IEC 62443-3-3:2013 Sistēmas drošības prasības rūpnieciskajai automatizācijai

Septiņas pamatprasības, 51 sistēmas prasība

100 prasības. Pēc šī standarta ir iespējams sertificēties akreditētā sertifikācijas institūcijā. Redakcija 07/2026.

IEC 62443-3-3 ir sertificējams, un sertificē sistēmu, nevis organizāciju un nevis personu. Ceļi ir ISASecure SSA un IECEE CB Scheme. Kas vēlas sertificēt organizāciju, tam nepieciešams 62443-2-1 vai 2-4, kas domā komponentu, tam nepieciešams 62443-4-2. Šajā sarakstā ir 51 sistēmas prasība un 49 prasību paplašinājumi. Kuras no tām ir spēkā, atkarīgs no izvēlētā drošības līmeņa: no SL 1 tās ir 38, no SL 2 tās ir 60, no SL 3 tās ir 90, SL 4 līmenī visas 100. Neviens paplašinājums nav spēkā jau SL 1 līmenī. Šis saraksts ir darba rīks pašnovērtējumam, nevis pierādījums.

Uzņēmums	Datums	Aizpildīja

5 FR 1: Kas pieprasa piekļuvi, un vai tas tiešām ir tas, par ko uzdodas 24

SR 1.1 **Cilvēku lietotāji ir identificēti un viņu identitāte ir pārbaudīta, pirms viņi iegūst piekļuvi, katrā vietā, kur viņi var vadīt vai konfigurēt automatizācijas sistēmu. Tas attiecas arī uz vadības paneļiem pie iekārtas, inženierijas piekļuvi un tīkla pakalpojumiem.**

Pēc kā to var atpazīt: Visu sistēmas pieteikšanās punktu uzskaite, proti, HMI, vadības telpa, PLC programmēšanas piekļuve, komutators, VPN un attālinātās apkopes klients, katrs ar tur izmantoto autentifikācijas mehānismu. Papildus konfigurācijas izraksts vai pieteikšanās ekrāna ekrānuzņēmums katrai ierīču klasei. Mazs uzņēmums sāk ar vienu tabulu katrai ierīcei, kolonnas: ierīce, saskarne, autentifikācija pastāv jā vai nē, pamatojums, ja nē. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.1 RE 1 **Katrs cilvēka lietotājs strādā ar individuālu identifikatoru, kas piešķirts tikai šai personai. Koplietošanas un maiņu konti ir atspējoti, atlikušie izņēmumi ir atsevišķi pamatoti un nodrošināti ar papildu pasākumiem.**

Pēc kā to var atpazīt: Kontu eksports katrai sistēmai ar identifikatora piesaisti personai, izņēmumu saraksts ar pamatojumu un kompensējošo pasākumu, piemēram, kamera vai apmeklējuma žurnāls operatora darba vietā. Šī rinda ir prasības paplašinājums un tāpēc nekad nav obligāta SL 1 līmenī, tā ir prasīta no SL 2.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.1 RE 2 **Ikviens, kas piesakās no neuzticama tīkla, piemēram, no interneta vai caur attālinātās apkopes savienojumu, apliecina savu identitāti ar vismaz diviem neatkarīgiem faktoriem.**

Pēc kā to var atpazīt: Attālinātās piekļuves konfigurācija ar iespējotu otro faktoru, pieteikšanās ieraksta paraugs, kas parāda abus faktorus, un izsniegto marķieru vai lietotņu reģistrāciju saraksts. Mazs uzņēmums izmanto esošās VPN vārtejas otro faktoru vai autentifikatora lietotni, kas neizmaksā neko papildus iestatīšanas laikam. Prasības paplašinājums, prasīts no SL 3, SL 1 līmenī nav prasīts.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.1 RE 3 **Apliecināšana ar diviem neatkarīgiem faktoriem attiecas ne tikai uz piekļuvi no ārpuses, bet uz katru cilvēka lietotāja pieteikšanos, tostarp pieteikšanos tīklā, kas klasificēts kā uzticams.**

Pēc kā to var atpazīt: Centrālā autentifikācijas pakalpojuma politikas izraksts, kas parāda, ka otrais faktors ir obligāts bez tīkla izņēmumiem, un pieteikšanās ierakstu paraugi no vadības telpas un vadības paneļa. Prasības paplašinājums, prasīts tikai no SL 4.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.2 **Ne tikai cilvēki, bet arī programmatūras procesi un ierīces autentificējas sistēmā, pirms tiem ir atļauts apmainīties ar datiem vai izmantot pakalpojumus. Tas attiecas arī uz kontrolleru savienojumiem savā starpā, datu saitēm uz augstāka līmeņa sistēmām un diagnostikas rīkiem.**

Pēc kā to var atpazīt: Iekārtu savstarpējo savienojumu saraksts ar avotu, mērķi, protokolu un katrā gadījumā izmantotajiem piekļuves datiem, piemēram, sertifikāts, pakalpojuma konts vai iepriekš koplietota atslēga. Papildus viena savienojuma konfigurācijas izraksts, kas padara autentifikāciju redzamu. Prasīts no SL 2, SL 1 līmenī nav prasīts.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.2 RE 1 **Katrs programmatūras process un katra ierīce uzrāda savu unikālu identifikatoru. Koplietošanas pakalpojuma konti vai viena atslēga, ko izmanto visā sistēmā daudzās ierīcēs, nav pieļaujami.** Dokuments

Pēc kā to var atpazīt: Ierīču piesaiste identifikatoram vai sertifikāta sērijas numuram, kas parāda, ka neviens identifikators neparādās divreiz. Prasības paplašinājums, prasīts no SL 3 un tāpēc neietilpst SL 1 līmenī.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.3 **Konti ir pārvaldīti visā to dzīves ciklā: izveide, tiesību maiņa, atspējošana pēc aiziešanas un dzēšana ir noteiktas ar noteikumiem un atbalstītas iesaistītajās sistēmās. Tas attiecas uz lietotāju kontiem, pakalpojumu kontiem un ārkārtas kontiem.** Dokuments

Pēc kā to var atpazīt: Kontu reģistrs ar veidu, īpašnieku, mērķi un statusu, kā arī pierādījumi par pieņemtajiem un aizgājušajiem darbiniekiem, piemēram, parakstīta nodošana vai pieteikums, kas parāda atspējošanu ar datumu. Ieteicama regulāra kontu pārskatīšana, un mazā uzņēmumā pietiek ar ikgadēju kontu saraksta salīdzināšanu ar personāla sarakstu. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.3 RE 1 **Kontu pārvaldība ir vienota visos sistēmas komponentos, tā ka konta atspējošana vienā vietā nepaliek bez sekām atsevišķās ierīcēs.**

Pēc kā to var atpazīt: Pierādījums par centrālā direktorija integrāciju, piemēram, direktoriju pakalpojums vai RADIUS, ar pievienoto komponentu sarakstu un atsevišķu sarakstu ar ierīcēm, kuras nav iespējams pievienot, kopā ar to alternatīvo procedūru. Pārbaudes ieraksts par atspējošanu, kas stājas spēkā visās pievienotajās sistēmās. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.4 **Identifikatori ir izsniegti pēc noteiktiem noteikumiem, nepārprotami piesaistīti personai, ierīcei vai lomai, izņemti no lietošanas, kad tie vairs netiek izmantoti, un vēlāk nekad netiek izsniegti citam turētājam.**

Pēc kā to var atpazīt: Identifikatoru nosaukumu veidošanas noteikums, piemēram, uzvārds un iniciāls vai iekārtas kods un numurs, kā arī izņemto identifikatoru vēsture, kas parāda, ka tie netiek izmantoti atkārtoti. Mazs uzņēmums uztur vienu nepārtrauktu sarakstu ar izsniegšanas datumu un izņemšanas datumu. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.5 **Autentifikatori, tādi kā paroles, atslēgas, sertifikāti un marķieri, ir izsniegti sakārtoti, tiek mainīti, ja rodas aizdomas par to izpaušanu, un pēc vajadzības atsaukti. Piegādes stāvoklī esošie noklusējuma konti un rūpnīcas paroles ir nomainīti pirms nodošanas ekspluatācijā.**

Pēc kā to var atpazīt: Izsniegto marķieru un sertifikātu saraksts ar saņēmēju un datumu, pierādījumi par maiņām un atsaukumiem, kā arī nodošanas ekspluatācijā kontrolsaraksts katrai ierīcei ar punktu rūpnīcas parole nomainīta, parakstīts. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.5 RE 1 **Programmatūras procesu piekļuves dati nav glabāti kā lasāms fails datu nesējā, bet gan aparatūras nodrošinātā krātuvē, kas neļauj nolasīt slepeno daļu.**

Pēc kā to var atpazīt: Izmantotā drošības komponenta tipa pierādījums, piemēram, TPM, drošs elements vai HSM, ar konfigurācijas izrakstu, kas apliecina, ka atslēga ir glabāta komponenta iekšienē. Kā tipa pierādījums pietiek ar iegādes ierakstu vai datu lapu. Prasības paplašinājums, prasīts no SL 3, SL 1 un SL 2 līmenī nav prasīts.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 1.6 **Bezvadu piekļuve sistēmai, piemēram, WLAN, radio tālvadības pultis vai Bluetooth diagnostika, ir izmantojama tikai pēc lietotāja un ierīces identifikācijas un autentifikācijas, un tā ir apzināti pārvaldīta.**

Pēc kā to var atpazīt: Visu bezvadu savienojumu uzskaite ar mērķi, darbības rādiusu un šifrēšanas metodi, piekļuves punkta konfigurācijas izraksts un apstiprināto gala ierīču saraksts. Mazs uzņēmums papildus dokumentē, kuras ierīču bezvadu saskarnes ir apzināti izslēgtas. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.6 RE 1 **Katra bezvadu piekļuve ir attiecināma uz vienu konkrētu lietotāju vai vienu konkrētu ierīci, kopīga tīkla atslēga visiem dalībniekiem nav pietiekama.**

Pēc kā to var atpazīt: Pierādījums par metodi ar individuāliem piekļuves datiem, piemēram, uzņēmuma WLAN autentifikācija pret direktoriju vai atsevišķi sertifikāti katrai ierīcei, kā arī savienojumu žurnāls, kas parāda individuālo identifikatoru. Prasības paplašinājums, prasīts no SL 2 un tāpēc nav prasīts SL 1 līmenī.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.7 **Visur, kur izmanto paroles, ir konfigurējama to minimālā stiprība, piemēram, minimālais garums un nepieciešamie rakstzīmju veidi, un konfigurētās vērtības ir spēkā visiem attiecīgajiem kontiem.**

Pēc kā to var atpazīt: Paroļu politikas konfigurācijas izraksts katrai sistēmai ar faktiski iestatītajām vērtībām, piemēram, garums >= 10 rakstzīmes un vismaz trīs rakstzīmju veidi, kā arī saraksts ar sistēmām, kas tehniski nespēj atbalstīt šo iestatījumu, kopā ar to kompensējošo pasākumu. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.7 RE 1 **Cilvēku lietotājiem paroļu veidošanu un darbības ilgumu nosaka papildu noteikumi: agrāko paroļu atkārtota izmantošana ir novērsta un derīgums ir ierobežots laikā.**

Pēc kā to var atpazīt: Konfigurācijas izraksts, kas parāda paroļu vēsturi, piemēram, pēdējo piecu paroļu atkārtota izmantošana ir bloķēta, un konfigurēto maksimālo derīgumu. Prasības paplašinājums, prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.7 RE 2 **Paroles darbības ilguma ierobežojums attiecas ne tikai uz cilvēkiem, bet uz visiem kontiem, tostarp pakalpojumu, apkopes un ierīču kontiem.**

Pēc kā to var atpazīt: Tehnisko kontu nomaiņas plāns ar pēdējo un nākamo maiņas datumu katram kontam, kā arī pierādījumi par maiņām, piemēram, izmaiņu ieraksts vai pieteikums. Prasības paplašinājums, prasīts tikai no SL 4.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.8 **Kur izmanto sertifikātus, tie nāk no sakārtotas sertifikātu pārvaldības ar noteiktiem noteikumiem pieprasīšanai, izsniegšanai, derīguma termiņam, atjaunošanai un atsaukšanai.** Dokuments

Pēc kā to var atpazīt: Sertifikātu politika vai īss rakstisks noteikums, kas nosaka atbildību, derīguma termiņus un atsaukšanas ceļu, kā arī izsniegto sertifikātu uzskaite ar to derīguma beigu datumiem. Mazs uzņēmums uztur tabulu ar sertifikātu, ierīci, derīguma beigu datumu un atgādinājuma datumu, kas novērš klusu iekārtas dīkstāvi beigušos sertifikātu dēļ. Prasīts no SL 2.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.9 **Ja autentifikācijai izmanto atslēgu pārus, sistēma pilnībā pārbauda sertifikātu: uzticamības ķēdi, derīguma termiņu, atsaukšanas statusu un pierādījumu, ka pretējā puse patiešām tur privāto atslēgu. Saikne starp sertifikātu un kontu ir nepārprotama.**

Pēc kā to var atpazīt: Konfigurācijas izraksts ar iespējotu atsaukšanas pārbaudi, piemēram, CRL vai OCSP, pārbaudes ieraksts par noraidītu pieteikšanos ar beigušos vai atsauktu sertifikātu, kā arī sertifikātu un kontu piesaistes tabula. Prasīts no SL 3, SL 1 un SL 2 līmenī nav prasīts.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.9 RE 1 **Privātās atslēgas atrodas tikai aparatūras nodrošinātā krātuvē, no kuras tās nav nolasāmas, un tās arī tiek izmantotas šīs krātuves iekšienē.**

Pēc kā to var atpazīt: Izmantotā drošības komponenta datu lapa vai sertifikācijas pierādījums un konfigurācijas izraksts, kas parāda, ka atslēga tiek ģenerēta komponenta iekšienē, tāpēc privātā atslēga to nekad neatstāj. Prasības paplašinājums, prasīts tikai no SL 4.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.10 **Pieteikšanās laikā sistēma neatklāj informāciju, ko varētu ļaunprātīgi izmantot. Ievadītās paroles ir noslēptas, un kļūdu paziņojumi neatklāj, vai nepareizs bija identifikators vai parole.**

Pēc kā to var atpazīt: Pieteikšanās ekrāna ekrānuzņēmums ar maskētu ievadi un kļūdas paziņojuma ekrānuzņēmums pēc neveiksmīga mēģinājuma. Ierīcēm, kas to tehniski nespēj, piemēram, vecākiem vadības paneļiem, papildus īsa piezīme par kompensējošo pasākumu, piemēram, ierobežota fiziska piekļuve uzstādīšanas vietai. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.11 **Secīgu neveiksmīgu pieteikšanās mēģinājumu skaits ir ierobežots, un reakcija uz to ir konfigurējama, piemēram, pagaidu bloķēšana. Izvēlētā reakcija netraucē ar drošumu saistītu iekārtas darbību.**

Pēc kā to var atpazīt: Konfigurācijas izraksts ar sliekšņa vērtību, piemēram, bloķēšana pēc <= 5 neveiksmīgiem mēģinājumiem, un bloķēšanas ilgumu, kā arī īss novērtējums par to, kāpēc bloķēšana nekavē ārkārtas darbību vai iekārtas drošu apturēšanu. Operatora darba vietās ar drošuma funkciju laikā ierobežota bloķēšana ir vēlamāka nekā pastāvīga konta slēgšana. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.12 **Pirms pieteikšanās ir iespējams parādīt lietošanas paziņojumu, kas norāda uz sistēmas lietošanas un uzraudzības noteikumiem. Tekstu un attēlošanu var konfigurēt aktīva īpašnieks.**

Pēc kā to var atpazīt: Parādītā paziņojuma teksta ekrānuzņēmums un apstiprinātais formulējums ar apstiprināšanas datumu. Mazi uzņēmumi formulējumu īsi saskaņo ar darbinieku pārstāvjiem vai ar vadību, pietiek ar vienu rindkopu. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.13 **Piekļuve no neuzticamiem tīkliem, piemēram, piegādātāju attālinātā apkope, ir ierobežota līdz noteiktiem ceļiem, tiek uzraudzīta un ir pārtraucama jebkurā laikā.**

Pēc kā to var atpazīt: Attālinātās piekļuves ceļu uzskaite ar mērķi, attālināto pusi, kontaktpersonu un izmantoto ceļu, kā arī savienojumu žurnāli un pierādījums par spēju atvienot, piemēram, atslēgas slēdzis, ugunsmūra noteikums vai izslēdzams attālinātās apkopes maršrutētājs. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 1.13 RE 1 **Katru atsevišķu sesiju no neuzticama tīkla atbildīgā persona nepārprotami apstiprina, pirms savienojums ir izveidots, pastāvīgi atvērts savienojums nav pietiekams.**

Pēc kā to var atpazīt: Apstiprinājuma ieraksti par katru attālinātās apkopes sesiju ar laiku, iemeslu, apstiprinātāju un ilgumu, tehniski, piemēram, ar atslēgas slēdzi pie piekļuves maršrutētāja vai ar apstiprināšanas portālu. Mazā uzņēmumā pietiek ar attālinātās apkopes žurnālu pie vadības skapja, ko apkopes tehniķis paraksta par katru sesiju. Prasības paplašinājums, prasīts no SL 2 un tāpēc nekad ne SL 1 līmenī.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

6 FR 2: Lietošanas kontrole (tiesības, sesijas, audita ieraksti) 24

SR 2.1 **Sistēma tehniski īsteno piešķirtās tiesības: katra pieteikusies persona, katra ierīce un katrs programmatūras process saņem tieši to piekļuvi, kas tam piešķirta, un ikviens mēģinājums pārsniegt to tiek noraidīts.**

Pēc kā to var atpazīt: Tiesību koncepcija ar kontu piesaisti atļaujām, kā arī ekrānuzņēmums vai konfigurācijas izraksts katrai vadības sistēmai, HMI un inženierijas darbstacijai, kas parāda aktīvās tiesības. Papildus pārbaudes ieraksts, kurā konts ar zemām tiesībām mēģina veikt bloķētu darbību un tiek noraidīts. Prasīts no SL 1. Mazs uzņēmums iztiek ar divām vai trim lomām, piemēram, vadīt, apkopt, projektēt, un dokumentē tās vienā lappusē.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.1 RE 1 **Tiesību īstenošana attiecas ne tikai uz cilvēkiem operatoriem, bet tikpat lielā mērā uz programmatūras procesiem un ierīcēm, kas piekļūst sistēmai patstāvīgi.**

Pēc kā to var atpazīt: Tehnisko un pakalpojumu kontu saraksts, piemēram, OPC UA klienti, vēstures datubāzes savienojumi, rezerves kopēšanas pakalpojumi, katrs ar tam piešķirto tiesību kopu. Izraksts no tiesību pārvaldības, kas parāda, ka šie konti nedarbojas ar administratora tiesībām. Prasības paplašinājums, prasīts no SL 2, SL 1 līmenī nav prasīts.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.1 RE 2 **Tiesības netiek piešķirtas atsevišķām personām pa vienai, bet gan caur lomām, un lomu piesaiste atļautajām darbībām ir izsekojami dokumentēta.** Dokuments

Pēc kā to var atpazīt: Lomu un tiesību matrica tabulas veidā: rindas ir lomas, kolonnas ir darbības, tādas kā mainīt uzstādījuma vērtību, ielādēt programmu, kvitēt trauksmi, izveidot kontu. Papildus saraksts ar personu piesaisti lomai. Prasības paplašinājums, prasīts no SL 2. Kā pierādījums pilnībā pietiek ar uzturētu izklājlapu, kurā norādīts izmaiņu datums.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.1 RE 3 **Šauri noteiktos izņēmuma gadījumos pilnvarots vadītājs var uz ierobežotu laiku atcelt tiesību ierobežojumu, un katra šāda atcelšana tiek reģistrēta audita ierakstos.**

Pēc kā to var atpazīt: Izņēmuma apstiprināšanas procedūras apraksts, kurā norādīts, kas to drīkst piešķirt un cik ilgi tā paliek spēkā, kā arī audita ieraksti par jau piešķirtajām atcelšanām, kas ņemti no sistēmas žurnāla. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.1 RE 4 **Īpaši kritiskām iejaukšanām nepieciešams divu neatkarīgu pilnvarotu personu apstiprinājums, pirms darbība tiek veikta.**

Pēc kā to var atpazīt: Saraksts ar darbībām, kurām nepieciešams dubults apstiprinājums, piemēram, drošuma parametru maiņa vai jaunas vadības programmas ielāde, kopā ar konfigurācijas pierādījumu un audita ierakstiem, kuros nosaukti abi apstiprinātāji. Prasības paplašinājums, prasīts tikai no SL 4.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.2 **Bezvadu savienojumu lietošana automatizācijas tīklā ir saistīta ar nepārprotamu pilnvarojumu, un tikai apstiprināti dalībnieki drīkst apmainīties ar datiem vai iejaukties pa gaisu.**

Pēc kā to var atpazīt: Visu bezvadu savienojumu uzskaite, piemēram, WLAN piekļuves punkti, Bluetooth pāra savienojumi, mobilo sakaru maršrutētāji, katrs ar savu mērķi un apstiprinātajiem dalībniekiem. Papildus piekļuves pārvaldības konfigurācija piekļuves punktā. Prasīts no SL 1. Kas procesa tīklā neizmanto nevienu bezvadu savienojumu, to tieši tā arī apliecina rakstiski un pamato ar konfigurācijas skatu, kurā redzams, ka bezvadu saskarne ir atspējota.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.2 RE 1 Nepilnvarotas bezvadu ierīces automatizācijas tīkla tuvumā tiek atklātas un par tām tiek ziņots.

Pēc kā to var atpazīt: Ieraksts no bezvadu tīkla uzraudzības vai regulāras bezvadu skenēšanas ar datumu, rezultātu sarakstu un piezīmi par katru nezināmu ierīci. Ziņošanas ceļš atbildīgajai funkcijai ir nosaukts. Prasības paplašinājums, prasīts no SL 2, SL 1 līmenī nav prasīts. Mazs uzņēmums var veikt skenēšanu reizi ceturksnī ar klēpjdatoru un rezultātu saglabāt kā ierakstu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.3 Pārnēsājamu un mobilu ierīču lietošana sistēmā, piemēram, apkopes klēpjdatori, USB datu nesēji vai planšetdatori, ir noteikta ar noteikumiem un tehniski ierobežota līdz nepārprotami apstiprinātām ierīcēm.

Pēc kā to var atpazīt: Ierīču lietošanas noteikumu kopa, apstiprināto apkopes ierīču saraksts ar to identifikatoriem un pierādījums par tehnisko ierobežojumu, piemēram, USB pieslēgvietas HMI un inženierijas darbstacijā ir atspējotas vai ierobežotas līdz konkrētām ierīcēm. Prasīts no SL 1. Mazs uzņēmums strādā ar divām marķētām apkopes USB zibatmiņām, kurās raksta tikai vienā nodošanas darbstacijā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.3 RE 1 Pirms pievienošanas pārnēsājamas vai mobilas ierīces drošības stāvoklis tiek pārbaudīts, un ierīcēm, kas neatbilst prasībām, piekļuve tiek liegta.

Pēc kā to var atpazīt: Ierīces stāvokļa pārbaudes kritēriji, piemēram, aktuāla aizsardzība pret ļaunprātīgu kodu un ielāpu līmenis, kā arī pārbaudes ieraksti katrai apkopes ierīcei un pierādījums par tehnisko īstenošanu, piemēram, ar nodošanas darbstaciju vai tīkla piekļuves pārvaldību. Prasības paplašinājums, prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.4 Mobilajam kodam, ko izpilda sistēmā, piemēram, skriptiem operatora saskarnēs vai aktīvam saturam atskaitēs, ir noteikts, kuri veidi ir atļauti, un neatļautiem veidiem izpilde ir liegta.

Dokuments

Pēc kā to var atpazīt: Noteikums par to, kurš mobilais kods ir atļauts kurās sistēmās, kā arī konfigurācijas pierādījums par ierobežojumu, piemēram, skriptu izpilde HMI pārlūkā ir atspējota, makro novērtējuma failos ir bloķēti. Prasīts no SL 1. Pietiek ar vienas lappuses noteikumu, kas aptver tos trīs vai četrus gadījumus, kuri patiešām pastāv.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.4 RE 1 Pirms mobilā koda izpildes ir pārbaudīts, ka tas nāk no gaidītā avota un nav mainīts.

Pēc kā to var atpazīt: Konfigurācijas pierādījums par paraksta pārbaudi vai kontrolsummas pārbaudi, kā arī pārbaudes ieraksts, kurā mainīts vai neparakstīts kods tiek noraidīts. Prasības paplašinājums, prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.5 Sesija tiek bloķēta pēc noteikta laika bez operatora darbības un tiek atbrīvota tikai pēc atkārtotas autentifikācijas, nezaudējot ar drošumu saistītas procesa informācijas attēlojumu.

Pēc kā to var atpazīt: Konfigurācijas izraksts ar konfigurēto bloķēšanas laiku katrai darbstacijai, kā arī pamatojums darbstacijām pastāvīgi apkalpotās vadības telpās, kur bloķēšana ir apzināti iestatīta citādi. Prasīts no SL 1. Vizuāls pierādījums: bloķēšanas ekrāna ekrānuzņēmums, kurā joprojām redzama trauksmju rinda.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.6 Attālinātās sesijas tiek pārtrauktas pēc noteikta laika bez darbības vai pēc operatora pieprasījuma, tā ka neviens atvērts attālinātais savienojums nepaliek bez uzraudzības.

Pēc kā to var atpazīt: Attālinātās piekļuves konfigurācija ar dīkstāves laika ierobežojumu, audita ieraksti par pārtrauktām attālinātajām sesijām un apraksts, kā operators var nekavējoties atvienot notiekošu attālinātās apkopes sesiju, piemēram, ar atslēgas slēdzi vai ar atļauju katrai sesijai atsevišķi. Prasīts no SL 2, SL 1 līmenī nav prasīts.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.7 **Vienlaicīgo sesiju skaits katram kontam vai lomai ir ierobežots, un pieteikšanās mēģinājumi virs šī ierobežojuma tiek noraidīti.**

Pēc kā to var atpazīt: Konfigurācijas izraksts ar noteikto augšējo robežu katrai lomai, piemēram, <= 1 vienlaicīga sesija inženierijas kontiem, kā arī pārbaudes ieraksts par noraidītu otro pieteikšanās mēģinājumu. Prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.8 **Ar drošību saistīti notikumi tiek reģistrēti, un katrs ieraksts nosauc vismaz laiku, avotu, izraisītāja kontu, notikuma veidu un iznākumu.** Dokuments

Pēc kā to var atpazīt: Noteikums par reģistrējamiem notikumu veidiem, piemēram, pieteikšanās, neveiksmīga pieteikšanās, tiesību maiņa, programmas maiņa, konfigurācijas maiņa, kā arī īsts audita žurnāla izraksts, kurā redzami nosauktie lauki. Prasīts no SL 1. Mazs uzņēmums vāc vadības sistēmas, HMI un ugunsmūra žurnālus vienā mapē ar noteiktu glabāšanas termiņu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.8 RE 1 **Atsevišķu komponentu audita ieraksti tiek apkopoti centrālā vietā un veido vienotu, sistēmas mēroga ierakstu kopumu, ko var novērtēt kopumā.**

Pēc kā to var atpazīt: Žurnālu apkopošanas arhitektūras skice, kurā redzami visi pievienotie avoti, kā arī novērtējums, kas notikumus no vismaz diviem komponentiem izvieto vienā laika asī. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.9 **Audita ierakstiem ir nodrošināta pietiekama krātuve, tā ka notikumi tiek saglabāti visu noteikto glabāšanas termiņu un netiek netīši pārrakstīti.**

Pēc kā to var atpazīt: Krātuves vajadzības aprēķins vai novērtējums no dienas žurnālu apjoma, kas reizināts ar glabāšanas termiņu, kā arī konfigurētais krātuves apjoms un arhivēšanas noteikums. Prasīts no SL 1. Praksē pietiek ar ikdienas kopiju atsevišķā glabāšanas vietā ar dokumentētu glabāšanas termiņu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.9 RE 1 **Kad audita krātuve sasniedz noteikto piepildījuma slieksni, atbildīgajai funkcijai tiek izdots brīdinājums, pirms krātuves ietilpība ir pilnībā izlietota.**

Pēc kā to var atpazīt: Sliekšņa konfigurācijas izraksts, piemēram, brīdinājums no >= 80 procentu piepildījuma, kā arī izraisītā paziņojuma paraugs un saņēmēju saraksts. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.10 **Ja audita žurnalēšana neizdodas vai audita krātuve piepildās, sistēma reaģē iepriekš noteiktā veidā un atbildīgā funkcija tiek informēta, neapdraudot iekārtas drošu darbību.**

Pēc kā to var atpazīt: Noteiktā reakcija katram kļūmes gadījumam, piemēram, pārrakstīt vecākus ierakstus un izdot paziņojumu, nevis apturēt iekārtu, ar pamatojumu no procesa viedokļa. Pierādījums ar izraisītu pārbaudes paziņojumu un atbilstošo audita ierakstu. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.11 **Katram audita ierakstam ir laika zīmogs no nosaukta laika avota, tā ka notikumus no dažādiem komponentiem var sakārtot secībā savā starpā.**

Pēc kā to var atpazīt: Norāde par katrā komponentā izmantoto laika avotu un žurnāla izraksts ar redzamu laika zīmogu, tostarp laika joslu. Prasīts no SL 2, SL 1 līmenī nav prasīts.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 2.11 RE 1 **Visu iesaistīto komponentu pulksteņi ir sinhronizēti ar kopīgu laika avotu, tā ka novirze paliek noteiktās robežās.**

Pēc kā to var atpazīt: Laika sinhronizācijas konfigurācija, piemēram, NTP serveris un sinhronizācijas intervāls, kā arī pārbaudes ieraksts ar izmērīto novirzi katram komponentam pret noteikto robežu, piemēram, <= 1 sekunde. Prasības paplašinājums, prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.11 RE 2 **Pats laika avots ir aizsargāts pret manipulācijām, un neticama vai izmainīta laika atsauce tiek atklāta un par to tiek ziņots.**

Pēc kā to var atpazīt: Apraksts par to, kā laika avots ir aizsargāts, piemēram, autentificēta laika sinhronizācija, ierobežošana līdz iekšējam avotam, laika lēcienu uzraudzība, kā arī paziņojumi vai audita ieraksti par atklātu novirzi. Prasības paplašinājums, prasīts tikai no SL 4.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.12 **Par noteiktām kritiskām darbībām vēlāk ir bez šaubām nosakāms, kas tās izraisījis, tāpēc rīkotājs nevar ticami noliegt to izdarīšanu.** Dokuments

Pēc kā to var atpazīt: Saraksts ar darbībām, uz kurām šis pierādījums attiecas, piemēram, receptes maiņa, partijas izlaišana, robežvērtību maiņa, kā arī atbilstošie ieraksti ar unikālu personas identifikatoru un pierādījums, ka grupu konti šīm darbībām ir izslēgti. Prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 2.12 RE 1 **Nenoliedzama rīkotāja piesaiste attiecas ne tikai uz atsevišķām kritiskām darbībām, bet uz visiem lietotājiem un visām darbībām, ko viņi izraisa.**

Pēc kā to var atpazīt: Pierādījums, ka katrs konts ir piesaistīts vienai personai un ka nav palikusi neviena koplietošanas pieteikšanās, kā arī žurnāla izraksts par patvaļīgi izvēlētām darbībām, kurā visur parādās unikāls personas identifikators. Prasības paplašinājums, prasīts tikai no SL 4.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

7 FR 3: Sistēmas integritāte, datu, programmatūras un sesiju aizsardzība pret nepilnvarotām izmaiņām 19

SR 3.1 **Vadības sistēma atklāj, kad informācija ir mainīta pārraides laikā sakaru kanālā, un tā to dara gan vadības datiem, gan konfigurācijas datiem, gan pārvaldības datplūsmai. Aizsardzība attiecas arī uz savienojumiem, kas iziet no sistēmas vai šķērso neuzticamus tīkla segmentus.**

Pēc kā to var atpazīt: Tīkla un protokolu pārskats, kurā norādīts, kurš kanāls izmanto kuru integritātes mehānismu (kontrolsumma, ziņojuma autentifikācijas kods, parakstītas telegrammas), lauka kopnes vai OPC UA drošības iestatījumu konfigurācijas izraksts un pārbaudes ieraksts, kas parāda, ka izmainīta telegramma tika pierādāmi noraidīta. Mazs uzņēmums to atspoguļo tabulā katram savienojumam ar kolonnām avots, mērķis, protokols un integritātes mehānisms, un rezultativitāti vienreiz pierāda ar datplūsmas ierakstu. Prasīts no SL 1.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 3.1 RE 1 **Integritātes aizsardzība pārraides laikā balstās uz kriptogrāfiskiem mehānismiem, tāpēc uzbrucēja apzināta manipulācija ar saviem līdzekļiem nevar palikt neatklāta. Vienkārša kontrolsumma pret pārraides kļūdām šeit nav pietiekama.**

Pēc kā to var atpazīt: Saraksts ar katrā kanālā izmantotajiem kriptogrāfiskajiem mehānismiem un atslēgu garumiem, atsauce uz pamatā esošo atslēgu pārvaldību un konfigurācijas izraksti (piemēram, TLS šifru komplekti, OPC UA SecurityPolicy, IPsec profili). Mazi uzņēmumi paļaujas uz savu kontrolleru drošajiem noklusējuma profiliem un saglabā aktīvā iestatījuma ekrānuzņēmumu. Prasības paplašinājums, prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 3.2 **Pastāv aizsardzības mehānismi pret ļaunprātīgu kodu, kas neļauj nevēlamam programmas kodam izpildīties sistēmas komponentos un kas ziņo par katru atklāšanu. Mehānismi ir izvēlēti tā, lai netraucētu iekārtas paredzēto darbību, un tie tiek uzturēti aktuāli.**

Pēc kā to var atpazīt: Pārskats par katru komponentu, kurā norādīts piemērojamais mehānisms (pretvīrusu programma, atļauto lietotņu saraksts, nostiprināta operētājsistēma bez izpildes tiesībām), pierādījums, ka paraksti vai atļauto lietotņu saraksti tiek atjaunināti, un aizsardzības sistēmas brīdinājumi. Kur pretvīrusu programma nav iespējama, piemēram, kontrollerī, kompensējošais pasākums ir dokumentēts kopā ar tā pamatojumu. Maziem uzņēmumiem labi noder atļauto lietotņu saraksts operatora datorā un rakstisks noteikums par USB datu nesējiem. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.2 RE 1 **Aizsardzība pret ļaunprātīgu kodu papildus darbojas iekārtas ieejas un izejas punktos, kur dati ienāk vai iziet, nevis tikai pašās gala ierīcēs.**

Pēc kā to var atpazīt: Saraksts ar visiem ieejas un izejas punktiem (attālinātās apkopes piekļuve, datu pārsūtīšanas vārteja, noņemamie datu nesēji, nodošana biroja tīklam, elektroniskā pasta ceļš programmu versijām) ar katrā punktā darbojošos skenēšanas mehānismu, kā arī ieraksti par pārbaudītajām nodošanām. Mazi uzņēmumi ierīko vienu nodošanas datoru ar vīrusu skenēšanu kā vārteju un nostiprina to darba instrukcijā. Prasības paplašinājums, prasīts no SL 2.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.2 RE 2 **Aizsardzības mehānismi pret ļaunprātīgu kodu ir pārvaldīti no centrālas vietas, atjauninājumi tiek izplatīti centralizēti, un atklājumi tiek apkopoti vienā vietā novērtēšanai.**

Pēc kā to var atpazīt: Centrālās pārvaldības konsoles konfigurācija, atskaite par visu pievienoto komponentu atjauninājumu stāvokli un ziņoto atklājumu novērtējums par kādu laika posmu. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.3 **Sistēmas drošības funkcijas tiek pārbaudītas plānotos intervālos un pēc izmaiņām, lai apstiprinātu, ka tās patiešām darbojas. Pārbaudes ir ieplānotas tā, lai neapdraudētu iekārtas darbību, un rezultāti tiek reģistrēti.**

Dokuments

Pēc kā to var atpazīt: Pārbaudes plāns, kurā norādīts pārbaudes objekts, intervāls un laika logs, kopā ar pārbaudes ierakstiem, kuros redzams datums, pārbaudītājs, gaidītā uzvedība un novērotā uzvedība. Noderīgas atsevišķas pārbaudes ir: pieteikšanās ar atspējotu kontu neizdodas, pretvīrusu programma reaģē uz pārbaudes failu, attālinātās apkopes piekļuve nav sasniedzama bez atļaujas. Mazi uzņēmumi pārbaudi piesaista jau tāpat plānotajai apkopes apturēšanai un strādā pēc noteikta kontrolsaraksta. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.3 RE 1 **Drošības funkciju pārbaude notiek ar automatizētiem līdzekļiem, tāpēc tā ir atkārtojama bez manuāla darba un dod saskanīgu rezultātu.**

Pēc kā to var atpazīt: Skripti vai pārbaudes rīki kopā ar to izpildes grafiku, to izvades faili un vairāku izpilžu salīdzinājums, kas parāda, ka novirzes tiek atklātas. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.3 RE 2 **Drošības funkciju pārbaude ir iespējama arī parastas darbības laikā, neapturot iekārtu un nepārslēdzot to īpašā stāvoklī.**

Pēc kā to var atpazīt: Pārbaudes procedūras apraksts ar pierādījumu, ka tai nav nelabvēlīgas ietekmes uz procesu, piemēram, ietekmes analīze par cikla laikiem un tīkla noslodzi, kā arī pārbaudes ieraksti no ražošanas darbības. Prasības paplašinājums, prasīts no SL 4.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.4 **Nepilnvarotas izmaiņas programmatūrā, aparātprogrammatūrā un glabātajā informācijā tiek atklātas. Tas vienlīdz attiecas uz vadības programmām, parametru kopām, receptēm un konfigurācijas failiem.**

Pēc kā to var atpazīt: Aizsargājamo versiju uzskaite ar saglabātām kontrolvērtībām vai parakstiem, integritātes salīdzinājumu rezultāti un dokumentēta salīdzināšana ar versiju kontrolē glabāto versiju. Mazi uzņēmumi izlaisto programmas versiju kopā ar tās kontrolsummu glabā pret rakstīšanu aizsargātā vietā un salīdzina, ja rodas aizdomas vai pēc apkopes. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.4 RE 1 **Ja tiek atklāts programmatūras vai informācijas integritātes pārkāpums, sistēma par to automātiski ziņo atbildīgajai vietai, un atklāšana nav atkarīga no tā, vai kāds to aktīvi meklē.**

Pēc kā to var atpazīt: Paziņošanas ceļu konfigurācija (trauksme vadības telpā, elektroniskais pasts, ziņojums uzraudzības sistēmai), saņēmēju saraksts ar aizvietošanas kārtību un vismaz viena pārbaudes trauksme ar dokumentētu reakcijas laiku. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.5 **Ievaddati, ko sistēma pieņem no procesa datiem, saskarnēm vai lietotāja saskarnēm, pirms apstrādes tiek pārbaudīti attiecībā uz atļauto sintaksi, atļauto vērtību diapazonu un atļauto garumu. Nederīgi ievaddati nerada nekontrolētu uzvedību.**

Pēc kā to var atpazīt: Robežu un formātu specifikācija katram ievaddatam, izraksti no validācijas loģikas kontrollerī vai lietotnē un testa gadījumi ar apzināti nederīgiem ievaddatiem (pārāk liela vērtība, nepareizs datu tips, pārmērīgi gara rakstzīmju virkne) kopā ar dokumentēto sistēmas uzvedību. Mazi uzņēmumi ticamības robežas katram mērpunktam reģistrē tabulā un pārbauda tās nodošanas ekspluatācijā laikā. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.6 **Kļūmes gadījumam ir noteikts, kādu stāvokli pieņem izejas uz iekārtu, un sistēma pieņem tieši šo stāvokli. Noteiktais stāvoklis ir saskaņots ar iekārtas funkcionālo drošumu.**

Pēc kā to var atpazīt: Noteikums katrai izejai vai izeju grupai (vērtības saglabāšana, noteikta aizstājējvērtība, drošas apturēšanas stāvoklis) ar pamatojumu no riska novērtēšanas, kontrollera konfigurācijas izraksts un pierādījums no kļūmes pārbaudes, piemēram, kabeļa pārrāvuma vai sakaru zuduma, kas parāda gaidīto uzvedību. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.7 **Sistēma apstrādā kļūdu stāvokļus tā, ka darbība paliek kontrolē un netiek izpausta informācija, kas palīdzētu uzbrucējam. Operatoriem rādītie kļūdu paziņojumi paliek īsi, bet tehniskās detaļas nonāk tikai iekšējos ierakstos.**

Pēc kā to var atpazīt: Kļūdu klašu pārskats ar katrai paredzēto sistēmas uzvedību, parādīto paziņojumu piemēri salīdzinājumā ar atbilstošajiem iekšējiem žurnāla ierakstiem un pārbaudes pierādījums, ka operatora saskarnē neparādās failu ceļi, kontu nosaukumi, datubāzes izvade vai versiju dati. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.8 **Aktīvās sesijas ir aizsargātas pret pārņemšanu un pret svešu ziņojumu ievadīšanu. Sesija beidzas pēc atteikšanās vai pēc noteikta laika bez darbības, un pēc tam tā nav izmantojama atkārtoti.**

Pēc kā to var atpazīt: Sesiju pārvaldības konfigurācija ar konfigurētajiem dīkstāves laika un maksimālā ilguma ierobežojumiem, pierādījums par mehānismu, kas aizsargā pret ziņojumu atkārtotu nosūtīšanu, un pārbaudes ieraksts, kurā pārtverta sesija pēc atteikšanās vairs nedarbojas. Prasīts no SL 2.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.8 RE 1 **Sesiju identifikatori zaudē derīgumu, kad sesija beidzas, un sistēma tos vairs nepieņem, arī tad ne, ja tie tiek atkārtoti uzrādīti no ārpuses.**

Pēc kā to var atpazīt: Sesiju pārvaldības konfigurācijas izraksts par derīguma atcelšanu, kā arī pārbaudes ieraksts, kurā iepriekš derīgs identifikators pēc atteikšanās tiek nosūtīts vēlreiz un sistēma to noraida. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.8 RE 2 **Katrai jaunai sesijai tiek ģenerēts atsevišķs vienreiz lietojams identifikators. Identifikatori netiek izmantoti atkārtoti citās sesijās, citiem lietotājiem vai citās ierīcēs.**

Pēc kā to var atpazīt: Ģenerēšanas procedūras apraksts un pierādījums no žurnāla vai datplūsmas ieraksta, ka vairākas secīgas pieteikšanās saņem atšķirīgus identifikatorus. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.8 RE 3 **Sesiju identifikatori tiek ģenerēti ar atzītiem nejaušības mehānismiem, tāpēc tos nevar ne uzminēt, ne atvasināt no iepriekšējiem identifikatoriem.**

Pēc kā to var atpazīt: Norāde par izmantoto nejaušo skaitļu ģeneratoru un tā entropijas avotu, piegādātāja deklarācija vai pārbaudes atskaite par to un ģenerēto identifikatoru izlases statistisks novērtējums. Prasības paplašinājums, prasīts no SL 4.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.9 **Ar drošību saistītie ieraksti un rīki, ko izmanto to novērtēšanai, ir aizsargāti pret nepilnvarotu piekļuvi, izmaiņām un dzēšanu. Personu loks, kas drīkst mainīt vai dzēst ierakstus, ir šaurs un nosaukts.** Dokuments

Pēc kā to var atpazīt: Žurnāla datu tiesību koncepcija ar vārdisku piesaisti, pārsūtīšanas konfigurācija uz atsevišķu žurnalēšanas sistēmu, glabāšanas termiņi un pārbaudes pierādījums, ka parasts operators nevar dzēst ierakstus. Mazi uzņēmumi žurnālus pārsūta uz atsevišķu ierīci, kurā iekārtas operatoriem nav rakstīšanas tiesību. Prasīts no SL 2.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 3.9 RE 1 **Ar drošību saistītie ieraksti papildus tiek glabāti datu nesējā, kas izslēdz vēlāku pārrakstīšanu, tāpēc jau ierakstīts ieraksts vairs nav maināms, arī ar administratora tiesībām ne.** Dokuments

Pēc kā to var atpazīt: Izmantotās krātuves apraksts (vienreiz rakstāms datu nesējs, pret izmaiņām noturīgs arhīvs, nepārtraukti papildināta parakstu ķēde), pierādījums par neveiksmīgu mēģinājumu mainīt ierakstu un noteikums par to, kā datu nesēji tiek glabāti un atgūti. Prasības paplašinājums, prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

8 FR 4: Datu konfidencialitāte 6

SR 4.1 **Automatizācijas sistēma aizsargā konfidenciālu informāciju pret nepilnvarotu izpaušanu gan pārraides laikā, gan glabāšanas laikā. Ir noteikts, kuri dati ir konfidenciāli, piemēram, receptes, parametru kopas, piekļuves dati, konfigurācijas faili vai diagnostikas dati ar saikni uz personu.** Dokuments

Pēc kā to var atpazīt: Aizsargājamo datu veidu saraksts ar norādi, kur tie tiek glabāti un kā tie tiek pārraidīti, kā arī konkrētais aizsardzības pasākums katram ierakstam, piemēram, šifrēts savienojums, šifrēts datu nesējs vai ierobežota koplietošanas mape. Mazs uzņēmums iztiek ar vienas lappuses tabulu: datu veids, kur tie atrodas, kas tos drīkst redzēt, kas tos aizsargā. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 4.1 RE 1 **Informācijai, kas ceļo pa neuzticamiem tīkliem vai tiek glabāta ārpus aizsargātās vides, konfidencialitāte ir nodrošināta ar tehniskiem līdzekļiem, nevis tikai apsolīta organizatoriskā noteikumā.**

Pēc kā to var atpazīt: Izmantotās pārraides šifrēšanas vai glabāšanas šifrēšanas konfigurācijas izraksts, piemēram, attālinātās apkopes VPN profils, vadības sistēmas saskarnes TLS iestatījumi vai rezerves kopiju datu nesēju šifrēšana. Kā pierādījums pietiek ar aktīvā iestatījuma ekrānuzņēmumu, kuram norādīts datums. Prasīts no SL 2, nevis no SL 1, jo šis ir prasības paplašinājums.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 4.1 RE 2 **Konfidencialitāte ir nodrošināta arī uz robežām starp zonām, tāpēc informācija nekļūst atklāti redzama, kad tā pāriet no vienas zonas uz otru.**

Pēc kā to var atpazīt: Zonu un savienojumu plāns ar atzīmi, kuras šķērsošanas vietas ir šifrētas, kopā ar robežkomponenta konfigurāciju, tādu kā vārteja, ugunsmūris vai datu diode. Datplūsmas ieraksts vai pārbaudes ieraksts, kas parāda, ka uz robežas neparādās atklāta teksta dati. Prasīts no SL 4.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 4.2 **Ir noteikts, kā konfidenciāla informācija tiek droši dzēsta, kad ierīces tiek izņemtas no ekspluatācijas, maina īpašnieku, nonāk remontā vai tiek izmantotas atkārtoti, tā ka nepaliek nolasāmi atlikuma dati.** Dokuments

Pēc kā to var atpazīt: Rakstiska izņemšanas no ekspluatācijas procedūra ar dzēšanas metodi katram ierīces veidam, kā arī dzēšanas ieraksti, kuros norādīta ierīces identifikācija, datums un persona, kas to veica. Mazs uzņēmums to reģistrē kā vienu rindu katrai ierīcei kopīgā sarakstā un tur klāt glabā ārējo utilizācijas uzņēmumu apliecinājumus. Prasīts no SL 2.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 4.2 RE 1 **Koplietotie atmiņas apgabali tiek attīrīti, pirms tie tiek piešķirti citam lietotājam vai procesam, tāpēc iepriekšējā lietotāja saturs nav nolasāms.**

Pēc kā to var atpazīt: Piegādātāja apliecinājums vai konfigurācijas ieraksts par atkārtoti izmantotās atmiņas un bufera apgabalu attīrīšanu, papildināts ar pārbaudes ierakstu no pieņemšanas pārbaudes vai apkopes. Kur komponents to nespēj, kā pierādījums kalpo dokumentēts kompensējošais pasākums, piemēram, ierīci nelieto kopīgi dažādās lomās. Prasīts no SL 3, nevis no SL 1, jo šis ir prasības paplašinājums.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 4.3 **Visur, kur izmanto kriptogrāfiju, algoritmi, atslēgu garumi un rīcība ar atslēgām atbilst atzītai labai praksei, un ir noteikts, kā atslēgas tiek ģenerētas, izplatītas, glabātas, nomainītas un atsauktas.** Dokuments

Pēc kā to var atpazīt: Pārskats par katrā sistēmā izmantotajiem mehānismiem ar algoritmu, atslēgas garumu un derīguma termiņu, kā arī atslēgu pārvaldības noteikumi un ieraksti par atslēgu nomaiņām un sertifikātu atjaunošanām. Par mērauklu kalpo publiskas rekomendācijas, piemēram, Vācijas BSI tehniskās vadlīnijas. Mazs uzņēmums uztur sertifikātu sarakstu ar derīguma beigu datumiem un atgādinājumu >= 30 dienas pirms termiņa beigām. Prasīts no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

9 FR 5: Ierobežota datu plūsma, zonas un savienojumi 11

SR 5.1 **Vadības sistēma ir sadalāma atsevišķās zonās, un datplūsma starp šīm zonām iet tikai caur noteiktiem savienojumiem. Sadalījums seko izskaidrojamam pamatojumam, piemēram, pēc aizsardzības vajadzības, piederības vai iesaistīto iekārtas daļu funkcijas.** Dokuments

Pēc kā to var atpazīt: Tīkla shēma ar zonām un savienojumiem starp tām, zonu saraksts ar pamatojumu katrai robežai un atdalošo komponentu konfigurācija, tāda kā VLAN definīcijas vai ugunsmūra saskarnes. Mazam uzņēmumam pietiek ar vienas lappuses skici, kurā birojs, iekārtu tīkls un attālinātā piekļuve attēloti kā trīs lodziņi ar saitēm starp tiem, kā arī ar komutatora VLAN konfigurācijas ekrānuzņēmumu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.1 RE 1 **Zonu atdalīšana ir īstenota fiziski, proti, ar atsevišķiem tīkla komponentiem un atsevišķu kabelējumu, un tā nebalstās tikai uz loģisku konfigurāciju koplietotās ierīcēs. Šā saraksta 9.1. sadaļa, prasīts no SL 2. Šā standarta prasību paplašinājumi nekad nav obligāti jau SL 1 līmenī.**

Pēc kā to var atpazīt: Tīkla komponentu uzskaite ar norādi, kurš komutators vai maršrutētājs apkalpo kuru zonu, fotoattēli vai skapja izkārtojums atdalītajiem sadalījumiem, kabeļu marķējums. Mazi uzņēmumi to pierāda ar diviem atsevišķiem, skaidri marķētiem komutatoriem viena koplietota aparāta vietā un ar vadības skapja fotoattēlu iekārtas dokumentācijā.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.1 RE 2 **Automatizācijas tīkls ir darbināms neatkarīgi no tīkliem ārpus automatizācijas. Ja biroja informācijas tehnoloģijas vai ārējs savienojums atsaka, iekārtas vadība un uzraudzība turpina darboties. Prasīts no SL 3.**

Pēc kā to var atpazīt: Automatizācijas tīklā izmantoto pakalpojumu atkarību saraksts, tādu kā laika serveris, nosaukumu izšķiršana, direktoriju pakalpojums vai licenču serveris, ar norādi, kur katrs no tiem darbojas, kopā ar pārbaudes ierakstu par atvienošanas mēģinājumu, kurā saite uz biroja informācijas tehnoloģijām tika atvienota. Mazs uzņēmums šāda mēģinājuma iznākumu atzīmē apkopes žurnālā: augšupsaite atvienota, iekārta turpināja darboties, trūka tikai biroja atskaišu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.1 RE 3 **Zonas ar īpaši kritiskām funkcijām, piemēram, drošuma vai aizsardzības funkcijām, ir atdalītas no pārējām zonām gan loģiski, gan fiziski. Prasīts no SL 4.**

Pēc kā to var atpazīt: Kritisko zonu atzīmēšana zonu shēmā ar klasifikācijas pamatojumu, pierādījums par atsevišķiem tīkla komponentiem un atsevišķu kabelējumu šīm zonām, savienojumu konfigurācija ar pierādījumu, ka kopīgs ceļš nepastāv.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.2 **Uz zonu robežām datplūsma tiek kontrolēta, uzraudzīta un atbilstoši noteiktiem noteikumiem vai nu atļauta, vai liegta. Starp divām zonām nav ceļa, kas apietu šo kontroles punktu.**

Pēc kā to var atpazīt: Ugunsmūra vai robežierīces eksportētā noteikumu kopa, žurnāli par liegtiem un atļautiem savienojumiem, pierādījums, ka blakusceļi nepastāv, piemēram, ar pārbaudi par papildu tīkla kartēm, modemiem vai mobilo sakaru maršrutētājiem iekārtu datoros. Mazs uzņēmums to pierāda ar sava vienīgā ugunsmūra noteikumu eksportu un īsu apgaitas piezīmi, kas apstiprina, ka nevienā vadības skapī nav neplānota maršrutētāja.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.2 RE 1 **Noteikumu kopa uz zonas robežas darbojas pēc principa, ka viss ir liegts, ja vien tas nav nepārprotami atļauts. Katrs atļaujas noteikums ir atsevišķi pamatots un piesaistīts mērķim. Prasīts no SL 2.**

Pēc kā to var atpazīt: Noteikumu kopa ar redzamu noslēdzošo noteikumu, kas atmet pārējo, un atļauju saraksts, kurā katram noteikumam norādīts avots, mērķis, pakalpojums, nolūks un atbildīgā persona. Mazi uzņēmumi šo sarakstu uztur kā piecu kolonnu tabulu blakus ugunsmūra eksportam un reizi gadā pārskata, vai nav noteikumu, kas vairs nevienam nav vajadzīgi.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.2 RE 2 **Automatizācijas tīklu ir iespējams apzināti atdalīt no visiem ārējiem savienojumiem un turpināt darbināt salas režīmā. Šo darbību ir iespējams izraisīt, neapturot iekārtu. Prasīts no SL 3.**

Pēc kā to var atpazīt: Atdalīšanas procedūras apraksts ar norādi, kas un kā to drīkst izraisīt, pierādījums par tehnisko īstenojumu, tādu kā ārkārtas noteikumu kopa vai marķēts atdalīšanas slēdzis, kā arī ieraksts par mācībām, kurās atdalīšana tika patiešām izmēģināta. Mazs uzņēmums mācības veic reizi gadā apkopes laikā un atzīmē datumu, ilgumu un visu neparasto.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.2 RE 3 **Ja ierīce uz zonas robežas atsaka vai zaudē savus noteikumus, tā liedz datplūsmu, nevis to laiž cauri. Pēc kļūmes nepaliek atvērts savienojums. Prasīts no SL 4.**

Pēc kā to var atpazīt: Piegādātāja apliecinājums vai konfigurācijas pierādījums par to, kā komponents uzvedas kļūmes un atkārtotas palaišanas gadījumā, pārbaudes ieraksts par apzināti izraisītu kļūmi ar novēroto rezultātu, saskaņošana ar iekārtas riska novērtēšanu, jo robeža, kas liedz datplūsmu, atkarībā no procesa pati var radīt sekas.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.3 **Vispārējus saziņas pakalpojumus starp cilvēkiem, tādus kā elektroniskais pasts, ziņapmaiņa vai videozvani, ir iespējams liegt automatizācijas ierīcēs un automatizācijas tīklos. Lieguma tvērums ir noteikts un pamatots.**

Pēc kā to var atpazīt: Noteikums par to, kuri pakalpojumi automatizācijas tīklā nav atļauti, kā arī tehniskais īstenojums: bloķētas pieslēgvietas un mērķi noteikumu kopā, noņemtas vai bloķētas lietotnes operatora darba vietās, pierādījums no ierīču programmatūras uzskaites. Mazs uzņēmums to atrisina ar lietotņu bloķēšanu HMI darbstacijā un ar noteikumu, ka izejošs pasts un tīmekļa datplūsma no iekārtu tīkla ir liegta.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.3 RE 1 **Šādi saziņas pakalpojumi starp cilvēkiem ir liegti visā automatizācijas tīklā, nevis tikai daļēji ierobežoti vai attiecināti uz atsevišķām ierīcēm. Prasīts no SL 2.**

Pēc kā to var atpazīt: Pierādījums, ka liegums attiecas uz katru zonas ierīci, piemēram, ar zonā esošo datoru uzstādītās programmatūras pārskatīšanu un savienojuma pārbaudi no patvaļīgi izvēlēta iekārtas datora. Mazi uzņēmumi to pierāda ar ierīču sarakstu, kurā katra rinda ir atzīmēta ar pārbaudes datumu, un ar neveiksmīgā savienojuma mēģinājuma ekrānuzņēmumu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 5.4 **Lietotņu dati un lietotņu funkcijas ir sadalīti tā, ka procesi ar atšķirīgu aizsardzības vajadzību vai atšķirīgām tiesībām nevar sasniegt vienus un tos pašus apgabalus. Nodalījums ir iestrādāts sistēmas arhitektūrā un nav atstāts uzstādīšanas nejaušībai.**

Pēc kā to var atpazīt: Lietotņu pārskats ar norādi, kurus datus un pakalpojumus tās izmanto un kuri konti aiz tām stāv, atsevišķu instanču, datubāzu, direktoriju vai virtuālo mašīnu konfigurācija un tiesību saraksts katram apgabalam. Mazs uzņēmums to atrisina ar atsevišķiem lietotāju kontiem un atsevišķām datu mapēm inženierijai un darbināšanai, kā arī ar piezīmi par to, kura lietotne kurai mapei piekļūst.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

10 FR 6: Savlaicīga reakcija uz notikumiem 3

SR 6.1 **Sistēmā apkopotos audita ierakstus var lasīt un novērtēt personas un lomas, kas tam ir pilnvarotas, netraucējot iekārtas darbību, un piekļuve šiem ierakstiem pati ir ierobežota līdz pilnvarotiem lietotājiem.**

Pēc kā to var atpazīt: Lomu un atļauju matrica, kas parāda, kas drīkst skatīt žurnāla datus, kā arī patiešām izgūta žurnāla skata ekrānuzņēmums vai eksports ar laika zīmogu. Papildus īsa piezīme par izgūšanai izmantoto ceļu, piemēram, kontrollera operatora saskarne, žurnālu serveris vai failu eksports. Maziem uzņēmumiem pietiek ar vienas lappuses pārskatu katrai iekārtai: kur žurnāls atrodas, kam ir lasīšanas piekļuve, kā to izgūst. Pārbaudes izgūšana reizi gadā, kas atzīmēta apkopes žurnālā, parāda, ka ceļš darbojas. Attiecas no SL 1 uz visiem drošības līmeņiem.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 6.1 RE 1 **Audita ierakstus ir iespējams izgūt caur mašīnas saskarni, tāpēc analīzes rīki tos var apstrādāt tālāk bez manuālas pārrakstīšanas, un dati tiek sniegti dokumentētā, plaši izmantotā formātā.**

Pēc kā to var atpazīt: Izmantotās saskarnes apraksts kopā ar formātu, piemēram, syslog, OPC UA Alarms and Conditions, REST vaicājums vai CSV eksports, kā arī ieraksta paraugs un saņemošās sistēmas konfigurācija. Pierādījums var būt izraksts no SIEM vai žurnālu savācēja konfigurācijas kopā ar apliecinājumu par ienākošajiem ierakstiem. Bez SIEM pietiek ar žurnālu savācēju uz vienkārša servera, kas ar skriptu naktī izgūst žurnālus un tos saglabā. Pierādījums ir pats skripts un savākto failu mapes saraksts. Kā paplašinājums tas ir prasīts tikai no SL 3, nevis no SL 1.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 6.2 **Ar drošību saistītā darbība sistēmā tiek uzraudzīta nepārtraukti, uzraudzība atklāj uzbrukumu mēģinājumus un ļaunprātīgu izmantošanu un nekavējoties ziņo par tiem nosauktam kontaktpunktam, un tam izmantotie rīki, ziņošanas ceļi un atbildības ir noteikti.**

Pēc kā to var atpazīt: Uzraudzības rīku pārskats katrai zonai, piemēram, tīkla sensors, pretvīrusu brīdinājumi, ugunsmūra trauksmes vai integritātes pārbaude, ar norādi, kas saņem brīdinājumu un kādā laikā tiek gaidīta reakcija. Kā pierādījums kalpo trauksmju konfigurācijas, pēdējos mēnešos izdoto brīdinājumu saraksts un piezīmes par to apstrādi. Maziem uzņēmumiem nav vajadzīga visu diennakti apkalpota vadības telpa: pietiek ar kopīgu pastkasti vai pieteikumu iesūtni, kas apkopo esošo sistēmu brīdinājumus, un ar noteiktu kārtību, ka nosaukta persona to pārskata katrā darba dienā, un to pierāda pastkastes vēsture. Prasīts no SL 2.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

11 FR 7: Resursu pieejamība 13

SR 7.1 **Pārslodzes vai apzinātu pārplūdināšanas uzbrukumu apstākļos sistēma paliek noteiktā darba stāvoklī, būtiskās vadības funkcijas turpina darboties, un atsevišķa pakalpojuma atteice nerauj sev līdzi iekārtu.**

Pēc kā to var atpazīt: Aizsardzības mehānismu konfigurācija (ātruma ierobežošana, savienojumu ierobežojumi, apraides vētras kontrole komutatoros), piegādātāja apliecinājumi par uzvedību slodzes apstākļos, kā arī ieraksts par slodzes pārbaudi vai par īstu pārslodzes notikumu ar vadības funkcijas novērojumu. Prasīts no SL 1. Mazs uzņēmums to nosedz ar komutatora un ugunsmūra iestatījumu ekrānuzņēmumiem un ar īsu piezīmi par to, kura funkcija turpināja darboties svarīgākās šūnas pārbaudes laikā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 7.1 RE 1 **Sakaru slodze, ko atsevišķi komponenti var ievadīt tīklā, ir ierobežota, tāpēc bojāts vai pārņemts komponents nevar pārplūdināt tīkla segmentu.**

Pēc kā to var atpazīt: Joslas platuma un daudzadresu pārraides ierobežojumi katrai pieslēgvietai tīkla komponentos, pierādījums par ierobežojumu katram savienojumam, kā arī faktiskās pamatslodzes mērījums katrai ierīcei. Prasīts no SL 2, nevis no SL 1. Bez pārvaldāmiem komutatoriem šo rindu nav iespējams pierādīt, un tas tad ir atklātais punkts.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 7.1 RE 2 **Pārslodzes situācija aplūkojamās sistēmas iekšienē nepārsviežas uz blakus esošām sistēmām vai tīkliem, ietekme uz āru ir tehniski ierobežota.**

Pēc kā to var atpazīt: Segmentēšanas un filtrēšanas noteikumi uz robežām, pierādījums, ka izejošā datplūsma ir ierobežota, kā arī pārbaudes ieraksts, kas parāda, ka šūnas tīklā radītā slodze nepasliktināja biroja vai kaimiņu tīklu. Prasīts no SL 3.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 7.2 **Apstrādes laika, operatīvās atmiņas, krātuves vietas un tīkla joslas platuma izmantošana ir ierobežota tā, ka atsevišķs process vai pakalpojums nevar patērēt vadībai nepieciešamos resursus.**

Pēc kā to var atpazīt: Resursu ierobežojumu konfigurācija (kvotas, procesu prioritātes, atmiņas ierobežojumi), noslodzes uzraudzības novērtējums par reprezentatīvu laika posmu, kā arī sliekšņi, pie kuriem tiek izdots brīdinājums. Prasīts no SL 1. Mazi uzņēmumi izmanto operētājsistēmas iebūvētos līdzekļus un vienkāršu uzraudzību ar brīdinājumu par diska vietu un procesora noslodzi pa elektronisko pastu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 7.3 **Sistēmas konfigurācijām, lietotņu datiem un programmu versijām pastāv rezerves kopijas, tās ir izveidojamas, nepārtraucot darbību, un ir aizsargātas pret nepilnvarotu piekļuvi un izmaiņām.** Dokuments

Pēc kā to var atpazīt: Rezerves kopēšanas koncepcija ar tvērumu, biežumu un glabāšanas termiņu, pēdējo izpilžu rezerves kopēšanas žurnāli, kā arī pierādījums par rezerves kopiju datu nesēju piekļuves aizsardzību (atsevišķa glabāšana, šifrēšana, atsevišķas atļaujas). Prasīts no SL 1. Mazs uzņēmums PLC projektus un HMI versijas kopē uz šifrētu datu nesēju, ko pēc kopēšanas fiziski atvieno, un datumu un versiju reģistrē vienkāršā sarakstā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR 7.3 RE 1 **Rezerves kopiju izmantojamība ir pārbaudīta, un ir pierādīts, ka no tām patiešām ir atjaunojams darbspējīgs stāvoklis.**

Pēc kā to var atpazīt: Ieraksts par atjaunošanas mēģinājumu ar datumu, pārbaudīto rezerves kopijas versiju, mērķa sistēmu un rezultātu, vismaz kritiskajiem komponentiem. Prasīts no SL 2, nevis no SL 1. Mazi uzņēmumi reizi gadā izlases veidā pārbauda vienu PLC programmu un vienu HMI attēlu uz rezerves ierīces un rezultātu pieraksta divos teikumos.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.3 RE 2 **Rezerves kopēšana notiek automātiski pēc noteikta grafika, neizdevusies izpilde tiek atklāta un par to tiek ziņots.**

Pēc kā to var atpazīt: Rezerves kopēšanas uzdevuma grafiks, izpildes žurnāli bez robiem, kā arī pierādījums par kļūmes paziņojumu izpildei, kas neizdevās (trauksme, pieteikums, pasts). Prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.4 **Pēc traucējuma, atteices vai uzbrukuma sistēmu ir iespējams atgriezt zināmā, drošā stāvoklī, atjaunošana ir izmēģināta un atbildības ir nosauktas.** Dokuments

Pēc kā to var atpazīt: Atkārtotas palaišanas plāns katram kritiskajam komponentam ar secību, nepieciešamajiem datu nesējiem, kontaktiem un mērķa laiku, kopā ar ierakstu par pēdējām atjaunošanas mācībām. Prasīts no SL 1. Mazam uzņēmumam pietiek ar vienas lappuses atkārtotas palaišanas karti katrai līnijai, ko glabā vadības skapī un pārbauda ikreiz, kad tiek nomainīta rezerves daļa.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.5 **Ja parastā elektroapgāde atsaka, sistēma pāriet noteiktā stāvoklī: vai nu apgādi uztur rezerves avots, vai notiek sakārtota apturēšana, nezaudējot drošo stāvokli.**

Pēc kā to var atpazīt: Nepārtrauktās barošanas avota vai ārkārtas ģeneratora jaudas aprēķina un apkopes pierādījumi, pēdējās akumulatora vai slodzes pārbaudes ieraksts, kā arī apraksts par uzvedību pārslēgšanās brīdī un tīkla sprieguma atgriešanās brīdī. Prasīts no SL 1. Mazi uzņēmumi nepārtrauktās barošanas avotu reizi gadā pārbauda ar slodzi un pieraksta pārbaudes datumu, pārtraukuma pārvarēšanas laiku un akumulatora vecumu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.6 **Sistēmas tīkla un drošības iestatījumi ir noteikti apstiprinātā mērķa stāvoklī, novirzes no šī mērķa stāvokļa ir atklājamas, un pašreizējais stāvoklis ir izgūstams jebkurā laikā.** Dokuments

Pēc kā to var atpazīt: Apstiprināta mērķa konfigurācija katrai ierīču klasei (nostiprināšanas specifikācija), ierīču pašreizējie konfigurācijas stāvokļi, kā arī mērķa un faktiskā stāvokļa salīdzinājuma rezultāts ar noviržu sarakstu un iemeslu katrai no tām. Prasīts no SL 1. Mazs uzņēmums konfigurācijas eksportus glabā versiju kontrolē un salīdzina tos pirms katras izmaiņas un pēc tās.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.6 RE 1 **Drošības iestatījumu pašreizējais stāvoklis ir izvadāms mašīnlasāmā veidā, tāpēc to var automātiski salīdzināt ar mērķa stāvokli.**

Pēc kā to var atpazīt: Izvades paraugs mašīnlasāmā formātā (konfigurācijas eksports, strukturēts fails, saskarnes vaicājums) un skripts vai rīks, kas veic salīdzinājumu ar mērķa stāvokli, kopā ar vienas izpildes rezultātu atskaiti. Prasīts no SL 3.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.7 **Sistēma ir ierobežota līdz darbībai nepieciešamajām funkcijām, nevajadzīgie pakalpojumi, pieslēgvietas, protokoli un saskarnes ir atspējoti vai noņemti.**

Pēc kā to var atpazīt: Aktīvo pakalpojumu un atvērto pieslēgvietu saraksts katram komponentam ar vajadzības pamatojumu, pierādījums, ka pārējās ir atspējotas (konfigurācija, pieslēgvietu skenēšanas rezultāts), kā arī noteikums par USB un apkopes saskarnēm. Prasīts no SL 1. Mazi uzņēmumi veic vienkāršu pieslēgvietu skenēšanu katram segmentam un pamato katru atvērto punktu vienā rindā.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SR 7.8 **Ir pieejama aktuāla visu sistēmas komponentu uzskaite ar ražotāju, tipu, aparātprogrammatūras vai programmatūras versiju un tīkla adresi, un tā tiek uzturēta aktuāla, kad notiek izmaiņas.**

Dokuments

Pēc kā to var atpazīt: Komponentu uzskaite ar pārskatīšanas datumu un īpašnieku, pierādījums par uzturēšanu ar izmaiņu vēsturi, kā arī salīdzinājums ar tīkla apzināšanu, lai atrastu ierīces, kas nav reģistrētas. Prasīts no SL 2, nevis no SL 1. Mazs uzņēmums uzskaiti uztur kā tabulu un kā stingru noteikumu to atjaunina ikreiz, kad tiek nomainīta ierīce un kad tiek atjaunināta aparātprogrammatūra.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums