po porazdeljenih podatkovnih bazah, vendar mora biti kljub temu zagotovljena ustrezna replikacija, ki jo zagotavlja sistem za upravljanje s podatkovno bazo in ne dodatna namensko razvita programska koda. Poglavje obravnava naslednja področja:

- Vpeljava nove ali nadgradnja obstoječe podatkovne baze
- Načrtovanje
- Porazdeljeno hranjenje podatkov
- Vpeljava podatkovnega skladišča

SIC-APL-HP-010:

Glede izbora podatkovnih baz se zahteva ustrezna uporaba glede na namen hranjene vsebine:

- *relacijske podatkovne baze (kot so PostgreSQL, MS SQL ali Oracle DB) v LNC, RNC in GNC za potrebe aplikacij upravljanja in nadzora prometa,*
- *"vgradne" relacijske podatkovne baze (kot so SQLite ali Firebird), ki ne potrebujejo ločenega strežnika in hranijo omejen nabor podatkov na manj zmogljivih sistemih v LP,*

- *tekstovne podatkovne baze za hranjenje revizijskih sledi (kot so Apache Solr, Elasticsearch), ki omogočajo enostavno izgradnjo nadzornih plošč in*
- *podatkovna skladišča (kot npr. Snowflake) za dolgoročno hranjenje večje količine podatkov z namenom izvajanja analitike in podpore odločanju v GNC.*

SIC-APL-HP-020:

Diskovna polja za hrambo aktualnih podatkovnih baz in arhivskih podatkov (arhivske baze, konfiguracijske datoteke, strežniki ipd.) naj bodo ločena in ustrezno dimenzionirana za njihov namen (hitrost dostopa, kapaciteta). Zahteva se uporaba ustrezne virtualizacijske porazdelitve podatkov (npr. RAID-6). Programska oprema, ki upravlja z izdelavo arhivskih kopij, naj skrbi za brisanje starih verzij skladno z zahtevami DARS (npr. shranjene največ 3 zadnje verzije baze).

Vpeljava nove ali nadgradnja obstoječe podatkovne baze

SIC-APL-HP-030:

Izbiri nove podatkovne baze je potrebno uskladiti in pridobiti potrditev s strani naročnika ter upoštevati naslednje ključne kriterije (vključno s SIC-APL-HP-010):

- *Podatkovna baza ima širok krog uporabnikov, aktivno skupnost (v primeru odprtokodne baze) in je relacijskega tipa (razen v posebnih primerih, kot na primer beleženje dostopov, podatkovno skladišče).*
- *Izbira podatkovne baze je skladna z obstoječimi podatkovnimi bazami v okolju DARS oz. dolgoročno vizijo poenotenja sistemov (kot na primer vpeljava PostgreSQL, MS SQL ali Oracle DB).*
- *Na bazi se ne bo izvajala poslovna logika (le ta bo izključno domena aplikacij). Glede na izredne situacije lahko obstajajo specifične bazne procedure, ki opravljajo nujno potrebne funkcije (kot na primer beleženje dostopov, preverjanje pravic izvajanja v varnostni shemi).*

SIC-APL-HP-040:

Pred uvedbo ali nadgradnjo obstoječih podatkovnih baz, se je potrebno odločiti, kako bo vsaka izmed faz življenjskega cikla razvoja podatkovnih baz izvedena. Za vsako fazo mora obstajati dokumentacija o njeni izvedbi. Pred začetkom dela mora izvajalec v dokumentaciji jasno opredeliti potrebo po podatkovni bazi in definirati njene natančne namene (angl. mission statement) ter zahteve (angl. mission objectives).

Načrtovanje

SIC-APL-HP-050:

Izvajalec na podlagi zahtev projekta izdelava uporabniško specifikacijo (npr. opis domene, opis aplikacij, ki bodo uporabljale podatkovno bazo), ki predstavlja osnovo za načrtovanje podatkovne baze.

SIC-APL-HP-060:

Izvajalec v dogovoru z naročnikom izbere načrtovalsko orodje, ki omogoča načrtovanje na konceptualnem in logičnem nivoju ter podpira izvoz modela ter njegovo posodabljanje. V primeru baze NoSQL se posebej določi način dokumentiranja. Vsakega izmed nivojev načrtovanja (konceptualno, logično in fizično) mora naročnik zaporedoma potrditi preden se lahko baza uporablja. Vsi nivoji morajo biti med seboj sinhronizirani, kar omogoči učinkovito posodabljanje podatkovne baze kasneje. Pri načrtovanju podatkovne baze je potrebno slediti splošnim smernicam glede konceptualnega, logičnega in fizičnega načrtovanja.

SIC-APL-HP-070:

V času načrtovanja mora izvajalec identificirati transakcije in preveriti, če jih konceptualni model podpira. Vsako transakcijo je potrebno opisati in pokazati, da model vsebuje vse entitetne tipe, povezave in attribute, ki so obvezni za izvedbo transakcije. Poročilo in celoten model mora izvajalec preveriti z naročnikom. Prvotni model in vsake nadaljnje spremembe modela mora naročnik potrditi.

SIC-APL-HP-080:

Zagotovljene morajo biti smernice poimenovanj objektov v podatkovnih bazah, ki se jih morajo držati vsi izvajalci. Smernice vsebujejo pravila za poimenovanja različnih objektov (npr. tabel, atributov, povezav), primere uporabe in prepovedi uporabe določenih znakov ali stilov (npr. velike začetnice, presledki, šumniki, množinska imena).

SIC-APL-HP-090:

Izvajalec pri načrtovanju podatkovnih baz poimenuje objekte skladno s smernicami poimenovanj objektov. Poleg tega uporablja imena, ki so skladna z izrazoslovjem domene oz. jih uporablja naročnik. Vsa imena objektov v fizičnem modelu podatkovne baze morajo biti usklajena in odobrena s strani naročnika.

SIC-APL-HP-100:

Pred implementacijo fizičnega podatkovnega modela izvajalec preveri logični model z naročnikom. Pri tem se preverja skladnosti glede obveznosti atributov, omejitve domen atributov, števnosti, omejitve entitet in povezav, splošne omejitve, uporabniške poglede (v primeru več uporabnikov/aplikacij). Namen preverjanja je ugotoviti, če model ustreza vsem uporabniškim zahtevam. Naročnik lahko za pregled celovitosti podatkovnega modela zahteva tudi specifikacijo podatkovnih tokov s pomočjo diagrama podatkovnih tokov.

SIC-APL-HP-110:

V določenih primerih lahko izdelava pogledov omogoči lažji varnostni nadzor nad podatkovno bazo, večjo neodvisnost med aplikacijami in podatkovno bazo v primeru sprememb ali pohitri delovanje podatkovne baze (npr. materializirani pogledi). Kjer je mogoče in upravičeno, se izvede izdelava pogledov nad podatkovno bazo.

SIC-APL-HP-120:

V času razvoja ali kasneje lahko prihaja do sprememb v podatkovni bazi, kar je potrebno ustrezno dokumentirati. Ob vsaki spremembi mora biti izdelana nova verzija celotne dokumentacije z jasnim opisom vseh sprememb v primerjavi s prejšnjo verzijo (angl. changelog). Posamezna verzija podatkovne baze in dokumentacije mora biti tudi ustrezno označena.

SIC-APL-HP-130:

Izvajalec je dolžan optimizirati programsko kodo in bazne objekte s ciljem zagotavljanja optimalnega delovanja. Vse neoptimalnosti, ki se izkažejo skozi obremenitveni test in skozi generalni preizkus, mora izvajalec odpraviti do trenutka produkcije. Enako pravilo velja tudi za obdobje garancije oziroma obdobje operativnega vzdrževanja. Vse postopke optimizacije mora izvajalec opisati v dokumentaciji.

SIC-APL-HP-140:

Optimalno delovanje sistema je odvisno tudi od obsega podatkovne zbirke. Podatke, ki po preteku zakonskih rokov ali podatki, ki ne bodo dalje uporabljeni v produkcijskih sistemih, mora informacijski sistem periodično brisati ali kopirati iz produkcijskih podatkovnih baz.

SIC-APL-HP-150:

Nekatere podatkovne baze (kot trenutno na primer PostGIS), ki so po svojem obsegu omejene, razmeroma statične in jih uporabljajo sistemi v različnih nadzornih centrih, morajo biti med seboj sinhronizirane. Prav tako morajo biti v primeru sprememb le teh prilagojeni sistemi v vseh nadzornih centrih DARS.

SIC-APL-HP-160:

Aplikacija oz. uporabnik lahko dostopa do podatkovne baze le z minimalnim naborom pravic, ki ji/mu omogoča izvrševanje poslovnih funkcij. Aplikacija ne sme do baze dostopati preko uporabniškega računa, ki bi bil lastnik baznih objektov (npr. tabel, baznih procedur). Vsak samostojen modul aplikacije (npr. pregled stanja cest, administracija) mora imeti definiran ločen uporabniški račun za dostop z opredeljenimi omejitvami.

SIC-APL-HP-170:

Aplikacijski moduli/storitve, ki so nameščene izven okolja, ki ima neposreden dostop do podatkovne baze (npr. oddaljen nadzorni center, javne spletne aplikacije) in ki zahtevajo podatke iz podatkovne baze, ne smejo neposredno dostopati do podatkovne baze. Takšni dostopi morajo biti urejeni s pomočjo ločenih programskih modulov, ki preko aplikacijskih programskih vmesnikov posredujejo le zahtevane podatke.

SIC-APL-HP-180:

Preden se lahko podatkovna baza uporablja v produkcijskem sistemu, mora biti zanjo izdelana vsa potrebna dokumentacija, ki vključuje naslednje:

- (1) opis podatkovne baze,*
- (2) pogledi in razlaga podatkovnega modela,*
- (3) izvoženi modeli posameznega načrtovalskega nivoja,*
- (4) opis izvedenih aktivnosti, vezanih na optimizacijo delovanja,*
- (5) primeri podatkov in predvidena velikost baze,*
- (6) definirani uporabniški računi/vloge z opisom njihovih pravic dostopa,*
- (7) opisani postopki za varnostno kopiranje in restavriranje podatkov, vključno z orodji za ta namen, in v primeru nadgradenj*
- (8) opis sprememb v primerjavi s predhodno verzijo ter*
- (9) opredelitev načina za migracijo podatkov na novo verzijo podatkovne baze.*

Naročnik lahko poleg tega zahteva še dodatne specifične dokumente oz. omeji potrebno dokumentacijo v primeru manjših podatkovnih baz. Vgradne podatkovne baze (npr. na lokalnih postajah), do katerih ne dostopa neposredno noben modul sistema DARS in vsebuje le podatke za podporo omejenemu delovanju specifične opreme (npr. vsebina portala) kot tesno sklopljen del namenske programske opreme, ne spadajo pod te zahteve.

Porazdeljeno hranjenje podatkov

SIC-APL-HP-190:

Za nadzor in vodenje prometa naj znotraj vsakega RNC obstaja centralna podatkovna baza, ki je lahko porazdeljena, mora pa biti popolno replicirana. Uvedba porazdeljene podatkovne baze se zahteva v primeru, da centralizirana podatkovna baza kljub vertikalnemu razširjanju resursov ne zagotavlja ustreznih performans. Aplikacijska integracija z ostalimi nadzornimi centri naj bo zagotovljena preko aplikacijskih programskih vmesnikov.

SIC-APL-HP-200:

Za vse podatkovne baze v okolju DARS mora biti zagotovljeno varnostno kopiranje. Izvajalec mora zagotoviti in dokumentirati orodja za periodično izvajanje varnostnih kopij ter restavriranje podatkov. Popolna replikacija podatkovne baze ali periodično arhiviranje se mora izvajati skladno z načrtom naročnika.

SIC-APL-HP-210:

Z namenom centraliziranega nadzora prometa se zahteva enosmerno replikacijo podatkovnih baz v GNC. Replicirane podatkovne baze v GNC so le bralne.

Vpeljava podatkovnega skladišča

SIC-APL-HP-220:

V primeru zbiranja agregacijskih podatkov za nadaljnje analize, naj se le ti hranijo v ločenih podatkovnih bazah, pri čemer naj se podatki pridobivajo iz replicirane bralne podatkovne baze, da se ne obremenjuje produkcijskih sistemov neposredno.

SIC-APL-HP-230:

Za ustrezno obvladovanje nad podatki je potrebno pripraviti strategijo/vizijo/akcijski načrt za upravljanje s podatki, pri čemer je potrebno:

- (a) določiti obseg hranjenja podatkov,*
- (b) določiti ekipo, ki bo skrbela za podatke in izvajala morebitne analize ter*
- (c) identificirati cilje, zaradi katerih naj se podatki izbirajo.*

SIC-APL-HP-240:

Pri definiciji podatkov za hranjenje v podatkovnih skladiščih ni nujno vključevati le podatkov glede vodenja in nadzora prometa, vendar tudi ostalih organizacijskih podatkov z namenom optimizacije (npr. revizijske sledi, prijave/odjave v sistem, izvedene akcije v določenih dogodkih).

SIC-APL-HP-250:

Vsako podatkovno skladišče je potrebno smiselno polniti s podatki, za kar je potrebno implementirati ali vzpostaviti ustrezna orodja za ekstrakcijo, transformacijo in shranjevanje (angl. extract-transfer-load, ETL). Pri vpeljavi novih aplikacijskih rešitev, ki generirajo podatke, je potrebno vedno razmisliti, če je smiselno katere od podatkov vključiti v podatkovno skladišče.

3.5. Testiranje aplikacij in testna okolja (SIC-APL-TST)

Pri obravnavanem sistemu za vodenje in nadzor prometa gre za kritični operativni sistem, kjer bi morali biti odgovorni za testiranje prisotni skozi celoten razvojni cikel programske opreme ter načrtovati in izvajati testiranje skladno z dobro prakso, standardi in priporočili. Ustrezno izvajano testiranje preprečuje kasnejše napake v delovanju sistema, zagotavlja ustrezen nivo kakovosti, zmanjšuje stroške vzdrževanja, predvsem pa zmanjšuje verjetnost izpada kritičnega sistema v delovanju. Poleg testiranja programske opreme mora faza testiranja vključevati tudi druge komponente končne rešitve, kar v praksi pomeni testiranje strojne in periferne opreme, strežnikov in komunikacij. Testiranje vseh aplikacijskih komponent rešitve je ključnega pomena v primerih večjih sprememb strojne opreme ali njihove menjave. Poglavje obravnava naslednja področja:

- Metodologija in proces testiranja
- Dokumentacija, testni podatki in orodja
- Okolja
- Varnostno testiranje

Metodologija in proces testiranja

SIC-APL-TST-010:

Testiranje se izvaja za vsako (novo/sprememba/popravek) programsko opremo z namenom zagotavljanja višje kakovosti, kar dokazano prispeva k manjšemu številu napak pri delovanju programske opreme in nižjim stroškom vzdrževanja.

SIC-APL-TST-020:

Aktivnosti, povezane s testiranjem, se izvajajo v celotnem razvojnem ciklu programske opreme, od analize in načrtovanja do vključno prehoda v produkcijo (v fazi analize in načrtovanja poteka načrtovanje testiranja).

SIC-APL-TST-030:

Izbrani zunanji izvajalec mora omogočiti prisotnost predstavnika naročnika na testiranjih v fazi razvoja z namenom spremljanja poteka testiranja in podajanja prvih odzivov iz vidika končnega uporabnika (agilni pristop, vključevanje končnih uporabnikov).

SIC-APL-TST-040:

Podlaga za izvajanje testiranja programske opreme je dokument „Načrt testiranja“. V primeru zunanjega izvajanja načrt pripravi odgovorna oseba za testiranje na strani izvajalca v fazi analize in načrtovanja. Dokument potrdi odgovorna oseba za testiranje pri naročniku. V primeru agilnega pristopa »Načrt testiranja« predstavlja predvsem okvir za testiranje, s smernicami in principi testiranja.

SIC-APL-TST-050:

Zunanji izvajalec (razvojno podjetje) mora imeti vzpostavljen proces v okviru razvojne metodologije, ki izdelke razvoja hrani v repozitoriju izvirne kode (SVN (Sub)VersionControl, GIT ali primerljivo) ter sproti izvaja teste (Unit testi). Izvajalec za testiranje na razvojnem okolju pripravi in osvežuje poročilo o testiranju, ki je na voljo naročniku.

SIC-APL-TST-060:

Naročnik vzpostavi repozitorij izvirne kode v katerega izvajalno podjetje dostavi namestitvene verzije programske opreme.

SIC-APL-TST-070:

Pri razvoju rešitev imajo prednost pristopi, ki vključujejo agilnost, predvsem tisti, ki vključujejo uporabnike skozi vse faze razvoja programske opreme in tisti, ki ob stalnem testiranju dostavljajo prioritete zmogljivosti rešitev prednostno, hitro in v iteracijah. Skladno s principi agilnega pristopa se prilagaja tudi spremljajoča dokumentacija testiranja in njeno sprotno osveževanje ter potrjevanje.

SIC-APL-TST-080:

S postopnim preходом na »agilne« in »lean« metodologije zasledovati principe testiranja aplikacijskih rešitev, kot ga priporočajo »lean« in »agile« metodologije razvoja programske opreme in sicer s t.i. »Build Quality In« ali »Continuous automated testing and integration« znotraj »DevOps« pristopa k razvoju programske opreme.

SIC-APL-TST-090:

Testiranje mora slediti uveljavljenim standardom in priporočilom na tem področju. Prednostno:

- ISO/IEC/IEEE 29119, ki podrobneje opredeljuje opravila testiranja, proces, dokumentacijo in tehnike.*
- ISO/IEC 12207, ki med drugim določa procese pomembne za zagotavljanje kakovosti programske opreme: »Quality management«, »Risk management«, »Configuration management«, »Verification«, »Validation«.*

Dokumentacija, testni podatki in orodja

SIC-APL-TST-090:

Dokument „Načrt testiranja“ v primeru zunanjega izvajanja pripravi odgovorna oseba za testiranje na strani izvajalca v fazi analize in načrtovanja. Vsebovati mora najmanj: aktivnosti in časovnico testiranja, vrste testiranja, definicijo okolij testiranja, odgovorne osebe, navedbo spremljajočih dokumentov testiranja, dogovor o uporabi orodij za testiranje ter obliko poročil(a) o testiranju/testiranjih.

SIC-APL-TST-100:

Dokument „Testni scenarij in testni primeri“ pripravi odgovorna oseba za testiranje na strani izvajalca. Testni scenarij in testni primer potrdi odgovorna oseba za testiranje pri naročniku. Testni scenarij in testni primer mora vsebovati najmanj naslednje: Ime in kratek opis testnega scenarija; Ime testnega primera znotraj scenarija; oznako funkcionalnosti oz. naročnikovo zahtevo, za katero se uporablja testni primer; naziv funkcionalnosti; opis funkcionalnosti; opis

pogojev in zahtev za izvedbo testiranja po testnem primeru; opis načrtovanega postopka izvedbe testiranja; opis pričakovanih rezultatov testiranja; dejanski rezultati testiranja (uspešno/neuspešno/opombe); datum testiranja; okolje testiranja; izvajalci testiranja; potrditve odgovornih za testiranje. V primeru iterativnega ali agilnega procesa razvoja se dokument stalno dopolnjuje v vsaki iteraciji/sprintu.

SIC-APL-TST-110:

Dokument „Poročilo o uporabniškem/potrditvenem/funkcionalnem“ testiranju (UAT) pripravi odgovorna oseba za testiranje na strani izvajalca, vsebovati mora najmanj: Splošni podatki o testiranju (npr. verzija programske opreme, konfiguracija strojne in programske opreme, relevantna dokumentacij, ki je podlaga za testiranje, osebe, ki testirajo, datumi), Statistika ugotovljenih neskladij (ocena dokumentacije, ocena poslovno ustreznih in neustreznih rešitev, pregled ugotovljenih napak, statistika odpravljenih napak in v reševanju), Rezultati testiranja (zahteve in priporočila glede dokumentacije, opis rezultatov testiranja, plan odprave napak, zaključna ocena). Predlaga se, da se vsi testni scenariji vodijo v namenskem orodju in ravno tako vse napake, ki se odkrijejo tekom testiranja.

SIC-APL-TST-120:

Za testiranje ponavljajočih se scenarijev ali pogosto testiranje istih funkcionalnosti programske opreme se smiselno uporabi avtomatizirana priprava testnih podatkov s pomočjo namenskega orodja. Tovrstna orodja omogočajo hitrejšo pripravo testnih podatkov, ponovljivost testiranja in primerljivost testiranj.

SIC-APL-TST-130:

Za testiranje ponavljajočih se scenarijev ali pogosto testiranje istih funkcionalnosti se smiselno uporabi orodja za avtomatizirano testiranje (uporabniško testiranje, integracijsko, regresijsko, unit). Tekom razvoja pa zunanji izvajalec sprotno razvija testne algoritme za preverjanje nove programske kode, bodisi s pomočjo orodja za avtomatizacijo testiranja (konfiguracija, skripte, scenariji) ali brez.

Okolja

SIC-APL-TST-140:

Uporabniško oz. potrditveno testiranje se izvede v testnem okolju naročnika, ki je v naprej določeno (platforme, zmogljivosti, frameworki, knjižnice) in predstavljeno zunanjemu izvajalcu.

SIC-APL-TST-150:

Zunanji izvajalec vedno pripravi navodila za namestitev programske opreme na testno okolje. Namestitev na testno okolje lahko izvede zunanji izvajalec ali na podlagi navodil lahko izvede naročnik, pri čemer je zahtevana čim višja stopnja avtomatizacije oz. nameščanje s pomočjo čarovnikov.

SIC-APL-TST-160:

Priprava podatkov za testno okolje se naj izvaja čim bolj avtomatizirano s pomočjo orodij za avtomatizacijo priprave testnih podatkov ter shranjevanje teh podatkov za obnovo testnih podatkov v testnem okolju.

SIC-APL-TST-170:

Razvojno okolje in testno okolje za razvojno testiranje mora vzpostaviti izbrani izvajalec na svoji infrastrukturi. Regresijske teste programske opreme mora predhodno izvesti izvajalec v svojem testnem okolju.

SIC-APL-TST-180:

Testna okolja morajo biti dostopna na različnih fizičnih lokacijah naročnika DARS z dostopom do namenskega in varnega omrežja za testiranje DARS.

SIC-APL-TST-190:

Za potrebe osnovne simulacije prometnih scenarijev (simulacijsko okolje) se uporabi programsko opremo, namestitve in konfiguracijo zadnjega potrjenega testnega okolja ali stage okolja v kombinaciji z orodjem za avtomatizirano pripravo/generiranje testnih podatkov (primer poteka simulacije: zajem podatkov kritične prometne situacije iz preteklosti, prilagoditev podatkov (spremembe datumov, frekvence), ustvarjanje novega toka podatkov proti simulacijskemu okolju, simuliranje ukrepov). Za potrebe stalnega simulacijskega okolja se vzpostavi ločeno simulacijsko okolje, ki je primerljivo stage okolju ali funkcionalnemu testnemu okolju.

Varnostno testiranje

SIC-APL-TST-200:

Informacijska rešitev, ki je predmet javnega naročila, naj sledi smernicam MJU za razvoj informacijskih rešitev (področje varnostne politike in aplikacijske varnosti) ter vseh dobrih praks in ustreznih rešitev, ki zagotavljajo visoko stopnjo informacijske varnosti. Rešitev ne sme imeti ranljivosti po OWASP TOP 10 seznamu, kjer so navedene najpogostejše napake spletnih aplikacij. Testiranje se lahko izvede ročno ali z avtomatskimi orodji. V primeru, da so bili testi izvedeni, je potrebno o tem predložiti tudi rezultate testiranja in v primeru pomanjkljivosti seznam teh in potrdilo o odpravi. Informacijska rešitev, ki je predmet tega naročila, mora pred prvo produkcijo uspešno prestat preverjanje ranljivosti po OWASP TOP 10; vse morebitne odkrite pomanjkljivosti mora izvajalec odpraviti pred začetkom produkcije. Upravljaivec infrastrukture lahko ponovno preverjanje od izvajalca zahteva kadarkoli kasneje v življenjskem ciklu sistema. Izvajalec mora pomanjkljivosti, ugotovljene bodisi z uporabo orodja za testiranje bodisi ob praktični uporabi, odpraviti.

SIC-APL-TST-210:

Upravitelj infrastrukture podvrže sistem varnostnim testiranjem – preverjanje izvirne kode. Preverjanje izvirne kode (z orodjem Checkmarx) se začnejo izvajati takoj, ko izvajalno podjetje v repozitorij kode naročnika dostavi prve namestitve verzije, zato da se morebitne neskladnosti ali varnostne pomanjkljivosti odkrijejo zgodaj v razvojnem ciklu. Izvajalec je odkrite ranljivosti dolžan odpraviti v najkrajšem možnem času.

SIC-APL-TST-220:

Upravitelj infrastrukture podvrže sistem varnostnim testiranjem (penetration testing) po postavitvi v testno okolje naročnika. Testiranje se izvede na zahtevo, po uspešno opravljeni namestitvi, njenem preizkusu delovanja, opravljenem funkcionalnem testiranju in pripravljenih ustreznih skrbniških/uporabniških računih za delo z aplikacijo. Pogoj je poročilo o opravljenem funkcionalnem testiranju v okolju naročnika. Izvajalec je odkrite ranljivosti dolžan odpraviti v najkrajšem možnem času. Pred odpravo odkritih pomanjkljivosti/ranljivosti sistema prehod v produkcijo ni možen.

SIC-APL-TST-230:

Stalno, ob pomoči varnostnega testiranja, se izvaja oceno varnostnih tveganj programske opreme za upravljanje kritične infrastrukture, sistema za nadzor in vodenje prometa. Na podlagi zaznanih varnostnih tveganj in skladno z ISO 27001 pripraviti ukrepe za zmanjšanje ali odpravo varnostnih tveganj.

SIC-APL-TST-240:

Pri upravljanju varnosti kritičnih sistemov je potrebno slediti priporočilom ENISA za zagotavljanje varnosti v sistemih kritične infrastrukture. Na podlagi priporočil in metodologij ter prihodnjih certifikacijskih shem se prilagaja zahteve za varnostno testiranje sistema za nadzor in vodenje prometa [13]. Na podlagi študije iz leta 2016 (Stocktaking, Analysis and Recommendations on the protection of CIs) ENISA predlaga 7 priporočil državam članicam EU glede zagotavljanja varnosti kritične infrastrukture [14]:

- 1. Okrepitev sodelovanja s privatnim sektorjem pri zaznavi nevarnosti, odzivih in analizi ter krepitvi znanja na tem področju.*
- 2. Uskladiti upravljanje zagotavljanja varnosti kritične infrastrukture z nacionalnimi strukturami za obvladovanje izrednih razmer.*
- 3. Sodelovanje v mednarodnih aktivnostih preizkušanja pripravljenosti na ukrepanje ob nevarnostih za kritično infrastrukturo.*
- 4. Vzpostavitev nujnega poročanja o varnostnih incidentih na kritični infrastrukturi.*
- 5. Ocenjevanje tveganj za kritično infrastrukturo na državnem nivoju.*
- 6. Uveljavitev najboljših pravno-formalnih okvirjev za izvajanje ukrepov in obveznosti v zvezi z zagotavljanjem varnosti v kritičnih infrastrukturah.*
- 7. Preučitev možnosti za uvedbo pozitivnih spodbud upravljalcem kritične infrastrukture za boljše izvajanje ukrepov zagotavljanja varnosti.*

SIC-APL-TST-250:

Izvajanje testa »failover« je potrebno najmanj enkrat letno, ali ob večjih spremembah in nadgradnjah sistema. Pod večjo spremembo sistema v tem kontekstu razumemo večjo spremembo na katerem koli nivoju sistema (aplikacije, sistemska oprema, strojna oprema, komunikacije). Na ta način DARS preveri doseganje dogovorjenih RTO in RPO časov določenih v pogodbah, SLA-jih ali OLA-jih. Vsako »failover« testiranja mora biti dokumentirano kot to zahtevajo smernice za dokumentacijo testiranja (Načrt, Testni scenarij, Poročilo). Dodatno morajo biti sestavni del dokumentacije tudi merljivi parametri, kot sta RPO in RTO in druge metrike, ki so del SLA in OLA dogovorov.

3.6. Zagotavljanje varnosti na aplikacijskem nivoju (SIC-APL-VAR)

Poudarki v poglavju zagotavljanja varnosti na aplikacijskem nivoju se nanašajo na vzpostavitev omrežne domene za segment nadzora in upravljanja s prometom. Z vzpostavitvijo aktivnega imenika je nato mogoče upravljati pravice uporabnikov in naprav v domeni s pomočjo vlog, ki morajo biti dobro definirane, da bi vsem nivojem uporabnikov omogočale izvajanje delovnih

nalog, hkrati pa preprečevalo prevelik obseg dostopov. Potrebno je vzpostaviti domene in imenske za segment upravljanja prometa. Predpisan je najnižji nivo dvostopenjske avtentikacije s pomočjo gesel in PIN kode ali s pomočjo USB ključev ter kartic. Izpostavljen je koncept delovanja prijave v sistem samo enkrat in povezava vseh ločenih sistemov v enotno okolje. Pomemben vidik je tudi izobraževanje uporabnikov, ki lahko s svojimi dejanji povzročijo varnostna tveganja. Priporoča se redno izobraževanje ter dvig zavedanja glede varnosti na vseh nivojih uporabnikov naročnikovih sistemov. V okolju naročnika se mora zaradi večjega nivoja varnosti ter vrsto drugih prednosti implementirati požarne zidove nove generacije, ki morajo biti sposobni zagotavljati vse funkcionalnosti obstoječih požarnih zidov, vključno z zmožnostjo kreiranja in upravljanja varnostne politike. Predstavljena so tudi priporočila za fizično varovanje IT infrastrukture od nivoja podatkovnih centrov do TK vozlišč. Poglavje obravnava naslednja področja:

- Omrežna domena
- Avtentikacija, avtorizacija in "single sign on"
- Upravljanje z uporabniki
- Izobraževanje
- Nadzor
- Požarni zidovi
- Upravljanje varnostnih dogodkov
- Fizično varovanje

SIC-APL-VAR-010:

Za vsa področja varnosti je ključno imeti sistem postavljen skladno z vsemi kontrolami ISO 27001, ISO27002. Naročnik ima podeljen in veljaven certifikat sistema vodenja ISO27001, posledično morajo biti vsi sistemi skladni s standardom ISO 27001 in upoštevanje ter vpeljavo vseh kontrol iz priloge standarda: Anex A.

Omrežna domena

SIC-APL-VAR-020:

Zagotovi se vzpostavitev omrežne domene naročnika za segment sistemov nadzora in upravljanja prometa, s katero se bo lahko centralizirano upravljalo in spreminjalo obstoječe nastavitve uporabnikov, skupin in skupinskih politik ter naprav za celotno ali del domene. S tem se zagotovi večja varnost in predvsem preglednost upravljanja z enotnimi pravili za naprave in uporabnike. Hkrati se prav tako skrajša čas namenjen za upravljanje s sistemom na strani upravljalca domene.

SIC-APL-VAR-030:

Omrežna domena naročnika mora temeljiti na MS Windows tehnologiji. Naročnik mora za vzpostavitev in upravljanje z MS domeno zagotoviti ustrezni kader.

SIC-APL-VAR-040:

Omrežna domena se najprej vzpostavi na testnem okolju podjetja. Po opravljeni analizi in preskusih ter potrditvi delovanja s strani upravljalca domene in testnih uporabnikov, se domena vzpostavi na produkcijskem okolju. Sisteme se v produkcijsko okolje dodaja postopoma, takrat ko izpolnjujejo pogoje za vključitev v domeno. Omenjeno velja predvsem za opremo, ki je višje od nivoja t.i. MK (master koncentratorja). Za nivo periferne opreme to ni zahtevano, lahko pa se uporabi principe avtentikacije in avtorizacije.

SIC-APL-VAR-050:

Z vzpostavitvijo Aktivnega imenika, je mogoče upravljanje s pravicami in rolami. Role se kreira na podlagi delovnih mest, natančneje opravil, ki jih mora uporabnik na posameznem delovnem mestu opravljati in za njihovo izvajanje potrebuje pravice dostopa. Upravljalci domene si s tem olajšajo upravljanje z uporabniki in pravicami ter ima pregled nad vlogami in uporabniki v različnih vlogah. Spreminjanje uporabnika ali uporabniških pravic mora biti logirano in sledljivo tako, da se za vsakega uporabnika (in pripadajoč/e uporabniške račune) ve, kdo, kdaj in kakšne spremembe je naredil.

SIC-APL-VAR-060:

Ob kreiranju role mora ta biti dobro definirana, kar pomeni da bo zaobjela številne pravice, ki se nanašajo na specifične dolžnosti, s katerimi rola sovpada. Role omogočajo hitro prilagajanje pravic ob spremembah delovnih aktivnosti uporabnikov, brez da bi bilo potrebno nastaviti pravice za vse uporabnike, ki so dodani v rolo. Izjeme so lahko specifični uporabniki za katere so pravice lahko nastavljene individualno, kot je management in podobno.

SIC-APL-VAR-070:

V role se doda vse uporabnike, tudi zunanje izvajalce, ki lahko imajo specifične pravice dostopa. Vsak dostop s strani zunanjih izvajalcev mora biti v naprej prijavljen preko centraliziranega sistema (kot je na primer HelpDesk sistem). Opisan mora biti razlog za dostop in z njimi povezane delovne aktivnosti, ki jih bodo opravljali zunanji izvajalci, ter opredeljen predviden čas dostopa. Vsak takšen dostop mora biti odobren.

SIC-APL-VAR-080:

V privzeti varnostni skupini Administratorji domene (angl. Domain administrators) ne smejo biti dodani drugi uporabniški računi. Izjema je lahko le privzeti račun domenskega administratorja. Razlog za to je varnostni, saj imajo člani te skupine pravice za upravljanje s katerim koli pridruženim sistemom v domene (npr. delovne postaje, strežniki, prenosni računalniki). V primeru, ko so te pravice potrebne, se lahko uporabniški račun doda v to skupino samo za čas ko se opravlja delo (npr. določen poseg na strežniku). Takoj po opravljenem delu, se uporabniški račun odstrani s skupine Administratorjev domene. Vsak takšen dostop, še posebno za zunanje izvajalce, mora biti potrjen, namen dostopa pa obrazložen.

SIC-APL-VAR-090:

Za IT strokovnjake naročnika, je priporočeno, da uporabljajo več računov (angl. account). Eden račun naj bo običajni, torej brez skrbniških pravic, drugi pa naj bo t.i. privilegiran račun (angl. privileged account), ki se uporablja izključno za opravljanje skrbniških nalog. Za opravljanje dnevnih nalog, kot je recimo preverjanje e-poštnih sporočil, se naj uporablja račun brez skrbniških pravic, medtem ko naj se privilegiran račun uporablja za opravljanje administratorskih posegov.

SIC-APL-VAR-100:

Dobra praksa pri opravljanju administrativnih nalog kot so na primer administracija aktivnega imenika, administracija skupinske politike (angl. Group policy), upravljanje z DNS in DHCP strežniki, administracija virtualizirane infrastrukture je uporaba varne administratorske delovne postaje (angl. Secure Admin Workstation). Takšne delovna postaja ne sme imeti dostopa do interneta. Razlog za uporabo t.i. SAW je predvsem zagotavljanje varnostni in transparenti. SAW mora imeti možnost snemanja sej administriranja s strani zunanjih izvajalcev ali IT oddelka naročnika. Takšne posnete seje se lahko v prihodnosti uporabi tudi kot video navodila (angl. video tutorial) za posamezna administrativna opravila.

SIC-APL-VAR-110:

Storitveni računi (angl. service accounts), ki se jih uporablja za izvajanje storitev (angl. service) in nalog (angl. task) so široko uporabljani in imajo navadno nastavljeno, da geslo ne preteče nikoli. Takšni uporabniški računi lahko imajo zato preveč pravic in so pogosto dodani v skupino domenskih administratorjev, pogosto zato, ker tako zahtevajo proizvajalci programske opreme. Storitveni računi morajo:

- *uporabljati močna gesla,*
- *imeti dostop le do tistega kar potrebujejo,*
- *ne smejo imeti lokalnih administratorskih pravic,*
- *ne smejo biti člani skupine domenski administratorjev.*

Prav tako je potrebno od dobaviteljev programske opreme zahtevati, da njihova programska oprema deluje brez dodajanja storitvenega računa v skupino domenski administratorjev.

SIC-APL-VAR-120:

Varnostne skupine (angl. Security roles) naj ne bodo poimenovane z generičnimi imeni. Uporaba generičnih imen varnostnih skupin lahko rezultira v tem, da se v takšno varnostno skupino dodaja vse vrste virov, tako pa se izgubi nadzor nad članstvom v skupini ter posledično nad varnostjo. Ob tem je potrebno poudariti, da ni sistema, ki bi ugotovil za kaj vse ima določena varnostna skupina dovoljenja. Zato je potrebno imeti nadzor nad varnostnimi skupinami tudi v smislu tega, kar varnostna skupina dovoljuje.

SIC-APL-VAR-130:

Ob dodajanju domene za segment nadzora in upravljanja prometa je potrebno na testnem okolju preučiti katera izmed možnosti je bolj optimalna za vpeljavo v DARS okolje. Na testnem okolju, ki mora kar najbolj odražati produkcijsko okolje je potrebno testirati scenarije, ki bodo pokazali na kakšen način je potrebno, če sploh vpeljati novo domeno za segment upravljanja prometa v smislu dosegljivosti sistemov, potrebe po prijavah v sisteme z nadzornega v poslovni del in obratno.

SIC-APL-VAR-140:

Za namen vzpostavitve domene za segment upravljanja prometa pri naročniku je ključnega pomena vzpostavitev DNS strežnika.

SIC-APL-VAR-150:

Domenski kontrolerji morajo imeti nameščeno omejeno programsko opremo ter nastavljene omejene vloge (angl. roles). Ker so domenski kontrolerji ključni element domenskega omrežja je pomembno, da se varnostnih tveganj ne poveča z namestitvijo dodatne programske opreme na domenski kontroler. Z večanjem nabora nameščene programske opreme ter dodanih vlog na domenskem kontrolerju večje je varnostno tveganje.

SIC-APL-VAR-160:

Za namen preprečevanja vstopa zlonamernega prometa v omrežje naročnika, se uporabi blokiranje zlonamernih poizvedb DNS. Obstaja več storitev, ki preverjajo DNS poizvedbe (angl. queries) s strani zlonamernih domen, ki takšne poizvedbe blokirajo. Večina sistemov IPS (angl. intrusion prevention system) zagotavlja sposobnost preverjanja DNS poizvedb glede na seznam zlonamernih domen.

SIC-APL-VAR-170:

Z vzpostavitvijo lokalnega DNS strežnika je mogoče preverjati zapise v logih za interne in zunanje DNS poizvedbe. V logih se lahko zapiše vsak poskus povezave z zlonamernim spletnim mestom. Loge je potrebno redno pregledovati in iskati zapise, ki bi lahko pomenili zlonamerno povezavo. Te odkrite zlonamerne povezave je potrebno vključevati v sezname blokiranih poizvedb.

SIC-APL-VAR-180:

V večjih organizacijah, kamor spada tudi naročnikova je za namen redundance vedno potrebno imeti najmanj dva DNS strežnika. DNS in Aktivni imenik (angl. Active directory) sta kritične storitve, katerih odpoved lahko pomeni velike težave za organizacijo. Z zagotovitvijo redundantnega DNS strežnika se zagotovi delovanje ob odpovedi enega strežnika.

SIC-APL-VAR-190:

Domenske kontrolerje naj se virtualizira s pomočjo hipervizorjev. Pred tem je na testnem okolju potrebno preskusiti delovanje virtualizirane opreme ter določiti postopke ob napakah in odpovedih. Na virtualno okolje se ne da prijaviti v primeru odpovedi domenskega kontrolerja, ki teče na istem virtualnem okolju. Zato je potrebno imeti redundanten domenski kontroler, ki mora omogočiti prijavo v primeru, da pride do okvare virtualnega okolja.

SIC-APL-VAR-200:

Za upravljanje virtualiziranih DNS in drugih strežnikov se predvidi zunanje izvajalce, ki so specializirani za upravljanje virtualne infrastrukture.

SIC-APL-VAR-210:

Naprave, ki se pridružijo naročnikovi domeni za segment upravljanja s prometom, morajo imeti primarni in sekundarni DNS nastavljeni na notranji strežnik DNS. Zunanji strežniki DNS ne morejo razrešiti notranjih imen gostiteljev, zato lahko to povzroči težave s povezljivostjo in prepreči dostop računalnika do notranjih virov. Prav tako se z notranjim DNS strežnikom pridobi na varnosti, saj so vse DNS poizvedbe kriptirane s pomočjo protokolov TLS ali HTTPS.

SIC-APL-VAR-220:

Za segment nadzora prometa se zahteva uporaba skupinskih politik. Prav tako je uporaba skupinskih politik priporočljiva za poslovni del sistema, torej za del, ki je pod nadzorom IT oddelka naročnika. Predvsem je uporaba skupinskih politik o zahtevana za segment nadzora in upravljanja prometa, saj je v tem segmentu varnost kritičnega pomena. Tudi s pomočjo Kerberos avtentikacije in tehnologij kontrole dostopa, je lahko uporabniški račun še vedno ranljiv. Skupinska politika znotraj ADja ima na voljo več mehanizmov kot na primer zaklepanje računa ali zahtevana kompleksnost gesla, ki znatno pripomore k zagotavljanju večje varnosti.

SIC-APL-VAR-230:

Vsak objekt Skupinske politike, ki bo nastavljen na nivoju domene, bo uporabljen za vse uporabnike in naprave v domeni. To lahko pomeni, da se določene nastavitve uveljavijo za uporabnike in naprave za katere to ni željeno. Za skupinske politike je priporočljivo, da se jih nastavlja za bolj granulirane sklope, kot je organizacijska enota (angl. Organizational Unit).

SIC-APL-VAR-240:

Za namene upravljanja skupinskih politik, so zahtevana opisna imena različnih skupinskih politik. Podobno kot pri imenovanju AD skupin, so opisna imena ključna za prepoznavanje namena skupinske politike.

SIC-APL-VAR-250:

Vsaka skupinska politika naj bo ustvarjena za točno določen namen. Odsvetuje se uporaba t.i. povezovanja (angl. linking), kjer lahko določena skupinska politika prevzame nastavitve druge skupinske politike. Takšen način se lahko uporablja le v primeru ko je več organizacijskih enot (angl. OU) podrejenih eni.

SIC-APL-VAR-260:

Prepovedano je onemogočanje skupinskih politik. V primeru, ko je skupinska politika vezana na organizacijsko enoto (OU), vendar od nekega trenutka dalje ne velja več za OU, je potrebno izbrisati povezavo med OU in skupinsko politiko in ne onemogočiti skupinske politike. V primeru, ko se skupinsko politiko onemogoči, to velja za celotno domeno, kar lahko privede do težav v primeru ko to skupinsko politiko uporablja druga organizacijska enota.

SIC-APL-VAR-270:

Spremembe skupinske politike, predvsem glede najpomembnejših sprememb, je potrebno redno dokumentirati. Pred spremembami skupinskih politik je potrebno doseči dogovor z vodstvom, ki se mora strinjati glede sprememb. Poleg tega je potrebno nastaviti sistem obveščanja ob spremembah kritičnih skupinskih politik (npr. preko elektronske pošte), saj morajo biti skrbniki sistemov obveščeni čim prej, da se lahko izogne izpadu sistema.

Avtentikacija, avtorizacija in »single sign on«

SIC-APL-VAR-280:

Vsi uporabniki in aplikacije morajo uporabljati enoten DARS sistem za upravljanje identitet in avtorizacij ter s tem povezane in sprejete standarde, protokole in nosilce. Aplikacije morajo imeti možnost uporabe lokalnega admina, ki se ga uporabi v primeru izrednih razmer nedelovanja domene.

SIC-APL-VAR-290:

Za zaposlene na DARS, kot tudi za zunanjo delovno silo, ki dela s ali vzdržuje kritične sisteme (npr. SCADA, NKS, SNVP in podsistemi, predvsem sistem za detekcijo prometa ter povezane senzorične naprave) je minimalna predvidena dvofaktorska avtentikacija na primer s pomočjo USB ključke ali kartice v kombinaciji z gesli ali še bolj pogosto s PIN kodo.

SIC-APL-VAR-300:

Za namen vzpostavljanja domene, se priporoča integracijo Linux strežnikov in drugih naprav ter uporabnikov v Microsoft Aktivni imenik. Aktivni imenik mora biti centralni imenik sistema.

SIC-APL-VAR-310:

Skladno z dobrimi praksami pri velikih mešanih sistemih (Linux in Windows) se zagotovi možnost enkratne prijave za uporabnike s katerim lahko z enkratno prijavo v sistem dostopajo do aplikacij in različnih naprav.

SIC-APL-VAR-320:

Enkratna prijava je potrebna tudi za IT oddelek, predvsem za sistemske administratorje, saj se tako pridobi na času in učinkovitosti pri opravljanju vzdrževalnih in drugih del na infrastrukturi.

SIC-APL-VAR-330:

Za samo zagotavljanje dvofaktorske avtentikacije zaposlenih na DARS se uporabi USB ključke ali kartice v kombinaciji z gesli ali še bolj pogosto s PIN kodo. Za zunanje sodelavce kot so na primer vzdrževalci, ki vpogledujejo v določene sloje rešitve pa kombinacija gesel in žetonov.

SIC-APL-VAR-340:

Z varnostnega vidika je zelo pomembno doreči protokol, ki predpisuje ukrepanja in aktivnosti v primeru izgube ključa ali druge naprave, ki omogoča dvostopenjsko avtentikacijo. Opisani morajo biti postopki ob poškodbi, nedelovanju ali izgubi takšne naprave. Prav tako je potrebno zagotoviti, da se takšnim uporabnikom zagotovi dostop do nujno potrebnih virov na drug način. V primeru nadzornega centra, se lahko v varnem prostoru nahaja generični medij ali pa se uporabi žeton, ki se v primeru takšne situacije uporabi s predpisanim postopkom. V primeru zunanjih uporabnikov je prav tako potrebno določiti protokol ob izgubi naprave, ki ima nameščeno aplikacijo za generiranje žetonov za dostop. V takšnih nujnih primerih je možna izdaja začasnega žetona, ob predhodni potrditvi.

Upravljanje z uporabniki

SIC-APL-VAR-350:

Zagotoviti je potrebno učinkovito uporaba načel »kategorizacije in klasifikacije«, »najmanjšega nivoja pravic«, »samo kar uporabnik mora vedeti« in »kontroliran dostop« na podatkih organizacije, skozi procese, tehnologijo in ljudi. Z učinkovito uporabo omenjenih načel bo zagotovljeno, da so tveganja povezana z uporabo podatkov pravilno nadzorovana, kar pomeni, da se avtoriziran dostop omogoči ter prepreči neavtoriziran dostop.

SIC-APL-VAR-360:

Uporabniki so bolj podvrženi napakam kot tehnologija. Majhne napake uporabnikov lahko vodijo v razkritje občutljivih podatkov ali nenamerno povzročanje ranljivosti računalniškega sistema s katerimi lahko napadalec pridobi občutljive podatke s sistema. Uporabniki ne smejo razkriti občutljivih informacij na javnih mestih, kot je na primer internet. Ne smejo pošiljati občutljivih informacij (kot so recimo podatki za vpis ali finančni podatki) neavtoriziranim prejemnikom preko elektronske pošte ali drugih kanalov komunikacije. Uporabniki morajo spoštovati dokumentirane varnostne predpise.

SIC-APL-VAR-370:

Kontrole dostopa, kot so na primer »single sign on«, večfaktorska avtentikacija in druge morajo biti pred implementacijo testirane na testnem okolju in dokumentirane v testnih postopkih. Testno okolje bi naj čim bolj ponazarjalo produkcijsko okolje, da bi se lahko v fazi testiranja razkrile pomanjkljivosti.

SIC-APL-VAR-380:

Vsi testni uporabniški računi morajo biti arhivirani po uporabi. Razlog za to je, da imajo testni uporabniški računi velikokrat dodeljen višji nivo pravic za dostop do sistemov in informacij. Prav tako z njimi velikokrat dela več uporabnikov. Za testne uporabniške račune je možno nastaviti tudi samodejno arhiviranje po določenem času ali na določen datum.

SIC-APL-VAR-390:

Uporabniki lahko menjajo delovno mesto, napredujejo ali se na kakšen drug način selijo po organizaciji. Ob spremembi delovnega mesta, je skoraj vedno potrebno spremeniti pravice uporabnikom. V primeru, ko se ob takšnih dogodkih uporabnikom pravice ne spremenijo tako, da odražajo dostope do sistemov in informacij, ki jih za trenutne delovne naloge potrebujejo, lahko to rezultira v napačnih pravicah za uporabnika. S tem lahko ima uporabnik dostop, ki ni v skladu z organizacijskimi predpisi. Zato je nujno, da se pravice uporabnikom ažurirajo pravočasno, ter da se vzpostavi možnost sledenja in revizije sprememb uporabniških pravic.

SIC-APL-VAR-400:

ISO standard 27001 definira štiri glavne kontrole za upravljanje z dostopom uporabnikov, ki so registracija uporabnikov, upravljanje s pravicami, upravljanje z gesli – žetoni ter pregled nad pravicami za dostop uporabnika. Vse štiri kategorije so ključne za upravljanje z uporabniki in morajo biti upoštevane glede na uporabljen princip upravljanja z uporabniškimi dostopi.

SIC-APL-VAR-410:

Za naročnika je potrebno vzpostaviti IdM sistem, ki omogoča upravljanje z identitetami ter posledično upravljanje s pravicami in dostopi. Razlog za to je, da se v velikih podjetjih pogosto pojavlja problem v obvladovanju dostopov in pravic zaposlenega, kontroli omenjenih dostopov in pravic ter sledljivostjo sprememb v dostopih in pravicah zaposlenih kot tudi zunanjih izvajalcev.

SIC-APL-VAR-420:

IdM sistem mora omogočati povezavo z aplikacijo/aplikacijami, ki so primarni vir podatkov o uporabnikih (npr. kadrovski informacijski sistem, ERP rešitev) ter omogočati sinhronizacijo podatkov z Aktivnim imenikom. Ob sinhronizaciji mora biti omogočen popoln uvoz podatkov za vse zaposlene ali samo spremembe. Sistem mora omogočati definicijo atributov uporabnikov, ki jih je potrebno vzdrževati ter, da se za vsak atribut določi primarni izvor podatka (npr. Kadrovski inf. sistem). Dobra praksa je, da se v IdM sistemu določi obvezne podatke o zaposlenemu in se definira katere akcije so potrebne v primeru manjkajočega podatka.

SIC-APL-VAR-430:

Natančno mora biti opredeljen postopek dodajanja uporabnikov. Predpisano mora biti kdo je zadolžen za dodajanje novega uporabnika v sistem, ter kdo in na kakšen način uporabniku dodeli potrebne pravice. Dobra praksa na tem področju je tudi povezava med kadrovsko aplikacijo, aktivnim imenikom ter IdM rešitvijo na način, da se lahko uporabnik ustvari v kadrovski rešitvi, saj navadno v organizacijah kadrovski oddelek pozna delovno mesto in druge podatke o uporabniku. Definirano mora biti pravilo po katerem se ustvari uporabniško ime. Uporabnik se nato s sinhronizacijo prenese v Aktivni imenik. Pravice se mu nato nastavi v IdM rešitvi in se po potrebi prenesejo v podrejene sisteme ob upoštevanju definiranih pravil. Obveščanje mora v takšnih primerih biti učinkovito in lahko poteka samodejno ob dodajanju novega uporabnika. Ob kreiranju se upošteva logična struktura aktivnega imenika, kar pomeni, da se objekt na podlagi določenega vhodnega atributa kreira v ustrezni organizacijski enoti.

SIC-APL-VAR-440:

Natančno mora biti opredeljen postopek arhiviranja uporabnika, ki je mogoče močno poenostaviti z vpeljavo aktivnega imenika in IdM rešitve. Natančno mora biti predpisano, kdo je zadolžen za arhiviranje uporabnikov in kdo ima za to potrebne pravice, ter opredeljen postopek hitre/nujne ukinitve uporabnika. Ko se v kadrovski rešitvi izvede izstop zaposlenega (uporabnika), mora IdM sistem poskrbeti, da se ob naslednji sinhronizaciji onemogoči račun uporabnika v Aktivnem imeniku. Tako se zagotovi, da se omogoči odstranitev vseh pravic uporabnika z eno akcijo.

SIC-APL-VAR-450:

IdM mora omogočati, da ob kreiranju elektronskega poštnega naslova ponudi predlog za poštni strežnik glede na definirano pravilo (npr. prve črka imena in priimka). Omogočati mora ročno izbiro poštnega strežnika.

SIC-APL-VAR-460:

IdM mora omogočati, da se vse samodejne procese po potrebi lahko opravi tudi ročno (npr. sprememba poštnega naslova zaradi spremembe priimka).

SIC-APL-VAR-470:

Aplikacije, ki se povezujejo v IdM sistem morajo obvezno biti povezane z imeniškimi storitvami. V primeru naročnika bo za ta namen predviden Aktivni imenik (angl. Active directory).

Izobraževanje

SIC-APL-VAR-480:

Uporabnike je potrebno izobraziti glede primerne uporabe informacijskih sistemov in jih podučiti glede principov omejevanja dostopov, kot je na primer »samo kar mora uporabnik vedeti« ter o razlogih za vpeljavo takšnih omejitev.

SIC-APL-VAR-490:

Uporabniki se morajo zavedati varnostnih tveganj, saj bodo v tem primeru bolj pazljivi na grožnje, ki se osredotočajo na človeški faktor ter hkrati poznali pravilne ukrepe za učinkovitejšo zaščito organizacijskega informacijskega sistema in drugih organizacijskih sredstev.

SIC-APL-VAR-500:

Uporabniki se morajo zavedati, da je potrebno preveriti avtorizacijo za vsako zahtevo za dostop do občutljivih podatkov ali drugih virov, ne glede na to, od kje oziroma koga prihaja zahteva.

Nadzor

SIC-APL-VAR-510:

V IKT okoljih kot je naročnikovo je smotrno uporabiti rešitev za nadzor in spremljanje vseh aplikacij, ki tečejo na produkcijskem okolju, da bi zagotovili, da aplikacije tečejo v skladu s pričakovanji oziroma jih presegajo.

SIC-APL-VAR-520:

Priporočeno je odkrivanje napak do nivoja naprav. Identificirati je potrebno, ali je slabo delovanje aplikacije pogojeno s slabim delovanjem naprav ali je vzrok drugje.

SIC-APL-VAR-530:

Rešitve za nadzor in spremljanje delovanja aplikacij morajo omogočati hiter »drill-down« od nivoja uporabniške izkušnje do zaznave napak na napravah uporabnikov, aplikacijskih zaledij (angl. Back end) in podporne infrastrukture.

SIC-APL-VAR-540:

Za velike sisteme je priporočena uporaba tehnologij umetne inteligence in strojnega učenja, da bi se lahko odkrile anomalije v velikih obsegih podatkov, ki jih obstoječa orodja in ljudje ne uspejo pregledati in zaznati.

SIC-APL-VAR-550:

Z zunanjimi podjetji, ki za naročnika razvijajo in skrbijo za kritične aplikacije je potrebno vzpostaviti SLA (angl. Service level agreement), ki definirajo še sprejemljivo delovanje aplikacije, odzivne čase izvajalcev v primeru napak, razpoložljivost aplikacij v letnem okviru in drugo.

SIC-APL-VAR-560:

Za vsako aplikacijo je priporočljivo oceniti finančno izgubo ob nedelovanju, ki temelji na oceni izgube zaradi potrebnega dodatnega razvoja ali podpore uporabnikov. Namen je prioritizacija naporov pri odkrivanju in odpravi napak ter podpora uporabnikov.

SIC-APL-VAR-570:

Pred implementacijo rešitve za nadzor in spremljanje delovanja aplikacij je potrebno pripraviti seznam kritičnih aplikacij, storitev ter spletnih naslovov, ki jih je potrebno nadzorovati. Nato se aplikacije, storitve in spletne naslove razdeli v logične skupine z namenom lažjega nadzora in posegov ob dnevnih opravilih.

SIC-APL-VAR-580:

Za naročnika se predvidi izbiro rešitve za nadzor in spremljanje delovanja aplikacij, ki lahko teče na virtualiziranem okolju, saj se virtualizacija že uporablja v podjetju. Na ta način je možno zmanjšati število fizičnih strežnikov za katere mora skrbeti IT oddelek, ter poenostaviti postopke nameščanja in nagrajevanja rešitev.

SIC-APL-VAR-590:

Za naročnika je priporočena implementacija centralnega nadzornega sistema za nadzor in spremljanje delovanja aplikacij. Distribuirane sisteme se uporablja v velikih omrežjih, ki so med seboj povezana s počasnimi povezavami.

SIC-APL-VAR-600:

Implementirani nadzorni sistem mora imeti možnost dostopa do nadzorovanih računalnikov na daljavo ter možnost prilagoditve pravil, alarmov poročil, uporabniškega vmesnika ter nadzornih plošč na način, da je vidno oziroma sistem opozarja le na tisto kar je potrebno. Priporočljiva je tudi možnost shranjevanja predlog, tako da si lahko vsak uporabnik ali uporabniška skupina, ki dela z rešitvijo postavi svoje preglede in sledi tistemu, za kar je zadolžena.

Požarni zidovi

SIC-APL-VAR-610:

Požarni zidovi nove generacije morajo zagotavljati vse funkcionalnosti obstoječih požarnih zidov, vključno z zmožnostjo kreiranja in upravljanja varnostne politike, podporo »site to site« VPN, WAN »failover« in »load balancing«, 3G in 4G WAN »failover«, IPsec in SSL VPN podporo oddaljenega dostopa, centralno upravljanje, poročanje ter visoko stopnjo razpoložljivosti.

SIC-APL-VAR-620:

Pred nameščanjem, posodabljanjem aplikacij in podobnimi posegi morajo zunanji izvajalci oddati zahtevo preko centraliziranega sistema v skladu z zapisano smernico SIC-APL-VAR-60. Na požarnih zidovih je potrebno vrata (angl. porte) odpirati le po potrebi, glede na zahtevo izvajalca, ki mora biti odobrena. Za zagotavljanje varnosti je možna je tudi vezava MAC naslova na omrežna vrata. Zunanjim izvajalcem se po potrebi zagotovi VPN dostop, ki mora biti odobren ter zabeležen. Vsak VPN dostop se po zaznavi »idle« uporabnika samodejno prekine po določenem časovnem okviru (npr. 15 minut).

SIC-APL-VAR-630:

Požarni zidovi nove generacije morajo zagotavljati preprečevanje vdorov. Integrirani »Intrusion Prevention Services« ščitijo pred množico aplikacijskih ranljivosti, ki lahko prihajajo z notranjega in zunanjega omrežja. IPS mora nadzorovati omrežje in iskati grožnje in nenavadne dogodke, ki jih nato blokira ali zapiše v log, glede na pred nastavljena pravila. Omogočeno mora biti samodejno posodabljanje, ki preprečuje nove grožnje.

SIC-APL-VAR-640:

Požarni zidovi morajo imeti možnost identificiranja in upravljanja z aplikacijami. Zagotavljati morajo prepoznavanje aplikacij glede na njihov podpis, ne glede na protokola ali uporabljena vrata (angl. port). Aplikacije so lahko vizualno predstavljene (na primer na kontrolni plošči) v realnem času, da bi se lahko nadzorovalo in zagotavljalo pasovne širine, ki jih potrebuje za izvajanje ter zagotovilo varnost na omrežju. Administratorji morajo imeti možnost nastavljanja prioritete aplikacij ter omejevati možnost dostopa za aplikacijo. Najboljše rešitve požarnih zidov zagotavljajo dvosmerno pregledovanje vsega prometa, ne glede na velikost paketov ali število aktivnih sej, s pomočjo samodejnega posodabljanja podpisov.

SIC-APL-VAR-650:

Pri mnogih grožnjah gre za poskus vdora preko varnih kanalov s pomočjo SSL enkripcije. Prav zato mora imeti požarni zid nove generacije zmožnost dekriptirati, preveriti in rekriptirati SSL promet.

SIC-APL-VAR-660:

S požarnimi zidovi nove generacije ni več potrebno slediti IP naslovu fizičnega uporabnika. Lahko se vežejo na LDAP in Aktivni imenik organizacije ter tako podprejo »single sign on« in samodejno povežejo uporabniški ID s končno točko (angl. Endpoint) za zagotavljanje kontrole dostopa.

SIC-APL-VAR-670:

Požarni zidovi nove generacije temeljijo na aplikacijskih, IPS in anti-malware podpisih. Ekipa, ki v organizaciji skrbi za varnost oziroma ponudniki požarih zidov morajo zagotavljati samodejno in ročno zbiranje aplikacijskih ter drugih podatkov, kreiranje novih podpisov in samodejno nameščanje novih podpisov na požarne zidove.

SIC-APL-VAR-680:

Ob namestitvi več požarnih zidov v organizaciji, je potrebno preveriti soodvisnost aplikacij. Ne sme se zgoditi, da bi požarni zid blokiral podatke ene aplikacije, ki jih druga potrebuje za svoje izvajanje.

Upravljanje varnostnih dogodkov

SIC-APL-VAR-690:

SIEM sistem mora zagotavljati zajem poljubne količine podatkov, izvajanja korelacij med podatki z neomejenega števila virov, najbolje v realnem času (sekunde, minute). V primeru, da spremljanja in odziva v realnem času ni mogoče zagotoviti, mora biti zaznava in odziv na varnostne dogodke prožen v najkrajšem možnem času.

SIC-APL-VAR-700:

SIEM sistem mora biti sposoben prikazovati rezultate korelacij in analiz podatkov v realnem času.

SIC-APL-VAR-710:

SIEM sistem mora omogočati upravljanje preko grafičnega vmesnika, brez dodatnega programiranja. Grafični vmesnik mora imeti možnosti upravljanja s pravili ter poizvedbami.

SIC-APL-VAR-720:

SIEM sistem mora biti povezljiv z drugimi, zunanjimi varnostnimi komponentami s katerimi je mogoče samodejno prepoznavati grožnje. SIEM sistem mora biti centralni sistem kamor se stekajo vsi varnostni podatki, ki jih organizacija mora spremljati. Možna mora biti povezava oziroma integracija z drugimi varnostnimi komponentami za samodejno izmenjavo relevantnih podatkov ter usklajeno delovanje.

SIC-APL-VAR-730:

SIEM mora zagotavljati upravljanje in zaščito revizijskih sledi.

SIC-APL-VAR-740:

Za izbran in implementiran SIEM sistem mora naročnik zagotavljati osebje za nadzor in upravljanje s sistemom. Možno je tudi, da se v ta namen najame zunanje izvajalce. V tem primeru morajo biti z SLA usklajeni odzivni časi zunanjih izvajalcev, časovni interval posodobitve sistema (na primer novi podpisi) ter zagotovljena podpora (če je potrebno 24/7).

Fizično varovanje

SIC-APL-VAR-750:

Električna omara ali soba, prostori centralne UPS, prostori kjer se nahajajo zunanji sistemi klimatizacije in ostali kritični deli infrastrukture, katerih izpad pomeni zaustavitev delovanja podatkovnega centra in posledično storitev, mora biti zaklenjena, dostop do nje pa imajo lahko samo pooblaščno osebe.

SIC-APL-VAR-760:

Okrog električne omare ali sobe je potrebno vzpostaviti fizično prepreko, kjer je to mogoče, z namenom, da bi se neavtoriziran dostop preprečil.

SIC-APL-VAR-770:

V električni omari ne sme biti prisotna katera koli vnetljiva snov ali predmet. Prav tako je vse nepotrebne predmete potrebno odstraniti z omare.

SIC-APL-VAR-780:

Obvezno mora biti prisoten sistem video nadzora v električni omari oziroma sobi.

SIC-APL-VAR-790:

Dostop do strežniške sobe in hrambe podatkov lahko ima samo pooblaščno osebo - sistemski administratorji zadolženi za strežnike. Strežniška soba naj ima le enega ali dva vhoda, ki sta primerno zavarovana. Za vstop v strežniško sobo se mora oseba avtenticirati s pomočjo dvo ali večstopnjske avtentikacijskih mehanizmov. Dostop do strežniške sobe je mogoč le v primerih posredovanja (nadgradenj, reševanju težav z opremo, vzdrževalnih delih...). Vsak vstop v strežniško sobo mora biti časovno opredeljen (čas vstopa, ter predviden čas trajanja dela) ter ustrezno evidentiran (kaj točno se je v določenem času izvajalo) v knjigi vstopa.

SIC-APL-VAR-800:

V strežniški sobi mora biti vzpostavljen neprestan sistem video nadzora. Vsi računalniki in strežniki morajo imeti zagotovljen neprestan dostop ter redundantni dostop do omrežja, napajanja in hlajenja. Strežniške sobe morajo imeti zagotovljeno klimatizacijo.

SIC-APL-VAR-810:

Temperatura v strežniških sobah mora biti primerna (nekje med 19 in 23 °C). Soba mora imeti tudi merilce vlažnosti in temperature. Priporočena vlažnost v strežniški sobi je 45-60%.

SIC-APL-VAR-820:

Strežniško sobo je potrebno postaviti tako, da je možna naknadna razširitev zaradi dodajanja naprav, načinov dostopa do sobe ali načinov vzdrževanja opreme.

SIC-APL-VAR-830:

V strežniški sobi mora biti nameščen protipožarni sistem. Priporočena je namestitev detektorjev dima po celotnem prostoru data centra. Alarmi se morajo sprožiti takoj, ko je dim zaznan. Vsi zaposleni morajo imeti kopijo evakuacijskega načrta v primeru požara. Evakuacijski načrt mora biti prav tako na vidnem mestu v strežniški sobi. Prav tako mora biti prisotna oprema za gašenje ter zagotovljen trening za zaposlene, za pravilno uporabo te opreme.

SIC-APL-VAR-840:

Za opremo v strežniški sobi mora biti vzpostavljeno varnostno kopiranje (angl. backup) in/ali redundantna lokacija.

SIC-APL-VAR-850:

Na nivoju podatkovnega centra naročnika je potrebno zagotoviti kontrolo dostopa do posameznih con, ki se lahko zagotovi s pomočjo visoko resolucijskega video nadzora ter analitike, ki lahko prepozna obraz. V primeru naročnika je v enem prostoru več sistemov in posledično integratorjev, ki vstopajo v prostor. Zato je potrebno zagotoviti kontrolo dostopa tudi na nivoju posamezne omare (angl. cabinet control). To se lahko doseže z oskrbo omar z elektronskimi sistemi zaklepanja, poleg tega pa se lahko zagotovi tudi kontrola dostopa s pomočjo biometričnih podatkov.

3.7. Integracija z zunanjimi sistemi (SIC-APL-INT)

Pri integraciji z zunanjimi sistemi se združuje več vidikov, ki so sicer opisani v namenskih poglavjih - na primer varnost, arhitektura, hranjenje podatkov, standardi in vmesniki. Veljati morajo vsa pravila, ki veljajo za interne sisteme, pri čemer je tu večji poudarek na varnosti, definiranju standardiziranih formatov sporočil in verzij aplikacijskih vmesnikov. Glede protokolov se izkaže, da komunikacija s sistemi za upravljanje in vodenje prometa drugih držav

že poteka skladno s standardi, večji zalogaj pa je povezovanje s sistemi zunanjih izvajalcev. Nekateri sicer sami predpišejo lastne in jasne sheme, medtem ko ostali ne zagotovijo niti potrebne dokumentacije. Ponovno se omeni dobra stran uporabe platforme za upravljanje z vmesniki, ki bi nudila predvsem pregled, pravice za dostop, beleženje uporabe in dokumentacijo nad vsemi vmesniki.

SIC-APL-INT-010:

Potrebno je definirati posamezne kategorije zunanjih sistemov in pravila za povezovanje z njimi (npr. zagotavljanje varnosti, potrjevanje podatkov, zanesljivost delovanja, omejevanje prometa, format sporočil). Trenutno identificirani zunanji sistemi so na primer:

- (a) splošni javni sistemi,*
- (b) sistemi kritične infrastrukture in*
- (c) sistemi pogodbenih partnerjev.*

SIC-APL-INT-020:

Pri povezovanju z zunanjimi sistemi je potrebno zagotoviti ločene komponente za komunikacijo z njimi in transformacijo podatkov, da se zagotovi šibka sklopljenost z jedrnim delom aplikacij in omogoči enostavnejše posodobitve ali zamenjavo storitev. Za zunanje sisteme, ki niso nujni za delovanje nadzornih sistemov, naj se zagotovi popolnoma ločen sistem, ki zanje zagotavlja dostop.

SIC-APL-INT-030:

Pri povezovanju z mednarodnimi sistemi in kjer je mogoče se zahteva izmenjava podatkov s pomočjo aktualnih standardiziranih sporočil (kot je trenutno na primer DATEX 2 v3.0).

SIC-APL-INT-040:

Pri integraciji z zunanjimi sistemi je potrebno slediti ustrezni metodologiji razvoja in testiranja programske opreme (kot na primer kontinuiran integracijski model). Integracijo mora izvajati izkušena ekipa, ki izvaja ustrezne regresijske teste in teste celostnega delovanja, da zagotovi robustno delovanje sistema.

SIC-APL-INT-050:

Pri prenašanju podatkov med sistemi DARS in zunanjimi sistemi je potrebno zagotoviti validacijo prenešenih podatkov in ustrezno šifriranje podatkov, ki ščiti podatke in vključuje identiteto zunanjega sistema.

SIC-APL-INT-060:

Ko DARS nastopa kot odjemalec v odnosu do zunanjega sistema, naj se zahteva, da aplikacijski programski vmesniki sledijo dogovorjenim predpisom, zagotavljajo ustrezen nivo varnosti, zanesljivosti in njihovi upravitelji ne spreminjajo dogovorjenih lastnosti brez predhodnega dogovora.

SIC-APL-INT-070:

V primerih, ko DARS nastopa kot ponudnik storitev/podatkov, je potrebno izbrati primeren protokol, preko katerega bo nudil podatke (kot na primer HTTP REST) in slediti aktualnim dobrim praksam/smernicam (kot na primer OpenAPI initiative) ali standardom.

SIC-APL-INT-080:

V primeru ponujanja podatkov v zvezi s stanjem prometa ali arhivskih podatkov, analiz, ipd. javnosti ali podjetjem brezplačno ali proti plačilu se priporoča uporaba temu namenjenih komponent izbrane platforme za upravljanje z vmesniki. To bo omogočilo celovito, nadzorovano in poceni upravljanje z zunanjimi odjemalci.

3.8. Podatkovni centri (SIC-APL-PDC)

DARS je že v letu 2012 vzpostavil interne standarde za ureditev TK in sistemskih prostorov. Standardi predstavljajo odlično izhodišče, ki bi ga bilo potrebno posodobiti v skladu z razvojem in trenutno veljavnimi standardi ter praksami. Na voljo obstaja nekaj glavnih standardizacij, ki so opisane in poleg odličnosti nudijo tudi ugled pri sodelovanju z mednarodnimi akterji. V smernicah se poleg aplikacijskega dela, ki je trenutno usmerjen v virtualizacijo/kontejnerizacijo, osredotočamo tudi na fizično varnost, vzdrževanje, dokumentacijo in nadzor podatkovnih centrov. Vse to so ključni deli, ki jih je potrebno nasloviti. Še bolj pomembno pa je zagotoviti usposobljene kadre za redni nadzor in upravljanje v skladu s standardi. Slednje je še bolj pomembno kot neposredna certifikacija, saj z vzpostavitvijo internih standardov po vzoru več uglednih usmeritev podjetje izkazuje zrelost in resnost na trgu ter zagotavlja nemoteno delovanje njegovih storitev. Poglavje obravnava naslednja področja:

- Standardi in dobre prakse
- Vzdrževanje in nadzor
- Dokumentacija

Standardi in dobre prakse

SIC-APL-PDC-010:

Področje standardizacije podatkovnih centrov se z zamikom prilagaja spremembam v industriji, poleg tega je drago za vpeljavo. Priporoča se, da se v okolju DARS na podlagi izkušenj vzpostavi in posodablja dokument s smernicami in dobrimi praksami oz. internimi standardi za vzpostavljanje, prenovo in vzdrževanje podatkovnih centrov. Pri tem naj se upošteva in tudi sklicuje na uveljavljene standarde kot so Data center Tier Classification Standard (Uptime institute), EN 50600 (CENELEC, ISO) ali AE360 (IDCA) ter ostale pomembne standarde, kot so ISO 20000, ISO 27001 ali ISO 22301.

SIC-APL-PDC-020:

Interna pravila/standardi glede podatkovnih centrov v DARS naj obravnavajo različne tipe podatkovnih centrov glede na njihovo funkcijo (kot so LNC, RNC ali GNC). Poleg tega naj se zahteve predpiše tudi za lokalne postaje, ki ne sodijo v sklop podatkovnih centrov, vendar so fizične enote v omrežju DARS, kjer se izvaja omejeno procesiranje podatkov, podobno kot manjša vozlišča, ki niso vezana na nadzor in vodenje prometa.

SIC-APL-PDC-030:

V vsakem podatkovnem centru naj se beležijo in analizirajo osnovne metrike, ki vplivajo na razpoložljivost sistemov, kot so zahteve po računski moči, pomnilniku, diskovnem prostoru in uporabi omrežja. Skladno z ugotovitvami analiz naj se izvajajo tudi nadgradnje opreme.

SIC-APL-PDC-040:

Pri implementaciji programskih rešitev naj se sledi uveljavljenim trendom v industriji in skrbi za skladnost med vsemi podatkovnimi centri DARS. Trenutni trendi kažejo, da se lahko z uporabo ustrezne orkestracije vsebnikov, kot je na primer Kubernetes, doseže večjo učinkovitost v podatkovnih centrih.

SIC-APL-PDC-050:

Pri implementaciji omrežne infrastrukture, segmenta videa in aplikacijskega nivoja v podatkovnih centrih naj se upoštevajo smernice, ki so nastale kot del priprave tehničnih zahtev integracije in centralizacije ITS sistemov v nadzornih centrih (št. 2019/2018).

Vzdrževanje in nadzor

SIC-APL-PDC-060:

Interna pravila/standardi glede podatkovnih centrov v DARS morajo predvidevati in definirati redno preverjanje delovanja sistemov. Poleg tega naj se beleži dodatne podatke o posameznih sistemih, kot so odvisnosti od ostalih sistemov, amortizacija, redno in izredno vzdrževanje ali nadzor nad dobavitelji. V pomoč slednjemu se lahko uporablja tudi namensko plaftormo za vzdrževanje sistemov (CMMS), ki je del sistemov DCIM (glej tudi SIC-APL-PDC-100).

SIC-APL-PDC-070:

Pri uvedbi ali nadgradnji sistemov v podatkovnem centru naj se sisteme dimenzionira glede na predvidene kratkoročne plane, saj se tehnologija lahko nepričakovano hitro spremeni, kot na primer klimatske naprave v odvisnosti od toplotnega odtisa strežnikov. Zaradi tega morajo biti sistemi zasnovani modularno z možnostmi razširitev.

SIC-APL-PDC-080:

Podatkovni centri v DARS sestojijo iz več različnih sistemov, ki jih vzdržujejo različni izvajalci. Zaradi tega je težko skladno zagotavljati varnost podatkovnih centrov in informacijski ravni. Tehnično varovanje je že jasno definirano in določeno s standardi (ISO 27001). Interna pravila/standardi glede podatkovnih centrov v DARS morajo definirati obdobja in obseg rednih penetracijskih testiranj. Na primer, letno penetracijsko testiranje izbranega regionalnega podatkovnega centra in upoštevanje ugotovitev v celotnem okolju DARS.

Dokumentacija

SIC-APL-PDC-090:

Pri pripravi načrtov in dokumentiranju podatkovnega centra je potrebno slediti strukturi določb v internih pravilih/standardih glede podatkovnih centrov v DARS z namenom poenotenja dokumentacije in označevanj med podatkovnimi centri.

SIC-APL-PDC-100:

Omrežni in aplikacijski sistemi se v podatkovnem centru spreminjajo pogosteje, na kar vpliva na primer posodobitev programske opreme, spremembe v povezljivosti ali dodajanje novih kapacitet. Ker je zaradi tega vzdrževanje fizične dokumentacije zamudno in zato pogosto v praksi ne odraža dejanskega stanja, se zahteva uvedba sistema za vodenje »žive dokumentacije.« Primer takšnega enostavnejšega sistema je NetBox (DigitalOcean). V primeru, da bi želeli na podoben način obravnavati vse vidike podatkovnih centrov, pa se priporoča uvedba dražjih celostnih sistemov DCIM, kot so na primer Ability Data Center (ABB), Device42 ali EcoStruxure (Schneider Electric).

3.9. Obravnava nepredvidenih dogodkov (SIC-APL-OND)

Obravnava nepredvidenih dogodkov je vezana predvsem na zagotovitev ustreznih postopkov in protokolov ukrepanja v primeru izpadov ali nedelovanj posameznih storitev. Pri tem je zelo pomembna izvedba rednih t.i. »požarnih vaj.« Izdelati je potrebno načrte, odgovornosti, odvisnosti storitev, deležnikov ter plan komuniciranja. Vse to definira posebno področje ITSCM (angl. IT Service Continuity Management), ki je del uveljavljenih procesov ITIL. V okviru tega je potrebno definirati maksimalne čase izpadov, preden lahko pride do katastrofe za podjetje. Postopki predvidevajo testiranje vseh nivojev storitev - od obnovitev do testov na živih sistemih (ne le v nadzorovanem okolju, kjer so pogoji velikokrat različni). Ker okolje DARS združuje mnogo različnih aplikacijskih storitev, je ugotavljanje napak še posebej oteženo, zaradi tega se predlaga sledenje »inženirstvu kaosa,« ki je postalo popularno predvsem zaradi kompleksnih oblačnih sistemov.

SIC-APL-OND-010:

Področje obravnave nepredvidenih dogodkov je del širšega področja za obravnavanje tveganj. V okviru sistemov za nadzor in vodenje prometa je potrebno zagotoviti ustrezne postopke za upravljanje z nepredvidenimi dogodki. Poleg obveznega sledenja dobrim praksam, ki jih definirajo standardi, se priporoča certificiranje v okviru ISO 22301.

SIC-APL-OND-020:

V okviru DARS morajo biti zagotovljeni postopki za zagotavljanje neprekinjenega delovanja storitev. Slednje se lahko doseže z vzpostavitvijo načrta neprekinjenega delovanja (angl. Business Continuity Planning) in rednim izvajanjem procesov za zagotavljanje neprekinjenega delovanja (angl. IT Service Continuity Management), ki jih definira ogrodje ITIL. Še posebej pomembno je redno izvajanje aktivnosti, posodabljanje dokumentov ITSCM ter identificiranje scenarijev, ki lahko povzročijo izpade storitev.

SIC-APL-OND-030:

V okviru DARS je potrebno določiti upravitelja neprekinjenega delovanja (angl. Service Continuity Manager), ki razume širše potrebe podjetja in je odgovoren za preventivne aktivnosti ter definicijo aktivnosti v primeru izpadov. Hkrati je skrbnik procesov in vseh dokumentov v zvezi z neprekinjenim delovanjem storitev ter odgovoren za poročila o testiranjih in za posodabljanje dokumentov. Upravitelj sodeluje z ekipo posameznikov, ki izvajajo aktivnosti v skladu z njegovimi navodili.

SIC-APL-OND-040:

IT v DARS sestoji iz več okolij, kot sta na primer nadzor in vodenje prometa in poslovni del. Zaradi skladnosti in učinkovitosti se priporoča, da so postopki za zagotavljanje neprekinjenega delovanja med okolji enaki. To velja tudi za tehnične postopke, kjer je to mogoče, kot na primer – zamrznitev varnostnih kopij za določeno časovno obdobje, preverjanje integritete izdelanih varnostnih kopij, šifriranje in podobno.

SIC-APL-OND-050:

DARS mora imeti pripravljen načrt obnovitev ob nesreči (angl. Disaster recovery plan) za vsak sistem IT. Načrt mora vsebovati jasna in nedvoumna navodila za vzpostavitev oz. obnovitev sistema IT v primeru njegovega izpada iz kakršnegakoli razlog, kot so na primer napaka strojne opreme ali problemi pri programskih posodobitvah. Načrt mora biti redno vzdrževan in posodabljan. Postopki za testiranje obnovitev morajo potekati sinhronizirano z testiranjem neprekinjenega delovanja, ki jih vodi upravitelj neprekinjenega delovanja.

SIC-APL-OND-060:

V okolju DARS morajo biti definirana točna pravila, kdaj in kateri obnovitveni testi se izvajajo. Priporoča se ob vsaki spremembi ali vsaj enkrat letno. Poleg rednih »požarnih vaj,« je potrebno obravnavati tudi druge oblike testov (angl. Paper test, Walk through test, Parallel test, Cutover test). Za izvedbo obnovitvenih testiranj se lahko najame zunanje izvajalca, vendar mora izvajalec zagotoviti in vzdrževati vse potrebne dokumente, kot so načrt neprekinjenega delovanja (angl. BCP), načrt obnovitev (angl. DR plan) ali ostali dokumenti iz področja neprekinjenega delovanja.

SIC-APL-OND-070:

V primeru izpada mora upravitelj neprekinjenega delovanja (angl. Service Continuity Manager) voditi celoten postopek obnovitve in skrbno opazovati potek. Po uspešni obnovitvi mora upravitelj:

- (1) Izdelati poročilo o obnavljanju, ki ga predloži v pregled vodstvu.*
- (2) Identificira vse pomanjkljivosti v načrtih za neprekinjeno delovanje (angl. business continuity plan) in načrtih za obnovitev (angl. disaster recovery plan), skladno z njimi posodobi dokumente in s celotno ekipo za izvajanje obnovitev stestira posodobljene dokumente.*

SIC-APL-OND-080:

V okolju DARS je mnogo sistemov vezanih na različne komponente ali senzorske podatke. Poleg delovanja aplikacij bi bilo smiselno meriti vplive izpadov posameznih zunanjih ali notranjih sistemov, procesov, aplikacij ali omrežij. V ta namen se priporoča uporaba inženirstva »kaosa,« saj lahko le tako zagotovimo robustno delovanje sistemov v nenadzorovanih pogojih. Uporaba tega inženirstva naj bo le komplementarna standardnim postopkom testiranja obnovitev oz. naj se ga vključi kot del standardnega testiranja.

4. Video nadzorni sistem (SIC-VID)

Dokument Video nadzorni sistem analizira tehnične lastnosti kamer in podrejenih sistemov ter opredeljuje in podaja smernice uvajanja oz. nadgrajevanja IP video sistema. V dokumentu so zajeti predlogi za razvoj in nadgradnjo sistema za video nadzor prometa (VNP) s poudarkom na združljivosti in povezljivosti v celovit sistem naročnika s centraliziranim upravljanjem. Kritični sistemi VNP, skupaj s podpornimi sistemi, kot so npr. induktivne zanke, števcji prometa, mikrovalovni in drugi detektorji, nadzornikom prometa omogočajo podporo pri odločanju ter hkrati tudi zagotavljajo avtomatsko detekcijo kritičnih dogodkov na cestah. Področje je tesno povezano z razvojem sodobnih inteligentnih transportnih sistemov s prenosom informacij v realnem času, saj je njihova uspešnost delovanja odvisna od ustreznih podsistemov tako na strojnem, omrežnem kot tudi aplikativnem nivoju. Skupaj z ostalimi sistemi upravljanja je VNP tako povezan v celovit sistem za nadzor, upravljanje, vzdrževanje in podporo odločanju. Smernice v dokumentu so razdeljene po naslednjih poglavjih:

- Arhitektura sistema za video nadzor prometa
- Povezljivost in omrežni nivo
- Kamere za video nadzor prometa
- Sistemi za video detekcijo prometa

4.1. Arhitektura sistema za video nadzor prometa (SIC-VID-AVS)

Arhitektura sistema za video nadzor prometa je trenutno zaradi razpršenosti in nehomogenosti kompleksna in segmentirana na različne rešitve in več podsistemov. V skladu s smernicami in primeri dobrih praks se celoten sistem VNP postopoma nadgrajuje, kar bo omogočalo izvedbo integracije in centraliziranega upravljanja vseh podsistemov. Arhitektura temelji na omrežnih tehnologijah in protokolih IP, zato je s stališča komunikacijskih omrežij potrebno zagotavljati skladnost z vsemi smernicami za komunikacijska omrežja v dokumentu SIC-OMR.

Zaradi narave sistemov IP je bistveno lažje vzpostaviti centralizirano upravljanje in nadzor ter, ob primernem načrtovanju komunikacijskega omrežja s podporo ustreznih protokolov, zagotoviti tudi vpogled v katerokoli kamero, povezano v tovrstni sistem. Centraliziran sistem upravljanja in nadzora naročniku omogoča učinkovito upravljanje in integracijo z različnih lokacij vse od GNC do pogonske centrale (PC) na posameznih objektih ter tudi z ustrezno zavarovanega delovnega mesta na kateri koli lokaciji naročnika.

Z možnostjo dostopa do sistema VNP od kjerkoli je potrebno na omrežnem in aplikacijskem nivoju zagotoviti tudi varnostne mehanizme, ki preprečujejo dostop do vsebin nepooblaščenim osebam v skladu z GDPR in področno zakonodajo. Poglavje Arhitektura za video nadzor prometa obravnava naslednja področja:

- Izhodišča
- Razvoj IP video nadzornega sistema
- Centralizirano upravljanje kamer.

Izhodišča

SIC-VID-AVS-010:

Za zagotavljanje učinkovitosti in prilagodljivosti morajo biti vsi sistemi in podsistemi VNP zasnovani tako, da omogočajo pooblaščenim administratorjem hiter dostop in administracijo sistema s katere koli lokacije naročnika v okviru internega omrežja naročnika.

SIC-VID-AVS -020:

Vsi sistemi VNP morajo vsebovati varnostne mehanizme, ki preprečujejo morebiten dostop nepooblaščenim osebam ali omogočajo zlorabe. Onemogočanje dostopa nepooblaščenim osebam mora biti zagotovljeno v skladu z GDPR in področno zakonodajo.

SIC-VID-AVS-030:

Arhitektura sistema za video nadzor prometa (VNP) mora biti v celoti zasnovana na tehnologiji IP in podpirati protokole, navedene v smernicah za video kamere (SIC-VID-CAM) in smernicah za komunikacijska omrežja (SIC-OMR), ter omogočati centralizirano upravljanje in integracijo s sistemi ITS.

Razvoj IP video nadzornega sistema

SIC-VID-AVS-040:

Novo vgrajeni sistemi in podsistemi VNP morajo biti združljivi z obstoječim sistemom za video nadzor prometa naročnika ter se med seboj ne smejo izključevati.

SIC-VID-AVS-050:

Kamere in druga strojna ter programska oprema morajo biti združljive s sistemom VNP naročnika brez dodatnih prilagoditev v obliki zunanjih kodirnikov oz. pretvornikov in morajo biti na seznamu združljive opreme s strani proizvajalca oz. ponudnika sistema VNP.

SIC-VID-AVS-060:

Kamere in druga strojna in programska oprema morajo imeti vgrajene oz. podpirati uporabo najmanj kodirnih postopkov H.264 in H.265, zaželena je tudi podpora vsaj še enega kodeka, ki je podprt s strani sistema VNP naročnika.

SIC-VID-AVS-070:

Sistem za zajem video vsebin mora omogočati hrambo posnetkov kamer do 1 meseca, pri čemer se izračuna potrebno kapaciteto na podlagi nastavljenih kodirnih postopkov in vrednosti bitnih pretokov v času vgradnje z upoštevanjem 20% rezerve ter možnosti nadgradnje in razširitve kapacitet v primeru povečanja števila kamer ali ločljivosti le-teh.

SIC-VID-AVS-080:

Pri nadgradnjah in/ali razširitvah je potrebno zagotoviti vse ustrezne licence za potrebe delovanja celotnega sistema z nastavitvami, vključno z dokupom dodatnih licenc obstoječih sistemov, v kolikor so le-te potrebne.

SIC-VID-AVS-090:

Pri nadgradnjah in/ali razširitvah je potrebno zagotoviti vse morebitne dodatne integracijske postopke in povezave za doseganje polne učinkovitosti, centraliziranega upravljanja in povezav z ostalimi podsistemi v skladu z načrti in zahtevami naročnika.

SIC-VID-AVS-100:

Vse arhitekturne nadgradnje in/ali spremembe morajo biti ob koncu del dokumentirane in predstavljene naročniku. Izvajalec je dolžan naročniku predati vso ustrezno dokumentacijo, vključno z dostopnimi podatki za upravljanje ter programsko kodo, v kolikor je bila le-ta spremenjena ali dodana s strani izvajalca. O načinu upravljanja se naročnik in izvajalec dogovorita pisno, vendar mora naročnik imeti na voljo vse dostopne podatke.

SIC-VID-AVS-110:

Izvajalec del pri spremembah ali dodatnih vgradnjah na sistemih VNP ne sme vzpostavljati dodatnih dostopovnih povezav brez pisnega soglasja naročnika, saj predstavljajo potencialno varnostno luknjo. Sistem mora zabeležiti vsako vzpostavljeno povezavo iz zunanjega omrežja in o tem tudi obvestiti administratorja na strani naročnika.

Centralizirano upravljanje kamer

SIC-VID-AVS-120:

Sistem centraliziranega upravljanja kamer mora omogočati varen način upravljanja kamer iz ene ali več lokacij v okviru naročnikovega internega omrežja prek centraliziranega sistema upravljanja.

SIC-VID-AVS-130:

Sistem centraliziranega upravljanja kamer mora omogočati najmanj:

- *upravljanje naslovov IP kamer,*
- *nadzor stanja kamer in delovanja le-teh,*
- *upravljanje pravic dostopa do nastavitev in video vsebin,*
- *varnostno kopiranje nastavitev kamer,*
- *obnovo varnostne kopije na kamero,*
- *upravljanje parametrov več kamer hkrati,*
- *vodenje oz. beleženje sprememb in dostopov ter*
- *daljinski popolni reset kamere.*

SIC-VID-AVS-140:

Sistem za ponovni zagon kamer, ki omogoča začasen izklop napajanja kamere, mora biti integriran v sistem za upravljanje in dostopen pooblaščenim osebam v nadzornih centrih in administratorju kamernega sistema.

SIC-VID-AVS-150:

Vsi dodatni sistemi in podsistemi morajo biti pred vgradnjo in uporabo v sistemu naročnika preizkušeni v testnem okolju. Izvajalec nadgradnje mora naročniku predložiti predlog nadgradnje ter na praktičnem testnem primeru prikazati ustrezno delovanje. Novi ali razširitveni podsistemi morajo biti razširljivi in upoštevati kapacitete ter obseg kamer v okviru celotnega video omrežja naročnika.

4.2. Povezljivost in omrežni nivo (SIC-VID-PON)

Na omrežnem segmentu je predviden tudi velik porast omrežnega prometa zaradi višje ločljivosti in dinamike videa, porast zasedanja virov je ocenjen na faktor 10-15× ob optimalnem kodiranju in uporabi kodirnega postopka H.265. Zaradi dinamike omrežnih pretokov in možnih manjših izbruhov se pri načrtovanju priporoča 20% varnostna meja. Pri načrtovanju prenove omrežja se priporoča tudi preučitev možnosti za ločevanje video prometa od ostalega prometa za upravljanje in nadzor sistemov. S tem bi se lahko zagotovila neodvisnost kritičnih sistemov za alarmiranje in upravljanje od video sistema, ki bi lahko v določenih primerih porasta predmeta povzročal zasičenje vmesnikov in s tem onemogočanje prenosa kritičnih podatkov v realnem času. Ob prenovah posameznih tras oz. odsekov je zato smiselno izdelati študijo nadgradnje komunikacijskega omrežja in prednosti oz. omejitve izgradnje ločenega omrežja za video nadzor prometa, ki bi z ločitvijo zmanjšal medsebojni vpliv in povečal zanesljivost obeh tako fizično ločenih omrežij.

Poglavje Povezljivost in omrežni nivo obravnava naslednja področja:

- Izhodišča
- Varnost
- Segmentacija in vključevanje v hrbtenično omrežje
- Protokoli

Izhodišča

SIC-VID-PON-010:

Kamere in podsistemi sistema VNP morajo podpirati IGMPv3 in zahtevane funkcionalnosti naročnikovega obstoječega sistema na lokacijah, kjer se video oprema priključuje v lokalna in dostopovna omrežja.

SIC-VID-PON-020:

Kamere morajo podpirati protokole za krmiljenje kamer na daljavo prek obstoječih povezav IP in sistema VNP naročnika.

Varnost

SIC-VID-PON-030:

Na nivoju video omrežja morajo biti implementirani varnostni protokoli za zagotavljanje varnostni sistema in preprečevanja nepooblaščenega dostopa do videoposnetkov, skladno s področno zakonodajo in GDPR.

Segmentacija in vključevanje v hrbtenično omrežje

SIC-VID-PON-040:

Povezovanje kamer v omrežje se izvaja v dveh ali treh vzporednih obročih po principu izmeničnega priključevanja, npr. 1,3,5,7.../2,4,6,8..., kar omogoči nadzornikom vsaj delno pokritost trase, objekta oz. področja v primeru izpada enega obroča. Kjer topologije obroča ni mogoče izvesti, se na identičen način izvede topologijo zvezda, kjer se kamere po enakem principu izmenično priključuje na veje.

SIC-VID-PON-050:

Za zagotavljanje večje kakovosti storitev podatkovnega in video segmenta se na nivoju LNC izvaja fizično in logično ločeno omrežje za video segment. Na video omrežju je potrebno izključiti QoS, jumbo packets in flow control ter omogočiti podporo IEEE 802.1BA/Q/AS ter IGMPv3.

SIC-VID-PON-060:

Ob prenovi posameznih cestnih odsekov in/ali nadgradenj s kamerami ločljivosti HD je potrebno izdelati študijo zasedanja virov. V kolikor bi pričakovani video promet presegel 60% kapacitete glavnih komunikacijskih povezav, je potrebno vzpostaviti fizično ločeno video omrežje tudi na hrbteničnih povezavah. V primeru manjšega prometa se povezava video omrežja in podatkovnega omrežja izvaja kombinirano s pomočjo rešitev VLAN in VRF.

Protokoli

SIC-VID-PON-070:

Sistem za upravljanje in nadzor kamer mora podpirati vsaj profila S in T standarda ONVIF, zaželen pa je tudi podpora za profil G.

SIC-VID-PON-080:

Sistem VNP in sistem za upravljanje kamer morata podpirati omrežne protokole IPv4, IPv6, HTTPs in HTTP, SSL/TLSa, IGMP, ICMP, DHCP, ARP, SMTP, LLDP, UPnP, SNMP v1/v2c/v3, DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, RTCP, SOCKS, SSH, NTCIP in ONVIF, ki so ključni standardi oz. protokoli za delovanje obstoječe opreme ter omogočajo tudi nadgradnjo in razširljivost VNP sistemov.

SIC-VID-PON-090:

Fiksne in vrtljive kamere s kupolo morajo podpirati tudi protokole SFTP za nalaganje intervalnih statičnih slik, ki so v uporabi v okviru zunanjih storitev oz. so na voljo širši javnosti preko aplikacijkih vmesnikov.

SIC-VID-PON-100:

Sistemi VDP ter SNVP morajo podpirati protokola TAMP in DEM XML zaradi združljivosti z naročnikovim obstoječim sistemom za upravljanje.

4.3. Kamere za video nadzor prometa (SIC-VID-CAM)

Veliko lastnosti kamer, ki vplivajo na končno kvaliteto slike, ni mogoče razbrati iz tehnične specifikacije kamer, zato je priporočljivo testiranje kamer v enotnem okolju in z enotnimi pogoji s pomočjo testnih kart in vzorcev. Prav tako je mogoče vzpostaviti testno okolje za vizualno in tehnično analizo odziva kamer na različne svetlobne pogoje in dinamičnega razpona ter preveriti tehnično ustreznost, izmeriti efektivne bruto bitne pretoke ter primerjati natančnost premikov in različne načine upravljanja, saj se pogosto le-ti lahko razlikujejo od teoretično izračunanih vrednosti. Na podlagi analize in primerjalnega testa se tako lahko določi seznam ustreznih in neustreznih kamer, ki morajo poleg zgoraj naštetih lastnosti ustrezati tudi vsem sistemskim in omrežnim zahtevam, določenim na omrežnem nivoju ter sistemih nadzornih centrov. Poglavje Kamere za video nadzor prometa obravnava naslednja področja:

- Tipi kamer, ohišja in pritrditev
- Optični sistem
- Tehnične lastnosti in zmogljivosti kamer
- Napajanje in priključitev kamer
- Bitni pretoki

Tipi kamer, ohišja in pritrditev

SIC-VID-CAM-010:

Vse kamere oz. ohišja kamer, ki so nameščene zunaj pokritih predelov, torej izven predorov, vkopov ipd., morajo imeti zaščitni razred IP minimalno IP66 ter zaščito pred udarci in vandalizmom minimalno IK08.

SIC-VID-CAM-020:

Vse kamere morajo imeti razpon delovne temperature minimalno med -40 °C in + 50 °C., razen pri termalnih kamerah, kjer je lahko razpon temperature od -30 °C do +50 °C.

SIC-VID-CAM-030:

Vse gibljive (PTZ) kamere morajo imeti vgrajeno ogrevanje kupole oz. sistem za odroševanje stekla ohišja.

SIC-VID-CAM-040:

Nosilci kamer morajo biti izdelani na način, da onemogočajo gibanje kamer zaradi vremenskih vplivov. V primeru montaže kamer na strukture objektov so dopustni premiki kamer največ +/- 2 mm od mirovne lege ter največ +/- 9 cm od mirovne lege na 10 m visokem drogu, ob sunkih vetra do 35 m/s.

SIC-VID-CAM-050:

Umestitev kamer na odprti trasi mora biti izvedena na način, da minimizira vpliv sončne svetlobe na zajet video. Primarni pogled kamere mora tako biti usmerjen v smeri med severovzhodom in severozahodom, razen v primeru, kadar fizične razmere tega ne dopuščajo, kot na primer vhod ali izhod iz predora.

Optični sistem

SIC-VID-CAM-060:

Vrtljive oz. »Speed dome« kamere z nastavljivo goriščno razdaljo (angl. zoom) morajo imeti minimalno 15-kratno optično povečavo pri ločljivosti 4K in 30-kratno povečavo pri ločljivosti HD.

SIC-VID-CAM-070:

Zaščitna stekla kamer, predvsem gibljivih s kupolo, morajo biti na celotni površini zaščitnega stekla v vidnem polju objektiva uniformna, brez stikov, šivov ali razlik v ukrivljenosti ali debelini.

SIC-VID-CAM-080:

Kamere, ki tehnično ustrezajo specifikacijam, se testira v laboratorijskem in realnem okolju s strani naročnika in neodvisnega laboratorija. Zagotoviti je potrebno testiranje vseh kamer pri enakih pogojih s pomočjo testnih vzorcev SMPTE ter inštrumentov za merjenje barv, osvetlitve in programske opreme za prepoznavo ukrivljanja črt, pik in vzorca šahovnice. Rezultate se razvrsti glede na končni rezultat vseh uteženih meritev, pri čemer je večji poudarek na geometrijski kot barvni pravilnosti slike. Meritve se izvede pri različnih goriščnih razdaljah in svetlobnih pogojih. Potrebno je zagotoviti enakovredne meritve, torej samo meritve, ki so izvedljive za vse kamere v testiranju.

SIC-VID-CAM-090:

Vse kamere morajo imeti integriran vsaj profil S in T odprtega standarda za povezovanje ONVIF, zaželeno pa tudi profil G.

Tehnične lastnosti in zmogljivosti kamer

SIC-VID-CAM-100:

Vse video nadzorne kamere morajo po tehničnih lastnostih ustrezati zahtevam, navedenim v tabelah 3 - 6 v dokumentu SIC-VID. Zaradi hitrega trenda razvoja trga morajo kamere ustrezati minimalnim zahtevam, a hkrati slediti razvoju in trendom. Naročnik si pridržuje pravico, da za določene odseke, v skladu s tehničnimi značilnostmi, zahteva višje parametre oz. boljšo kakovost.

SIC-VID-CAM-110:

Vse kamere morajo biti združljive z obstoječim sistemom naročnika za nadzor in vodenje prometa in morajo biti navedene kot ustrezne na seznamu združljivih naprav.

SIC-VID-CAM-120:

Fiksne in vrtljive kamere morajo za primere izpada določene povezave do kamere podpirati lokalno snemanje na kartico SD ali notranji disk. S tem lahko naročnik zagotavlja hrambo posnetkov v dolžini vsaj 1 dneva na lokalnem mediju. Video posnetki na mediju morajo biti kriptirani, da v primeru odtujitve kamere niso dostopni nepooblaščenim osebam.

Napajanje in priključitev kamer

SIC-VID-CAM-130:

Vse kamere morajo imeti vgrajene omrežne vmesnike tipa Ethernet RJ-45 ali SFP oz. SFP+ za optično povezavo do oddaljenega vozlišča, pri čemer naročnik predpiše tip vmesnika glede na mesto vgradnje in razpoložljivo omrežno opremo.

SIC-VID-CAM-140:

Kamere se lahko napajajo prek ločenih fizičnih napajalnikov ali prek stikala UPoE in kabla UTP. Napajanje mora biti izvedeno na način, da naročniku omogoča »trdi« ponovni zagon oz. izklop/vklop napajanja. Za to morajo biti zagotovljeni pogoji proženja iz vseh predvidenih lokacij, predvsem iz delovnih postaj v GNC in RNC, ter integracija z aplikativno programsko opremo naročnika, to je brez neposrednega dostopa do omrežnih stikal.

Bitni pretoki

SIC-VID-CAM-150:

Fiksne in vrtljive kamere morajo obvezno podpirati video kodeka H.264 in H.265 ter opcijsko Motion JPEG, termalne in bispektralne kamere pa H.264 in Motion JPEG, opcijsko tudi H.265.

SIC-VID-CAM-160:

Kamere morajo omogočati nastavljanje stopnje kompresije in ciljnega bitnega pretoka ter izbiro ustreznega kodeka.

SIC-VID-CAM-170:

Kamere morajo omogočati tudi pošiljanje statičnih slik prek FTP, SFTP in HTTPS protokolov za namen zunanjih storitev, kot sta npr. spletni portal promet.si ali mobilna aplikacija Promet+, ki do teh slik dostopajo preko aplikacijskih vmesnikov.

4.4. Sistemi za video detekcijo prometa (*SIC-VID-VDP*)

Sodobne kamere imajo že lahko vgrajen sistem za sledenje in avtomatsko detekcijo dogodkov, štetje prometa in podobno, hkrati pa omogočajo tudi dodatne možnosti, kot so SMART IR in bispektralno delovanje. Detekcija dogodkov na sami kameri odločilno vpliva na kompleksnost zalednega sistema, kot tudi potrebo po višji zmogljivosti le-tega, saj se tako obdelava videa porazdeli po obrobni elementih sistema (kamere). Naročnik trenutno v večini uporablja video detekcijo prometa na zunanjih karticah na podlagi vhodne digitalizirane slike. V naprednih sistemih za videonadzor prometa se vse pogosteje uporablja razpršeno procesiranje, kjer detekcijo prometa in incidentov lahko izvajamo neposredno na kamerah, pri čemer se močno zmanjša vpliv pretvarjanja video signalov na uspešnost detekcije.

SIC-VID-VDP-010:

V primeru eksplicitnih zahtev po vgrajeni detekciji s strani naročnika morajo kamere za avtomatsko detekcijo prometa podpirati avtomatsko detekcijo dogodkov na sami kameri - brez dodajanja zunanjih enot, npr. zunanjih kartic za video detekcijo.

SIC-VID-VPD-020:

Kamere za avtomatsko detekcijo prometa morajo omogočati vsaj prepoznavo vozil in objektov, prehode vozil čez določeno območje in zaznavo ustavljenega vozila s pomočjo standarda ONVIF.

5. Zaključek

Smernice za integracijo in centralizacijo sistemov za nadzor in vodenje prometa v nadzornih centrih DARS podajajo krovne usmeritve pri nadgradnjah ali uvajanju novih rešitev na področjih arhitekture in delovanja nadzornih centrov, komunikacijskih omrežij na različnih ravneh, video nadzora in detekcije prometa ter aplikacijskih in informacijskih rešitev. Ob tem so izpostavljeni tudi vidiki kadrovske kompetence, nujne za vpeljavo, vzdrževanje in uporabo posameznih sistemov in storitev.

Dokumenti smernic predstavljajo prvi korak k poenotenju tehnoloških podlag za varno, zanesljivo in učinkovito vodenje prometa. Globina podanih vsebin zato odraža več splošnih principov dobrih praks v okolju naročnika kot globljih poudarkov na posameznih segmentih ali rešitvah. Temu so namenjeni nadaljnji koraki poglobljanja pravil na posameznih področjih z jasnim ciljem priprave repozitorija tehničnih specifikacij, neposredno uporabnih pri sodelovanju z zunanjimi izvajalci in dobavitelji, pri javnih naročilih in pri lastnem notranjem obvladovanju kritične infrastrukture.

Področje informacijskih in komunikacijskih tehnologij je nadvse dinamično, zato so predstavljeni dokumenti z utemeljenimi smernicami zgolj začetek nujnega in stalnega procesa spremljanja tehnologij in principov upravljanja ter njihovega uvajanja in posodabljanja. Le tako bo možno doseči največjo mero varnosti, zanesljivosti in učinkovitosti sodobnih transportnih poti.