# IEC 62443-3-3:2013 Tööstusautomaatika süsteemi turvanõuded

Seitse alusnõuet, 51 süsteeminõuet

100 nõuet. Selle standardi järgi on võimalik sertifitseerida akrediteeritud sertifitseerimisasutuses. Versioon 07/2026.

IEC 62443-3-3 on sertifitseeritav ja sertifitseeritakse süsteem, mitte organisatsioon ega isik. Võimalikud teed on ISASecure SSA ja IECEE CB Scheme. Organisatsiooni sertifitseerimiseks on vaja 62443-2-1 või 2-4, komponendi puhul 62443-4-2. Käesolev loend sisaldab 51 süsteeminõuet ja 49 nõude täiendust. Nende kohaldumine sõltub taotletavast turvatasemest: alates SL 1 on neid 38, alates SL 2 on neid 60, alates SL 3 on neid 90, tasemel SL 4 kõik 100. Ükski täiendus ei kohaldu juba tasemel SL 1. See loend on töövahend enesehindamiseks, mitte tõend.

| Ettevõte | Kuupäev | Täitja |
|---|---|---|
| | | |

## 5 FR 1: Kes või mis pääsu taotleb ja kas tegemist on tõepoolest väidetud osapoolega 24

### SR 1.1 Inimkasutajad on tuvastatud ja nende isikusamasus on kontrollitud enne pääsu saamist igas punktis, kus nad saavad automaatikasüsteemi käitada või seadistada. Siia kuuluvad masina juures asuvad operaatoripaneelid, inseneripääs ja võrguteenused.

Mille järgi seda näeb: Süsteemi kõigi sisselogimispunktide loetelu, see tähendab HMI, juhtimisruum, PLC-programmeerimispääs, kommutaator, VPN ja kaughoolduse klient, igaühe juures seal kasutatav autentimismehhanism. Lisaks konfiguratsiooniväljavõte või sisselogimisekraani kuvatõmmis iga seadmeklassi kohta. Väike ettevõte alustab ühest tabelist seadme kohta, veerud: seade, liides, autentimine olemas jah või ei, põhjendus kui ei. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 1.1 RE 1 Iga inimkasutaja töötab isikliku tunnuse all, mis on antud ainult sellele isikule. Jagatud ja vahetusekontod on välja lülitatud, allesjäänud erandid on juhtumipõhiselt põhjendatud ja täiendavate meetmetega kaetud.

Mille järgi seda näeb: Kontode väljavõte süsteemide kaupa, kus tunnus on seotud isikuga, erandite loend koos põhjenduse ja kompenseeriva meetmega, näiteks kaamera või kohalolekupäevik operaatorikoha juures. Käesolev rida on nõude täiendus ega ole seetõttu kunagi kohustuslik tasemel SL 1, nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 1.1 RE 2 Igaüks, kes logib sisse mitteusaldusväärsest võrgust, näiteks internetist või kaughooldusühenduse kaudu, tõendab oma isikusamasust vähemalt kahe sõltumatu teguriga.

Mille järgi seda näeb: Kaugpääsu konfiguratsioon sisselülitatud teise teguriga, näidiskirje sisselogimisest, kus mõlemad tegurid on näha, ning tokenite või rakenduseregistreeringute väljastusloend. Väike ettevõte kasutab olemasoleva VPN-lüüsi teist tegurit või autentimisrakendust, mis ei maksa peale seadistusaja midagi. Nõude täiendus, nõutav alates SL 3, tasemel SL 1 mitte.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 1.1 RE 3 Tõendamine kahe sõltumatu teguriga kehtib mitte ainult väljastpoolt tulevale pääsule, vaid iga inimkasutaja sisselogimisele, sealhulgas sisselogimistele usaldusväärseks liigitatud võrgu sees.

Mille järgi seda näeb: Keskse autentimisteenuse poliitika väljavõte, mis näitab, et teine tegur on jõustatud ilma võrgupõhiste eranditeta, lisaks näidiskirjed sisselogimistest juhtimisruumis ja operaatoripaneelil. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 1.2 Peale inimeste autendivad end süsteemis ka tarkvaraprotsessid ja seadmed, enne kui neil lubatakse andmeid vahetada või teenuseid kasutada. Siia kuuluvad kontrollerite vahelised sidestused, andmeühendused kõrgema taseme süsteemidega ja diagnostikavahendid.

Mille järgi seda näeb: Masinatevaheliste ühenduste loend koos allika, sihtkoha, protokolli ja igas ühenduses kasutatavate autentimisandmetega, näiteks sertifikaat, teenusekonto või eeljagatud võti. Lisaks ühe sidestuse konfiguratsiooniväljavõte, kus autentimine on nähtav. Nõutav alates SL 2, tasemel SL 1 ei ole nõutav.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.2 RE 1** **Iga tarkvaraprotsess ja iga seade esitab oma kordumatu tunnuse. Jagatud teenusekontod või üks kogu süsteemis paljudes seadmetes kasutatav võti ei ole lubatud.** Dokument

Mille järgi seda näeb: Seadme ja tunnuse või sertifikaadi seerianumbri vastavustabel, mis näitab, et ükski tunnus ei esine kaks korda. Nõude täiendus, nõutav alates SL 3 ega kuulu seetõttu taseme SL 1 hulka.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.3** **Kontosid hallatakse kogu nende olelusringi vältel: loomine, õiguste muutmine, väljalülitamine lahkumisel ja eemaldamine on reeglitega korraldatud ning asjaomaste süsteemidega toetatud. Siia kuuluvad kasutajakontod, teenusekontod ja hädaolukorra kontod.** Dokument

Mille järgi seda näeb: Kontode register koos tüübi, omaniku, otstarbe ja olekuga, lisaks tõendid tööle tulnute ja lahkunute kohta, näiteks allkirjastatud üleandmisakt või pilet, millel on näha väljalülitamine koos kuupäevaga. Korduv kontode ülevaatus on soovitatav ja väikeses ettevõttes piisab kontode loendi iga-aastasest võrdlemisest personali nimekirjaga. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.3 RE 1** **Kontode haldus on kõigis süsteemi komponentides ühtne, nii et konto väljalülitamine ühes kohas ei jää üksikutes seadmetes mõjuta.**

Mille järgi seda näeb: Tõend keskse kataloogi liidestamise kohta, näiteks kataloogiteenus või RADIUS, koos ühendatud komponentide loendiga ja selgesõnalise loendiga seadmetest, mida ei saa ühendada, ning nende alternatiivse korraga. Testikirje väljalülitamisest, mis jõustub kõigis ühendatud süsteemides. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.4** **Tunnused väljastatakse kindlate reeglite järgi, seotakse üheselt isiku, seadme või rolliga, võetakse kasutuselt maha, kui neid enam ei kasutata, ja neid ei anta hiljem kunagi uuesti teisele omanikule.**

Mille järgi seda näeb: Tunnuste nimetamise reegel, näiteks perekonnanimi koos initsiaaliga või käitise kood koos numbriga, lisaks kasutuselt maha võetud tunnuste ajalugu, mis näitab, et neid ei kasutata uuesti. Väike ettevõte hoiab ühte jooksvat loendit koos väljastamise ja kasutuselt mahavõtmise kuupäevaga. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.5** **Autentimisvahendid nagu paroolid, võtmed, sertifikaadid ja tokenid väljastatakse korrastatud viisil, vahetatakse lekke kahtluse korral ja tühistatakse vajaduse korral. Tarnitud vaikekontod ja tehaseparoolid vahetatakse enne kasutuselevõttu.**

Mille järgi seda näeb: Tokenite ja sertifikaatide väljastusloend koos saaja ja kuupäevaga, tõendid vahetuste ja tühistamiste kohta, lisaks kasutuselevõtu kontrollnimekiri iga seadme kohta, kus punkt tehaseparool vahetatud on allkirjastatud. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.5 RE 1** **Tarkvaraprotsesside autentimisandmeid ei hoita andmekandjal loetava failina, vaid riistvaralises hoidlas, mis takistab salajase osa väljalugemist.**

Mille järgi seda näeb: Kasutatava turvakomponendi tüübitõend, näiteks TPM, turvaelement või HSM, koos konfiguratsiooniväljavõttega, mis tõendab, et võti on salvestatud komponendi sisse. Tüübitõendiks piisab ostukirjest või andmelehest. Nõude täiendus, nõutav alates SL 3, tasemetel SL 1 ja SL 2 ei ole nõutav.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.6** **Traadita pääs süsteemi, näiteks WLAN, raadiokaugjuhtimispuldid või Bluetooth-diagnostika, on kasutatav alles pärast nii kasutaja kui ka seadme tuvastamist ja autentimist ning seda hallatakse teadlikult.**

Mille järgi seda näeb: Kõigi traadita ühenduste loetelu koos otstarbe, leviulatuse ja krüpteerimismeetodiga, pääsupunkti konfiguratsiooniväljavõte ja lubatud lõppseadmete loend. Väike ettevõte dokumenteerib lisaks, millised seadmete traadita liidesed on teadlikult välja lülitatud. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.6 RE 1** **Iga traadita pääs on omistatav ühele kindlale kasutajale või ühele kindlale seadmele, kõigile osalistele ühine võrguvõti ei ole piisav.**

Mille järgi seda näeb: Tõend isiklike autentimisandmetega meetodi kohta, näiteks ettevõtte WLAN-autentimine kataloogi vastu või seadmepõhised sertifikaadid, lisaks ühenduslogi, kus on näha isiklik tunnus. Nõude täiendus, nõutav alates SL 2 ega kehti seetõttu tasemel SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.7** **Kõikjal, kus kasutatakse paroole, on nende minimaalne tugevus seadistatav, näiteks minimaalne pikkus ja nõutavad märgitüübid, ning seadistatud väärtused jõustuvad kõigi asjaomaste kontode jaoks.**

Mille järgi seda näeb: Parooli poliitika konfiguratsiooniväljavõte süsteemide kaupa koos tegelikult seatud väärtustega, näiteks pikkus >= 10 märki ja vähemalt kolm märgitüüpi, lisaks loend süsteemidest, mis seda seadistust tehniliselt ei toeta, koos nende kompenseeriva meetmega. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.7 RE 1** **Inimkasutajate puhul reguleerivad täiendavad reeglid parooli loomist ja eluiga: varasemate paroolide taaskasutamine on tõkestatud ja kehtivus on ajaliselt piiratud.**

Mille järgi seda näeb: Konfiguratsiooniväljavõte, kus on näha parooliajalugu, näiteks viie viimase parooli taaskasutamine on tõkestatud, ja seadistatud maksimaalne kehtivus. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.7 RE 2** **Parooli eluea piirang kehtib mitte ainult inimestele, vaid kõigile kontodele, sealhulgas teenuse-, hooldus- ja seadmekontodele.**

Mille järgi seda näeb: Tehniliste kontode vahetusplaan koos viimase ja järgmise vahetuskuupäevaga konto kohta, lisaks tõendid vahetuste kohta, näiteks muudatuse kirje või pilet. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.8** **Kus kasutatakse sertifikaate, pärinevad need korrastatud sertifikaadihaldusest, millel on määratletud reeglid taotlemiseks, väljastamiseks, kehtivusajaks, uuendamiseks ja tühistamiseks.** Dokument

Mille järgi seda näeb: Sertifikaadipoliitika või lühike kirjalik reegel, milles on toodud vastutus, kehtivusajad ja tühistamise tee, lisaks väljastatud sertifikaatide loetelu koos aegumiskuupäevadega. Väike ettevõte hoiab tabelit, kus on sertifikaat, seade, aegumiskuupäev ja meeldetuletuse kuupäev, mis hoiab ära aegunud sertifikaatidest põhjustatud märkamatud käitise seisakud. Nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.9** **Kui autentimiseks kasutatakse võtmepaare, valideerib süsteem sertifikaadi täielikult: usaldusahel, kehtivusaeg, tühistamise olek ja tõend, et vastaspool tegelikult omab privaatvõtit. Seos sertifikaadi ja konto vahel on üheselt määratud.**

Mille järgi seda näeb: Konfiguratsiooniväljavõte sisselülitatud tühistuskontrolliga, näiteks CRL või OCSP, testikirje tagasi lükatud sisselogimisest aegunud või tühistatud sertifikaadiga, lisaks sertifikaadi ja konto vastavustabel. Nõutav alates SL 3, tasemetel SL 1 ja SL 2 ei ole nõutav.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.9 RE 1** **Privaatvõtmed asuvad ainult riistvaralises hoidlas, kust neid ei saa välja lugeda, ja neid kasutatakse samuti selle hoidla sees.**

Mille järgi seda näeb: Kasutatava turvakomponendi andmeleht või sertifitseerimise tõend ja konfiguratsiooniväljavõte, mis näitab, et võti luuakse komponendi sees, nii et privaatvõti ei lahku sellest kunagi. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.10** **Sisselogimise ajal ei avalda süsteem teavet, mida saaks ära kasutada. Sisestatud paroolid on varjatud ja veateated ei avalda, kas vale oli tunnus või parool.**

Mille järgi seda näeb: Sisselogimisekraani kuvatõmmis varjatud sisestusega ja veateate kuvatõmmis pärast ebaõnnestunud katset. Seadmete puhul, mis seda tehniliselt ei suuda, näiteks vanemad operaatoripaneelid, lisandub lühike märkus kompenseeriva meetme kohta, näiteks piiratud füüsiline pääs paigalduskohta. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.11** **Järjestikuste ebaõnnestunud sisselogimiskatsete arv on piiratud ja reaktsioon sellele on seadistatav, näiteks ajutine lukustus. Valitud reaktsioon ei takista käitise ohutusega seotud käitamist.**

Mille järgi seda näeb: Konfiguratsiooniväljavõte koos lävendiga, näiteks lukustus pärast <= 5 ebaõnnestunud katset, ja lukustuse kestus, lisaks lühike hinnang selle kohta, miks lukustus ei takista hädakäitamist ega käitise ohutut seiskamist. Ohutusfunktsiooniga operaatorikohtadel on ajaliselt piiratud lukustus eelistatavam püsivale konto lukustusele. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.12** **Enne sisselogimist on võimalik kuvada kasutusteade, mis osutab süsteemi kasutamise ja seire reeglitele. Teksti ja kuvamist saab vara omanik seadistada.**

Mille järgi seda näeb: Kuvatava teate teksti kuvatõmmis ja kinnitatud sõnastus koos kinnitamise kuupäevaga. Väikesed ettevõtted lepivad sõnastuse lühidalt kokku töötajate esindusega või juhtkonnaga, ühest lõigust piisab. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.13** **Pääs mitteusaldusväärsetest võrkudest, näiteks tarnijate kaughooldus, on piiratud määratletud teedega, seda seiratakse ja see on igal ajal katkestatav.**

Mille järgi seda näeb: Kaugpääsu teede loetelu koos otstarbe, kaugosapoole, kontaktisiku ja kasutatava teega, lisaks ühenduslogid ja tõend katkestamise võimaluse kohta, näiteks võtmelüliti, tulemüürireegel või väljalülitatav kaughooldusmarsruuter. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 1.13 RE 1** **Iga üksikut seanssi mitteusaldusväärsest võrgust kooskõlastab vastutav isik selgesõnaliselt enne ühenduse loomist, püsivalt avatud ühendus ei ole piisav.**

Mille järgi seda näeb: Kooskõlastuse kirjed iga kaughooldusseansi kohta koos aja, põhjuse, kooskõlastava isiku ja kestusega, tehniliselt näiteks võtmelüliti kaudu pääsumarsruuteril või kooskõlastusportaali kaudu. Väikeses ettevõttes piisab juhtkapi juures asuvast kaughoolduse päevikust, mille hooldustehnik iga seansi kohta allkirjastab. Nõude täiendus, nõutav alates SL 2 ega kehti seetõttu kunagi tasemel SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 6 FR 2: Kasutuse ohjamine (õigused, seansid, auditikirjed) 24

**SR 2.1** **Süsteem jõustab antud õigused tehniliselt: iga sisselogitud isik, iga seade ja iga tarkvaraprotsess saab täpselt talle määratud pääsu ning iga sellest kaugemale ulatuv katse lükatakse tagasi.**

Mille järgi seda näeb: Õiguste kontseptsioon, mis seob kontod lubadega, lisaks kuvatõmmis või konfiguratsiooniväljavõte iga juhtimissüsteemi, HMI ja inseneritööjaama kohta, kus on näha kehtivad õigused. Lisaks testikirje, kus väheste õigustega konto üritab tõkestatud toimingut ja lükatakse tagasi. Nõutav alates SL 1. Väike ettevõte saab hakkama kahe või kolme rolliga, näiteks käitamine, hooldus, inseneritöö, ja dokumenteerib need ühel leheküljel.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.1 RE 1** **Õiguste jõustamine kehtib mitte ainult inimoperaatoritele, vaid samavõrra tarkvaraprotsessidele ja seadmetele, mis pääsevad süsteemi iseseisvalt.**

Mille järgi seda näeb: Tehniliste ja teenusekontode loend, näiteks OPC UA kliendid, ajaloobaasi ühendused, varunduse teenused, igaüks koos talle määratud õiguste komplektiga. Väljavõte õiguste haldusest, mis näitab, et need kontod ei tööta administraatori õigustega. Nõude täiendus, nõutav alates SL 2, tasemel SL 1 mitte.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.1 RE 2** **Õigusi ei anta üksikisikutele ükshaaval, vaid rollide kaudu, ja rolli seos lubatud toimingutega on jälgitaval kujul kirjas.** Dokument

Mille järgi seda näeb: Rollide ja õiguste maatriks tabelina: read on rollid, veerud toimingud nagu seadeväärtuse muutmine, programmi allalaadimine, alarmi kviteerimine, konto loomine. Lisaks loend, mis seob isiku rolliga. Nõude täiendus, nõutav alates SL 2. Tõendiks piisab täiesti ajakohasena hoitud arvutustabelist, millel on muutmise kuupäev.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.1 RE 3** **Kitsalt määratletud erijuhtudel saab volitatud järelevaataja õiguste piirangu piiratud ajaks tühistada ja iga selline erandkorras tühistamine on auditijäljes kirjas.**

Mille järgi seda näeb: Erandi kooskõlastamise korra kirjeldus, milles on toodud, kes seda anda võib ja kui kaua see kehtib, lisaks auditikirjed juba antud eranditest süsteemi logist. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.1 RE 4** **Eriti kriitilised sekkumised vajavad enne toimingu tegemist kahe sõltumatu volitatud isiku kooskõlastust.**

Mille järgi seda näeb: Kahekordset kooskõlastust nõudvate toimingute loend, näiteks ohutusparameetrite muutmine või uue juhtimisprogrammi allalaadimine, koos konfiguratsioonitõendi ja auditikirjetega, kus on nimetatud mõlemad kooskõlastajad. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.2** **Traadita ühenduste kasutamine automaatikavõrgus on seotud selgesõnalise volitusega ja ainult heakskiidetud osalised tohivad õhu kaudu andmeid vahetada või sekkuda.**

Mille järgi seda näeb: Kõigi traadita ühenduste loetelu, näiteks WLAN-pääsupunktid, Bluetooth-seosed, mobiilsidemarsruuterid, igaüks koos otstarbe ja heakskiidetud osalistega. Lisaks pääsu ohjamise konfiguratsioon pääsupunktis. Nõutav alates SL 1. Kes protsessivõrgus ühtegi traadita ühendust ei käita, märgib täpselt seda kirjalikult ja toetab seda konfiguratsioonivaatega, kus traadita side on välja lülitatud.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.2 RE 1** **Volitamata traadita seadmed automaatikavõrgu läheduses tuvastatakse ja neist teatatakse.**

Mille järgi seda näeb: Traadita side seire kirje või korduv traadita side skaneering koos kuupäeva, tulemuste loendi ja märkusega iga tundmatu seadme kohta. Teavitustee vastutava üksuseni on nimetatud. Nõude täiendus, nõutav alates SL 2, tasemel SL 1 mitte. Väike ettevõte saab teha kvartaalse skaneeringu sülearvutiga ja lisada tulemuse kirjena toimikusse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.3** **Kaasaskantavate ja mobiilsete seadmete kasutamine süsteemis, näiteks hooldussülearvutid, USB-andmekandjad või tahvelarvutid, on reeglitega korraldatud ja tehniliselt piiratud selgesõnaliselt heakskiidetud seadmetega.**

Mille järgi seda näeb: Seadmete kasutamise reeglistik, heakskiidetud hooldusseadmete loend koos nende tunnustega ja tõend tehnilise piirangu kohta, näiteks HMI ja inseneritööjaama USB-pesad välja lülitatud või piiratud kindlate seadmetega. Nõutav alates SL 1. Väike ettevõte kasutab kahte märgistatud hooldusmälupulka, millele kirjutatakse ainult ühes üleandmisjaamas.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.3 RE 1** **Enne ühendamist on kaasaskantava või mobiilse seadme turvaseisund kontrollitud ja nõuetele mittevastavad seadmed ei saa pääsu.**

Mille järgi seda näeb: Seadme seisundi kontrollikriteeriumid, näiteks ajakohane pahavaratõrje ja paikade tase, lisaks kontrollikirjed iga hooldusseadme kohta ja tõend tehnilise jõustamise kohta, näiteks üleandmisjaama või võrgupääsu ohjamise kaudu. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.4** **Süsteemis käivitatava mobiilse koodi kohta, näiteks skriptid operaatoriliidestes või aktiivne sisu aruannetes, on määratletud, millised tüübid on lubatud, ja lubamatud tüübid ei pääse käivituma.** Dokument

Mille järgi seda näeb: Määratlus, milline mobiilne kood on millistes süsteemides lubatud, lisaks konfiguratsioonitõend piirangu kohta, näiteks skriptide käivitamine HMI-brauseris välja lülitatud, makrod hindamisfailides tõkestatud. Nõutav alates SL 1. Piisab ühe lehekülje pikkusest määratlusest, mis katab kolm või neli tegelikult esinevat juhtu.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.4 RE 1** **Enne mobiilse koodi käivitamist on tõendatud, et see pärineb oodatud allikast ja seda ei ole muudetud.**

Mille järgi seda näeb: Konfiguratsioonitõend allkirja kontrollimise või kontrollsumma kontrolli kohta, lisaks testikirje, kus muudetud või allkirjastamata kood lükatakse tagasi. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.5** **Seanss lukustub pärast määratletud aega ilma operaatori tegevuseta ja vabaneb uuesti alles pärast korduvat autentimist, ilma et kaoks ohutuse seisukohalt oluliste protsessiandmete kuva.**

Mille järgi seda näeb: Konfiguratsiooniväljavõte koos seadistatud lukustusajaga iga tööjaama kohta, lisaks põhjendus tööjaamade kohta pidevalt mehitatud juhtimisruumides, kus lukustus on teadlikult teisiti seatud. Nõutav alates SL 1. Visuaalne tõend: lukustusekraani kuvatõmmis, kus alarmirida on endiselt nähtav.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.6** **Kaugseansid lõpetatakse pärast määratletud tegevusetut aega või operaatori nõudmisel, nii et ükski avatud kaugühendus ei jää järelevalveta.**

Mille järgi seda näeb: Kaugpääsu konfiguratsioon koos tegevusetuse ajapiiranguga, auditikirjed lõpetatud kaugseanssidest ja kirjeldus, kuidas operaator saab käimasoleva kaughooldusseansi kohe katkestada, näiteks võtmelüliti või seansipõhise vabastuse kaudu. Nõutav alates SL 2, tasemel SL 1 mitte.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.7** **Samaaegsete seansside arv konto või rolli kohta on piiratud ja seda piiri ületavad sisselogimiskatsed lükatakse tagasi.**

Mille järgi seda näeb: Konfiguratsiooniväljavõte koos määratletud ülempiiriga rolli kohta, näiteks <= 1 samaaegne seanss inseneritöö kontode puhul, lisaks testikirje tagasi lükatud teisest sisselogimiskatsest. Nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.8** **Turvalisuse seisukohalt olulised sündmused registreeritakse ja iga kanne nimetab vähemalt aja, allika, käivitanud konto, sündmuse liigi ja tulemuse.** Dokument

Mille järgi seda näeb: Registreeritavate sündmuseliikide määratlus, näiteks sisselogimine, ebaõnnestunud sisselogimine, õiguste muutmine, programmi muutmine, konfiguratsiooni muutmine, lisaks tegelik väljavõte auditilogist, kus nimetatud väljad on näha. Nõutav alates SL 1. Väike ettevõte kogub juhtimissüsteemi, HMI ja tulemüüri logid ühte kausta koos kindla säilitusajaga.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.8 RE 1** **Üksikute komponentide auditikirjed koondatakse keskselt kokku ja moodustavad ühtse, kogu süsteemi hõlmava kirje, mida saab tervikuna hinnata.**

Mille järgi seda näeb: Logikogumise arhitektuuri visand, kus on näha kõik ühendatud allikad, lisaks hindamine, mis paigutab vähemalt kahe komponendi sündmused ühele ajateljele. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.9** **Auditikirjete jaoks on ette nähtud piisav salvestusruum, nii et sündmused säilitatakse määratletud säilitusaja jooksul ja neid ei kirjutata tahtmatult üle.**

Mille järgi seda näeb: Salvestusvajaduse arvutus või hinnang päevase logimahu ja säilitusaja korrutisena, lisaks seadistatud salvestusruumi suurus ja arhiveerimisreegel. Nõutav alates SL 1. Praktikas piisab igapäevasest koopiast eraldi salvestuskohta koos dokumenteeritud säilitusajaga.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.9 RE 1** **Auditihoidla määratletud täituvuse lävendi saavutamisel antakse vastutavale üksusele hoiatus enne, kui salvestusmaht on täielikult ära kasutatud.**

Mille järgi seda näeb: Lävendi konfiguratsiooniväljavõte, näiteks hoiatus alates >= 80 protsendi täituvusest, lisaks näide käivitunud teatest ja saajate loend. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.10** **Kui auditilogimine tõrgub või auditihoidla saab täis, reageerib süsteem eelnevalt määratletud viisil ja vastutavat üksust teavitatakse, ilma et see ohustaks käitise ohutut käitamist.**

Mille järgi seda näeb: Määratletud reaktsioon iga tõrkejuhu kohta, näiteks vanemate kannete ülekirjutamine ja teate saatmine käitise seiskamise asemel, koos protsessist lähtuva põhjendusega. Tõendiks on käivitatud testteade ja vastav auditikanne. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.11** **Iga auditikirje kannab nimetatud ajaallikast pärinevat ajatemplit, nii et eri komponentide sündmused on üksteise suhtes järjestatavad.**

Mille järgi seda näeb: Ülevaade sellest, millist ajaallikat iga komponent kasutab, ja logiväljavõte nähtava ajatempliga, sealhulgas ajavöönd. Nõutav alates SL 2, tasemel SL 1 mitte.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.11 RE 1** **Kõigi osalevate komponentide kellad on sünkroniseeritud ühise ajaallikaga, nii et hälve püsib määratletud piirides.**

Mille järgi seda näeb: Ajasünkroniseerimise konfiguratsioon, näiteks NTP-server ja sünkroniseerimise sagedus, lisaks kontrollikirje mõõdetud hälbega komponendi kohta võrreldes määratletud piiriga, näiteks <= 1 sekund. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.11 RE 2** **Ajaallikas ise on kaitstud manipuleerimise vastu ning ebausutav või muudetud ajaviide tuvastatakse ja sellest teatatakse.**

Mille järgi seda näeb: Kirjeldus, kuidas ajaallikas on kaitstud, näiteks autenditud ajasünkroniseerimine, piiramine sisemise allikaga, ajahüpete seire, lisaks teated või auditikirjed tuvastatud hälbest. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.12** **Määratletud kriitiliste toimingute puhul on tagantjärele kahtluseta tuvastatav, kes need käivitas, nii et tegutsenud isik ei saa seda usutavalt eitada.** Dokument

Mille järgi seda näeb: Loend toimingutest, mille kohta see tõend kehtib, näiteks retsepti muutmine, partii vabastamine, piirväärtuste muutmine, lisaks vastavad kirjed kordumatu isikutunnusega ja tõend, et rühmakontod on nende toimingute puhul välistatud. Nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 2.12 RE 1** **Tegutsenud isiku eitamatu omistamine kehtib mitte ainult valitud kriitilistele toimingutele, vaid kõigile kasutajatele ja kõigile nende käivitatud toimingutele.**

Mille järgi seda näeb: Tõend, et iga konto on seotud ühe isikuga ja jagatud sisselogimisi ei ole alles, lisaks logiväljavõte suvalistest toimingutest, kus kordumatu isikutunnus esineb läbivalt. Nõude täiendus, nõutav alles alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 7 FR 3: Süsteemi terviklus, andmete, tarkvara ja seansside kaitse volitamata muutmise eest 19

**SR 3.1** **Juhtimissüsteem tuvastab, kui teavet on sidekanalis edastamise ajal muudetud, ja teeb seda ühtviisi juhtimisandmete, konfiguratsiooniandmete ja haldusliikluse puhul. Kaitse hõlmab ka ühendusi, mis lahkuvad süsteemist või läbivad mitteusaldusväärseid võrgusegmente.**

Mille järgi seda näeb: Võrgu ja protokollide ülevaade, milles on toodud, milline kanal kasutab millist terviklusmehhanismi (kontrollsumma, sõnumi autentimiskood, allkirjastatud telegrammid), tööstussiini või OPC UA turvaseadistuste konfiguratsiooniväljavõte ja testikirje, mis näitab, et rikutud telegramm lükati tõendatavalt tagasi. Väike ettevõte koondab selle tabelisse iga ühenduse kohta veergudega allikas, sihtkoht, protokoll ja terviklusmehhanism ning tõendab tulemuslikkust ühe korra liiklussalvestusega. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.1 RE 1** **Terviklusekaitse edastamise ajal tugineb krüptograafilistele mehhanismidele, nii et ründaja tahtlik omavahenditega tehtud manipuleerimine ei saa märkamatult läbi minna. Lihtsast kontrollsummast edastusvigade vastu siin ei piisa.**

Mille järgi seda näeb: Kanali kaupa kasutatavate krüptograafiliste mehhanismide ja võtmepikkuste loend, viide aluseks olevale võtmehaldusele ja konfiguratsiooniväljavõtted (näiteks TLS-šifrikomplektid, OPC UA SecurityPolicy, IPsec-profiilid). Väikesed ettevõtted tuginevad oma kontrollerite turvalistele vaikeprofiilidele ja lisavad toimikusse kehtiva seadistuse kuvatõmmise. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.2** **Pahatahtliku koodi vastased kaitsemehhanismid on olemas, need takistavad soovimatu programmikoodi käivitumist süsteemi komponentides ja teatavad igast tuvastusest. Mehhanismid on valitud nii, et need ei häiri käitise ettenähtud tööd, ja neid hoitakse ajakohasena.**

Mille järgi seda näeb: Ülevaade komponentide kaupa, milline mehhanism kehtib (viirusetõrje, rakenduste lubaloend, turvakarastatud operatsioonisüsteem ilma käivitusõigusteta), tõend, et signatuure või lubaloendeid uuendatakse, ja kaitsesüsteemi hoiatused. Kus viirusetõrje ei ole teostatav, näiteks kontrolleril, on kompenseeriv meede koos põhjendusega kirja pandud. Väikesed ettevõtted saavad hästi hakkama lubaloendiga operaatori arvutil ja kirjaliku reegliga USB-andmekandjate kohta. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.2 RE 1** **Pahatahtliku koodi vastane kaitse toimib lisaks käitise sisse- ja väljapääsupunktides, kus andmed sisenevad või väljuvad, mitte ainult lõppseadmetes endis.**

Mille järgi seda näeb: Kõigi sisse- ja väljapääsupunktide loend (kaughoolduse pääs, andmeedastuse lüüs, irdkandjad, üleandmine kontorivõrku, programmiversioonide e-posti tee) koos igas punktis toimiva skaneerimismehhanismiga, lisaks kirjed kontrollitud üleandmiste kohta. Väikesed ettevõtted seavad lüüsina üles ühe viirusekontrolliga üleandmisarvuti ja fikseerivad selle tööjuhendis. Nõude täiendus, nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.2 RE 2** **Pahatahtliku koodi vastaseid kaitsemehhanisme hallatakse keskselt ühest kohast, uuendusi jaotatakse keskselt ja tuvastused kogutakse hindamiseks ühte kohta.**

Mille järgi seda näeb: Keskse halduskonsooli konfiguratsioon, aruanne kõigi ühendatud komponentide uuenduste oleku kohta ja teatatud tuvastuste hindamine teatava ajavahemiku jooksul. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.3** **Süsteemi turvafunktsioone tõendatakse kavandatud sagedusega ja pärast muudatusi, et kinnitada nende tegelikku toimimist. Testid on ajastatud nii, et need ei ohusta käitise tööd, ja tulemused registreeritakse.** Dokument

Mille järgi seda näeb: Testiplaan, milles on toodud testitav objekt, sagedus ja ajaaken, koos testikirjetega, kus on näha kuupäev, testija, oodatud käitumine ja täheldatud käitumine. Kasulikud üksiktestid on: sisselogimine väljalülitatud kontoga ebaõnnestub, viirusetõrje reageerib testfailile, kaughoolduse pääs ei ole ilma vabastuseta kättesaadav. Väikesed ettevõtted seovad testimise niikuinii kavandatud hooldusseisakuga ja töötavad läbi kindla kontrollnimekirja. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.3 RE 1** **Turvafunktsioonide tõendamine toimub automatiseeritud vahenditega, nii et see on korratav ilma käsitsi tehtava tööta ja annab ühtlase tulemuse.**

Mille järgi seda näeb: Skriptid või testivahendid koos nende ajakavaga, nende väljundfailid ja mitme käivituse võrdlus, mis näitab, et hälbed tuvastatakse. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.3 RE 2** **Turvafunktsioonide tõendamine on võimalik ka tavakäitamise ajal, ilma käitist seiskamata või erilisse olekusse viimata.**

Mille järgi seda näeb: Testikorra kirjeldus koos tõendiga, et sellel ei ole protsessile kahjulikku mõju, näiteks analüüs mõjust tsükliaegadele ja võrgukoormusele, lisaks tootmiskäitamisest võetud testikirjed. Nõude täiendus, nõutav alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.4** **Volitamata muudatused tarkvaras, püsivaras ja salvestatud teabes tuvastatakse. See kehtib ühtviisi juhtimisprogrammide, parameetrikomplektide, retseptide ja konfiguratsioonifailide kohta.**

Mille järgi seda näeb: Kaitset väärivate versioonide loetelu koos salvestatud kontrollväärtuste või allkirjadega, tervikluse võrdluste tulemused ja dokumenteeritud võrdlus versioonihalduses hoitava versiooniga. Väikesed ettevõtted hoiavad vabastatud programmiversiooni koos kontrollsummaga kirjutuskaitstud kohas ja võrdlevad kahtluse korral või pärast hooldust. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.4 RE 1** **Kui tuvastatakse tarkvara või teabe tervikluse rikkumine, teatab süsteem sellest automaatselt vastutavale kohale ja aktiivne otsimine ei ole selleks vajalik.**

Mille järgi seda näeb: Teavitusteede konfiguratsioon (alarm juhtimisruumis, e-post, teade seiresüsteemile), saajate loend koos asendamise korraldusega ja vähemalt üks testalarm koos dokumenteeritud reageerimisajaga. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.5** **Sisendeid, mida süsteem võtab vastu protsessiandmetest, liidestest või kasutajaliidestest, kontrollitakse enne töötlemist lubatud süntaksi, lubatud väärtusvahemiku ja lubatud pikkuse suhtes. Vigased sisendid ei põhjusta ohjamatut käitumist.**

Mille järgi seda näeb: Piiride ja vormingute spetsifikatsioon iga sisendi kohta, väljavõtted kontrolleris või rakenduses olevast valideerimisloogikast ja testijuhtumid tahtlikult vigaste sisenditega (liiga suur väärtus, vale andmetüüp, ülipikk märgijada) koos süsteemi dokumenteeritud käitumisega. Väikesed ettevõtted panevad usutavuse piirid iga mõõtepunkti kohta tabelisse ja tõendavad need kasutuselevõtu ajal. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.6** **Tõrke puhuks on määratletud, millisesse olekusse käitise väljundid lähevad, ja süsteem läheb täpselt sellesse olekusse. Määratletud olek on kooskõlas käitise funktsionaalse ohutusega.**

Mille järgi seda näeb: Määratlus iga väljundi või väljundirühma kohta (väärtuse hoidmine, määratletud asendusväärtus, ohutu seiskamise olek) koos riskihindamisest tuleneva põhjendusega, kontrolleri konfiguratsiooniväljavõte ja tõend tõrketestist, näiteks kaablikatkestus või side kadu, mis näitab oodatud käitumist. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.7** **Süsteem käsitleb veaolukordi nii, et käitamine jääb ohje alla ja ei avaldata teavet, mis ründajat aitaks. Operaatoritele kuvatavad veateated jäävad lühikeseks, tehnilised üksikasjad lähevad ainult sisemistesse kirjetesse.**

Mille järgi seda näeb: Veaklasside ülevaade koos igaühe jaoks ettenähtud süsteemi käitumisega, näited kuvatavatest teadetest võrdluses vastavate sisemiste logikannetega ja testitõend, et operaatoriliidesele ei ilmu failiteid, kontonimesid, andmebaasi väljundit ega versiooniandmeid. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.8** **Aktiivsed seansid on kaitstud ülevõtmise ja võõraste sõnumite sisestamise vastu. Seanss lõpeb pärast väljalogimist või pärast määratletud tegevusetut aega ja pärast seda ei ole see uuesti kasutatav.**

Mille järgi seda näeb: Seansihalduse konfiguratsioon koos seadistatud piiridega tegevusetuse ajale ja maksimaalsele kestusele, tõend sõnumite kordusesituse vastase mehhanismi kohta ja testikirje, kus salvestatud seanss pärast väljalogimist enam ei toimi. Nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.8 RE 1** **Seansitunnused kaotavad seansi lõppedes kehtivuse ja süsteem ei võta neid uuesti vastu, ka siis mitte, kui neid väljastpoolt uuesti esitatakse.**

Mille järgi seda näeb: Seansihalduse konfiguratsiooniväljavõte, mis hõlmab kehtetuks muutmist, lisaks testikirje, kus varem kehtinud tunnus saadetakse pärast väljalogimist uuesti ja süsteem lükkab selle tagasi. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.8 RE 2** **Iga uue seansi jaoks luuakse eraldi ühekordselt kasutatav tunnus. Tunnuseid ei kasutata uuesti üle seansside, kasutajate ega seadmete.**

Mille järgi seda näeb: Loomiskorra kirjeldus ja tõend logist või liiklussalvestusest, et mitu järjestikust sisselogimist saavad erinevad tunnused. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.8 RE 3** **Seansitunnused luuakse tunnustatud juhuslikkuse mehhanismidega, nii et neid ei saa ära arvata ega tuletada eelnevatest tunnustest.**

Mille järgi seda näeb: Ülevaade kasutatavast juhuarvugeneraatorist ja selle entroopiaallikast, tarnija kinnitus või katsearuanne selle kohta ja loodud tunnuste valimi statistiline hindamine. Nõude täiendus, nõutav alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.9** **Turvalisusega seotud kirjed ja nende hindamiseks kasutatavad vahendid on kaitstud volitamata pääsu, muutmise ja kustutamise eest. Kirjeid muuta või eemaldada tohtivate inimeste ring on kitsas ja nimeliselt teada.** Dokument

Mille järgi seda näeb: Logiandmete õiguste kontseptsioon koos nimelise määramisega, eraldi logimissüsteemi edastamise konfiguratsioon, säilitusajad ja testitõend, et tavaoperaator ei saa kandeid kustutada. Väikesed ettevõtted edastavad logid eraldi seadmesse, kuhu käitise operaatoritel ei ole kirjutusõigust. Nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 3.9 RE 1** **Turvalisusega seotud kirjeid hoitakse lisaks andmekandjal, mis välistab hilisema ülekirjutamise, nii et kord kirjutatud kannet ei saa enam muuta, ka mitte administraatori õigustega.** Dokument

Mille järgi seda näeb: Kasutatava hoidla kirjeldus (ühekordselt kirjutatav andmekandja, muutmiskindel arhiiv, pidevalt pikenev allkirjaahel), tõend ebaõnnestunud katsest kannet muuta ja reegel, kuidas andmekandjaid säilitatakse ja välja otsitakse. Nõude täiendus, nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 8 FR 4: Andmete konfidentsiaalsus 6

**SR 4.1** **Automaatikasüsteem kaitseb konfidentsiaalset teavet volitamata avaldamise eest nii edastamise ajal kui ka salvestatuna. On määratletud, millised andmed loetakse konfidentsiaalseks, näiteks retseptid, parameetrikomplektid, autentimisandmed, konfiguratsioonifailid või isikuga seostatavad diagnostikaandmed.** Dokument

Mille järgi seda näeb: Kaitset väärivate andmetüüpide loend koos märkega, kus neid hoitakse ja kuidas neid edastatakse, lisaks iga kirje konkreetne kaitsemeede, näiteks krüpteeritud ühendus, krüpteeritud andmekandja või piiratud jagatud kaust. Väike ettevõte saab hakkama ühe lehekülje pikkuse tabeliga: andmetüüp, kus see asub, kes seda näha tohib, mis seda kaitseb. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 4.1 RE 1** **Teabe puhul, mis liigub mitteusaldusväärsete võrkude kaudu või on salvestatud väljaspool kaitstud keskkonda, tagatakse konfidentsiaalsus tehniliste vahenditega, mitte pelgalt korralduslikus reeglis lubatuna.**

Mille järgi seda näeb: Kasutatava transpordikrüpteerimise või salvestuskrüpteerimise konfiguratsiooniväljavõte, näiteks kaughoolduse VPN-profiil, juhtimissüsteemi liidese TLS-seadistused või varukoopia andmekandjate krüpteerimine. Tõendiks piisab kehtiva seadistuse kuupäevastatud kuvatõmmisest. Nõutav alates SL 2, mitte alates SL 1, sest tegemist on nõude täiendusega.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 4.1 RE 2** **Konfidentsiaalsus tagatakse ka tsoonide vahelistel piiridel, nii et teave ei muutu avatekstina nähtavaks, kui see liigub ühest tsoonist teise.**

Mille järgi seda näeb: Tsoonide ja ühendusteede plaan, kus on märgitud, millised ületused on krüpteeritud, koos piirikomponendi konfiguratsiooniga, nagu lüüs, tulemüür või andmediood. Liiklussalvestus või testikirje, mis näitab, et piiril ei ilmu avatekstis andmeid. Nõutav alates SL 4.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 4.2** **On määratletud, kuidas konfidentsiaalne teave usaldusväärselt eemaldatakse, kui seadmed kasutuselt kõrvaldatakse, omanikku vahetavad, remonti lähevad või uuesti kasutusele võetakse, nii et loetavaid jääkandmeid ei jää alles.** Dokument

Mille järgi seda näeb: Kirjalik kasutuselt kõrvaldamise kord koos puhastusmeetodiga iga seadmetüübi kohta, lisaks kustutamise kirjed, kus on seadme tunnus, kuupäev ja teostanud isik. Väike ettevõte kirjutab selle ühise loendi ühele reale seadme kohta ja lisab kõrvale väliste jäätmekäitlejate tõendid. Nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 4.2 RE 1** **Jagatud salvestusalad puhastatakse enne, kui need eraldatakse uuesti teisele kasutajale või protsessile, nii et eelmise kasutaja sisu ei ole väljaloetav.**

Mille järgi seda näeb: Tarnija kinnitus või konfiguratsioonikirje, mis katab taaskasutatavate mälu- ja puhvrialade puhastamise, täiendatuna vastuvõtukatsetest või hooldusest pärineva testikirjega. Kus komponent seda ei suuda, on tõendiks dokumenteeritud kompenseeriv meede, näiteks seadme mittejagamine eri rollide vahel. Nõutav alates SL 3, mitte alates SL 1, sest tegemist on nõude täiendusega.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 4.3** **Kõikjal, kus kasutatakse krüptograafiat, järgivad algoritmid, võtmepikkused ja võtmete käsitsemine tunnustatud head tava ning on määratletud, kuidas võtmeid luuakse, jaotatakse, hoitakse, vahetatakse ja tühistatakse.** Dokument

Mille järgi seda näeb: Ülevaade süsteemide kaupa kasutatavatest mehhanismidest koos algoritmi, võtmepikkuse ja kehtivusajaga, lisaks võtmehalduse reeglid ning kirjed võtmevahetuste ja sertifikaatide uuendamiste kohta. Mõõdupuuks on avalikud soovitused, näiteks Saksamaa BSI tehnilised juhised. Väike ettevõte hoiab sertifikaatide loendit koos aegumiskuupäevade ja meeldetuletusega >= 30 päeva enne aegumist. Nõutav alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 9 FR 5: Piiratud andmevoog, tsoonid ja ühendusteed 11

**SR 5.1** **Juhtimissüsteem on jaotatav eraldi tsoonideks ja liiklus nende tsoonide vahel läbib ainult määratletud ühendusteid. Jaotus järgib selgitatavat põhjendust, näiteks kaitsevajadust, omandit või asjaomaste käitiseosade funktsiooni.** Dokument

Mille järgi seda näeb: Võrguskeem, kus on näha tsoonid ja nendevahelised ühendusteed, tsoonide loend koos iga piiri põhjendusega ja eraldavate komponentide konfiguratsioon, nagu VLAN-määratlused või tulemüüri liidesed. Väike ettevõte saab hakkama ühe lehekülje visandiga, kus kontor, masinavõrk ja kaugpääs on kolm kasti koos nendevaheliste ühendustega, lisaks kommutaatori VLAN-konfiguratsiooni kuvatõmmis.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.1 RE 1** **Tsoonide eraldamine on teostatud füüsiliselt, see tähendab eraldi võrgukomponentide ja eraldi kaabelduse abil, ega tugine ainuüksi loogilisele konfiguratsioonile jagatud seadmetes. Käesoleva loendi punkt 9.1, nõutav alates SL 2. Selle standardi nõude täiendused ei ole kunagi kohustuslikud juba tasemel SL 1.**

Mille järgi seda näeb: Võrgukomponentide loetelu, kus on toodud, milline kommutaator või marsruuter teenindab millist tsooni, fotod või kapi paigutusjoonis eraldatud jaotustest, kaablite märgistus. Väikesed ettevõtted tõendavad seda kahe eraldi selgelt märgistatud kommutaatoriga ühe jagatud seadme asemel ja juhtkapi fotoga käitise dokumentatsioonis.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.1 RE 2** **Automaatikavõrk on käitatav sõltumatult väljaspool automaatikat asuvatest võrkudest. Kui kontori IT või välisühendus tõrgub, jätkub käitise juhtimine ja seire. Nõutav alates SL 3.**

Mille järgi seda näeb: Automaatikavõrgus kasutatavate teenuste sõltuvusloend, nagu ajaserver, nimelahendus, kataloogiteenus või litsentsiserver, koos märkega, kus igaüht majutatakse, ning testikirje lahutamise katsest, kus ühendus kontori IT-ga eemaldati. Väike ettevõte märgib sellise katse tulemuse hoolduspäevikusse: ülesvooluühendus eemaldatud, käitis jätkas tööd, puudu olid ainult kontori aruanded.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.1 RE 3** **Eriti kriitilisi funktsioone kandvad tsoonid, näiteks ohutus- või kaitsefunktsioonid, on ülejäänud tsoonidest eraldatud nii loogiliselt kui ka füüsiliselt. Nõutav alates SL 4.**

Mille järgi seda näeb: Kriitiliste tsoonide märgistus tsooniskeemil koos liigituse põhjendusega, tõend nende tsoonide eraldi võrgukomponentide ja eraldi kaabelduse kohta, ühendusteede konfiguratsioon koos tõendiga, et jagatud teed ei ole olemas.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.2** **Tsoonide piiridel liiklust ohjatakse, seiratakse ning lubatakse või keelatakse määratletud reeglite järgi. Kahe tsooni vahel ei ole teed, mis seda kontrollpunkti mööda läheks.**

Mille järgi seda näeb: Tulemüüri või piiriseadme eksporditud reeglistik, logid keelatud ja lubatud ühendustest, tõend, et kõrvalteid ei ole, näiteks käitise arvutites lisavõrgukaartide, modemite või mobiilsidemarsruuterite kontrolli kaudu. Väike ettevõte tõendab seda oma ainsa tulemüüri reeglieksportiga ja lühikese ülevaatuskäigu märkusega, mis kinnitab, et üheski juhtkapis ei ole kavandamata marsruuterit.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.2 RE 1** **Tsoonipiiri reeglistik toimib põhimõttel, et kõik on keelatud, kui seda ei ole selgesõnaliselt lubatud. Iga lubav reegel on eraldi põhjendatud ja otstarbega seotud. Nõutav alates SL 2.**

Mille järgi seda näeb: Reeglistik nähtava lõppreegliga, mis ülejäänu ära viskab, ja lubade loend, kus iga reegli kohta on toodud allikas, sihtkoht, teenus, otstarve ja vastutav isik. Väikesed ettevõtted hoiavad seda loendit viie veeruga tabelina tulemüüri ekspordi kõrval ja vaatavad selle kord aastas üle, et leida reegleid, mida keegi enam ei vaja.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.2 RE 2** **Automaatikavõrk on teadlikult kõigist välisühendustest lahutatav ja saarerežiimis edasi käitatav. Toimingut saab käivitada käitist seiskamata. Nõutav alates SL 3.**

Mille järgi seda näeb: Isoleerimiskorra kirjeldus, milles on toodud, kes seda käivitada tohib ja kuidas, tõend tehnilise teostuse kohta, nagu hädaolukorra reeglistik või märgistatud lahutuslüliti, lisaks õppuse kirje, kus isoleerimine tegelikult läbi tehti. Väike ettevõte teeb õppuse kord aastas hoolduse ajal ja märgib üles kuupäeva, kestuse ja kõik ebatavalise.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.2 RE 3** **Kui tsoonipiiril olev seade tõrgub või kaotab oma reeglid, keelab see liikluse selle edastamise asemel. Tõrge ei jäta järele avatud ühendust. Nõutav alates SL 4.**

Mille järgi seda näeb: Tarnija kinnitus või konfiguratsioonitõend selle kohta, kuidas komponent tõrke ja taaskäivituse korral käitub, testikirje tahtlikult esile kutsutud tõrkest koos täheldatud tulemusega, kooskõlastamine käitise riskihindamisega, sest liiklust keelaval piiril võivad olenevalt protsessist olla omaenda tagajärjed.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.3** **Üldised inimestevahelise suhtluse teenused, nagu e-post, sõnumivahetus või videokõned, on automaatikaseadmetes ja automaatikavõrkudes tõkestatavad. Tõkestuse ulatus on määratletud ja põhjendatud.**

Mille järgi seda näeb: Määratlus, millised teenused ei ole automaatikavõrgus lubatud, lisaks tehniline teostus: tõkestatud pordid ja sihtkohad reeglistikus, operaatorikohtadelt eemaldatud või tõkestatud rakendused, tõend seadmete tarkvaraloetelust. Väike ettevõte lahendab selle rakenduste tõkestusega HMI-tööjaamas ja reegliga, mis keelab masinavõrgust väljuva posti- ja veebiliikluse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.3 RE 1** **Sellised inimestevahelise suhtluse teenused on tõkestatud kogu automaatikavõrgus, mitte üksnes osaliselt piiratud või üksikute seadmetega piirduvad. Nõutav alates SL 2.**

Mille järgi seda näeb: Tõend, et tõkestus kehtib tsooni igas seadmes, näiteks tsooni iga arvuti paigaldatud tarkvara ülevaatuse ja suvalisest käitise arvutist tehtud ühendustesti kaudu. Väikesed ettevõtted tõendavad seda seadmete loendiga, kus iga rida on kontrollikuupäevaga märgitud, ja ebaõnnestunud ühenduskatse kuvatõmmisega.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 5.4** **Rakenduse andmed ja rakenduse funktsioonid on jaotatud nii, et erineva kaitsevajaduse või erinevate õigustega protsessid ei pääse samadesse aladesse. Eraldus on kavandatud süsteemi arhitektuuri sisse ega ole jäetud paigalduse juhuse hooleks.**

Mille järgi seda näeb: Rakenduste ülevaade, kus on toodud, milliseid andmeid ja teenuseid need kasutavad ja millised kontod nende taga on, eraldi eksemplaride, andmebaaside, kataloogide või virtuaalmasinate konfiguratsioon ja õiguste loend iga ala kohta. Väike ettevõte lahendab selle eraldi kasutajakontodega ja eraldi andmekaustadega inseneritöö ja käitamise jaoks, lisaks märkus, milline rakendus millisele kaustale ligi pääseb.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 10 FR 6: Õigeaegne reageerimine sündmustele 3

**SR 6.1** **Süsteemis kogutud auditikirjeid saavad selleks volitatud isikud ja rollid lugeda ja hinnata käitise jooksvat tööd häirimata ning pääs nendele kirjetele on ise piiratud volitatud kasutajatega.**

Mille järgi seda näeb: Rollide ja lubade maatriks, kus on näha, kes tohib logiandmeid vaadata, lisaks tegelikult välja võetud logivaate kuvatõmmis või eksport koos ajatempliga. Lisandub lühike märkus väljavõtmiseks kasutatud tee kohta, näiteks kontrolleri operaatoriliides, logiserver või failieksport. Väikesed ettevõtted saavad hakkama ühe lehekülje ülevaatega käitise kohta: kus logi asub, kellel on lugemisõigus, kuidas seda välja võetakse. Kord aastas tehtud testväljavõte, mis on hoolduspäevikusse kirja pandud, näitab, et tee toimib. Kehtib alates SL 1 kõigi turvatasemete puhul.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 6.1 RE 1** **Auditikirjed on masinliidese kaudu väljavõetavad, nii et analüüsivahendid saavad neid edasi töödelda ilma käsitsi ümber tippimata, ja andmed antakse dokumenteeritud, üldkasutatavas vormingus.**

Mille järgi seda näeb: Kasutatava liidese kirjeldus koos vorminguga, näiteks syslog, OPC UA Alarms and Conditions, REST-päring või CSV-eksport, lisaks näidiskirje ja vastuvõtva süsteemi konfiguratsioon. Tõendiks võib olla väljavõte SIEM või logikoguja konfiguratsioonist koos tõendiga saabuvate kirjete kohta. SIEM puudumisel piisab logikogujast lihtsal serveril, mis tõmbab logid öösel skriptiga kokku ja salvestab need; tõendiks on skript ise koos kogutud failide kataloogiloendiga. Täiendusena on see nõutav alles alates SL 3, mitte alates SL 1.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 6.2** **Turvalisuse seisukohalt olulist tegevust süsteemis seiratakse pidevalt, seire tuvastab ründekatsed ja väärkasutuse ning teatab neist viivitamata nimetatud kontaktpunktile, ja selleks kasutatavad vahendid, teavitusteed ning vastutused on määratletud.**

Mille järgi seda näeb: Seirevahendite ülevaade tsoonide kaupa, näiteks võrguandur, viirusetõrje teated, tulemüüri alarmid või tervikluse kontroll, koos märkega, kes teate saab ja millise aja jooksul reageerimist oodatakse. Tõendiks on alarmide konfiguratsioonid, viimaste kuude teadete loend ja nende käsitlemise märkmed. Väikesed ettevõtted ei vaja ööpäevaringset juhtimisruumi: piisab ühiskasutatavast postkastist või piletite postkastist, mis koondab olemasolevate süsteemide teated, ja kindlast reeglist, et nimetatud isik vaatab selle igal tööpäeval läbi, ning tõendiks on postkasti ajalugu. Nõutav alates SL 2.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

## 11 FR 7: Ressursside käideldavus 13

**SR 7.1** **Ülekoormuse või tahtlike ummistusrünnete korral püsib süsteem määratletud töörežiimis, olulised juhtimisfunktsioonid jätkavad tööd ja üksiku teenuse tõrge ei tõmba käitist endaga kaasa.**

Mille järgi seda näeb: Kaitsemehhanismide konfiguratsioon (kiiruse piiramine, ühenduste piirangud, üldlevi tormi ohjamine kommutaatorites), tarnija kinnitused käitumise kohta koormuse all, lisaks kirje koormustestist või tegelikust ülekoormussündmusest koos juhtimisfunktsiooni vaatlusega. Nõutav alates SL 1. Väike ettevõte katab selle kommutaatori ja tulemüüri seadistuste kuvatõmmistega ja lühikese märkusega selle kohta, milline funktsioon tähtsaima tootmisüksuse testi ajal edasi töötas.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 7.1 RE 1** **Sidekoormus, mida üksikud komponendid võrku saata saavad, on ülempiiriga piiratud, nii et vigane või ülevõetud komponent ei saa võrgusegmenti üle ujutada.**

Mille järgi seda näeb: Pordipõhised ribalaiuse ja multiedastuse piirangud võrgukomponentides, tõend ülempiiri kohta iga ühenduse jaoks, lisaks tegeliku baaskoormuse mõõtmine seadme kohta. Nõutav alates SL 2, mitte alates SL 1. Hallatavate kommutaatoriteta ei ole seda rida võimalik tõendada ja see ongi siis lahtine punkt.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 7.1 RE 2** **Vaadeldava süsteemi sisene ülekoormusolukord ei kandu üle naabersüsteemidesse ega võrkudesse; väljapoole ulatuv mõju on tehniliselt piiratud.**

Mille järgi seda näeb: Segmenteerimise ja filtreerimise reeglid piiridel, tõend, et väljuv liiklus on ülempiiriga piiratud, lisaks testikirje, mis näitab, et tootmisüksuse võrgus tekitatud koormus ei halvendanud kontori ega naabervõrku. Nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 7.2** **Töötlusaja, mälu, salvestusruumi ja võrguribalaiuse kasutamine on piiratud nii, et üksik protsess või teenus ei saa ära tarbida juhtimiseks vajalikke ressursse.**

Mille järgi seda näeb: Ressursipiirangute konfiguratsioon (kvoodid, protsesside prioriteedid, mälupiirangud), kasutuse seire hindamine esindusliku ajavahemiku jooksul, lisaks lävendid, mille juures antakse hoiatus. Nõutav alates SL 1. Väikesed ettevõtted kasutavad operatsioonisüsteemi sisseehitatud vahendeid ja lihtsat seiret koos kettaruumi ja protsessori teatega e-posti teel.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 7.3** **Süsteemikonfiguratsioonidest, rakenduse andmetest ja programmiversioonidest on olemas varukoopiad; neid saab teha jooksvat tööd katkestamata ja need on kaitstud volitamata pääsu ja muutmise eest.** Dokument

Mille järgi seda näeb: Varunduse kontseptsioon, mis katab käsitlusala, sageduse ja säilitusaja, viimaste käivituste varunduslogid, lisaks tõend varukoopia andmekandjate pääsukaitse kohta (eraldi hoiukoht, krüpteerimine, eraldi load). Nõutav alates SL 1. Väike ettevõte varundab PLC-projektid ja HMI-versioonid krüpteeritud andmekandjale, mis pärast varundamist füüsiliselt lahutatakse, ja märgib kuupäeva ja versiooni lihtsasse loendisse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.3 RE 1 Varukoopiate kasutatavus on tõendatud; on tõendatud, et neist saab tegelikult taastada töötava oleku.

Mille järgi seda näeb: Taastamise testi kirje koos kuupäeva, testitud varukoopia versiooni, sihtsüsteemi ja tulemusega, vähemalt kriitiliste komponentide kohta. Nõutav alates SL 2, mitte alates SL 1. Väikesed ettevõtted kontrollivad kord aastas pisteliselt ühte PLC-programmi ja ühte HMI-tõmmist varuseadmel ja panevad tulemuse kahe lausega kirja.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.3 RE 2 Varundus käivitub automaatselt määratletud ajakava järgi; ebaõnnestunud käivitus tuvastatakse ja sellest teatatakse.

Mille järgi seda näeb: Varundustöö ajakava, katkestusteta täitmislogid, lisaks tõend tõrketeate kohta käivituse puhul, mis ei õnnestunud (alarm, pilet, kiri). Nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.4 Pärast häiret, tõrget või rünnet on süsteem taastatav teadaolevasse turvalisse olekusse; taastamine on läbi harjutatud ja vastutused on nimetatud.

Dokument

Mille järgi seda näeb: Taaskäivituse plaan iga kriitilise komponendi kohta koos järjekorra, vajalike andmekandjate, kontaktide ja sihtajaga, koos viimase taastamisõppuse kirjega. Nõutav alates SL 1. Väike ettevõte saab hakkama ühe lehekülje taaskäivituskaardiga liini kohta, mida hoitakse juhtkapis ja kontrollitakse iga kord, kui varuosa vahetatakse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.5 Kui tavapärane toide katkeb, läheb süsteem määratletud olekusse: kas toidet hoiab üleval varuallikas või toimub korrakohane seiskamine ilma turvalise oleku kaotuseta.

Mille järgi seda näeb: Katkematu toiteallika või hädaolukorra generaatori dimensioneerimise ja hoolduse tõendid, viimase aku- või koormustesti testikirje, lisaks käitumise kirjeldus ümberlülitumisel ja võrgutoite naasmisel. Nõutav alates SL 1. Väikesed ettevõtted testivad katkematut toiteallikat koormuse all kord aastas ja panevad kirja testi kuupäeva, sildamise aja ja aku vanuse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.6 Süsteemi võrgu- ja turvaseadistused on fikseeritud kinnitatud sihtolekusse, kõrvalekalded sellest sihtolekust on tuvastatavad ja hetkeolek on igal ajal väljavõetav.

Dokument

Mille järgi seda näeb: Kinnitatud sihtkonfiguratsioon iga seadmeklassi kohta (turvakarastuse spetsifikatsioon), seadmete praegused konfiguratsiooniolekud, lisaks sihi ja tegeliku oleku võrdluse tulemus koos kõrvalekallete loendi ja igaühe põhjusega. Nõutav alates SL 1. Väike ettevõte hoiab konfiguratsioonieksporte versioonihalduses ja võrdleb neid enne ja pärast iga muudatust.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.6 RE 1 Turvaseadistuste hetkeolek on väljastatav masinloetaval kujul, nii et seda saab automaatselt sihtolekuga võrrelda.

Mille järgi seda näeb: Näidisväljund masinloetavas vormingus (konfiguratsioonieksport, struktureeritud fail, liidesepäring) ja skript või vahend, mis teeb võrdluse sihtolekuga, koos ühe käivituse tulemuste aruandega. Nõutav alates SL 3.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

### SR 7.7 Süsteem on piiratud käitamiseks vajalike funktsioonidega; teenused, pordid, protokollid ja liidesed, mida ei vajata, on välja lülitatud või eemaldatud.

Mille järgi seda näeb: Aktiivsete teenuste ja avatud portide loend komponendi kohta koos vajaduse põhjendusega, tõend, et ülejäänud on välja lülitatud (konfiguratsioon, pordiskaneeringu tulemus), lisaks reegel USB- ja hooldusliideste kohta. Nõutav alates SL 1. Väikesed ettevõtted teevad lihtsa pordiskaneeringu segmendi kohta ja põhjendavad iga avatud punkti ühe reaga.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus

**SR 7.8** **Kõigi süsteemi komponentide ajakohane loetelu koos tootja, tüübi, püsivara või tarkvara versiooni ja võrguaadressiga on kättesaadav ja seda hoitakse muudatuste korral ajakohasena.** Dokument

Mille järgi seda näeb: Komponentide loetelu koos ülevaatamise kuupäeva ja omanikuga, tõend ajakohasena hoidmise kohta muudatuste ajaloo kaudu, lisaks võrdlus võrguavastuse tulemusega, et leida seadmeid, mis ei ole kirjas. Nõutav alates SL 2, mitte alates SL 1. Väike ettevõte hoiab loetelu tabelina ja uuendab seda kindla reeglina iga kord, kui seade vahetatakse ja kui püsivara uuendatakse.

◯ Avatud ◯ Töös ◯ Täidetud ◯ Ei kohaldu

Tõend / põhjendus