

IEC 62443-4-1:2018 Saugaus produkto kūrimo būvio ciklas pramoninėje automatikoje

Saugaus kūrimo būvio ciklas, aštuonios praktikos

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

Pagal IEC 62443-4-1 galima sertifikuotis, tačiau sertifikavimo objektas yra neįprastas: sertifikuojamas įvardytos kūrimo organizacijos kūrimo procesas, tai yra viena konkreti dokumentuota saugaus būvio ciklo versija. Nesertifikuojamas nei produktas, nei asmuo. Galimi keliai yra ISASecure SDLA ir IEC EE CB Scheme. Pagal šiandienos padėtį toks sertifikatas nesukuria atitikties prezumpcijos pagal EU Cyber Resilience Act. Jo nedera painioti su IEC 62443-4-2, kuris kelia reikalavimus pačiam komponentui. Šis sąrašas yra darbo priemonė įsivertinimui, o ne įrodymas.

Įmonė	Data	Pildė
-------	------	-------

5 1 praktika: Saugumo valdymas (SM)13

SM-1 Yra nustatytas produkto kūrimo būvio ciklas, kuris saugumą perneša per kiekvieną etapą nuo pradinės koncepcijos iki produkto eksploatacijos nutraukimo, ir būtent šio ciklo iš tikrųjų laikomasi kasdieniame darbe. Dokumentas

Iš ko tai galima atpažinti: Proceso aprašas arba darbo instrukcija, kurioje išvardyti etapai, kiekvieno etapo rezultatai ir perdavimo taškai, kartu su vykdomo projekto įrodymu, rodančiu, kad etapai iš tikrųjų buvo pereiti. Maža įmonė apsieina su vienu puslapiu kiekvienam etapui ir kontroliniu sąrašu užduočių sistemoje; svarbiausia, kad dokumentuotas procesas ir kasdienė praktika sutaptų.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SM-2 Kiekviena saugaus kūrimo būvio ciklo užduotis turi paskirtą atsakingąjį, ir šis paskyrimas yra žinomas dalyvaujantiems žmonėms. Dokumentas

Iš ko tai galima atpažinti: Vaidmenų ir atsakomybių matrica, kurioje kiekvienas proceso žingsnis susietas su įvardytu vaidmeniu, papildyta esamu tų vaidmenų užėmimu. Kai žmonių yra tik keletas, pakanka lentelės su vaidmeniu, užduotimi ir asmeniu; svarbiausia yra pavadavimo tvarka atostogų ir ligos atvejais.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SM-3 Atsekamai nustatyta, kurie produktai, variantai, laidos ir komponentai patenka į saugaus kūrimo būvio ciklą, o kurie ne. Dokumentas

Iš ko tai galima atpažinti: Į taikymo sritį patenkančių produktų ir versijų būsenų sąrašas su įtraukimo ir neįtraukimo pagrindimu, atnaujinamas su kiekviena nauja laida. Praktikoje gerai veikia stulpelis produktų apžvalgoje, kuriame kiekvienoje eilutėje yra taip arba ne ir vienas pagrindimo sakiny.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SM-4 Žmonės, kurie imasi saugumo užduočių, turi joms reikalingą dalykinę kompetenciją, ir ši kompetencija yra sąmoningai ugdoma bei atnaujinama.

Iš ko tai galima atpažinti: Kiekvieno saugumo vaidmens kompetencijos profilis, kvalifikacijos įrašai, mokymo planas ir dalyvavimo įrašai, papildyti spragų apžvalga. Mažos įmonės tai įrodo pažymėjimais, dalyvavimu konferencijose ar internetiniuose seminaruose ir trumpa metinė peržiūra, kas kurią spragą iki kada uždaro, o kur reikia, perka išorinę kompetenciją.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SM-5 Saugaus kūrimo būvio ciklo taikymo sritis yra apibrėžta ir įvardija dalyvaujančias vietas, organizacinius padalinius, tiekėjų indėlį ir kūrimo aplinkas kartu su tos srities ribomis. Dokumentas

Iš ko tai galima atpažinti: Taikymo srities aprašas, apimantis vietas, komandas, perduotas vykdyti dalis ir sistemas, kartu su išorinių sąsajų eskizu. Kas kuria vienoje vietoje, tai užrašo keliaisakiniais ir aiškiai įvardija, kas lieka už ribų, pavyzdžiui, išorėje sukurti mazgai arba trečiosios šalies prieglobos paslauga.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SM-6	Kiekvienam naudotojams perduodamam elementui, programinei įrangai, programinei aparatinei įrangai, konfigūracijoms ir lydimiesiems failams, yra galima vientisumo patikra, kad gavėjai galėtų atpažinti nepastebėtą pakeitimą. Iš ko tai galima atpažinti: Kiekvieno pristatymo paketo parašai arba paskelbtos kontrolinės sumos, metodo aprašas ir vienas pavyzdys iš tikros laidos kartu su nurodymais klientui, kaip atlikti patikrą. Mažoms komandoms pakanka pasirašyto kontrolinių sumų failo šalia atsisiuntimo ir vienos pastraipos laidos aprašyme. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	
Atviras	Vykdomas	Įvykdytas	Netaikomas			
SM-7	Kūrimo, kompiliavimo ir testavimo aplinkos yra apsaugotos nuo neteisėtos prieigos ir nuo pirminio kodo, kompiliavimo įrankių bei artefaktų klastojimo. Iš ko tai galima atpažinti: Saugyklos, kompiliavimo serverio ir testavimo sistemų prieigos valdymo koncepcija, prieigų sąrašai su paskutinės peržiūros data, su saugumu susijusių pakeitimų įrašai ir įrodymas, kad gamybinė ir kūrimo prieigos yra atskirtos. Neturint savo informacinių technologijų padalinio, pakanka dviejų veiksmų prisijungimo, apsaugotos pagrindinės šakos su būtina peržiūra ir kas pusmetį atliekamos peržiūros, kas dar turi prieigą. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	
Atviras	Vykdomas	Įvykdytas	Netaikomas			
SM-8	Privatieji raktai, kuriais pasirašomi pristatymai, yra apsaugoti nuo atskleidimo ir netinkamo naudojimo, o jų naudojimas leidžiamas tik įgaliojams žmonėms ir sistemoms. Iš ko tai galima atpažinti: Rakto saugojimo, prieigos, atnaujinimo ir atšaukimo aprašas, apsaugoto saugojimo įrodymas, pavyzdžiui, aparatinė raktų laikmena arba raktų valdymo paslauga, ir pasirašymo veiksmų įrašai. Maža įmonė laiko pasirašymo raktą aparatinėje raktų laikmenoje, dokumentuoja du prieigą turinčius žmones ir turi parengtą procedūrą praradimo atvejui. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	
Atviras	Vykdomas	Įvykdytas	Netaikomas			
SM-9	Perkamiems arba perimamiems komponentams, įskaitant atvirojo kodo programinę įrangą, tiekėjui keliama saugumo lūkesčiai yra nustatyti ir taikomi atrenkant. Iš ko tai galima atpažinti: Saugumo reikalavimai tiekėjų specifikacijose arba sutartyse, trečiųjų šalių komponentų atrankos kriterijai, visų trečiųjų šalių komponentų sąrašas su versija ir šaltiniu bei vertinimas, ar tiekėjas atitinka lūkesčius. Neturint pirkimų padalinio, pakanka palaikomo komponentų sąrašo su stulpeliu, kuriame žymima, ar buvo patikrinti tiekėjo saugumo atnaujinimai ir pranešimo kanalai. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	Dokumentas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
SM-10	Trečiosios šalies pagal užsakymą sukurtiems komponentams taikomi tie patys saugumo reikalavimai kaip ir savam kūrimui, o jų laikymasis yra tikrinamas. Iš ko tai galima atpažinti: Užsakymas arba sutarties dokumentai, kuriuose nurodyti reikalaujami saugumo įsipareigojimai, paslaugų teikėjo įrodymai apie taikomas praktikas, priėmimo įrašai ir savų pateikto darbo patikrų rezultatai. Neturint audito biudžeto, pakanka sutartinio patikinimo, teikėjo testavimo rezultatų pateikimo ir vienos savos atrankinės patikros prieš priėmimą. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	
Atviras	Vykdomas	Įvykdytas	Netaikomas			
SM-11	Su saugumu susiję pastebėjimai iš visų šaltinių, testų, peržiūrų, naudotojų pranešimų ir trečiųjų šalių informacijos, yra registruojami, vertinami pagal poveikį, jiems paskiriamas atsakingas asmuo ir terminas, o jie sekami iki uždarymo. Iš ko tai galima atpažinti: Defektų arba užduočių sistema su atskira saugumo temų žyma, o kiekviename įrašė poveikio vertinimas, atsakingas asmuo, terminas ir uždarymo pastaba, kartu su ataskaita apie neuždarytus punktus. Maža komanda naudoja žymą esamoje užduočių sistemoje ir nuolatinį darbotvarkės punktą savaitiniame susitikime. <table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table> Įrodymas / pagrindimas	Atviras	Vykdomas	Įvykdytas	Netaikomas	Dokumentas
Atviras	Vykdomas	Įvykdytas	Netaikomas			

SM-12

Prieš išleidžiant produktą yra patikrinama ir įrodoma, kad numatyti saugaus kūrimo būvio ciklo žingsniai iš tikrųjų buvo atlikti ir kad susiję įrašai buvo parengti.

[Dokumentas](#)

Iš ko tai galima atpažinti: Kiekvienos laidos peržiūra lyginant su proceso žingsniais, nuorodos į atitinkamus įrašus ir dokumentuotas išleidimo sprendimas su data ir parašu. Praktikoje gerai veikia laidos kontrolinis sąrašas, kuris neleidžia išsiųsti be visų varnelių; neuždaryti punktai pagrindžiami ir jiems nustatoma data.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SM-13

Pats saugaus kūrimo būvio ciklas yra reguliariai kritiškai vertinamas ir gerinamas remiantis incidentų, testavimo rezultatų, klientų atsiliepimų ir grėsmių aplinkos įžvalgomis.

Iš ko tai galima atpažinti: Proceso peržiūros įrašai, pavyzdžiui, vadovybinė vertinamoji analizė arba retrospektyva, su inicijuotais proceso pakeitimais, jų įgyvendinimo būseną ir nuoroda į pagrindinę priežastį. Kas naudoja standarto brandos lygius, užrašo esamą ir siekiamą būklę kiekvienai praktikai; 4 brandos lygis reikalauja būti šio nuolatinio gerinimo įrodymo. Mažai įmonei pakanka vieno susitikimo per metus su protokolu ir trijų konkrečių patobulinimų.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

6 2 praktika: Saugumo reikalavimų specifikavimas (SR)

5

SR-1

Numatytas produkto kontekstas yra aprašytas: tikėtina veikimo aplinka, saugumo priemonės, kurių tikimasi iš tos aplinkos, numatytos naudotojų grupės ir vaidmenys, prielaidos apie pasitikėjimo ribas ir naudojimo atvejai, kuriems produktas aiškiai nėra skirtas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Produkto saugumo konteksto aprašas kaip atskiras dokumentas arba kaip pastovus produkto specifikacijos skyrius, apimantis tinklo aplinką, numanomas išorines apsaugas, pavyzdžiui, užkardą ar fizinės prieigos valdymą, vaidmenų sąrašą ir aiškų į taikymo sritį nepatenkančių naudojimo atvejų sąrašą. Maža įmonė apsiriboja dviem puslapiais, prideda paprastą gamyklos aplinkos eskizą, o produkto savininkas jį patvirtina ir nurodo datą.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SR-2

Produktui yra parengtas grėsmių modelis, kuris atvaizduoja duomenų srautus, sąsajas, pasitikėjimo ribas ir atakų kelius, įvardija iš jų kylančias grėsmes ir galimą jų poveikį bei priskiria atsakomąsias priemones. Jis peržiūrimas ir atnaujinamas įvykus reikšmingiems pakeitimams ir bent kartą kiekvienai produkto laidai, o neuždaryti punktai sekami, kol uždaromi.

[Dokumentas](#)

Iš ko tai galima atpažinti: Grėsmių modelis su duomenų srautų diagrama, kiekvienos sąsajos grėsmių sąrašas, priskirtomis atsakomosiomis priemonėmis ir neuždarytų punktų būseną, kartu su pakeitimų istorija, kurioje nurodyta data ir autorius. Maža įmonė gali dirbti su viena lentele kiekvienai sąsajai, kurios stulpeliai rodo, kas ten gali nutikti blogo, kiek tai būtų rimta, ką dėl to daroma ir kas tai peržiūri.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SR-3

Produkto saugumo reikalavimai yra nustatyti ir dokumentuoti. Jie apima grėsmių modelio rezultatus, aprašytą produkto saugumo kontekstą, taikomus teisinius ir sutartinius įsipareigojimus bei siekiamą saugumo lygį, taip pat saugumo galimybes, kurias užtikrina pats produktas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Reikalavimų sąrašas arba reikalavimų valdymo įrankis su unikaliu kiekvieno reikalavimo identifikatoriumi, kiekvieno įrašo šaltiniu, pavyzdžiui, grėsme, kliento sutartimi ar teisiniu įsipareigojimu, ir siekiamu saugumo lygiu. Maža įmonė tai tvarko kaip vieną lentelę su pastovių identifikatoriaus stulpeliu, prie kurio vėliau kabinasi verifikavimas ir testavimas.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SR-4

Kiekvienas atskiras saugumo reikalavimas suformuluotas taip, kad būtų vienareikšmis, be prieštaravimų, patikrinamas testais ir atsekamas iki konkrečios produkto funkcijos ar sąsajos, ir jame yra informacija, reikalinga vėliau jį verifikuoti be papildomų paaiškinimų.

Iš ko tai galima atpažinti: Reikalavimų sąrašo pavyzdys, rodantis kiekvieno reikalavimo išmatuojamą priėmimo kriterijų ir susijusią funkciją ar sąsają, kartu su reikalavimų ir testavimo atvejų susiejimu. Maža įmonė tai tikrina pastoviu formuluotės šablonu ir kontroliniu klausimu, ar iš reikalavimo galima parašyti testavimo atvejį nieko papildomai neklausiant.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SR-5 Saugumo reikalavimai yra peržiūrimi prieš juos naudojant projektuojant ir įgyvendinant, dalyvaujant susijusioms pusėms, tokioms kaip kūrimas, testavimas, produkto savininkas ir, kur naudinga, pardavimai arba klientas. Peržiūra apima išsamumą pagal grėsmių modelį ir produkto saugumo kontekstą, teisingumą ir patikrinamumą testais. Pastebėjimai registruojami ir sekami iki uždarymo.

Iš ko tai galima atpažinti: Peržiūros įrašas su data, dalyviais ir jų vaidmenimis, peržiūrėta reikalavimų versija, pastebėjimų sąrašas su atsakingu asmeniu ir uždarymo būseną bei patvirtinimo pastaba. Maža įmonė tai atlieka kaip dviejų asmenų peržiūrą tarp kūrimo ir testavimo su trumpu įrašu ir patvirtinimo eilute reikalavimų sąrašė.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

7 3 praktika: Saugumas jau projektuojant (SD)

4

SD-1 Kiekvienas produktas turi projekto aprašą, kuriame užfiksuoti su saugumu susiję architektūros aspektai: kokie komponentai yra, kaip jie tarpusavyje susisiečia, kur eina pasitikėjimo ribos, kokios išorinės sąsajos yra atviros ir kokiais mechanizmais anksčiau nustatyti saugumo reikalavimai įgyvendinami projekte.

[Dokumentas](#)

Iš ko tai galima atpažinti: Architektūros dokumentas arba projekto specifikacija su diagrama, rodančia komponentus, duomenų srautus ir pasitikėjimo ribas, bei susiejimo lentelė nuo kiekvieno saugumo reikalavimo iki jį įgyvendinančio projekto elemento. Mažas tiekėjas apsieina su viena palaikoma diagrama ir dviem trimis puslapiais paaiškinimo; svarbiausia, kad ji būtų saugykloje su versijų kontrole ir atnaujinama kaskart pasikeitus architektūrai.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SD-2 Projektas yra sistemingai analizuojamas dėl grėsmių. Analizė įvardija užpuoliko tikslus, susijusias pasitikėjimo ribas ir sąsajas, iš jų kylančias grėsmes kartu su jų vertinimu ir projekte taikomas atsakomosios priemonės. Ji kartojama kaskart iš esmės pasikeitus architektūrai ar aplinkai, o nustatytos grėsmės sekamos, kol dėl kiekvienos jų priimamas sprendimas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Grėsmių modelis kiekvienam produktui arba kiekvienai pagrindinei laidai, pavyzdžiui, lentelė su stulpeliais grėsmė, susijusi sąsaja, vertinimas, atsakomoji priemonė ir būseną, kartu su modeliavimo sesijos protokolu, kuriame nurodyti dalyviai ir data. Maža komanda modeliuoja pragmatiškai per dviejų ar trijų valandų dirbtuves pagal architektūros diagramą ir neuždarytus punktus registruoja kaip užduotis, todėl sekimo įrodymas atsiranda be papildomų pastangų.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SD-3 Projektas įrodomai laikosi pripažintų saugaus projektavimo principų, tarp jų mažiausios privilegijos, mažiausio atakos paviršiaus, giliosios gynybos, saugių numatytųjų nuostatų, saugaus elgesio sutrikus veikimui bei kuo paprastesnių ir kuo lengviau patikrinamų saugumo mechanizmų. Šių principų taikymas matomas projekte ir yra pagrįstas.

Iš ko tai galima atpažinti: Projekto aprašo skyrius arba vidinė projektavimo gairė, įvardijanti principus, ir konkretus kiekvieno principo įrodymas produkte, pavyzdžiui, paslaugų privilegijų matrica, atvirų prievadų sąrašas su pagrindu, pristatomos numatytosios nuostatos arba dokumentuotas klaidų apdorojimo elgesys. Mažas tiekėjas naudoja trumpą šių principų kontrolinį sąrašą kaip pastovų projekto peržiūros punktą ir užpildytą lapą laiko kartu su projektu.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SD-4 Projektą prieš prasidedant įgyvendinimui peržiūri kvalifikuoti kolegos. Peržiūra apima išsamumą pagal saugumo reikalavimus, saugumo mechanizmų teisingumą ir rezultatyvumą bei grėsmių analizės rezultatus. Dalyvauja žmonės, turintys pakankamą saugumo kompetenciją, pastebėjimai registruojami ir sekami iki uždarymo.

[Dokumentas](#)

Iš ko tai galima atpažinti: Peržiūros įrašas su data, peržiūrimi objektu ir jo versija, dalyviais ir jų vaidmenimis, pastebėjimų sąrašas su būseną ir išleidimo sprendimu. Maža komanda peržiūrą susieja su projekto dokumentų sujungimo prašymu ir pastebėjimus palieka kaip komentarus su uždarymo pastaba, taip sekimas įrodomas be jokių papildomų įrankių. Kur savo saugumo kompetencijos trūksta, pragmatiškas kelias yra išorinis peržiūrėtojas, samdomas valandiniu pagrindu kritiniams projektams.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

8 4 praktika: Saugus įgyvendinimas (SI)

2

SI-1 Yra nustatytas procesas, kaip faktinis įgyvendinimas tikrinamas pagal saugų projektą: peržiūra patvirtina, kad projekte numatytos apsaugos priemonės kode iš tikrųjų yra ir veikia, kad gilioji gynyba išlaikoma ir kad įgyvendinant nebuvo įnešta naujų pažeidžiamumų. Peržiūrą atlieka tinkamai kvalifikuoti darbuotojai, o rasti nukrypimai registruojami ir sekami iki uždarymo.

Iš ko tai galima atpažinti: Rašytinė įgyvendinimo peržiūros procedūra kartu su kiekvieno komponento ar laidos peržiūros įrašais: peržiūrėtas modulis, nuoroda į projekto dokumentą, data, peržiūrėtojas, pastebėjimai ir jų sprendimo būseną. Tinkami įrodymai yra sujungimo prašymų peržiūros su būtinu saugumo kontroliniu sąrašu, statinės kodo analizės rezultatai su dokumentuotu kiekvieno radinio vertinimu ir peržiūros sesijų protokolai. Maža komanda tai užtikrina keturių akių principu, saugykloje laikomu peržiūros šablonu, kuriame kiekviena projekto priemonė pažymima atskirai, ir viena užduotimi kiekvienam neuždarytam pastebėjimui. Svarbiausia, kad kodo autorius niekada nebūtų to paties kodo peržiūrėtojas.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SI-2 Visam su saugumu susijusiam kūrimo darbui galioja įpareigojančios saugaus programavimo taisyklės, kurios apima bent žinomų nesaugių konstrukcijų ir funkcijų vengimą, įvesties ir klaidų tvarkymą, atminties bei išteklių valdymą ir patikrinto saugumo kodo naudojimą vietoj savo rašytų realizacijų. Taisyklės galioja kiekvienai naudojamai programavimo kalbai, yra žinomos visiems kūrėjams ir atnaujinamos, kai reikia, pavyzdžiui, atsiradus naujiems atakų būdams ar naujiems įrankiams.

[Dokumentas](#)

Iš ko tai galima atpažinti: Patvirtintas saugaus programavimo standartas su versijos būseną, taikymo sritimi kiekvienai kalbai ir patvirtinimo data, papildytas įrodymu, kad jis veikia kasdieniame darbe: kodo tikrintuvų ir analizės įrankių konfigūracija saugykloje, kompiliavimo taisyklė, kuri iškelia pažeidimus, ir instruktažo dalyvių sąrašas. Mažos įmonės nerašo standarto nuo nulio; jos paskelbia įpareigojančiu nusistovėjusį viešą taisyklių rinkinį, prideda trumpą savų papildomų taisyklių sąrašą ir įtvirtina patikrą kūrimo grandinėje, kad laikymasis būtų parodomas automatiškai.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

9 5 praktika: Saugumo verifikavimo ir validavimo testavimas (SVV)

5

SVV-1 Kiekvienam su saugumu susijusiam produkto reikalavimui priskirtas bent vienas testavimo atvejis, rodantis, kad apsaugos funkcija įprastai veikiant veikia kaip numatyta, kad gavusi netinkamą įvestį ar naudojama netinkamai ji elgiasi kaip nurodyta ir kad su produktu pateikiamos numatytosios nuostatos atitinka saugią būseną. Vykdytas ir rezultatas registruojami kiekvienai testuotai programinės įrangos versijai.

[Dokumentas](#)

Iš ko tai galima atpažinti: Atsekamumo matrica, siejanti reikalavimą su testavimo atveju ir rezultatu, bei testavimo įrašai su data, testuojama versija arba kompiliacija ir testą atlikusio asmens vardu. Mažas tiekėjas tiesiog prideda testavimo atvejo identifikatoriaus stulpelį prie savo reikalavimų sąrašo, o automatinio testavimo iš kūrimo grandinės išvesties žurnalą archyvuoja kaip failą prie atitinkamos versijos.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SVV-2 Iš grėsmių modelio kylančios atsakomosios priemonės testuojamos tikslingai, siekiant patvirtinti, kad jos iš tikrųjų uždaro numatytą atakos kelią. Testuojama pagal nustatytas grėsmes, o ne tik pagal tvarkingą naudojimą, ir neuždaryti punktai perduodami į defektų tvarkymo procesą.

Iš ko tai galima atpažinti: Testavimo atvejai, tiesiogiai nurodantys grėsmių modelio įrašus, pavyzdžiui, vienas piktnaudžiavimo atvejis kiekvienam grėsmės identifikatoriui su laukiamu gynybiniu elgesiu, kartu su tų vykdymų įrašais. Be sudėtingų priemonių pakanka grėsmių modelyje pridėti stulpelį su nuoroda į testavimo atvejį ir paskutinės sėkmingos patikros data.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SVV-3

Prieš išleidimą produktas sistemingai tiriamas dėl pažeidžiamumų. Į apimtį patenka bent: iš išorės pasiekiamų sąsajų ir paslaugų tyrimas, testavimas netaisyklinga ir atsitiktinai keičiama įvestimi, naudojamų trečiųjų šalių komponentų palyginimas su žinomais paskelbtais pažeidžiamumais ir savo kodo patikra dėl žinomų silpnųjų klasių. Pastebėjimai registruojami kartu su jų vertinimu.

[Dokumentas](#)

Iš ko tai galima atpažinti: Naudotų įrankių ataskaitos su įrankio pavadinimu, versija ir pažeidžiamumų duomenų bazės duomenų atnaujinimo data, atsitiktinės įvesties testavimo įrašai, trečiųjų šalių komponentų sąrašas su paskutinio palyginimo data ir pastebėjimų sąrašas su vertinimu bei sprendimu. Mažas tiekėjas derina nemokamus standartinius įrankius, priklausomybių patikrą ir įdiegto produkto prievadų bei paslaugų patikrą, o kiekvienos laidos išvestis laiko viename aplanke.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SVV-4

Laidos kandidatas realiomis sąlygomis patiria atakos bandymą, kuris aktyviai siekia apeiti apsaugos mechanizmus, o ne tik juos užklausti. Testo apimtis, kraštinės sąlygos ir ribos sutiriamos iš anksto, o rastos silpnybės tvarkomos ir sekamos kaip defektai.

Iš ko tai galima atpažinti: Užsakymas arba testavimo pavedimas su apimtimi ir testavimo aplinka, ataskaita apie taikytą metodą, išnaudotas silpnybės ir jų vertinimą, bei įrašai defektų arba užduočių sistemoje su ištaisymo arba pagrįsto rizikos prisiėmimo įrodymu. Maži tiekėjai šį testą paprastai perka išorėje kaip ribotą laiko biudžetą arba paveda jį atlikti asmeniui, kuris produkto nekūrė.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SVV-5

Testuojančių darbuotojų nepriklausomumas yra nustatytas ir atitinka siekiamą brandos lygį. Kas komponentą sukūrė, neišleidžia jo remdamasis vien savo paties testavimu, o kylant brandos lygiui už testavimą atsako organizaciškai atskiras padalinys arba išorės šalis. Faktinis paskyrimas yra atsekamas kiekvienam testui.

Iš ko tai galima atpažinti: Vaidmenų apibrėžimas kūrimo procese, rodantis kūrimo ir testavimo atskyrimą, ir kiekvienam testavimo vykdymui ar testavimo ataskaitai užrašytas testą atlikusio asmens vardas bei vaidmuo. Dviejų asmenų įmonė tai sprendžia abipusė peržiūra su dokumentuota keturių akių pastaba, o giluminiam saugumo testavimui pasitelkia išorės asmenį.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

10 6 praktika: Saugumo defektų valdymas (DM)

6

DM-1

Yra nustatytas kanalas, kuriuo iš visų pusių priimami ir registruojami pranešimai apie produkto saugumo silpnības: iš pačios kūrimo komandos, iš testavimo ir peržiūrų, iš klientų ir integruotojų, iš išorės pranešėjų ir iš įspėjimų apie naudojamus trečiųjų šalių bei atvirojo kodo komponentus. Pranešimo kanalą išorės šalys gali rasti, o kiekvienas pranešimas registruojamas su gavimo data ir šaltiniu.

[Dokumentas](#)

Iš ko tai galima atpažinti: Pranešimo kanalo aprašas, viešai pasiekiamas kontaktinis taškas (saugumo puslapis, security.txt failas arba pašto dėžutė, tokia kaip security@), ir priėmimo registras, kuriame kiekvienam pranešimui nurodyta data, šaltinis ir trumpas aprašymas. Maža įmonė gali dirbti su bendra pašto dėžute ir viena skaičiuokle ar užduočių žyma, jei tik ten patenka kiekvienas pranešimas, įskaitant tuos, kurie iškyla vidiniame kūrėjų pokalbyje.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

DM-2

Kiekvienas gaunamas pranešimas yra rūšiuojamas ir tiriamas siekiant nustatyti, ar jis susijęs su saugumu ir kuriems produktams, versijoms bei komponentams daro poveikį. Pranešimai, kurie pasirodo esą nesusiję su saugumu arba netaikytini, taip pat uždaromi nurodant priežastį, o ne tyliai atmetami.

Iš ko tai galima atpažinti: Kiekvieno pranešimo rūšiavimo pastaba su rezultatu (susijęs su saugumu taip arba ne), paveiktomis versijomis ir atmetimo priežastimi, kur ji taikoma, matoma užduotyje arba priėmimo sąraše. Komandos, gaunančios nedaug pranešimų, gali rūšiuoti per trumpą pasikartojantį susitikimą ir rezultatą užrašyti dviem sakiniiais kiekvienam įrašui.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

DM-3

Patvirtinti saugumo defektai vertinami nuosekliu metodu: pagrindinė priežastis, paveiktos versijos ir konfigūracijos, galimas poveikis eksploatacijai ir saugumui, išnaudojamumas ir pavojingumas pagal nustatytą skalę. Vertinimo rezultatas registruojamas ir yra atsekamas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Kiekvieno defekto vertinimo įrašas arba užduoties laukų rinkinys, apimantis pagrindinę priežastį, pavojingumą ir taikytą skalę (pavyzdžiui, plačiai naudojama pavojingumo vertinimo sistema su dokumentuotu vektoriumi), kartu su paveiktų versijų sąrašu. Mažos komandos gali remtis pastovių laukų šablonu užduočių sistemoje ir puse puslapio, kuriame aprašyta skalė ir ribos, nuo kurių imamas neatidėliotinių veiksmų.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

DM-4

Kiekvienam įvertintam saugumo defektui priimamas sprendimas, kaip jis bus tvarkomas: ištaisyimas, kompensuojanti priemonė arba pagrįstas rizikos prisiėmimas. Sprendimas kyla iš pavojingumo, jam paskiriamas atsakingas asmuo ir terminas, o defektas sekamas iki uždarymo.

[Dokumentas](#)

Iš ko tai galima atpažinti: Veiksmų sąrašas arba užduoties būseną su atsakingu asmeniu, terminu, priemonės rūšimi ir uždarymo pastaba, susieta su kodo baze arba laida, kurioje pataisa įsigalioja. Priimtoms liekamosioms rizikoms reikia trumpo rašytinio pagrindimo, kurį patvirtina produkto savininkas. Maža įmonė tai gali laikyti užduočių lentoje su terminais, be jokių papildomų įrankių.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

DM-5

Paveikti naudotojai, integruotojai ir kitos suinteresuotosios šalys informuojami apie saugumo defektus, kai tik vertinimas to reikalauja, nurodant paveiktas versijas, poveikį ir prieinamą pataisą ar kompensuojančią priemonę. Tokio atskleidimo terminai ir gavėjų ratas nustatomi iš anksto, kaip ir elgesys su trečiųjų šalių pranešimais, turinčiais savo atskleidimo terminą.

Iš ko tai galima atpažinti: Paskelbti saugumo pranešimai ar įspėjimai su data ir versijos nuoroda, platinimo sąrašas arba prenumeratorių kanalas ir rašytinė taisyklė dėl terminų bei koordinuoto atskleidimo. Tiekėjai, turintys nedaug klientų, gali naudoti vieną laišką pagal palaikomą klientų sąrašą ir įspėjimų puslapį su data, kurio pakeitimai yra versijuojami.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

DM-6

Saugumo defektų tvarkymas peržiūrimas nustatytais intervalais. Peržiūra apžvelgia neuždarytus ir pavėluotus atvejus, laiką nuo pranešimo iki ištaisymo, pasikartojančias pagrindines priežastis ir taikytų priemonių rezultatyvumą. Iš peržiūros kylantys proceso patobulinimai įgyvendinami, o jų įgyvendinimas sekamas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Pasikartojančios peržiūros protokolas su data, dalyviais, neuždarytų ir pavėluotų atvejų skaičiais bei sutartų patobulinimų sąrašu su atsakingu asmeniu ir terminu. Maža įmonė šį punktą gali prijungti prie esamo ketvirtinio susitikimo ir skaičius bei sprendimus laikyti viename puslapyje.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

11 7 praktika: Saugumo atnaujinimų valdymas (SUM)**5**

SUM-1

Kiekvienas produkto saugumo atnaujinimas prieš išleidžiant klientams yra patikrinamas su palaikomomis produkto versijomis ir veikimo aplinkomis, o įrašas rodo, kad atnaujinimas uždaro pažeidžiamumą netrikdydamas numatytos produkto funkcijos.

[Dokumentas](#)

Iš ko tai galima atpažinti: Kiekvienos pataisos testavimo įrašas su testuota produkto versija, platforma, testavimo atvejais (rezultatyvumas prieš pažeidžiamumą ir pagrindinių funkcijų regresija) ir išleidimo patvirtinimu. Mažas tiekėjas gali dirbti su trumpu pataisos patvirtinimo įrašu užduotyje: užduoties identifikatorius, kas patikrino, kada patikrino, rezultatas, pridėdamas automatinio testavimo žurnalą.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SUM-2

Visiems produkto komponentams, kurie sukurti ne savo jėgomis (trečiųjų šalių bibliotekos, operacinė sistema, vykdymo aplinkos), yra nustatyta ir įrodyta, kaip jų saugumo atnaujinimai vertinami ir arba perimami į produktą, arba atmetami su dokumentuotu pagrindu.

[Dokumentas](#)

Iš ko tai galima atpažinti: Trečiųjų šalių dalių komponentų sąrašas su versija ir šaltiniu bei vienas vertinimo įrašas kiekvienam paskelbtam trečiosios šalies pažeidžiamumui su sprendimu (perimti, nepaveikta, padengta kompensuojančia priemone) ir pagrindu. Mažos komandos kompiliavimo metu paleidžia automatinę priklausomybių patikrą ir sprendimus laiko kaip komentarus prie patikros rezultato arba trumpame išimčių sąrašė.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SUM-3

Su kiekvienu pateikiamu saugumo atnaujinimu naudotojai gauna suprantamą lydimąją informaciją: kurios produkto versijos yra paveiktos, kuris pažeidžiamumas ištaisytas, koks jo pavojingumas, ar reikia paisyti šalutinių poveikių bei kompensuojančių priemonių ir kaip atnaujinimas įdiegiamas.

[Dokumentas](#)

Iš ko tai galima atpažinti: Paskelbti saugumo įspėjimai arba laidos aprašai su pažeidžiamumo identifikatoriumi, paveiktomis versijomis, pavojingumo vertinimu, diegimo žingsniais ir nurodymais, kaip grįžti į ankstesnę būseną. Maži tiekėjai laiko vieną viešą puslapį su chronologiniu saugumo įspėjimų sąrašu ir pateikia nuorodą į jį iš paties produkto.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SUM-4

Yra nustatytas ir nuo klastojimo apsaugotas kelias, kuriuo naudotojai gauna saugumo atnaujinimus, o atnaujinimo autentiškumą ir vientisumą naudotojo pusėje galima patikrinti prieš diegiant.

Iš ko tai galima atpažinti: Pateikimo kanalo aprašas (atsisiuntimo sritis, atnaujinimų serveris, fizinės laikmenos) kartu su jo apsaugos priemonėmis, kiekvieno paketo skaitmeninis parašas arba kontrolinė suma ir nurodymai naudotojui, kaip tai patikrinti. Maži tiekėjai tai pasiekia pasirašydami kompiliavimo serveryje, skelbdami kontrolinę sumą šalia atsisiuntimo ir įvardydami vieną aiškią vietą, kurioje laikomas viešasis raktas.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SUM-5

Yra nustatyti saugumo atnaujinimų pateikimo laiko tikslai, suskirstyti pagal pažeidžiamumo pavojingumą; faktiškai pasiekti laikai yra sekami, o kiekvienas nepasiektas tikslas pagrindžiamas ir palaikomas laikina priemone naudotojams.

[Dokumentas](#)

Iš ko tai galima atpažinti: Vidinis aprašas su laiko langų kiekvienai pavojingumo kategorijai (pavyzdžiui, kritinis ≤ 30 dienų, aukštas ≤ 90 dienų) ir kiekvieno pažeidžiamumo įvertinimas: pranešimo data, pataisos išleidimo data, praėjusios dienos, nukrypimo priežastis. Maži tiekėjai tai laiko kaip du datos laukus pažeidžiamumo užduotyje ir sąrašą peržiūri kartą per ketvirtį, užuot kūrę atskirą rodiklių sistemą.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

12 8 praktika: Saugumo gairės produktui diegti ir eksploatuoti (SG)

7

SG-1

Su kiekvienu produktu pateikiamas jo giliaios gynybos strategijos aprašas: jis įvardija į patį produktą įdiegtus apsaugos sluoksnius, susieja juos su grėsmėmis, nuo kurių jie saugo, ir parodo, kuris apsaugos poveikis atsiranda tik keliems sluoksniams veikiant kartu.

[Dokumentas](#)

Iš ko tai galima atpažinti: Pateikiamos produkto dokumentacijos skyrius arba atskira saugumo koncepcija, kurioje kiekvienam apsaugos sluoksniui nurodytas mechanizmas, grėsmė, nuo kurios apsaugoma, ir jo poveikio ribos. Maža įmonė tai laiko kaip dviejų puslapių lentelę: stulpelis apsaugos sluoksnis, stulpelis grėsmė iš savo grėsmių modelio, stulpelis liekamoji rizika. Pakanka kryžminės nuorodos į SR-2 grėsmių modelį, turinio nereikia palaikyti du kartus.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

SG-2

Dokumentacija įvardija saugumo priemonės, kurių produktas pats neužtikrina, bet tikisi iš diegimo aplinkos, pavyzdžiui, tinklo segmentavimą, priešais esančias užkardas, fizinės prieigos valdymą ar išorinę laiko paslaugą, ir aiškiai nurodo, kad be šių priemonių patikintas saugumo lygis nepasiekiamas.

Iš ko tai galima atpažinti: Vadovo skyrius apie diegimo išankstines sąlygas arba pavyzdinės architektūros brėžinys su zonomis ir jungtimis, kuriame aiškiai pažymėtos priemonės, kurias pateikia turto savininkas. Praktikoje pasiteisino prielaidų apie aplinką sąrašas, išvestas tiesiai iš produkto saugumo konteksto ir peržiūrimas kiekvienai produkto versijai.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

SG-3

Yra saugios bazinės konfigūracijos vadovas, kuriame išvardytos visos su saugumu susijusios nuostatos, paslaugos, prievadai ir sąsajos, nurodyta rekomenduojama pateikimo būseną ir aprašytas nukrypimo nuo tos rekomendacijos poveikis.

Iš ko tai galima atpažinti: Apsaugos sugriežtinimo vadovas su nuostatų lentele: parametras, rekomenduojama vertė, poveikis, šalutinis poveikis nukrypęs. Kartu paslaugų ir prievadų, veikiančių numatytojoje konfigūracijoje, sąrašas su pagrindimu, kodėl jie lieka įjungti. Maža komanda šią lentelę laiko saugykloje šalia konfigūracijos failo ir eksportuoja ją į pateikimo dokumentaciją, todėl ji išlieka suderinta su produktu.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

SG-4

Nuolatinei eksploatacijai yra vadovas, aprašantis, kaip produktas saugiai eksploatuojamas, stebimas ir išlaikomas saugios būsenos, įskaitant atsarginę kopiją ir atkūrimą, įvykių registravimą ir su saugumu susijusių įvykių pranešimų tvarkymą.

Iš ko tai galima atpažinti: Eksploatacijos vadovas su skyriais apie įvykių registravimą, atsargines kopijas, paleidimą iš naujo ir įvykių pranešimus. Kaip papildomas įrodymas, produkto siunčiamų su saugumu susijusių pranešimų sąrašas, kiekvienam su trumpu rekomenduojamu veiksmu, kad turto savininkui nereikėtų jų aiškintis vienas.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

SG-5

Dokumentacija paaiškina, kaip produkto naudotojų paskyros, vaidmenys ir teisės sukuriamos ir palaikomos, ypač vaidmenų atskyrimą, numatytųjų prisijungimo duomenų keitimą ir nebereikalingų paskyrų šalinimą.

Iš ko tai galima atpažinti: Paskyrų valdymo skyrius su vaidmenų apžvalga ir kiekvienam vaidmeniui priskirtomis teisėmis bei aiškia pastaba apie numatytuosius prisijungimo duomenis ir jų keitimą paleidžiant eksploatuoti. Praktikoje gerai veikia trumpas paleidimo eksploatuoti kontrolinis sąrašas vadove, kurį turto savininkas gali pažymėti ir įsidėti į bylą.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

SG-6

Yra saugaus eksploatacijos nutraukimo vadovas, aprašantis visišką jautrių duomenų, tokių kaip prisijungimo duomenys, raktai, konfigūracijos duomenys ir žurnalai, pašalinimą iš produkto prieš perduodant, pakartotinai naudojant ar utilizuojant įrenginį.

Iš ko tai galima atpažinti: Eksploatacijos nutraukimo skyrius, kuriame išvardytos visos jautrių duomenų saugojimo vietos produkte ir atitinkama trynimo procedūra, įskaitant atvejus, kai trynimas techniškai neįmanomas ir aparatinę įrangą tenka fiziškai sunaikinti. Čia padeda iš architektūros aprašo paimtas nuolatinių atminčių sąrašas, jis neleidžia pamiršti saugojimo vietos.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

SG-7

Naudotojams pateikiama saugumo dokumentacija peržiūrima prieš išleidimą: ji yra techniškai teisinga, suderinta su pateikiama produkto versija, išsami pagal numatytą turinį ir suprantama numatytai auditorijai, o pasikeitus produktui ji atnaujinama.

Iš ko tai galima atpažinti: Kiekvieno dokumento ir produkto versijos peržiūros įrašas su peržiūrėtoju, data, pastebėjimais ir jų uždarymu, susietas su išleidimo patvirtinimu. Maža įmonė tai sprendžia keturių akių principu dokumentacijos sujungimo prašyme: vienas kūrėjas tikrina techninį turinį, antras asmuo tikrina suprantamumą, o patvirtinimas registruojamas užduotyje. Versiją galima siųsti tik tada, kai peržiūra yra dokumentuota.

Atviras

Vykdomas

Įvykdytas

Netaikomas

Įrodymas / pagrindimas

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 ISA Secure SSA ir IEC 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 savikontrolėi, o ne įrodymas.

Įmonė	Data	Pildė
-------	------	-------

5 FR 1: kas arba kokia programa ar įrenginys prašo prieigos ir ar tai tikrai tas, kuo prisistato24

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 pridamas 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 išimties 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 veiksnium, pavyzdinis prisijungimo įrašas, kuriame matomi abu veiksniai, ir išduotų atpažinties raktų arba programėlių registracijų sąrašas. Maža įmonė naudoja esamo VPN siuvu antrąjį veiksnių 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 autentifikuoja sistemose, prieš gaudami leidimą keisti 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 išėinant 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 turėtojų.

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, pridamas trumpas paaiškinimas apie kompensuojamą 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 rodytą turto savininkas gali konfigūruoti.

Iš ko tai galima atpažinti: Rodomo pranešimo teksto ekrano nuotrauka ir patvirtinta formuluočių su patvirtinimo data. Mažos įmonės formuluočių 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 raktų 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 raktų 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 teisės 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 įgaliojantis 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 belaidžių ryšių 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 būseną, 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 Mobiliam 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 mobiliąjį 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 priežiūromose 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 atmetą antrąjį prisijungimo bandymą. Reikalaujama nuo SL 3.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

SR 2.8

Su saugumu susiję įvykiai registruojami, o kiekviename įrašė nurodomas bent laikas, šaltinis, veiksmą sukėlusį 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 nustatyto 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 padaliniiui 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 įrašė 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 stebėseną, 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 unikalūs 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 suklustota 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 įrašų. 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 įsėga 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 pagrindu. 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 sietai, 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 sietai 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 nepasiekia. 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 nuoseklių rezultatų.

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: Saugotinių 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 pavojus 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 išraišai 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 funkcinė 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 nustatytais neveiklumo laiko ir ilgiausios trukmės ribomis, mechanizmo, saugančio nuo pranešimų pakartojimo, įrodymas ir bandymo įrašas, kuriame perimtas seansas po atsijungimo neveikia. 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 jų 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 nuotrauka 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 naikavimo 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 pažymą. 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 veiks 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 parinktų 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 patyby, kuriose atskyrimas buvo iš tikrųjų atliktas, įrašas. Maža įmonė patybas 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 sukkelto 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 įveda 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 įgalinti asmenys ir vaidmenys gali skaityti ir vertinti netrikdydami vykstančio gamyklos darbo, o prieiga prie tų įrašų pati yra apribota įgaliojais 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 paaimamas. 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, stebėseną 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: Išteklų 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: Išteklų ribų konfigūracija (kvotos, procesų prioritetai, atminties ribos), naudojimo stebėsenos vertinimas per tipiską 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, tikslinė 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 atnauja ją kaskart pakeitus įrenginį ir kaskart atnaujinus programinę aparatinę įrangą.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas