IEC 62443-3-3:2013 Pramoninio automatizavimo sistemų saugumo reikalavimai

Septyni pagrindiniai reikalavimai, 51 sistemos reikalavimas

100 reikalavimai. Pagal šį standartą galima sertifikuotis akredituotoje sertifikavimo įstaigoje. Redakcija 07/2026.

Pagal IEC 62443-3-3 galima sertifikuoti, o sertifikuojama yra sistema, ne organizacija ir ne asmuo. Keliai yra ISASecure SSA ir IECEE CB Scheme. Kas nori sertifikuoti organizaciją, tam reikia 62443-2-1 arba 2-4, o kas kalba apie komponentą, tam reikia 62443-4-2. Šiame sąraše yra 51 sistemos reikalavimas ir 49 reikalavimų išplėtimai. Kurie iš jų taikomi, priklauso nuo siekiamo saugumo lygio: nuo SL 1 jų yra 38, nuo SL 2 jų yra 60, nuo SL 3 jų yra 90, o SL 4 lygiu visi 100. Nė vienas išplėtimas nėra reikalaujamas jau SL 1 lygiu. Šis sąrašas yra darbo priemonė savikontrolei, o ne įrodymas.

Įmonė	Data	Pildė

5 FR 1: kas arba kokia programa ar įrenginys prašo prieigos ir ar tai tikrai tas, kuo prisistato 24

SR 1.1 **Naudotojai žmonės yra atpažįstami ir jų tapatybė patvirtinama prieš suteikiant prieigą, kiekviename taške, kuriame galima valdyti ar konfigūruoti automatizavimo sistemą. Tai apima operatoriaus pultus prie mašinos, inžinerinę prieigą ir tinklo paslaugas.**

Iš ko tai galima atpažinti: Visų sistemos prisijungimo taškų sąrašas, tai yra HMI, valdymo patalpa, PLC programavimo prieiga, komutatorius, VPN ir nuotolinės priežiūros klientas, kiekvienas su ten naudojamu autentifikavimo mechanizmu. Prie kiekvienos įrenginių klasės pridedamas konfigūracijos išrašas arba prisijungimo lango ekrano nuotrauka. Maža įmonė pradeda nuo vienos lentelės kiekvienam įrenginiui, stulpeliai: įrenginys, sąsaja, autentifikavimas taip ar ne, pagrindimas, jei ne. Reikalaujama nuo SL 1.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.1 RE 1 **Kiekvienas naudotojas žmogus dirba su asmeniniu identifikatoriumi, priskirtu tik tam asmeniui. Bendros ir pamainos paskyros yra išjungtos, likusios išimtys pagrindžiamos kiekviena atskirai ir paremiamos papildomomis priemonėmis.**

Iš ko tai galima atpažinti: Kiekvienos sistemos paskyrų eksportas, kuriame identifikatorius susietas su asmeniu, išimčių sąrašas su pagrindimu ir kompensuojamąja priemone, pavyzdžiui kamera arba buvimo žurnalas prie operatoriaus darbo vietos. Ši eilutė yra reikalavimo išplėtimas, todėl SL 1 lygiu niekada nereikalaujama, ji reikalaujama nuo SL 2.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.1 RE 2 **Kiekvienas, kuris jungiasi iš nepatikimo tinklo, pavyzdžiui iš interneto arba per nuotolinės priežiūros ryšį, savo tapatybę įrodo bent dviem nepriklausomais veiksniais.**

Iš ko tai galima atpažinti: Nuotolinės prieigos konfigūracija su įjungtu antruoju veiksniu, pavyzdinis prisijungimo įrašas, kuriame matomi abu veiksniai, ir išduotų atpažinties raktų arba programėlių registracijų sąrašas. Maža įmonė naudoja esamo VPN sietuvo antrąjį veiksnį arba autentifikavimo programėlę, o tai nekainuoja nieko, išskyrus nustatymo laiką. Reikalavimo išplėtimas, reikalaujamas nuo SL 3, o SL 1 lygiu nereikalaujamas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.1 RE 3 **Įrodymas dviem nepriklausomais veiksniais taikomas ne tik prieigai iš išorės, bet ir kiekvienam naudotojo žmogaus prisijungimui, įskaitant prisijungimus tinkle, kuris priskirtas patikimiems.**

Iš ko tai galima atpažinti: Centrinės autentifikavimo tarnybos politikos išrašas, rodantis, kad antrasis veiksnys taikomas be jokios tinklo išimties, ir pavyzdiniai prisijungimo įrašai iš valdymo patalpos ir operatoriaus pulto. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.2 **Ne tik žmonės, bet ir programinės įrangos procesai bei įrenginiai autentifikuojasi sistemoje, prieš gaudami leidimą keistis duomenimis ar naudotis paslaugomis. Tai apima valdiklių tarpusavio sujungimus, duomenų ryšius su aukštesnio lygio sistemomis ir diagnostikos priemones.**

Iš ko tai galima atpažinti: Mašinų tarpusavio ryšių sąrašas su šaltiniu, paskirties tašku, protokolu ir kiekvienu atveju naudojamais prisijungimo duomenimis, pavyzdžiui sertifikatu, tarnybine paskyra arba iš anksto bendrintu raktu. Pridedamas vieno sujungimo konfigūracijos išrašas, kuriame matomas autentifikavimas. Reikalaujama nuo SL 2, o SL 1 lygiu nereikalaujama.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.2 RE 1 **Kiekvienas programinės įrangos procesas ir kiekvienas įrenginys pateikia savo unikalų identifikatorių. Bendros tarnybinės paskyros arba vienas raktas, naudojamas visoje sistemoje daugelyje įrenginių, neleidžiami.** Dokumentas

Iš ko tai galima atpažinti: Įrenginių susiejimas su identifikatoriumi arba sertifikato serijos numeriu, rodantis, kad nė vienas identifikatorius nepasikartoja. Reikalavimo išplėtimas, reikalaujamas nuo SL 3, todėl SL 1 lygiui nepriklauso.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.3 **Paskyros valdomos per visą jų būvio ciklą: sukūrimas, teisių keitimas, išjungimas išeinant iš darbo ir pašalinimas yra reglamentuoti taisyklėmis ir palaikomi susijusių sistemų. Tai apima naudotojų paskyras, tarnybines paskyras ir avarines paskyras.** Dokumentas

Iš ko tai galima atpažinti: Paskyrų registras su tipu, savininku, paskirtimi ir būsena, taip pat įrodymas dėl priimtų ir išėjusių darbuotojų, pavyzdžiui pasirašytas perdavimas arba registruota užklausa, rodanti išjungimą su data. Pravartu reguliariai peržiūrėti paskyras, o mažoje įmonėje pakanka kartą per metus sutikrinti paskyrų sąrašą su personalo sąrašu. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.3 RE 1 **Paskyrų valdymas yra suvienodintas visuose sistemos komponentuose, kad paskyros išjungimas vienoje vietoje neliktų neveiksmingas atskiruose įrenginiuose.**

Iš ko tai galima atpažinti: Centrinio katalogo integracijos įrodymas, pavyzdžiui katalogų tarnyba arba RADIUS, su prijungtų komponentų sąrašu ir aiškiu sąrašu įrenginių, kurių prijungti negalima, kartu su jiems taikoma alternatyvia procedūra. Bandymo įrašas apie išjungimą, kuris įsigalioja visose prijungtose sistemose. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.4 **Identifikatoriai išduodami pagal nustatytas taisykles, vienareikšmiškai priskiriami asmeniui, įrenginiui arba vaidmeniui, nebenaudojami yra išimami iš apyvartos ir niekada vėliau neišduodami kitam turėtojui.**

Iš ko tai galima atpažinti: Identifikatorių sudarymo taisyklė, pavyzdžiui pavardė ir vardo raidė arba gamyklos kodas ir numeris, taip pat išimtų identifikatorių istorija, rodanti, kad jie nenaudojami pakartotinai. Maža įmonė veda vieną nuoseklų sąrašą su išdavimo ir išėmimo data. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.5 **Autentifikavimo priemonės, tokios kaip slaptažodžiai, raktai, sertifikatai ir atpažinties raktai, išduodamos tvarkingai, keičiamos įtarus atskleidimą ir atšaukiamos, kai reikia. Numatytosios paskyros ir gamykliniai slaptažodžiai, kokie gauti su preke, pakeičiami prieš atiduodant eksploatuoti.**

Iš ko tai galima atpažinti: Išduotų atpažinties raktų ir sertifikatų sąrašas su gavėju ir data, pakeitimų ir atšaukimų įrodymas, taip pat kiekvieno įrenginio atidavimo eksploatuoti kontrolinis sąrašas su pasirašytu punktu apie pakeistą gamyklinį slaptažodį. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.5 RE 1 **Programinės įrangos procesų prisijungimo duomenys laikomi ne kaip skaitoma byla laikmenoje, o aparatinės įrangos saugomoje atmintyje, kuri neleidžia nuskaityti slaptosios dalies.**

Iš ko tai galima atpažinti: Naudojamo saugumo komponento tipo įrodymas, pavyzdžiui TPM, saugusis elementas arba HSM, su konfigūracijos išrašu, patvirtinančiu, kad raktas laikomas komponento viduje. Kaip tipo įrodymas pakanka pirkimo įrašo arba techninių duomenų lapo. Reikalavimo išplėtimas, reikalaujamas nuo SL 3, o SL 1 ir SL 2 lygiais nereikalaujamas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.6 **Belaidė prieiga prie sistemos, pavyzdžiui WLAN, radijo bangomis valdomi nuotoliniai pultai arba Bluetooth diagnostika, naudojama tik nustačius ir autentifikavus ir naudotoją, ir įrenginį, ir yra sąmoningai valdoma.**

Iš ko tai galima atpažinti: Visų belaidžių ryšių sąrašas su paskirtimi, veikimo nuotoliu ir šifravimo būdu, prieigos taško konfigūracijos išrašas ir patvirtintų galinių įrenginių sąrašas. Maža įmonė papildomai dokumentuoja, kurios įrenginių belaidės sąsajos yra sąmoningai išjungtos. Reikalaujama nuo SL 1.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.6 RE 1 **Kiekviena belaidė prieiga yra priskiriama vienam konkrečiam naudotojui arba vienam konkrečiam įrenginiui, bendro tinklo rakto visiems dalyviams nepakanka.**

Iš ko tai galima atpažinti: Metodo su asmeniniais prisijungimo duomenimis įrodymas, pavyzdžiui įmonės WLAN autentifikavimas kataloge arba atskiro įrenginio sertifikatai, taip pat ryšio žurnalas, kuriame matomas asmeninis identifikatorius. Reikalavimo išplėtimas, reikalaujamas nuo SL 2, todėl SL 1 lygiu netaikomas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.7 **Ten, kur naudojami slaptažodžiai, jų mažiausias stiprumas yra konfigūruojamas, pavyzdžiui mažiausias ilgis ir reikalaujami ženklų tipai, o nustatytos vertės galioja visoms susijusioms paskyroms.**

Iš ko tai galima atpažinti: Kiekvienos sistemos slaptažodžių politikos konfigūracijos išrašas su faktiškai nustatytomis vertėmis, pavyzdžiui ilgis >= 10 ženklų ir bent trys ženklų tipai, taip pat sąrašas sistemų, kurios techniškai negali palaikyti šio nustatymo, kartu su jų kompensuojamąja priemone. Reikalaujama nuo SL 1.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.7 RE 1 **Naudotojams žmonėms slaptažodžių sudarymą ir galiojimo trukmę reglamentuoja papildomos taisyklės: ankstesnių slaptažodžių pakartotinis naudojimas užkardomas, o galiojimas ribojamas laike.**

Iš ko tai galima atpažinti: Konfigūracijos išrašas, rodantis slaptažodžių istoriją, pavyzdžiui užblokuotą paskutinių penkių slaptažodžių pakartotinį naudojimą, ir nustatytą ilgiausią galiojimo trukmę. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.7 RE 2 **Slaptažodžio galiojimo trukmės ribojimas taikomas ne tik žmonėms, bet ir visoms paskyroms, įskaitant tarnybines, priežiūros ir įrenginių paskyras.**

Iš ko tai galima atpažinti: Techninių paskyrų keitimo planas su paskutine ir kita kiekvienos paskyros keitimo data, taip pat pakeitimų įrodymas, pavyzdžiui pakeitimo įrašas arba registruota užklausa. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.8 **Ten, kur naudojami sertifikatai, jie gaunami iš tvarkingo sertifikatų valdymo su nustatytomis prašymo, išdavimo, galiojimo trukmės, atnaujinimo ir atšaukimo taisyklėmis.** Dokumentas

Iš ko tai galima atpažinti: Sertifikatų politika arba trumpa rašytinė taisyklė, nurodanti atsakomybę, galiojimo trukmes ir atšaukimo kelią, taip pat išduotų sertifikatų sąrašas su galiojimo pabaigos datomis. Maža įmonė veda lentelę su sertifikatu, įrenginiu, galiojimo pabaigos data ir priminimo data, o tai apsaugo nuo tylių gamyklos prastovų dėl pasibaigusių sertifikatų. Reikalaujama nuo SL 2.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 1.9 **Kai autentifikavimui naudojamos raktų poros, sistema visapusiškai patikrina sertifikatą: pasitikėjimo grandinę, galiojimo trukmę, atšaukimo būseną ir įrodymą, kad kita pusė iš tikrųjų valdo privatųjį raktą. Sertifikato ir paskyros sąsaja yra vienareikšmė.**

Iš ko tai galima atpažinti: Konfigūracijos išrašas su įjungtu atšaukimo tikrinimu, pavyzdžiui CRL arba OCSP, bandymo įrašas apie atmestą prisijungimą su pasibaigusiu arba atšauktu sertifikatu, taip pat sertifikatų ir paskyrų susiejimo lentelė. Reikalaujama nuo SL 3, o SL 1 ir SL 2 lygiais nereikalaujama.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.9 RE 1 **Privatieji raktai laikomi tik aparatinės įrangos saugomoje atmintyje, iš kurios jų nuskaityti negalima, ir naudojami taip pat tos atminties viduje.**

Iš ko tai galima atpažinti: Naudojamo saugumo komponento techninių duomenų lapas arba sertifikavimo įrodymas ir konfigūracijos išrašas, rodantis, kad raktas sukuriamas komponento viduje, todėl privatusis raktas jo niekada nepalieka. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.10 **Prisijungimo metu sistema neatskleidžia informacijos, kuria būtų galima pasinaudoti. Įvedami slaptažodžiai paslepiami, o klaidų pranešimai neatskleidžia, ar buvo neteisingas identifikatorius, ar slaptažodis.**

Iš ko tai galima atpažinti: Prisijungimo lango ekrano nuotrauka su paslėpta įvestimi ir klaidos pranešimo po nepavykusio bandymo ekrano nuotrauka. Prie įrenginių, kurie techniškai to negali, pavyzdžiui senesnių operatoriaus pultų, pridedamas trumpas paaiškinimas apie kompensuojamąją priemonę, pavyzdžiui apribotą fizinę prieigą prie įrengimo vietos. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.11 **Iš eilės einančių nepavykusių prisijungimo bandymų skaičius yra ribojamas, o atsakas į juos konfigūruojamas, pavyzdžiui laikinas užblokavimas. Pasirinktas atsakas netrukdo su sauga susijusiam gamyklos veikimui.**

Iš ko tai galima atpažinti: Konfigūracijos išrašas su riba, pavyzdžiui užblokavimas po <= 5 nepavykusių bandymų, ir užblokavimo trukmė, taip pat trumpas įvertinimas, kodėl užblokavimas netrukdo avariniam veikimui ar saugiam gamyklos išjungimui. Operatoriaus darbo vietose su saugos funkcija laikinas užblokavimas yra tinkamesnis už nuolatinį paskyros užrakinimą. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.12 **Prieš prisijungimą galima rodyti naudojimo pranešimą, nurodantį sistemos naudojimo ir stebėsenos taisykles. Tekstą ir rodymą turto savininkas gali konfigūruoti.**

Iš ko tai galima atpažinti: Rodomo pranešimo teksto ekrano nuotrauka ir patvirtinta formuluotė su patvirtinimo data. Mažos įmonės formuluotę trumpai suderina su darbuotojų atstovais arba su vadovybe, pakanka vienos pastraipos. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.13 **Prieiga iš nepatikimų tinklų, pavyzdžiui tiekėjų nuotolinė priežiūra, apribota nustatytais keliais, yra stebima ir bet kada gali būti nutraukiama.**

Iš ko tai galima atpažinti: Nuotolinės prieigos kelių sąrašas su paskirtimi, nuotoline šalimi, kontaktiniu asmeniu ir naudojamu keliu, taip pat ryšio žurnalai ir įrodymas apie galimybę atjungti, pavyzdžiui rakto jungiklis, užkardos taisyklė arba išjungiamas nuotolinės priežiūros maršruto parinktuvas. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 1.13 RE 1 **Kiekvieną atskirą seansą iš nepatikimo tinklo prieš užmezgant ryšį aiškiai patvirtina atsakingas asmuo, nuolat atviro ryšio nepakanka.**

Iš ko tai galima atpažinti: Kiekvieno nuotolinės priežiūros seanso patvirtinimo įrašai su laiku, priežastimi, patvirtinančiu asmeniu ir trukme, techniškai, pavyzdžiui, per rakto jungiklį prie prieigos maršruto parinktuvo arba per patvirtinimo portalą. Mažoje įmonėje pakanka nuotolinės priežiūros žurnalo prie valdymo spintos, kurį prie kiekvieno seanso pasirašo priežiūros technikas. Reikalavimo išplėtimas, reikalaujamas nuo SL 2, todėl SL 1 lygiu niekada netaikomas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

6 FR 2: naudojimo valdymas (teisės, seansai, audito įrašai) 24

SR 2.1 **Sistema techniškai įgyvendina suteiktas teises: kiekvienas prisijungęs asmuo, kiekvienas įrenginys ir kiekvienas programinės įrangos procesas gauna būtent jam priskirtą prieigą, o kiekvienas bandymas peržengti šią ribą atmetamas.**

Iš ko tai galima atpažinti: Teisių schema, siejanti paskyras su leidimais, taip pat kiekvienos valdymo sistemos, HMI ir inžinerinės darbo vietos ekrano nuotrauka arba konfigūracijos išrašas su galiojančiomis teisėmis. Papildomai bandymo įrašas, kuriame mažas teises turinti paskyra bando atlikti uždraustą veiksmą ir yra atmetama. Reikalaujama nuo SL 1. Mažai įmonei pakanka dviejų ar trijų vaidmenų, pavyzdžiui valdyti, prižiūrėti, projektuoti, ir jie dokumentuojami viename puslapyje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.1 RE 1 **Teisių įgyvendinimas taikomas ne tik operatoriams žmonėms, bet lygiai taip pat programinės įrangos procesams ir įrenginiams, kurie prie sistemos jungiasi savarankiškai.**

Iš ko tai galima atpažinti: Techninių ir tarnybinių paskyrų sąrašas, pavyzdžiui OPC UA klientai, duomenų archyvo ryšiai, atsarginių kopijų tarnybos, kiekviena su jai priskirtu teisių rinkiniu. Teisių valdymo išrašas, rodantis, kad šios paskyros neveikia administratoriaus teisėmis. Reikalavimo išplėtimas, reikalaujamas nuo SL 2, o SL 1 lygiu ne.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.1 RE 2 **Teisės suteikiamos ne pavieniams asmenims po vieną, o per vaidmenis, o vaidmens ir leidžiamų veiksmų sąsaja registruojama atsekamai.** Dokumentas

Iš ko tai galima atpažinti: Vaidmenų ir teisių matrica kaip lentelė: eilutės yra vaidmenys, stulpeliai veiksmai, tokie kaip keisti nustatytąją vertę, įkelti programą, patvirtinti pavojaus signalą, sukurti paskyrą. Taip pat asmenų ir vaidmenų susiejimo sąrašas. Reikalavimo išplėtimas, reikalaujamas nuo SL 2. Kaip įrodymo visiškai pakanka prižiūrimos skaičiuoklės su pakeitimo data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.1 RE 3 **Siaurai apibrėžtais išimtiniais atvejais įgaliotas vadovaujantis asmuo gali ribotam laikui panaikinti teisių apribojimą, o kiekvienas toks panaikinimas registruojamas audito įrašuose.**

Iš ko tai galima atpažinti: Išimties patvirtinimo procedūros aprašas, nurodantis, kas gali ją suteikti ir kiek laiko ji galioja, taip pat jau suteiktų panaikinimų audito įrašai iš sistemos žurnalo. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.1 RE 4 **Ypač svarbiems įsikišimams prieš atliekant veiksmą reikia dviejų nepriklausomų įgaliotų asmenų patvirtinimo.**

Iš ko tai galima atpažinti: Veiksmų, kuriems taikomas dvigubas patvirtinimas, sąrašas, pavyzdžiui saugos parametrų keitimas arba naujos valdymo programos įkėlimas, kartu su konfigūracijos įrodymu ir audito įrašais, kuriuose įvardyti abu tvirtintojai. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.2 **Belaidžių ryšių naudojimas automatizavimo tinkle susietas su aiškiu leidimu, o duomenimis keistis ar įsikišti belaidžiu ryšiu gali tik patvirtinti dalyviai.**

Iš ko tai galima atpažinti: Visų belaidžių ryšių sąrašas, pavyzdžiui WLAN prieigos taškai, Bluetooth poravimai, mobiliojo ryšio maršruto parinktuvai, kiekvienas su savo paskirtimi ir patvirtintais dalyviais. Taip pat prieigos valdymo konfigūracija prieigos taške. Reikalaujama nuo SL 1. Kas proceso tinkle neturi jokio belaidžio ryšio, tas būtent tai užrašo raštu ir paremia konfigūracijos vaizdu, kuriame matyti išjungtas belaidis ryšys.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.2 RE 1 **Neteisėti belaidžiai įrenginiai automatizavimo tinklo aplinkoje yra aptinkami ir apie juos pranešama.**

Iš ko tai galima atpažinti: Belaidžio ryšio stebėsenos įrašas arba reguliaraus belaidžio ryšio nuskaitymo įrašas su data, rezultatų sąrašu ir pastaba apie kiekvieną nežinomą įrenginį. Įvardytas pranešimo kelias atsakingam padaliniui. Reikalavimo išplėtimas, reikalaujamas nuo SL 2, o SL 1 lygiu ne. Maža įmonė gali kas ketvirtį atlikti nuskaitymą nešiojamuoju kompiuteriu ir rezultatą įsegti kaip įrašą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.3 **Nešiojamųjų ir mobiliųjų įrenginių naudojimas sistemoje, pavyzdžiui priežiūros nešiojamųjų kompiuterių, USB laikmenų ar planšečių, reglamentuotas taisyklėmis ir techniškai apribotas aiškiai patvirtintais įrenginiais.**

Iš ko tai galima atpažinti: Įrenginių naudojimo taisyklių rinkinys, patvirtintų priežiūros įrenginių sąrašas su jų identifikatoriais ir techninio apribojimo įrodymas, pavyzdžiui išjungti arba tik konkrečiais įrenginiais apriboti USB prievadai HMI ir inžinerinėje darbo vietoje. Reikalaujama nuo SL 1. Maža įmonė dirba su dviem paženklintomis priežiūros atmintinėmis, į kurias rašoma tik vienoje perdavimo vietoje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.3 RE 1 **Prieš prijungiant patikrinama nešiojamojo arba mobiliojo įrenginio saugumo būsena, o reikalavimų neatitinkantiems įrenginiams prieiga neleidžiama.**

Iš ko tai galima atpažinti: Įrenginio būsenos tikrinimo kriterijai, pavyzdžiui esama apsauga nuo kenkėjiškos programinės įrangos ir pataisų lygis, taip pat kiekvieno priežiūros įrenginio tikrinimo įrašai ir techninio įgyvendinimo įrodymas, pavyzdžiui per perdavimo vietą arba tinklo prieigos valdymą. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.4 **Mobiliajam kodui, vykdomam sistemoje, pavyzdžiui operatoriaus sąsajų scenarijams arba aktyviam ataskaitų turiniui, yra nustatyta, kurie tipai leidžiami, o neleidžiamų tipų vykdymas užkardomas.** Dokumentas

Iš ko tai galima atpažinti: Nustatymas, koks mobilusis kodas leidžiamas kuriose sistemose, taip pat apribojimo konfigūracijos įrodymas, pavyzdžiui išjungtas scenarijų vykdymas HMI naršyklėje, užblokuotos makrokomandos vertinimo bylose. Reikalaujama nuo SL 1. Pakanka vieno puslapio nustatymo, apimančio tris ar keturis iš tikrųjų esančius atvejus.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.4 RE 1 **Prieš vykdant mobiliųjį kodą patikrinama, ar jis gautas iš laukiamo šaltinio ir ar nebuvo pakeistas.**

Iš ko tai galima atpažinti: Parašo tikrinimo arba kontrolinės sumos tikrinimo konfigūracijos įrodymas, taip pat bandymo įrašas, kuriame pakeistas arba nepasirašytas kodas atmetamas. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.5 **Seansas užrakinamas po nustatyto laiko be operatoriaus veiksmų ir atrakinamas tik pakartotinai autentifikavus, neprarandant su sauga susijusios proceso informacijos rodymo.**

Iš ko tai galima atpažinti: Konfigūracijos išrašas su kiekvienai darbo vietai nustatytu užrakinimo laiku, taip pat pagrindimas dėl darbo vietų nuolat prižiūrimose valdymo patalpose, kuriose užrakinimas sąmoningai nustatytas kitaip. Reikalaujama nuo SL 1. Vaizdinis įrodymas: užrakinto ekrano nuotrauka, kurioje toliau matoma pavojaus signalų eilutė.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.6 **Nuotoliniai seansai nutraukiami po nustatyto neveiklumo laiko arba operatoriui pareikalavus, kad neliktų be priežiūros atviro nuotolinio ryšio.**

Iš ko tai galima atpažinti: Nuotolinės prieigos konfigūracija su neveiklumo laiko riba, nutrauktų nuotolinių seansų audito įrašai ir aprašas, kaip operatorius gali nedelsdamas atjungti vykstantį nuotolinės priežiūros seansą, pavyzdžiui rakto jungikliu arba atskiro seanso leidimu. Reikalaujama nuo SL 2, o SL 1 lygiu ne.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.7 **Vienu metu vykstančių seansų skaičius vienai paskyrai ar vaidmeniui yra ribojamas, o šią ribą viršijantys prisijungimo bandymai atmetami.**

Iš ko tai galima atpažinti: Konfigūracijos išrašas su nustatyta viršutine riba kiekvienam vaidmeniui, pavyzdžiui <= 1 vienu metu vykstantis seansas inžinerinėms paskyroms, taip pat bandymo įrašas apie atmestą antrąjį prisijungimo bandymą. Reikalaujama nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.8 **Su saugumu susiję įvykiai registruojami, o kiekviename įraše nurodomas bent laikas, šaltinis, veiksmą sukėlusi paskyra, įvykio tipas ir rezultatas.** Dokumentas

Iš ko tai galima atpažinti: Registruotinų įvykių tipų nustatymas, pavyzdžiui prisijungimas, nepavykęs prisijungimas, teisių pakeitimas, programos pakeitimas, konfigūracijos pakeitimas, taip pat tikras audito žurnalo išrašas su įvardytais laukais. Reikalaujama nuo SL 1. Maža įmonė surenka valdymo sistemos, HMI ir užkardos žurnalus į vieną aplanką su nustatytu saugojimo laikotarpiu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.8 RE 1 **Atskirų komponentų audito įrašai sujungiami vienoje centrinėje vietoje ir sudaro vientisą visos sistemos įrašą, vertinamą kaip visuma.**

Iš ko tai galima atpažinti: Žurnalų surinkimo architektūros eskizas su visais prijungtais šaltiniais, taip pat vertinimas, kuriame bent dviejų komponentų įvykiai sudėti į vieną laiko ašį. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.9 **Audito įrašams skirta pakankamai saugojimo vietos, kad įvykiai išliktų visą nustatytą saugojimo laikotarpį ir nebūtų netyčia perrašyti.**

Iš ko tai galima atpažinti: Saugojimo vietos poreikio skaičiavimas arba įvertis iš dienos žurnalų apimties, padaugintos iš saugojimo laikotarpio, taip pat nustatytas saugojimo vietos dydis ir archyvavimo taisyklė. Reikalaujama nuo SL 1. Praktikoje pakanka kasdienės kopijos į atskirą saugojimo vietą su dokumentuotu saugojimo laikotarpiu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.9 RE 1 **Pasiekus nustatytą audito saugojimo vietos užpildymo ribą, atsakingam padaliniui pateikiamas įspėjimas dar prieš visiškai išnaudojant jos talpą.**

Iš ko tai galima atpažinti: Ribos konfigūracijos išrašas, pavyzdžiui įspėjimas nuo >= 80 procentų užimtumo, taip pat suveikusio pranešimo pavyzdys ir gavėjų sąrašas. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.10 **Jei audito registravimas sutrinka arba audito saugojimo vieta prisipildo, sistema reaguoja iš anksto nustatytu būdu, o atsakingas padalinys informuojamas, nekeliant pavojaus saugiam gamyklos veikimui.**

Iš ko tai galima atpažinti: Kiekvienam sutrikimo atvejui nustatyta reakcija, pavyzdžiui perrašyti senesnius įrašus ir pateikti pranešimą, užuot stabdžius gamyklą, su pagrindimu iš proceso pusės. Įrodymas per suveikusį bandomąjį pranešimą ir atitinkamą audito įrašą. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.11 **Kiekviename audito įraše yra laiko žyma iš įvardyto laiko šaltinio, kad skirtingų komponentų įvykius būtų galima išdėstyti tarpusavio eilės tvarka.**

Iš ko tai galima atpažinti: Kiekviename komponente naudojamo laiko šaltinio nurodymas ir žurnalo išrašas su matoma laiko žyma, įskaitant laiko juostą. Reikalaujama nuo SL 2, o SL 1 lygiu ne.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.11 RE 1 **Visų dalyvaujančių komponentų laikrodžiai sinchronizuojami pagal bendrą laiko šaltinį, kad nuokrypis neviršytų nustatytos ribos.**

Iš ko tai galima atpažinti: Laiko sinchronizavimo konfigūracija, pavyzdžiui NTP serveris ir sinchronizavimo intervalas, taip pat patikros įrašas su išmatuotu kiekvieno komponento nuokrypiu, palygintu su nustatyta riba, pavyzdžiui <= 1 sekundė. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.11 RE 2 **Pats laiko šaltinis apsaugotas nuo klastojimo, o netikėtina ar pakeista laiko nuoroda aptinkama ir apie ją pranešama.**

Iš ko tai galima atpažinti: Aprašas, kaip apsaugotas laiko šaltinis, pavyzdžiui autentifikuotas laiko sinchronizavimas, apribojimas iki vidinio šaltinio, laiko šuolių stebėsena, taip pat pranešimai arba audito įrašai apie aptiktą nuokrypį. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.12 **Nustatytų svarbių veiksmų atveju vėliau be abejonių nustatoma, kas juos atliko, todėl veikęs asmuo negali įtikinamai to neigti.** Dokumentas

Iš ko tai galima atpažinti: Veiksmų, kuriems taikomas šis įrodymas, sąrašas, pavyzdžiui receptūros keitimas, partijos išleidimas, ribinių verčių keitimas, taip pat atitinkami įrašai su unikaliu asmens identifikatoriumi ir įrodymas, kad šiems veiksmams grupinės paskyros netaikomos. Reikalaujama nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 2.12 RE 1 **Neginčijamas veikusio asmens priskyrimas taikomas ne tik pasirinktiems svarbiems veiksmams, bet visiems naudotojams ir visiems jų atliekamiems veiksmams.**

Iš ko tai galima atpažinti: Įrodymas, kad kiekviena paskyra susieta su vienu asmeniu ir kad neliko bendrų prisijungimų, taip pat bet kokių veiksmų žurnalo išrašas, kuriame visur matomas unikalus asmens identifikatorius. Reikalavimo išplėtimas, reikalaujamas tik nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

7 FR 3: sistemos vientisumas, duomenų, programinės įrangos ir seansų apsauga nuo neteisėto keitimo 19

SR 3.1 **Valdymo sistema aptinka, kai informacija buvo pakeista perduodant ją ryšio kanalu, ir tai daro tiek su valdymo duomenimis, tiek su konfigūracijos duomenimis, tiek su administravimo srautu. Apsauga apima ir ryšius, kurie išeina iš sistemos arba kerta nepatikimus tinklo segmentus.**

Iš ko tai galima atpažinti: Tinklo ir protokolų apžvalga, nurodanti, kuris kanalas naudoja kurį vientisumo mechanizmą (kontrolinę sumą, pranešimo autentiškumo kodą, pasirašytas telegramas), lauko magistralės arba OPC UA saugumo nustatymų konfigūracijos išrašas ir bandymo įrašas, rodantis, kad suklastota telegrama buvo įrodomai atmesta. Maža įmonė tai surašo į lentelę kiekvienam ryšiui su stulpeliais šaltinis, paskirties taškas, protokolas ir vientisumo mechanizmas, o rezultatyvumą vieną kartą įrodo srauto įrašu. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.1 RE 1 **Vientisumo apsauga perdavimo metu remiasi kriptografiniais mechanizmais, kad tyčinis užpuoliko klastojimas savomis priemonėmis nepraeitų neaptiktas. Paprastos kontrolinės sumos nuo perdavimo klaidų čia nepakanka.**

Iš ko tai galima atpažinti: Kiekviename kanale naudojamų kriptografinių mechanizmų ir raktų ilgių sąrašas, nuoroda į juos pagrindžiantį raktų valdymą ir konfigūracijos išrašai (pavyzdžiui TLS šifrų rinkiniai, OPC UA SecurityPolicy, IPsec profiliai). Mažos įmonės remiasi saugiais numatytaisiais savo valdiklių profiliais ir įsega veikiančio nustatymo ekrano nuotrauką. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.2 **Sistemoje veikia apsaugos nuo kenkėjiško kodo mechanizmai, kurie neleidžia nepageidaujamam programos kodui vykdytis sistemos komponentuose ir praneša apie kiekvieną aptikimą. Mechanizmai parinkti taip, kad netrikdytų numatyto gamyklos veikimo, ir yra nuolat atnaujinami.**

Iš ko tai galima atpažinti: Kiekvieno komponento apžvalga, kuris mechanizmas taikomas (antivirusinė programa, leidžiamų programų sąrašas, sugriežtinta operacinė sistema be vykdymo teisių), įrodymas, kad parašai arba leidžiamų programų sąrašai atnaujinami, ir apsaugos sistemos įspėjimai. Kur antivirusinė programa neįmanoma, pavyzdžiui valdiklyje, kompensuojamoji priemonė užrašoma kartu su pagrindimu. Mažoms įmonėms gerai tinka leidžiamų programų sąrašas operatoriaus kompiuteryje ir rašytinė USB laikmenų taisyklė. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.2 RE 1 **Apsauga nuo kenkėjiško kodo papildomai veikia gamyklos įėjimo ir išėjimo taškuose, kuriuose duomenys patenka arba išeina, o ne tik pačiuose galiniuose įrenginiuose.**

Iš ko tai galima atpažinti: Visų įėjimo ir išėjimo taškų sąrašas (nuotolinės priežiūros prieiga, duomenų perdavimo sietuvas, keičiamosios laikmenos, perdavimas į biuro tinklą, elektroninio pašto kelias programų versijoms) su kiekviename jų veikiančiu tikrinimo mechanizmu, taip pat patikrintų perdavimų įrašai. Mažos įmonės įrengia vieną perdavimo kompiuterį su virusų tikrinimu kaip sietuvą ir tai įtvirtina darbo instrukcijoje. Reikalavimo išplėtimas, reikalaujamas nuo SL 2.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.2 RE 2 **Apsaugos nuo kenkėjiško kodo mechanizmai valdomi iš vienos centrinės vietos, atnaujinimai platinami centralizuotai, o aptikimai vertinimui renkami vienoje vietoje.**

Iš ko tai galima atpažinti: Centrinio valdymo pulto konfigūracija, ataskaita apie visų prijungtų komponentų atnaujinimo būseną ir per tam tikrą laikotarpį praneštų aptikimų vertinimas. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.3 **Sistemos saugumo funkcijos tikrinamos suplanuotais intervalais ir po pakeitimų, kad būtų patvirtinta, jog jos iš tikrųjų veikia. Bandymai planuojami taip, kad nekeltų pavojaus gamyklos veikimui, o rezultatai registruojami.** Dokumentas

Iš ko tai galima atpažinti: Bandymų planas, nurodantis bandymo objektą, intervalą ir laiko langą, kartu su bandymų įrašais, rodančiais datą, bandytoją, laukiamą ir stebėtą elgseną. Naudingi atskiri bandymai yra: prisijungimas su išjungta paskyra nepavyksta, antivirusinė programa reaguoja į bandomąją bylą, nuotolinės priežiūros prieiga be leidimo nepasiekiama. Mažos įmonės bandymus pririša prie ir taip planuojamo priežiūros sustabdymo ir punktas po punkto pereina nustatytą kontrolinį sąrašą. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.3 RE 1 **Saugumo funkcijų tikrinimas vyksta automatinėmis priemonėmis, todėl jis pakartojamas be rankų darbo ir duoda nuoseklų rezultatą.**

Iš ko tai galima atpažinti: Scenarijai arba bandymų priemonės kartu su jų tvarkaraščiu, jų išvesties bylos ir kelių paleidimų palyginimas, rodantis, kad nuokrypiai aptinkami. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.3 RE 2 **Saugumo funkcijų tikrinimas galimas ir įprasto veikimo metu, nesustabdant gamyklos ir neperjungiant jos į ypatingą būseną.**

Iš ko tai galima atpažinti: Bandymo procedūros aprašas su įrodymu, kad ji neturi neigiamo poveikio procesui, pavyzdžiui poveikio ciklo laikams ir tinklo apkrovai analizė, taip pat bandymų įrašai iš gamybinio veikimo. Reikalavimo išplėtimas, reikalaujamas nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.4 **Neteisėti programinės įrangos, programinės aparatinės įrangos ir saugomos informacijos pakeitimai aptinkami. Tai vienodai taikoma valdymo programoms, parametrų rinkiniams, receptūroms ir konfigūracijos byloms.**

Iš ko tai galima atpažinti: Saugotinų versijų sąrašas su išsaugotomis kontrolinėmis vertėmis arba parašais, vientisumo palyginimų rezultatai ir dokumentuotas sutikrinimas su versijų valdymo sistemoje esančia versija. Mažos įmonės išleistą programos versiją kartu su jos kontroline suma laiko nuo rašymo apsaugotoje vietoje ir palygina kilus įtarimui arba po priežiūros darbų. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.4 RE 1 **Aptikus programinės įrangos ar informacijos vientisumo pažeidimą, sistema apie tai automatiškai praneša atsakingai vietai, ir niekam nereikia to aktyviai ieškoti.**

Iš ko tai galima atpažinti: Pranešimo kelių konfigūracija (pavojaus signalas valdymo patalpoje, elektroninis paštas, žinutė stebėsenos sistemai), gavėjų sąrašas su pavadavimo tvarka ir bent vienas bandomasis pavojaus signalas su dokumentuotu atsako laiku. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.5 **Įvestys, kurias sistema priima iš proceso duomenų, sąsajų ar naudotojo sąsajų, prieš apdorojimą tikrinamos dėl leidžiamos sintaksės, leidžiamos verčių srities ir leidžiamo ilgio. Netinkamos įvestys nesukelia nevaldomos elgsenos.**

Iš ko tai galima atpažinti: Kiekvienos įvesties ribų ir formatų specifikacija, valdiklio arba programos tikrinimo logikos išrašai ir testavimo atvejai su sąmoningai netinkamomis įvestimis (per didelė vertė, netinkamas duomenų tipas, per ilga ženklų eilutė) kartu su dokumentuota sistemos elgsena. Mažos įmonės tikėtinumo ribas kiekvienam matavimo taškui surašo į lentelę ir patikrina atiduodamos eksploatuoti. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.6 **Sutrikimo atvejui yra nustatyta, kokią būseną įgyja išėjimai į gamyklą, ir sistema įgyja būtent tą būseną. Nustatyta būsena suderinta su gamyklos funkcine sauga.**

Iš ko tai galima atpažinti: Kiekvieno išėjimo arba išėjimų grupės nustatymas (vertės išlaikymas, nustatyta pakaitinė vertė, saugaus išjungimo būsena) su pagrindimu iš rizikos vertinimo, valdiklio konfigūracijos išrašas ir sutrikimo bandymo įrodymas, pavyzdžiui kabelio nutrūkimo arba ryšio praradimo, rodantis laukiamą elgseną. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.7 **Sistema tvarko klaidų būsenas taip, kad veikimas liktų valdomas ir nebūtų atskleista informacija, galinti padėti užpuolikui. Operatoriams rodomi klaidų pranešimai lieka trumpi, o techninės smulkmenos patenka tik į vidinius įrašus.**

Iš ko tai galima atpažinti: Klaidų klasių apžvalga su kiekvienai numatyta sistemos elgsena, rodomų pranešimų pavyzdžiai, palyginti su atitinkamais vidinio žurnalo įrašais, ir bandymų įrodymas, kad operatoriaus sąsajoje nesimato bylų kelių, paskyrų vardų, duomenų bazės išvesties ar versijų smulkmenų. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.8 **Aktyvūs seansai apsaugoti nuo perėmimo ir nuo svetimų pranešimų įterpimo. Seansas baigiasi atsijungus arba praėjus nustatytam neveiklumo laikui, ir po to jo pakartotinai naudoti negalima.**

Iš ko tai galima atpažinti: Seansų valdymo konfigūracija su nustatytomis neveiklumo laiko ir ilgiausios trukmės ribomis, mechanizmo, saugančio nuo pranešimų pakartojimo, įrodymas ir bandymo įrašas, kuriame perimtas seansas po atsijungimo nebeveikia. Reikalaujama nuo SL 2.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.8 RE 1 **Seansų identifikatoriai netenka galios pasibaigus seansui ir sistemos daugiau nepriimami, net jei pateikiami pakartotinai iš išorės.**

Iš ko tai galima atpažinti: Seansų valdymo konfigūracijos išrašas, apimantis galios panaikinimą, taip pat bandymo įrašas, kuriame anksčiau galiojęs identifikatorius po atsijungimo siunčiamas dar kartą ir sistemos atmetamas. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.8 RE 2 **Kiekvienam naujam seansui sukuriamas atskiras vienkartinis identifikatorius. Identifikatoriai pakartotinai nenaudojami nei skirtinguose seansuose, nei skirtingiems naudotojams, nei skirtingiems įrenginiams.**

Iš ko tai galima atpažinti: Sukūrimo procedūros aprašas ir įrodymas iš žurnalo arba srauto įrašo, kad keli iš eilės einantys prisijungimai gauna skirtingus identifikatorius. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.8 RE 3 **Seansų identifikatoriai kuriami pripažintais atsitiktinumo mechanizmais, todėl jų negalima nei atspėti, nei išvesti iš ankstesnių identifikatorių.**

Iš ko tai galima atpažinti: Naudojamo atsitiktinių skaičių generatoriaus ir jo entropijos šaltinio nurodymas, tiekėjo deklaracija arba bandymų ataskaita apie jį ir sukurtų identifikatorių imties statistinis vertinimas. Reikalavimo išplėtimas, reikalaujamas nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.9 **Su saugumu susiję įrašai ir jiems vertinti naudojamos priemonės apsaugoti nuo neteisėtos prieigos, keitimo ir trynimo. Asmenų, kuriems leidžiama keisti ar šalinti įrašus, ratas laikomas siauras ir yra įvardytas.** Dokumentas

Iš ko tai galima atpažinti: Žurnalų duomenų teisių schema su įvardytu priskyrimu, persiuntimo į atskirą įvykių registravimo sistemą konfigūracija, saugojimo laikotarpiai ir bandymų įrodymas, kad paprastas operatorius įrašų ištrinti negali. Mažos įmonės persiunčia žurnalus į atskirą įrenginį, kuriame gamyklos operatoriai rašymo teisių neturi. Reikalaujama nuo SL 2.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 3.9 RE 1 **Su saugumu susiję įrašai papildomai saugomi laikmenoje, kurioje vėlesnis perrašymas neįmanomas, todėl kartą įrašyto įrašo pakeisti nebegalima net administratoriaus teisėmis.** Dokumentas

Iš ko tai galima atpažinti: Naudojamos saugyklos aprašas (vienkartinio įrašymo laikmena, nuo klastojimo apsaugotas archyvas, nuolat pratęsiama parašų grandinė), nesėkmingo bandymo pakeisti įrašą įrodymas ir taisyklė, kaip laikmenos saugomos ir gaunamos. Reikalavimo išplėtimas, reikalaujamas nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8 FR 4: duomenų konfidencialumas 6

SR 4.1 **Automatizavimo sistema saugo konfidencialią informaciją nuo neteisėto atskleidimo tiek ją perduodant, tiek ją laikant. Yra nustatyta, kurie duomenys laikomi konfidencialiais, pavyzdžiui receptūros, parametrų rinkiniai, prisijungimo duomenys, konfigūracijos bylos arba su asmeniu susiję diagnostikos duomenys.** Dokumentas

Iš ko tai galima atpažinti: Saugotinų duomenų tipų sąrašas su nurodymu, kur jie laikomi ir kaip perduodami, taip pat konkreti kiekvieno įrašo apsaugos priemonė, pavyzdžiui šifruotas ryšys, šifruota laikmena arba apribota bendrinama sritis. Mažai įmonei pakanka vieno puslapio lentelės: duomenų tipas, kur jie yra, kas gali juos matyti, kas juos saugo. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 4.1 RE 1 **Informacijai, kuri keliauja per nepatikimus tinklus arba laikoma už apsaugotos aplinkos ribų, konfidencialumas užtikrinamas techninėmis priemonėmis, o ne vien pažadamas organizacine taisykle.**

Iš ko tai galima atpažinti: Naudojamo perdavimo šifravimo arba saugojimo šifravimo konfigūracijos išrašas, pavyzdžiui nuotolinės priežiūros VPN profilis, valdymo sistemos sąsajos TLS nustatymai arba atsarginių kopijų laikmenų šifravimas. Kaip įrodymo pakanka veikiančio nustatymo ekrano nuotraukos su data. Reikalaujama nuo SL 2, o nuo SL 1 ne, nes tai yra reikalavimo išplėtimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 4.1 RE 2 **Konfidencialumas užtikrinamas ir zonų ribose, kad informacija netaptų matoma atviru tekstu pereidama iš vienos zonos į kitą.**

Iš ko tai galima atpažinti: Zonų ir jungčių planas su pažymėtais šifruotais perėjimais kartu su ribinio komponento, tokio kaip sietuvas, užkarda ar duomenų diodas, konfigūracija. Srauto įrašas arba bandymo įrašas, rodantis, kad riboje nesimato atviro teksto duomenų. Reikalaujama nuo SL 4.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 4.2 **Yra nustatyta, kaip patikimai pašalinama konfidenciali informacija, kai įrenginiai nurašomi, keičia savininką, išvežami taisyti arba naudojami pakartotinai, kad neliktų skaitomų likusių duomenų.** Dokumentas

Iš ko tai galima atpažinti: Rašytinė nurašymo procedūra su kiekvieno įrenginio tipo duomenų naikinimo būdu, taip pat ištrynimo įrašai su įrenginio identifikavimu, data ir tai atlikusiu asmeniu. Maža įmonė tai užrašo po vieną eilutę kiekvienam įrenginiui bendrame sąraše ir šalia įsega išorės atliekų tvarkytojų pažymas. Reikalaujama nuo SL 2.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 4.2 RE 1 **Bendrai naudojamos atminties sritys išvalomos prieš perduodant jas kitam naudotojui ar procesui, kad ankstesniam naudotojui priklausiusio turinio nebūtų galima nuskaityti.**

Iš ko tai galima atpažinti: Gamintojo pareiškimas arba konfigūracijos įrašas apie pakartotinai naudojamos atminties ir buferių sričių išvalymą, papildytas priėmimo bandymų arba priežiūros darbų bandymo įrašu. Kur komponentas to negali, įrodymu tarnauja dokumentuota kompensuojamoji priemonė, pavyzdžiui to paties įrenginio nedalijimas skirtingiems vaidmenims. Reikalaujama nuo SL 3, o nuo SL 1 ne, nes tai yra reikalavimo išplėtimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 4.3 **Ten, kur naudojama kriptografija, algoritmai, raktų ilgiai ir raktų tvarkymas atitinka pripažintą gerąją praktiką, ir yra nustatyta, kaip raktai kuriami, platinami, saugomi, keičiami ir atšaukiami.** Dokumentas

Iš ko tai galima atpažinti: Kiekvienoje sistemoje naudojamų mechanizmų apžvalga su algoritmu, rakto ilgiu ir galiojimo trukme, taip pat raktų valdymo taisyklės ir raktų keitimo bei sertifikatų atnaujinimo įrašai. Matu tarnauja viešos rekomendacijos, pavyzdžiui Vokietijos BSI techninės gairės. Maža įmonė veda sertifikatų sąrašą su galiojimo pabaigos datomis ir priminimu >= 30 dienų prieš pabaigą. Reikalaujama nuo SL 1.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9 FR 5: apribotas duomenų srautas, zonos ir jungtys 11

SR 5.1 **Valdymo sistemą galima padalyti į atskiras zonas, o srautas tarp tų zonų eina tik per nustatytas jungtis. Padalijimas remiasi paaiškinamu pagrindimu, pavyzdžiui apsaugos poreikiu, nuosavybe arba susijusių gamyklos dalių funkcija.**

Dokumentas

Iš ko tai galima atpažinti: Tinklo schema su zonomis ir jungtimis tarp jų, zonų sąrašas su kiekvienos ribos pagrindimu ir skiriančių komponentų konfigūracija, tokia kaip VLAN aprašai ar užkardos sąsajos. Mažai įmonei pakanka vieno puslapio eskizo, kuriame biuras, mašinų tinklas ir nuotolinė prieiga pavaizduoti trimis langeliais su ryšiais tarp jų, taip pat komutatoriaus VLAN konfigūracijos ekrano nuotraukos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.1 RE 1 **Zonų atskyrimas įgyvendintas fiziškai, tai yra atskirais tinklo komponentais ir atskira kabeline sistema, ir remiasi ne vien logine konfigūracija bendrai naudojamų įrenginių viduje. Šio sąrašo 9.1 punktas, reikalaujama nuo SL 2. Šios normos reikalavimų išplėtimai niekada nėra reikalaujami jau nuo SL 1.**

Iš ko tai galima atpažinti: Tinklo komponentų sąrašas su nurodymu, kuris komutatorius ar maršruto parinktuvas aptarnauja kurią zoną, atskirtų skirstyklų nuotraukos arba spintos išdėstymas, kabelių ženklinimas. Mažos įmonės tai įrodo dviem atskirais, aiškiai paženklintais komutatoriais vietoj vieno bendro įrenginio ir valdymo spintos nuotrauka gamyklos dokumentuose.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.1 RE 2 **Automatizavimo tinklas gali veikti nepriklausomai nuo tinklų už automatizavimo ribų. Sutrikus biuro informacinėms technologijoms ar išoriniam ryšiui, gamyklos valdymas ir stebėsena veikia toliau. Reikalaujama nuo SL 3.**

Iš ko tai galima atpažinti: Automatizavimo tinkle naudojamų paslaugų priklausomybių sąrašas, tokių kaip laiko serveris, vardų sprendimas, katalogų tarnyba ar licencijų serveris, su nurodymu, kur kiekviena iš jų veikia, kartu su atjungimo bandymo įrašu, kuriame buvo ištrauktas ryšys su biuro informacinėmis technologijomis. Maža įmonė tokio bandymo rezultatą užsirašo priežiūros žurnale: ryšys ištrauktas, gamykla veikė toliau, trūko tik biuro ataskaitų.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.1 RE 3 **Zonos su ypač svarbiomis funkcijomis, pavyzdžiui saugos ar apsaugos funkcijomis, atskirtos nuo likusių zonų ir logiškai, ir fiziškai. Reikalaujama nuo SL 4.**

Iš ko tai galima atpažinti: Svarbių zonų pažymėjimas zonų schemoje su priskyrimo pagrindimu, atskirų tinklo komponentų ir atskiros kabelinės sistemos toms zonoms įrodymas, jungčių konfigūracija su įrodymu, kad bendro kelio nėra.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.2 **Zonų ribose srautas valdomas, stebimas ir pagal nustatytas taisykles leidžiamas arba draudžiamas. Tarp dviejų zonų nėra kelio, kuris apeitų šį kontrolės tašką.**

Iš ko tai galima atpažinti: Eksportuotas užkardos arba ribinio įrenginio taisyklių rinkinys, uždraustų ir leistų ryšių žurnalai, įrodymas, kad šalutinių kelių nėra, pavyzdžiui per papildomų tinklo plokščių, modemų ar mobiliojo ryšio maršruto parinktuvų patikrą gamyklos kompiuteriuose. Maža įmonė tai įrodo savo vienintelės užkardos taisyklių eksportu ir trumpu apžiūros užrašu, patvirtinančiu, kad nė vienoje valdymo spintoje nėra nenumatyto maršruto parinktuvo.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.2 RE 1 **Zonos riboje taisyklių rinkinys veikia pagal principą, kad draudžiama viskas, kas nėra aiškiai leista. Kiekviena leidžiamoji taisyklė pagrįsta atskirai ir susieta su paskirtimi. Reikalaujama nuo SL 2.**

Iš ko tai galima atpažinti: Taisyklių rinkinys su matoma baigiamąja taisykle, kuri atmeta visa kita, ir leidimų sąrašas su kiekvienos taisyklės šaltiniu, paskirties tašku, paslauga, paskirtimi ir atsakingu asmeniu. Mažos įmonės šį sąrašą veda kaip penkių stulpelių lentelę šalia užkardos eksporto ir kartą per metus peržiūri, ar nėra niekam nebereikalingų taisyklių.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 5.2 RE 2 **Automatizavimo tinklą galima sąmoningai atjungti nuo visų išorinių ryšių ir palikti veikti salos režimu. Šį veiksmą galima atlikti nesustabdant gamyklos. Reikalaujama nuo SL 3.**

Iš ko tai galima atpažinti: Atskyrimo procedūros aprašas su nurodymu, kas ir kaip gali ją pradėti, techninio įgyvendinimo įrodymas, toks kaip avarinis taisyklių rinkinys ar paženklintas atjungiklis, taip pat pratybų, kuriose atskyrimas buvo iš tikrųjų atliktas, įrašas. Maža įmonė pratybas rengia kartą per metus per priežiūros darbus ir užsirašo datą, trukmę ir viską, kas buvo neįprasta.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 5.2 RE 3 **Jei zonos riboje esantis įrenginys sutrinka arba praranda savo taisykles, jis srautą draudžia, o ne praleidžia. Sutrikimas nepalieka po savęs atviro ryšio. Reikalaujama nuo SL 4.**

Iš ko tai galima atpažinti: Tiekėjo pareiškimas arba konfigūracijos įrodymas, kaip komponentas elgiasi sutrikus ir paleidžiamas iš naujo, sąmoningai sukelto sutrikimo bandymo įrašas su stebėtu rezultatu, suderinimas su gamyklos rizikos vertinimu, nes srautą draudžianti riba, priklausomai nuo proceso, pati gali sukelti pasekmių.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 5.3 **Bendrąsias asmenų tarpusavio ryšio paslaugas, tokias kaip elektroninis paštas, žinutės ar vaizdo skambučiai, galima užkardyti automatizavimo įrenginiuose ir automatizavimo tinkluose. Draudimo apimtis yra nustatyta ir pagrįsta.**

Iš ko tai galima atpažinti: Nustatymas, kurios paslaugos automatizavimo tinkle neleidžiamos, taip pat techninis įgyvendinimas: užblokuoti prievadai ir paskirties taškai taisyklių rinkinyje, pašalintos arba užblokuotos programos operatoriaus darbo vietose, įrodymas iš įrenginių programinės įrangos sąrašo. Maža įmonė tai išsprendžia programų blokavimu HMI darbo vietoje ir taisykle, kad išeinantis pašto ir saityno srautas iš mašinų tinklo draudžiamas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 5.3 RE 1 **Tokios asmenų tarpusavio ryšio paslaugos užkardomos visame automatizavimo tinkle, o ne tik iš dalies apribojamos ar apribojamos atskiruose įrenginiuose. Reikalaujama nuo SL 2.**

Iš ko tai galima atpažinti: Įrodymas, kad draudimas taikomas kiekvienam zonos įrenginiui, pavyzdžiui per kiekviename zonos kompiuteryje įdiegtos programinės įrangos peržiūrą ir ryšio bandymą iš bet kurio gamyklos kompiuterio. Mažos įmonės tai įrodo įrenginių sąrašu, kuriame kiekviena eilutė pažymėta su patikros data, ir nepavykusio ryšio bandymo ekrano nuotrauka.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 5.4 **Programų duomenys ir programų funkcijos padalyti taip, kad skirtingo apsaugos poreikio ar skirtingų teisių procesai nepasiektų tų pačių sričių. Atskyrimas numatytas sistemos architektūroje, o ne paliktas įdiegimo atsitiktinumui.**

Iš ko tai galima atpažinti: Programų apžvalga su nurodymu, kuriuos duomenis ir paslaugas jos naudoja ir kurios paskyros už jų stovi, atskirų egzempliorių, duomenų bazių, katalogų ar virtualiųjų mašinų konfigūracija ir kiekvienos srities teisių sąrašas. Maža įmonė tai išsprendžia atskiromis naudotojų paskyromis ir atskirais duomenų aplankais projektavimui ir eksploatavimui, taip pat užrašu, kuri programa kurį aplanką pasiekia.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

10 FR 6: reagavimas į įvykius laiku 3

SR 6.1 **Sistemoje surinktus audito įrašus tam įgalioti asmenys ir vaidmenys gali skaityti ir vertinti netrikdydami vykstančio gamyklos darbo, o prieiga prie tų įrašų pati yra apribota įgaliotais naudotojais.**

Iš ko tai galima atpažinti: Vaidmenų ir leidimų matrica, rodanti, kas gali peržiūrėti žurnalų duomenis, taip pat iš tikrųjų gauto žurnalo vaizdo ekrano nuotrauka arba eksportas su laiko žyma. Pridedamas trumpas užrašas apie gavimo kelią, pavyzdžiui valdiklio operatoriaus sąsają, žurnalų serverį ar bylos eksportą. Mažoms įmonėms pakanka vieno puslapio apžvalgos kiekvienai gamyklai: kur yra žurnalas, kas gali jį skaityti, kaip jis paimamas. Kartą per metus atliktas bandomasis paėmimas, užrašytas priežiūros žurnale, parodo, kad kelias veikia. Taikoma nuo SL 1 visiems saugumo lygiams.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 6.1 RE 1 **Audito įrašus galima gauti per mašininę sąsają, kad analizės priemonės galėtų juos toliau apdoroti be rankinio perrašymo, o duomenys pateikiami dokumentuotu, plačiai naudojamu formatu.**

Iš ko tai galima atpažinti: Naudojamos sąsajos aprašas kartu su formatu, pavyzdžiui syslog, OPC UA Alarms and Conditions, REST užklausa ar CSV eksportas, taip pat pavyzdinis įrašas ir priimančiosios sistemos konfigūracija. Įrodymas gali būti SIEM arba žurnalų surinktuvo konfigūracijos išrašas kartu su gaunamų įrašų įrodymu. Be SIEM pakanka žurnalų surinktuvo paprastame serveryje, kuris per naktį scenarijumi surenka žurnalus ir juos išsaugo, o įrodymas yra pats scenarijus ir surinktų bylų katalogo sąrašas. Kaip išplėtimas tai reikalaujama tik nuo SL 3, o nuo SL 1 ne.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 6.2 **Su saugumu susijusi veikla sistemoje stebima nuolat, stebėsena aptinka bandymus užpulti ir piktnaudžiauti ir nedelsdama praneša apie juos įvardytam kontaktiniam asmeniui, o tam naudojamos priemonės, pranešimo keliai ir atsakomybės yra nustatytos.**

Iš ko tai galima atpažinti: Kiekvienos zonos stebėsenos priemonių apžvalga, pavyzdžiui tinklo jutiklis, antivirusinės programos įspėjimai, užkardos pavojaus signalai ar vientisumo tikrinimas, su nurodymu, kas gauna įspėjimą ir per kiek laiko laukiama atsako. Įrodymu tarnauja pavojaus signalų konfigūracijos, per pastaruosius mėnesius pateiktų įspėjimų sąrašas ir jų nagrinėjimo užrašai. Mažoms įmonėms nereikia visą parą veikiančios valdymo patalpos: pakanka bendros pašto dėžutės ar užklausų dėžutės, kurioje sutelkiami esamų sistemų įspėjimai, ir nustatytos taisyklės, kad įvardytas asmuo ją peržiūri kiekvieną darbo dieną, o tai įrodoma pašto dėžutės istorija. Reikalaujama nuo SL 2.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

11 FR 7: išteklių prieinamumas 13

SR 7.1 **Esant perkrovai ar tyčinėms užtvindymo atakoms sistema lieka nustatytoje veikimo būsenoje, esminės valdymo funkcijos veikia toliau, o atskiros paslaugos sutrikimas nenutraukia visos gamyklos darbo.**

Iš ko tai galima atpažinti: Apsaugos mechanizmų konfigūracija (srauto spartos ribojimas, ryšių skaičiaus ribos, transliavimo audrų valdymas komutatoriuose), gamintojo pareiškimai apie elgseną esant apkrovai, taip pat apkrovos bandymo arba tikro perkrovos įvykio įrašas su valdymo funkcijos stebėjimu. Reikalaujama nuo SL 1. Maža įmonė tai padengia komutatoriaus ir užkardos nustatymų ekrano nuotraukomis ir trumpu užrašu, kuri funkcija veikė toliau bandant svarbiausią gamybos ląstelę.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 7.1 RE 1 **Ryšio apkrova, kurią atskiri komponentai gali sukurti tinkle, yra apribota, kad sugedęs ar užvaldytas komponentas negalėtų užtvindyti tinklo segmento.**

Iš ko tai galima atpažinti: Kiekvieno prievado pralaidumo ir daugiaadresio siuntimo ribos tinklo komponentuose, kiekvieno ryšio ribojimo įrodymas, taip pat faktinės kiekvieno įrenginio bazinės apkrovos matavimas. Reikalaujama nuo SL 2, o nuo SL 1 ne. Be valdomų komutatorių šios eilutės įrodyti negalima, ir tada tai yra atviras klausimas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 7.1 RE 2 **Perkrovos padėtis nagrinėjamoje sistemoje nepersiduoda į gretimas sistemas ar tinklus, poveikis į išorę techniškai sulaikomas.**

Iš ko tai galima atpažinti: Segmentavimo ir filtravimo taisyklės ribose, įrodymas, kad išeinantis srautas ribojamas, taip pat bandymo įrašas, rodantis, kad ląstelės tinkle sukurta apkrova nepablogino biuro ar gretimo tinklo veikimo. Reikalaujama nuo SL 3.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 7.2 **Skaičiavimo laiko, operatyviosios atminties, saugojimo vietos ir tinklo pralaidumo naudojimas apribotas taip, kad atskiras procesas ar paslauga negalėtų sunaudoti valdymui reikalingų išteklių.**

Iš ko tai galima atpažinti: Išteklių ribų konfigūracija (kvotos, procesų prioritetai, atminties ribos), naudojimo stebėsenos vertinimas per tipišką laikotarpį, taip pat ribos, kurias pasiekus pateikiamas įspėjimas. Reikalaujama nuo SL 1. Mažos įmonės naudoja operacinės sistemos įtaisytas priemones ir paprastą stebėseną su įspėjimu elektroniniu paštu apie disko vietą ir procesoriaus apkrovą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SR 7.3 **Sistemos konfigūracijų, programų duomenų ir programų versijų atsarginės kopijos yra sukurtos, jos daromos nenutraukiant vykstančio darbo ir apsaugotos nuo neteisėtos prieigos ir keitimo.** Dokumentas

Iš ko tai galima atpažinti: Atsarginių kopijų darymo koncepcija su taikymo sritimi, dažnumu ir saugojimo laikotarpiu, paskutinių paleidimų kopijavimo žurnalai, taip pat kopijų laikmenų prieigos apsaugos įrodymas (atskira saugojimo vieta, šifravimas, atskiri leidimai). Reikalaujama nuo SL 1. Maža įmonė PLC projektus ir HMI versijas kopijuoja į šifruotą laikmeną, kuri po kopijavimo fiziškai atjungiama, o datą ir versiją užrašo paprastame sąraše.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.3 RE 1 **Atsarginių kopijų tinkamumas patikrintas, ir įrodyta, kad iš jų iš tikrųjų galima atkurti veikiančią būseną.**

Iš ko tai galima atpažinti: Atkūrimo patikros įrašas su data, tikrinta kopijos versija, tiksline sistema ir rezultatu, bent svarbiausiems komponentams. Reikalaujama nuo SL 2, o nuo SL 1 ne. Mažos įmonės kartą per metus atrankos būdu patikrina vieną PLC programą ir vieną HMI atvaizdą atsarginiame įrenginyje ir rezultatą užrašo dviem sakiniais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.3 RE 2 **Atsarginis kopijavimas vyksta automatiškai pagal nustatytą tvarkaraštį, o nepavykęs paleidimas aptinkamas ir apie jį pranešama.**

Iš ko tai galima atpažinti: Kopijavimo užduoties tvarkaraštis, vykdymo žurnalai be tarpų, taip pat pranešimo apie nepavykusį paleidimą įrodymas (pavojaus signalas, registruota užklausa, laiškas). Reikalaujama nuo SL 3.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.4 **Po trikdžio, gedimo ar atakos sistemą galima grąžinti į žinomą, saugią būseną, atkūrimas išbandytas pratybose, o atsakomybės įvardytos.** Dokumentas

Iš ko tai galima atpažinti: Kiekvieno svarbaus komponento paleidimo iš naujo planas su seka, reikalingomis laikmenomis, kontaktais ir tiksliniu laiku, kartu su paskutinių atkūrimo pratybų įrašu. Reikalaujama nuo SL 1. Mažai įmonei pakanka vieno puslapio paleidimo kortelės kiekvienai linijai, laikomos valdymo spintoje ir tikrinamos kaskart keičiant atsarginę dalį.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.5 **Sutrikus įprastam maitinimui sistema pereina į nustatytą būseną: arba maitinimas palaikomas atsarginiu šaltiniu, arba vyksta tvarkingas išjungimas neprarandant saugios būsenos.**

Iš ko tai galima atpažinti: Nepertraukiamo maitinimo šaltinio arba avarinio generatoriaus parinkimo ir priežiūros įrodymas, paskutinio akumuliatoriaus ar apkrovos bandymo įrašas, taip pat aprašas, kaip elgiamasi persijungiant ir grįžus tinklo maitinimui. Reikalaujama nuo SL 1. Mažos įmonės kartą per metus išbando nepertraukiamo maitinimo šaltinį su apkrova ir užrašo bandymo datą, palaikymo trukmę ir akumuliatoriaus amžių.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.6 **Sistemos tinklo ir saugumo nustatymai įtvirtinti patvirtintoje tikslinėje būsenoje, nuokrypiai nuo tos tikslinės būsenos aptinkami, o esamą būseną galima gauti bet kada.** Dokumentas

Iš ko tai galima atpažinti: Kiekvienos įrenginių klasės patvirtinta tikslinė konfigūracija (apsaugos sugriežtinimo specifikacija), esamos įrenginių konfigūracijos būsenos, taip pat tikslinės ir faktinės būsenos palyginimo rezultatas su nuokrypių sąrašu ir kiekvieno priežastimi. Reikalaujama nuo SL 1. Maža įmonė konfigūracijų eksportus laiko versijų valdymo sistemoje ir palygina juos prieš kiekvieną pakeitimą ir po jo.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.6 RE 1 **Esamą saugumo nustatymų būseną galima pateikti mašininio skaitymo pavidalu, kad ją būtų galima automatiškai palyginti su tiksline būsena.**

Iš ko tai galima atpažinti: Pavyzdinė išvestis mašininio skaitymo formatu (konfigūracijos eksportas, struktūrizuota byla, sąsajos užklausa) ir scenarijus arba priemonė, atliekanti palyginimą su tiksline būsena, kartu su vieno paleidimo rezultatų ataskaita. Reikalaujama nuo SL 3.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.7 **Sistema apribota veikimui reikalingomis funkcijomis, o nereikalingos paslaugos, prievadai, protokolai ir sąsajos išjungtos arba pašalintos.**

Iš ko tai galima atpažinti: Kiekvieno komponento veikiančių paslaugų ir atvirų prievadų sąrašas su poreikio pagrindimu, įrodymas, kad likusios yra išjungtos (konfigūracija, prievadų nuskaitymo rezultatas), taip pat USB ir priežiūros sąsajų taisyklė. Reikalaujama nuo SL 1. Mažos įmonės kiekviename segmente atlieka paprastą prievadų nuskaitymą ir kiekvieną atvirą punktą pagrindžia viena eilute.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR 7.8 **Esamas visų sistemos komponentų sąrašas su gamintoju, tipu, programinės aparatinės įrangos ar programinės įrangos versija ir tinklo adresu yra prieinamas ir atnaujinamas įvykus pakeitimams.** Dokumentas

Iš ko tai galima atpažinti: Komponentų sąrašas su peržiūros data ir savininku, priežiūros įrodymas per pakeitimų istoriją, taip pat palyginimas su tinklo aptikimo rezultatu, siekiant rasti neįrašytus įrenginius. Reikalaujama nuo SL 2, o nuo SL 1 ne. Maža įmonė sąrašą veda kaip lentelę ir kaip tvirtą taisyklę atnaujina jį kaskart pakeitus įrenginį ir kaskart atnaujinus programinę aparatinę įrangą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas