

IEC 62443-4-1:2018 Levenscyclus voor veilige productontwikkeling voor industriële automatisering

Levenscyclus voor veilige ontwikkeling, acht praktijken

47 eisen. Deze norm is certificeerbaar door een geaccrediteerde instelling. Versie van 07/2026.

IEC 62443-4-1 kan gecertificeerd worden, maar het certificeringsobject is ongebruikelijk: wat wordt gecertificeerd is het ontwikkelproces van een met naam genoemde ontwikkelorganisatie, dus een concrete gedocumenteerde versie van de veilige levenscyclus. Niet een product en niet een persoon wordt gecertificeerd. De routes zijn ISASecure SDLA en het IECCE CB Scheme. Op dit moment leidt een dergelijk certificaat niet tot een vermoeden van conformiteit met de Cyberweerbaarheidsverordening van de EU (Cyber Resilience Act). Verwar dit niet met IEC 62443-4-2, die eisen stelt aan het component zelf. Deze lijst is een hulpmiddel voor zelfevaluatie, geen bewijs.

Bedrijf

Datum

Opgesteld door

5 Praktijk 1: Beveiligingsbeheer (SM)

13

SM-1 Er bestaat een gedefinieerde productontwikkelingscyclus die beveiliging door alle fasen heen borgt, van het eerste concept tot de buitengebruikstelling van het product, en deze cyclus is degene die in de praktijk daadwerkelijk wordt gevolgd.

[Document](#)

Waarvan je het vaststelt: Procesbeschrijving of werkinstructie met de fasen, de op te leveren resultaten per fase en de overdrachtpunten, samen met bewijs uit een lopend project waaruit blijkt dat de fasen daadwerkelijk zijn doorlopen. Een kleine organisatie kan volstaan met een pagina per fase plus een checklist in het ticketsysteem; belangrijk is dat het gedocumenteerde proces en de dagelijkse praktijk overeenkomen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-2 Elke taak in de veilige ontwikkelingscyclus heeft een aangewezen verantwoordelijke, en deze toewijzing is bekend bij de betrokken personen.

[Document](#)

Waarvan je het vaststelt: Rollen- en verantwoordelijkhedenmatrix die elke processtap koppelt aan een met naam genoemde rol, aangevuld met de actuele bezetting van die rollen. Met slechts een handvol mensen volstaat een tabel met rol, taak en persoon; belangrijk is de vervangingsregeling voor vakantie en ziekte.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-3 Er is traceerbaar vastgelegd welke producten, varianten, releases en componenten onder de veilige ontwikkelingscyclus vallen en welke niet.

[Document](#)

Waarvan je het vaststelt: Lijst van de producten en versiestatussen binnen de reikwijdte met een onderbouwing voor opname en uitsluiting, bijgewerkt bij elke nieuwe release. In de praktijk werkt een kolom in het productoverzicht goed, met per rij een ja of nee plus een zin toelichting.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-4 De mensen die beveiligingstaken op zich nemen, beschikken over de daarvoor benodigde technische competentie, en die competentie wordt bewust opgebouwd en actueel gehouden.

Waarvan je het vaststelt: Competentieprofiel per beveiligingsrol, kwalificatieoverzichten, opleidingsplan en aanwezigheidsregistraties, aangevuld met een overzicht van openstaande hiaten. Kleine organisaties tonen dit aan met certificaten, deelname aan conferenties of webinars en een korte jaarlijkse evaluatie van wie welk hiaat wanneer sluit, waarbij indien nodig externe expertise wordt ingehuurd.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-5	De reikwijdte van de veilige ontwikkelingscyclus is afgebakend en benoemt de betrokken locaties, organisatieonderdelen, leveranciersbijdragen en ontwikkelomgevingen, samen met de grenzen van die reikwijdte.	Document
Waaraan je het vaststelt: Reikwijdteverklaring die locaties, teams, uitbestede onderdelen en systemen omvat, plus een schets van de externe interfaces. Wie op één locatie ontwikkelt, legt dit in enkele zinnen vast en benoemt expliciet wat erbuiten valt, zoals extern ontwikkelde samenstellingen of hosting door derden.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		
SM-6	Voor elk element dat aan gebruikers wordt geleverd, software, firmware, configuraties en bijbehorende bestanden, is een integriteitscontrole mogelijk, zodat ontvangers een ongemerkte wijziging kunnen detecteren.	
Waaraan je het vaststelt: Handtekeningen of gepubliceerde controlesommen per opleverpakket, een beschrijving van de methode en een voorbeeld uit een echte release, samen met instructies voor de klant over hoe de controle uit te voeren. Voor kleine teams volstaat een ondertekend controlesombestand naast de download plus een alinea in de release notes.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		
SM-7	De omgevingen die worden gebruikt voor ontwikkeling, build en test zijn beschermd tegen ongeautoriseerde toegang en tegen manipulatie van broncode, buildhulpmiddelen en artefacten.	
Waaraan je het vaststelt: Toegangsbeveiligingsconcept voor repository, buildserver en testsystemen, toegangslijsten met de datum van de laatste beoordeling, registraties van beveiligingsrelevante wijzigingen en bewijs dat productie- en ontwikkeltoegang gescheiden zijn. Zonder eigen IT-afdeling volstaan tweefactorauthenticatie, een beschermde hoofdbranch met verplichte review en een halfjaarlijkse controle van wie nog toegang heeft.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		
SM-8	Privésleutels die worden gebruikt om leveringen te ondertekenen, zijn beschermd tegen openbaarmaking en misbruik, en het gebruik ervan is beperkt tot geautoriseerde personen en systemen.	
Waaraan je het vaststelt: Beschrijving van sleutelopslag, toegang, vernieuwing en intrekking, bewijs van beschermde opslag zoals een hardwaretoken of een sleutelbeheerdienst, plus registraties van ondertekeningshandelingen. Een kleine organisatie bewaart de ondertekenings sleutel op een hardwaretoken, documenteert de twee personen met toegang en houdt een procedure klaar voor het geval van verlies.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		
SM-9	Voor ingekochte of overgenomen componenten, met inbegrip van opensourcesoftware, zijn de beveiligingsverwachtingen ten aanzien van de leverancier vastgelegd en worden deze toegepast bij de selectie.	Document
Waaraan je het vaststelt: Beveiligingseisen in leveranciersspecificaties of contracten, selectiecriteria voor componenten van derden, een inventarisatie van alle componenten van derden met versie en herkomst, plus de beoordeling of de leverancier aan de verwachtingen voldoet. Zonder inkoopafdeling volstaat een bijgehouden componentenlijst met een kolom waarin wordt vastgelegd of de beveiligingsupdates en meldkanalen van de leverancier zijn gecontroleerd.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		
SM-10	Componenten die in opdracht door een derde partij zijn ontwikkeld, zijn onderworpen aan dezelfde beveiligingseisen als interne ontwikkeling, en de naleving ervan wordt geverifieerd.	
Waaraan je het vaststelt: Inkooporder of contractdocumenten waarin de vereiste beveiligingsverplichtingen zijn vastgelegd, bewijs van de dienstverlener over de toegepaste werkwijzen, acceptatieregistraties en resultaten van eigen controles op het opgeleverde werk. Zonder auditbudget volstaan een contractuele garantie, het aanleveren van de testresultaten van de leverancier en een eigen steekproefcontrole voorafgaand aan acceptatie.		
OpenIn behandelingVoldaanNiet van toepassing		
Bewijs / onderbouwing		

SM-11

Beveiligingsgerelateerde bevindingen uit alle bronnen, tests, reviews, gebruikersmeldingen en meldingen van derden, worden vastgelegd, beoordeeld op hun impact, toegewezen aan een verantwoordelijke met een streefdatum, en opgevolgd tot afsluiting.

[Document](#)

Waaraan je het vaststelt: Defecten- of ticketsysteem met een specifieke markering voor beveiligingsonderwerpen, en per item de impactbeoordeling, de verantwoordelijke, de streefdatum en de afsluitnotitie, plus een overzicht van openstaande punten. Een klein team gebruikt een label in het bestaande ticketsysteem en een vast agendapunt in het wekelijkse overleg.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-12

Voordat een product wordt vrijgegeven, wordt geverifieerd en aangetoond dat de beoogde stappen van de veilige ontwikkelingscyclus daadwerkelijk zijn uitgevoerd en dat de bijbehorende registraties zijn opgesteld.

[Document](#)

Waaraan je het vaststelt: Releasebeoordeling per release waarbij wordt getoetst aan de processtappen, met verwijzingen naar de betreffende registraties en een gedocumenteerd releasebesluit met datum en handtekening. In de praktijk werkt een releasechecklist goed die geen levering toestaat zonder volledig afgevinkte punten; openstaande punten worden onderbouwd en van een datum voorzien.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SM-13

De veilige ontwikkelingscyclus zelf wordt regelmatig ter discussie gesteld en verbeterd, op basis van inzichten uit incidenten, testresultaten, feedback van klanten en het dreigingslandschap.

Waaraan je het vaststelt: Registraties van de procesbeoordeling, bijvoorbeeld een directiebeoordeling of retrospectief, met de daaruit voortvloeiende procesveranderingen, de status van implementatie en een verwijzing naar de grondoorzaak. Wie de volwassenheidsniveaus van de norm gebruikt, legt per praktijk de huidige stand en het streefniveau vast; volwassenheidsniveau 4 vereist precies dit bewijs van continue verbetering. Voor een kleine organisatie volstaat een jaarlijkse bijeenkomst met notulen en drie concrete verbeteringen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

6 Praktijk 2: Specificatie van beveiligingseisen (SR)

5

SR-1

De beoogde productcontext is beschreven: de verwachte operationele omgeving, de beveiligingsmaatregelen waarvan wordt aangenomen dat die omgeving ze levert, de beoogde gebruikersgroepen en rollen, de veronderstelde vertrouwensgrenzen, en de toepassingen waarvoor het product expliciet niet is bedoeld.

[Document](#)

Waaraan je het vaststelt: Een beschrijving van de beveiligingscontext van het product, hetzij als apart document, hetzij als vast onderdeel van de productspecificatie, die de netwerk omgeving, veronderstelde externe beschermingsmaatregelen zoals een firewall of fysieke toegangsbeveiliging, een lijst van rollen, en een expliciete lijst van toepassingen buiten de reikwijdte omvat. Een kleine organisatie beperkt dit tot twee pagina's, voegt een eenvoudige schets van de installatieomgeving toe en laat de producteigenaar dit dateren en goedkeuren.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR-2

Er bestaat een dreigingsmodel voor het product dat gegevensstromen, interfaces, vertrouwensgrenzen en aanvalspaden in kaart brengt, de daaruit voortvloeiende dreigingen en hun mogelijke impact benoemt, en tegenmaatregelen toewijst. Het wordt beoordeeld en bijgewerkt bij relevante wijzigingen en ten minste eenmaal per productrelease, en openstaande punten worden opgevolgd tot ze zijn afgesloten.

[Document](#)

Waaraan je het vaststelt: Dreigingsmodel met een gegevensstroomdiagram, een dreigingslijst per interface, toegewezen tegenmaatregelen en de status van openstaande punten, plus een revisiegeschiedenis met datum en auteur. Een kleine organisatie kan werken met een tabel per interface, met kolommen voor wat er mis kan gaan, hoe ernstig dat zou zijn, wat eraan wordt gedaan, en wie het beoordeelt.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR-3

De beveiligingseisen voor het product zijn vastgesteld en gedocumenteerd. Ze omvatten de resultaten van het dreigingsmodel, de beschreven beveiligingscontext van het product, de toepasselijke wettelijke en contractuele verplichtingen en het beoogde beveiligingsniveau, en ze bevatten de beveiligingsfuncties die het product zelf moet leveren.

[Document](#)

Waarvan je het vaststelt: Eisenlijst of tool voor eisenbeheer met een uniek identificatienummer per eis, de bron van elk item zoals een dreiging, een klantcontract of een wettelijke verplichting, en het beoogde beveiligingsniveau. Een kleine organisatie werkt dit uit als één tabel met een vaste ID-kolom waarop verificatie en tests later aansluiten.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR-4

Elke afzonderlijke beveiligingseis is zo geformuleerd dat deze ondubbelzinnig, vrij van tegenstrijdigheden, toetsbaar en herleidbaar is tot een specifieke productfunctie of interface, en de eis bevat de informatie die nodig is om deze later zonder verdere toelichting te verifiëren.

Waarvan je het vaststelt: Een steekproef uit de eisenlijst die voor elke eis een meetbaar acceptatiecriterium en de betrokken functie of interface toont, samen met de koppeling tussen eis en testgeval. Een kleine organisatie controleert dit met een vast formuleringssjabloon en de controlevraag of er een testgeval uit de eis kan worden geschreven zonder terugvraag.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR-5

De beveiligingseisen worden beoordeeld voordat ze worden gebruikt in ontwerp en implementatie, met betrokkenheid van de betrokken partijen, zoals ontwikkeling, test, producteigenaarschap en, waar nuttig, verkoop of de klant. De beoordeling omvat volledigheid ten opzichte van het dreigingsmodel en de beveiligingscontext van het product, juistheid en toetsbaarheid. Bevindingen worden vastgelegd en opgevolgd tot afsluiting.

Waarvan je het vaststelt: Beoordelingsverslag met datum, deelnemers en hun rollen, de beoordeelde versie van de eisen, een lijst van bevindingen met een verantwoordelijke en afsluitstatus, en een goedkeuringsnotitie. Een kleine organisatie regelt dit als een beoordeling door twee personen, ontwikkeling en test, met een kort verslag en een goedkeuringsregel in de eisenlijst.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

7 Praktijk 3: Beveiliging door ontwerp (SD)

4

SD-1

Elk product heeft een ontwerpbeschrijving die de beveiligingsrelevante aspecten van de architectuur vastlegt: welke componenten er zijn, hoe ze onderling communiceren, waar de vertrouwensgrenzen lopen, welke externe interfaces worden blootgesteld en met welke mechanismen de eerder vastgestelde beveiligingseisen in het ontwerp worden gerealiseerd.

[Document](#)

Waarvan je het vaststelt: Architectuurdocument of ontwerpspecificatie met een diagram dat componenten, gegevensstromen en vertrouwensgrenzen toont, plus een koppelingstabel van elke beveiligingseis naar het ontwerpelement dat deze realiseert. Een kleine leverancier komt uit met één bijgehouden diagram plus twee of drie pagina's toelichting; belangrijk is dat het versiebeheerd is in de repository en wordt bijgewerkt telkens wanneer de architectuur verandert.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SD-2

Het ontwerp wordt systematisch geanalyseerd op dreigingen. De analyse benoemt de doelstellingen van de aanvaller, de betrokken vertrouwensgrenzen en interfaces, de daaruit voortvloeiende dreigingen met hun waardering, en de in het ontwerp getroffen tegenmaatregelen. De analyse wordt herhaald telkens wanneer de architectuur of de omgeving wezenlijk verandert, en geïdentificeerde dreigingen worden opgevolgd totdat over elk ervan een besluit is genomen.

[Document](#)

Waarvan je het vaststelt: Dreigingsmodel per product of per grote release, bijvoorbeeld een tabel met kolommen voor dreiging, betrokken interface, waardering, tegenmaatregel en status, samen met de notulen van de modelleersessie met deelnemers en datum. Een klein team modelleert pragmatisch in een workshop van twee tot drie uur aan de hand van het architectuurdiagram en legt openstaande punten vast als tickets, zodat het bewijs van opvolging zonder extra inspanning ontstaat.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SD-3 Het ontwerp volgt aantoonbaar erkende principes voor veilig ontwerpen, waaronder minimale rechten, minimaal aanvalsoppervlak, gelaagde verdediging, veilige standaardinstellingen, veilig gedrag bij storingen en beveiligingsmechanismen die zo eenvoudig en toetsbaar mogelijk zijn. De toepassing van deze principes is zichtbaar in het ontwerp en onderbouwd.

Waarvan je het vaststelt: Een paragraaf in de ontwerpbeschrijving of een interne ontwerprijtlijn die de principes benoemt, plus concreet bewijs per principe in het product, zoals de rechtenmatrix van de diensten, de lijst van open poorten met onderbouwing, de standaardinstellingen bij levering of het gedocumenteerde foutafhandelingsgedrag. Een kleine leverancier gebruikt een korte checklist van deze principes als vast onderdeel van de ontwerpbeoordeling en bewaart het ingevulde formulier bij het ontwerp.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SD-4 Het ontwerp wordt door gekwalificeerde collega's beoordeeld voordat de implementatie begint. De beoordeling omvat volledigheid ten opzichte van de beveiligingseisen, de juistheid en doeltreffendheid van de beveiligingsmechanismen en de resultaten van de dreigingsanalyse. Personen met voldoende beveiligingscompetentie nemen deel, bevindingen worden vastgelegd en opgevolgd tot afsluiting.

Document

Waarvan je het vaststelt: Beoordelingsverslag met datum, het beoordeelde item inclusief versie, deelnemers en hun rollen, lijst van bevindingen met status en het releasebesluit. Een klein team koppelt de beoordeling aan de pull request van de ontwerpdocumenten en laat de bevindingen als opmerkingen achter met een afsluitnotitie, wat opvolging aantoont zonder aanvullende hulpmiddelen. Wanneer beveiligingscompetentie intern ontbreekt, is een extern beoordelaar die per uur wordt ingeschakeld voor de kritieke ontwerpen de pragmatische route.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

8 Praktijk 4: Veilige implementatie (SI)

2

SI-1 Er bestaat een gedefinieerd proces om de daadwerkelijke implementatie te toetsen aan het veilige ontwerp: de beoordeling bevestigt dat de in het ontwerp voorziene beschermingsmaatregelen daadwerkelijk aanwezig en doeltreffend zijn in de code, dat de gelaagde verdediging behouden blijft, en dat er tijdens de implementatie geen nieuwe kwetsbaarheden zijn geïntroduceerd. De beoordeling wordt uitgevoerd door voldoende gekwalificeerd personeel, en eventuele geconstateerde afwijkingen worden vastgelegd en opgevolgd tot afsluiting.

Waarvan je het vaststelt: Een schriftelijke procedure voor implementatiebeoordeling samen met beoordelingsverslagen per component of release: de beoordeelde module, de verwijzing naar het ontwerpdocument, de datum, de beoordelaar, de bevindingen en hun oplossingsstatus. Geschikt bewijs zijn pull request reviews met een verplichte beveiligingschecklist, resultaten van statische codeanalyse met een gedocumenteerde beoordeling van elke treffer, en notulen van beoordelingssessies. Een klein team dekt dit af met het vierogenprincipe, een beoordelingssjabloon in de repository waarin elke ontwerpmaatregel afzonderlijk wordt afgevinkt, en één ticket per openstaande bevinding. Het essentiële punt is dat de auteur van de code nooit de beoordelaar van diezelfde code is.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SI-2 Bindende regels voor veilig programmeren gelden voor al het beveiligingsrelevante ontwikkelwerk en omvatten ten minste het vermijden van bekende onveilige constructies en functies, de omgang met invoer en fouten, het beheer van geheugen en resources, en het gebruik van beproefde beveiligingscode in plaats van zelf geschreven implementaties. De regels gelden per gebruikte programmeertaal, zijn bekend bij alle ontwikkelaars, en worden bijgewerkt wanneer nodig, bijvoorbeeld wanneer nieuwe aanvalspatronen of nieuwe hulpmiddelen opkomen.

Document

Waarvan je het vaststelt: Een goedgekeurde standaard voor veilig programmeren met versiestatus, reikwijdte per taal en goedkeuringsdatum, aangevuld met bewijs dat deze in het dagelijkse werk wordt toegepast: de configuratie van linters en analysehulpmiddelen in de repository, een buildregel die overtredingen zichtbaar maakt, en de aanwezigheidslijst van de instructiesessie. Kleine organisaties schrijven geen standaard vanaf nul; ze verklaren een gevestigde openbare regelset bindend, voegen een korte lijst met eigen aanvullende regels toe, en verankeren de controle in de pipeline, zodat naleving automatisch wordt aangetoond.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

9 Praktijk 5: Beveiligingsverificatie en -validatietests (SVV)

5

SVV-1

Elke beveiligingsgerelateerde producteis heeft ten minste één testgeval toegewezen gekregen, waarmee wordt aangetoond dat de beschermingsfunctie tijdens normaal gebruik werkt zoals bedoeld, dat deze zich gedraagt zoals gespecificeerd bij ongeldige invoer of misbruik, en dat de standaardinstellingen waarmee het product wordt geleverd overeenkomen met de veilige toestand. Uitvoering en uitkomst worden vastgelegd voor elke geteste softwareversie.

[Document](#)

Waarvan je het vaststelt: Een traceerbaarheidsmatrix die eis, testgeval en resultaat aan elkaar koppelt, plus testverslagen met de datum, de geteste versie of build, en de naam van de persoon die de test heeft uitgevoerd. Een kleine leverancier voegt eenvoudig een kolom met testgeval-ID toe aan de eisenlijst en archiveert het uitvoerlogboek van de geautomatiseerde testrun uit de buildpipeline als bijlage bij de betreffende versie.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SVV-2

De uit het dreigingsmodel afgeleide tegenmaatregelen worden specifiek getest om te bevestigen dat ze het veronderstelde aanvalspad daadwerkelijk afsluiten. Er wordt getest tegen de geïdentificeerde dreigingen, niet alleen tegen correct gebruik, en openstaande punten worden ingebracht in het defectafhandelingsproces.

Waarvan je het vaststelt: Testgevallen die rechtstreeks verwijzen naar de items van het dreigingsmodel, bijvoorbeeld één misbruikscenario per dreigings-ID met het verwachte verdedigingsgedrag, samen met de verslagen van die testruns. Zonder zwaar instrumentarium volstaat het om aan het dreigingsmodel een kolom toe te voegen die verwijst naar het testgeval en de datum van de laatste geslaagde controle.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SVV-3

Het product wordt vóór vrijgave systematisch onderzocht op kwetsbaarheden. De reikwijdte omvat ten minste: onderzoek van de extern bereikbare interfaces en diensten, tests met misvormde en willekeurig gemuteerde invoer, toetsing van de gebruikte componenten van derden aan bekende gemelde kwetsbaarheden, en een controle op bekende zwakteklassen in de eigen code van de leverancier. Bevindingen worden vastgelegd samen met hun beoordeling.

[Document](#)

Waarvan je het vaststelt: Rapporten van de gebruikte hulpmiddelen, met vermelding van naam, versie en de gegevensstand van de kwetsbaarheidendatabase, fuzzingverslagen, een lijst van componenten van derden met de datum van de laatste vergelijking, en de bevindingenlijst met beoordeling en besluit. Een kleine leverancier combineert gratis standaardtools, een dependencyscan en een poort- en dienstenscan tegen het geïnstalleerde product, en bewaart de uitvoer per release in één map.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SVV-4

De releasekandidaat wordt onderworpen aan een aanvalspoging onder realistische omstandigheden, waarbij actief wordt geprobeerd de beschermingsmechanismen te omzeilen in plaats van deze alleen te bevragen. Reikwijdte, randvoorwaarden en grenzen van de test worden vooraf overeengekomen, en de gevonden zwakheden worden behandeld en opgevolgd als defecten.

Waarvan je het vaststelt: De opdracht of testorder met vermelding van reikwijdte en testomgeving, een rapport over de aanpak, de benutte zwakheden en hun beoordeling, plus de items in het defecten- of ticketsysteem met bewijs van herstel of van een onderbouwde risicoacceptatie. Kleine leveranciers kopen deze test doorgaans extern in met een afgebakend tijdsbudget, of laten deze uitvoeren door iemand die het product niet heeft ontwikkeld.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SVV-5

De onafhankelijkheid van het testpersoneel is vastgelegd en passend bij het beoogde volwassenheidsniveau. Wie een component heeft ontwikkeld, geeft deze niet vrij op basis van uitsluitend eigen tests, en naarmate het volwassenheidsniveau stijgt, ligt de verantwoordelijkheid voor het testen bij een organisatorisch gescheiden eenheid of een externe partij. De daadwerkelijke toewijzing is voor elke test herleidbaar.

Waarvan je het vaststelt: Een rollenverdeling binnen het ontwikkelproces waaruit de scheiding tussen creatie en testen blijkt, plus, voor elke testrun of elk testrapport, de vastgelegde naam en rol van de persoon die de test heeft uitgevoerd. Een bedrijf met twee personen regelt dit via wederzijdse beoordeling met een gedocumenteerde vierogennotitie, en schakelt een externe persoon in voor de diepgaande beveiligingstests.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

10 Praktijk 6: Beheer van beveiligingsdefecten (DM)

6

DM-1

Er bestaat een vastgesteld kanaal waarlangs meldingen van beveiligingszwakheden in het product vanuit alle richtingen worden ontvangen en geregistreerd: van het ontwikkelteam zelf, van tests en beoordelingen, van klanten en integrators, van externe melders, en van adviezen over gebruikte componenten van derden en opensourcecomponenten. Het meldkanaal is vindbaar voor externe partijen, en elke melding wordt vastgelegd met de ontvangstdatum en de herkomst.

[Document](#)

Waaraan je het vaststelt: Een beschrijving van het meldkanaal, het publiek bereikbare contactpunt (een beveiligingspagina, een security.txt bestand, of een postbus zoals security@), en het intakeregister met datum, herkomst en een korte beschrijving per melding. Een kleine organisatie kan werken met een gedeelde postbus en één spreadsheet of ticketlabel, zolang elke melding daar terecht komt, inclusief meldingen die in de interne ontwikkelaarschat naar voren komen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

DM-2

Elke binnenkomende melding wordt getrieerd en onderzocht om vast te stellen of deze beveiligingsrelevant is en welke producten, versies en componenten worden geraakt. Meldingen die niet beveiligingsrelevant blijken te zijn, of niet van toepassing zijn, worden ook afgesloten met een vermelde reden in plaats van stilzwijgend terzijde gelegd.

Waaraan je het vaststelt: Een triagenotitie per melding met de uitkomst (beveiligingsrelevant ja of nee), de betrokken versies, en de reden van afwijzing waar van toepassing, zichtbaar in het ticket of in de intakelijst. Teams met een laag meldingsvolume kunnen de triage uitvoeren in een korte terugkerende sessie en de uitkomst in twee zinnen per item vastleggen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

DM-3

Bevestigde beveiligingsdefecten worden beoordeeld volgens een consistente methode: grondoorzaak, betrokken versies en configuraties, potentiële impact op werking en beveiliging, uitbuitbaarheid, en ernst tegen een vastgestelde schaal. Het resultaat van de beoordeling wordt vastgelegd en is herleidbaar.

[Document](#)

Waaraan je het vaststelt: Een beoordelingsverslag of een set ticketvelden per defect met grondoorzaak, ernst, en de toegepaste schaal (bijvoorbeeld een gangbaar puntensysteem met een gedocumenteerde vector), samen met de lijst van betrokken versies. Kleine teams kunnen steunen op een vast veldensjabloon in het ticketsysteem plus een halve pagina die de schaal en de drempels beschrijft die onmiddellijke actie vereisen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

DM-4

Voor elk beoordeeld beveiligingsdefect wordt een besluit genomen over de aanpak: herstel, compenserende maatregel, of een onderbouwde risicoacceptatie. Het besluit volgt uit de ernst, wordt toegewezen aan een verantwoordelijke persoon en een streefdatum, en het defect wordt opgevolgd tot afsluiting.

[Document](#)

Waaraan je het vaststelt: Een actielijst of ticketstatus met verantwoordelijke, streefdatum, type maatregel, en een afsluitnotitie, gekoppeld aan de codebasislijn of de release waarin de oplossing van kracht wordt. Geaccepteerde restrisico's vereisen een korte schriftelijke onderbouwing die door het producteigenaarschap wordt goedgekeurd. Een kleine organisatie kan dit bijhouden op een ticketbord met streefdata, zonder aanvullende hulpmiddelen.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

DM-5

Betrokken gebruikers, integrators en andere belanghebbenden worden over beveiligingsdefecten geïnformeerd zodra de beoordeling daartoe aanleiding geeft, met vermelding van de betrokken versies, de impact, en de beschikbare oplossing of compenserende maatregel. Tijdlijnen en de doelgroep van een dergelijke openbaarmaking zijn vooraf vastgesteld, evenals de aanpak voor meldingen van derden die met een eigen openbaarmakingstermijn komen.

Waaraan je het vaststelt: Gepubliceerde beveiligingsmeldingen of adviezen met een datum en versievermelding, de distributielijst of het abonneekanaal, en de schriftelijke regel over tijdlijnen en gecoördineerde openbaarmaking. Leveranciers met weinig klanten kunnen volstaan met één mailing naar een bijgehouden klantenlijst plus een gedateerde adviespagina waarvan de wijzigingen worden bijgehouden in versies.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

DM-6

De afhandeling van beveiligingsdefecten wordt op vaste tijdstippen beoordeeld. De beoordeling kijkt naar openstaande en achterstallige gevallen, de tijd van melding tot herstel, terugkerende grondoorzaken, en de doeltreffendheid van de getroffen maatregelen. Procesverbeteringen die uit de beoordeling voortvloeien, worden doorgevoerd en de doorvoering ervan wordt opgevolgd.

[Document](#)

Waaraan je het vaststelt: Notulen van de terugkerende beoordeling met datum, deelnemers, cijfers over openstaande en achterstallige gevallen, en een lijst van overeengekomen verbeteringen met verantwoordelijke en streefdatum. Een kleine organisatie kan dit punt koppelen aan een bestaand kwartaaloverleg en de cijfers en besluiten op één pagina bijhouden.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

11 Praktijk 7: Beheer van beveiligingsupdates (SUM)

5

SUM-1

Elke beveiligingsupdate voor het product wordt geverifieerd tegen de ondersteunde productversies en operationele omgevingen voordat deze aan klanten wordt vrijgegeven, en er is een registratie die aantoont dat de update de kwetsbaarheid verhelpt zonder de beoogde productfunctie te verstoren.

[Document](#)

Waaraan je het vaststelt: Testverslag per patch met de geteste productversie, het platform, de testgevallen (doeltreffendheid tegen de kwetsbaarheid plus regressie van kernfuncties) en de vrijgavegoedkeuring. Een kleine leverancier kan werken met een korte goedkeuringsvermelding voor de patch in het ticket: ticket-ID, geverifieerd door, geverifieerd op, resultaat, met het logboek van de geautomatiseerde testrun als bijlage.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SUM-2

Voor alle productcomponenten die niet intern zijn ontwikkeld (bibliotheken van derden, besturingssysteem, runtime-omgevingen), is vastgelegd en aangetoond hoe hun beveiligingsupdates worden beoordeeld en ofwel in het product worden opgenomen ofwel worden afgewezen met een gedocumenteerde onderbouwing.

[Document](#)

Waaraan je het vaststelt: Componenteninventaris van de onderdelen van derden met versie en herkomst, plus één beoordelingsvermelding per gemelde kwetsbaarheid van derden met het besluit (opnemen, niet geraakt, afgedekt door een compenserende maatregel) en de onderbouwing. Kleine teams voeren een geautomatiseerde dependencyscan uit in de build en houden de besluiten bij als opmerkingen bij het scanresultaat of in een beknopte uitzonderingslijst.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SUM-3

Bij elke uitgebrachte beveiligingsupdate ontvangen gebruikers begrijpelijke begeleidende informatie: welke productversies worden geraakt, welke kwetsbaarheid wordt verholpen, hoe ernstig deze is, of er bijwerkingen of compenserende maatregelen in acht moeten worden genomen, en hoe de update wordt geïnstalleerd.

[Document](#)

Waaraan je het vaststelt: Gepubliceerde beveiligingsadviezen of release notes met het kwetsbaarheidsidentificatienummer, de betrokken versies, de ernstclassificatie, de installatiestappen en instructies voor het terugzetten naar de vorige toestand. Kleine leveranciers houden één publieke pagina bij met een chronologische lijst van beveiligingsadviezen en verwijzen ernaar vanuit het product.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SUM-4

Er is een vastgestelde en tegen manipulatie beschermde route waarlangs gebruikers beveiligingsupdates verkrijgen, en de authenticiteit en integriteit van een update kunnen aan gebruikerszijde worden geverifieerd voordat deze wordt geïnstalleerd.

Waaraan je het vaststelt: Beschrijving van het leveringskanaal (downloadgebied, updateserver, fysieke media) samen met de beschermingsmaatregelen ervan, plus de digitale handtekening of controlesom per pakket en instructies die de gebruiker vertellen hoe deze te verifiëren. Kleine leveranciers bereiken dit door te ondertekenen op de buildserver, de controlesom naast de download te publiceren en één duidelijke locatie te benoemen waar de publieke sleutel wordt bewaard.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SUM-5

Er bestaan vastgestelde tijddoelen voor het beschikbaar stellen van beveiligingsupdates, gegradueerd naar de ernst van de kwetsbaarheid; de daadwerkelijk gehaalde tijden worden bijgehouden, en elk gemist doel wordt onderbouwd en ondersteund door een tussentijdse maatregel voor gebruikers.

[Document](#)

Waaraan je het vaststelt: Interne specificatie met een tijdvenster per ernstcategorie (bijvoorbeeld kritiek <= 30 dagen, hoog <= 90 dagen) en een evaluatie per kwetsbaarheid: meldingsdatum, datum van patchuitgifte, verstreken dagen, reden van afwijking. Kleine leveranciers houden dit bij als twee datumvelden in het kwetsbaarheidsticket en beoordelen de lijst eenmaal per kwartaal in plaats van een apart metriekensysteem op te zetten.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

12 Praktijk 8: Beveiligingsrichtlijnen voor inzet en gebruik van het product (SG)

7

SG-1

Elk product wordt geleverd met een beschrijving van de strategie voor gelaagde verdediging: deze benoemt de beschermingslagen die in het product zelf zijn ingebouwd, koppelt ze aan de dreigingen die ze tegengaan, en toont welk beschermend effect pas ontstaat door de samenwerking van meerdere lagen.

[Document](#)

Waaraan je het vaststelt: Een paragraaf in de geleverde productdocumentatie, of een apart beveiligingsconcept, die per beschermingslaag het mechanisme, de gedekte dreiging en de grenzen van het effect vermeldt. Een kleine organisatie houdt dit bij als een tabel van twee pagina's: kolom beschermingslaag, kolom dreiging overgenomen uit het eigen dreigingsmodel, kolom restrisico. Een kruisverwijzing naar het dreigingsmodel uit SR-2 volstaat, de inhoud hoeft niet dubbel te worden bijgehouden.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-2

De documentatie benoemt de beveiligingsmaatregelen die het product niet zelf levert maar verwacht van de inzetomgeving, bijvoorbeeld netwerksegmentatie, voorgeschakelde firewalls, fysieke toegangsbeveiliging of een externe tijddienst, en maakt duidelijk dat het gewaarborgde beveiligingsniveau zonder deze maatregelen niet wordt bereikt.

[Document](#)

Waaraan je het vaststelt: Een hoofdstuk over inzetvoorwaarden in de handleiding, of een referentiearchitectuurtekening met zones en verbindingen waarin de door de asset-eigenaar te leveren maatregelen expliciet zijn gemarkeerd. Een lijst met aannames over de omgeving heeft zich in de praktijk bewezen, rechtstreeks afgeleid van de beveiligingscontext van het product en opnieuw doorgenomen bij elke productversie.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-3

Er bestaat een handleiding voor een veilige basisconfiguratie die alle beveiligingsrelevante instellingen, diensten, poorten en interfaces opsomt, de aanbevolen toestand bij levering vermeldt en het effect van afwijking van die aanbeveling beschrijft.

[Document](#)

Waaraan je het vaststelt: Hardeningshandleiding met een instellingentabel: parameter, aanbevolen waarde, effect, bijwerking bij afwijking. Plus de lijst van diensten en poorten die in de standaardconfiguratie actief zijn, met de onderbouwing waarom ze ingeschakeld blijven. Een klein team houdt deze tabel direct naast het configuratiebestand in de repository en exporteert deze naar de opleverdocumentatie, zodat deze afgestemd blijft op het product.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-4

Voor het lopende gebruik bestaat er een handleiding die beschrijft hoe het product veilig wordt gebruikt, bewaakt en in zijn veilige toestand wordt gehouden, met inbegrip van back-up en herstel, logging en de omgang met beveiligingsrelevante gebeurtenismeldingen.

[Document](#)

Waaraan je het vaststelt: Gebruikshandleiding met paragrafen over logging, back-ups, herstart en gebeurtenismeldingen. Als aanvullend bewijs een lijst van de beveiligingsrelevante meldingen die het product uitzendt, elk met een korte aanbevolen actie, zodat de asset-eigenaar deze niet alleen hoeft te interpreteren.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-5

De documentatie legt uit hoe gebruikersaccounts, rollen en rechten van het product worden ingesteld en onderhouden, in het bijzonder scheiding van rollen, het wijzigen van standaardreferenties en het verwijderen van accounts die niet langer nodig zijn.

[Document](#)

Waarom je het vaststelt: Een hoofdstuk over accountbeheer met een overzicht van rollen en de aan elke rol toegekende rechten, plus een expliciete vermelding over standaardreferenties en het wijzigen ervan bij ingebruikname. Een korte checklist voor ingebruikname in de handleiding werkt in de praktijk goed, die de asset-eigenaar kan afvinken en archiveren.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-6

Er bestaat een handleiding voor veilige buitengebruikstelling die de volledige verwijdering van gevoelige gegevens uit het product beschrijft, zoals referenties, sleutels, configuratiegegevens en logbestanden, voordat het apparaat wordt doorgegeven, hergebruikt of afgevoerd.

[Document](#)

Waarom je het vaststelt: Een paragraaf over buitengebruikstelling die elke opslaglocatie van gevoelige gegevens binnen het product en de bijbehorende wisprocedure vermeldt, met inbegrip van de gevallen waarin wissen technisch onmogelijk is en de hardware fysiek moet worden vernietigd. Een lijst van persistente opslag, overgenomen uit de architectuurbeschrijving, helpt hierbij; deze voorkomt dat een opslaglocatie wordt vergeten.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SG-7

De aan gebruikers geleverde beveiligingsdocumentatie wordt vóór vrijgave beoordeeld: deze is technisch juist, consistent met de geleverde productversie, volledig ten opzichte van de beoogde inhoud en begrijpelijk voor de beoogde doelgroep, en wordt bijgewerkt telkens wanneer het product verandert.

Waarom je het vaststelt: Een beoordelingsverslag per document en productversie met beoordelaar, datum, bevindingen en hun afsluiting, gekoppeld aan de vrijgavegoedkeuring. Een kleine organisatie lost dit op met het vierogenprincipe in de pull request van de documentatie: één ontwikkelaar controleert de technische inhoud, een tweede persoon controleert de begrijpelijkheid, en de goedkeuring wordt vastgelegd in het ticket. Een versie mag pas worden uitgeleverd zodra de beoordeling is gedocumenteerd.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

IEC 62443-3-3:2013 Systeembeveiligingseisen voor industriële automatisering

Zeven fundamentele eisen, 51 systeemeisen

100 eisen. Deze norm is certificeerbaar door een geaccrediteerde instelling. Versie van 07/2026.

IEC 62443-3-3 kan worden gecertificeerd, en wat wordt gecertificeerd is een systeem, niet een organisatie en niet een persoon. De routes zijn ISASecure SSA en het IECCEB Scheme. Wie de organisatie wil certificeren heeft 62443-2-1 of 2-4 nodig, wie het component bedoelt heeft 62443-4-2 nodig. Deze lijst bevat de 51 systeemeisen en de 49 eisverbeteringen. Welke daarvan van toepassing zijn, hangt af van het beveiligingsniveau dat wordt nagestreefd: 38 vanaf SL 1, 60 vanaf SL 2, 90 vanaf SL 3, alle 100 bij SL 4. Geen enkele verbetering geldt al bij SL 1. Deze lijst is een werkhulpmiddel voor zelfevaluatie, geen bewijs.

Bedrijf

Datum

Opgesteld door

5 FR 1: Wie of wat om toegang vraagt, en of dit werkelijk is wie het beweert te zijn

24

SR 1.1 Menselijke gebruikers worden geïdentificeerd en hun identiteit wordt geverifieerd voordat ze toegang krijgen, op elk punt waar ze het automatiseringssysteem kunnen bedienen of configureren. Dit omvat operatorpanelen bij de machine, engineering-toegang en netwerkdiensten.

Waaraan je het vaststelt: Inventarisatie van alle aanmeldpunten in het systeem, dat wil zeggen HMI, controlekamer, PLC-programmeertoegang, switch, VPN en client voor onderhoud op afstand, elk met het daar gebruikte authenticatiemechanisme. Voeg een configuratie-uitreksel van een scherm afbeelding van het aanmeldscherm toe voor elke apparaatklasse. Een kleine organisatie begint met een tabel per apparaat, kolommen: apparaat, interface, authenticatie aanwezig ja of nee, motivering indien nee. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.1 RE 1 Elke menselijke gebruiker werkt onder een individuele identificatie die uitsluitend aan die persoon is toegewezen. Gedeelde accounts en ploegenaccounts zijn uitgeschakeld, resterende uitzonderingen worden per geval gemotiveerd en onderbouwd met aanvullende maatregelen.

Waaraan je het vaststelt: Accountexport per systeem die identificatie aan persoon koppelt, uitzonderingenlijst met motivering en compenserende maatregel, bijvoorbeeld een camera of een aanwezigheidsregistratie bij het operatorstation. Deze regel is een eisverbetering en is dus nooit verplicht bij SL 1, ze is vereist vanaf SL 2.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.1 RE 2 Wie zich aanmeldt vanuit een niet-vertrouwd netwerk, bijvoorbeeld vanaf internet of via een verbinding voor onderhoud op afstand, bewijst zijn identiteit met minstens twee onafhankelijke factoren.

Waaraan je het vaststelt: Configuratie van de toegang op afstand met de tweede factor ingeschakeld, een voorbeeldregistratie van een aanmelding die beide factoren toont, en de uitgiftelijst van tokens of app-registraties. Een kleine organisatie gebruikt de tweede factor van de bestaande VPN-gateway of een authenticator-app, wat naast de configuratietijd niets kost. Eisverbetering, vereist vanaf SL 3, niet bij SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.1 RE 3 Het bewijs met twee onafhankelijke factoren geldt niet alleen voor toegang van buitenaf, maar voor elke aanmelding van een menselijke gebruiker, inclusief aanmeldingen binnen het netwerk dat als vertrouwd is geclassificeerd.

Waaraan je het vaststelt: Beleidsuittreksel van de centrale authenticatiedienst waaruit blijkt dat de tweede factor wordt afgedwongen zonder enige netwerkuitzondering, plus voorbeeldregistraties van aanmeldingen uit de controlekamer en het operatorpaneel. Eisverbetering, pas vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.2 Niet alleen mensen, maar ook softwareprocessen en apparaten authenticeren zich bij het systeem voordat ze gegevens mogen uitwisselen of diensten mogen gebruiken. Dit omvat koppelingen tussen controllers, datakoppelingen naar hoger gelegen systemen en diagnosetools.

Waaraan je het vaststelt: Lijst van machine-naar-machineverbindingen met bron, bestemming, protocol en de in elk geval gebruikte credential, bijvoorbeeld certificaat, service-account of vooraf gedeelde sleutel. Voeg een configuratie-uittreksel van één koppeling toe waaruit de authenticatie blijkt. Vereist vanaf SL 2, niet vereist bij SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.2 RE 1 Elk softwareproces en elk apparaat presenteert een eigen unieke identificatie. Gedeelde service-accounts of één sleutel die systeembreed door veel apparaten wordt gebruikt, zijn niet toegestaan.

[Document](#)

Waaraan je het vaststelt: Koppeling van apparaat aan identificatie of certificaatserienummer waaruit blijkt dat geen enkele identificatie tweemaal voorkomt. Eisverbetering, vereist vanaf SL 3 en dus geen onderdeel van SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.3 Accounts worden beheerd over hun volledige levenscyclus: aanmaak, wijziging van rechten, uitschakeling bij vertrek en verwijdering zijn geregeld door regels en worden ondersteund door de betrokken systemen. Dit omvat gebruikersaccounts, service-accounts en noodaccounts.

[Document](#)

Waaraan je het vaststelt: Accountregister met type, eigenaar, doel en status, plus bewijs voor indiensttreding en uitdiensttreding, bijvoorbeeld een ondertekende overdracht of een ticket dat de uitschakeling met datum toont. Een periodieke accountbeoordeling is aan te raden, en bij een kleine organisatie volstaat een jaarlijkse afstemming van de accountlijst met de personeelslijst. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.3 RE 1 Accountbeheer is geünificeerd over alle onderdelen van het systeem, zodat het uitschakelen van een account op één plek niet zonder effect blijft op afzonderlijke apparaten.

Waaraan je het vaststelt: Bewijs van de centrale directory-integratie, bijvoorbeeld directory-service of RADIUS, met een lijst van de aangesloten onderdelen en een expliciete lijst van de apparaten die niet kunnen worden aangesloten, samen met hun alternatieve procedure. Testregistratie van een uitschakeling die effect heeft op alle aangesloten systemen. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.4 Identificaties worden uitgegeven volgens vaste regels, ondubbelzinnig toegewezen aan een persoon, een apparaat of een rol, ingetrokken zodra ze niet meer worden gebruikt en later nooit opnieuw toegewezen aan een andere houder.

Waaraan je het vaststelt: Naamgevingsregel voor identificaties, bijvoorbeeld achternaam plus initiaal of vestigingscode plus nummer, plus de historie van ingetrokken identificaties waaruit blijkt dat ze niet worden hergebruikt. Een kleine organisatie houdt één doorlopende lijst bij met uitgiftedatum en intrekingsdatum. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.5 Authenticatiemiddelen zoals wachtwoorden, sleutels, certificaten en tokens worden op een geordende manier uitgegeven, gewijzigd bij vermoeden van openbaarmaking en ingetrokken wanneer nodig. Standaardaccounts en fabriekswachtwoorden zoals geleverd worden vóór de inbedrijfstelling gewijzigd.

Waaraan je het vaststelt: Uitgiftelijst van tokens en certificaten met ontvanger en datum, bewijs van wijzigingen en intrekkingen, plus een inbedrijfstellingschecklist per apparaat met het punt fabriekswachtwoord gewijzigd, afgetekend. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.5 RE 1 De credentials van softwareprocessen worden niet opgeslagen als leesbaar bestand op het opslagmedium, maar in hardware-ondersteunde opslag die voorkomt dat het geheime deel kan worden uitgelezen.

Waarvan je het vaststelt: Typebewijs van het gebruikte beveiligingscomponent, bijvoorbeeld TPM, secure element of HSM, met een configuratie-uittreksel dat aantoont dat de sleutel binnen het component wordt opgeslagen. Een aankoopregistratie of datasheet volstaat als typebewijs. Eisverbetering, vereist vanaf SL 3, niet vereist bij SL 1 en SL 2.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.6 Draadloze toegang tot het systeem, bijvoorbeeld WLAN, radiografische afstandsbediening of Bluetooth-diagnose, is alleen bruikbaar na identificatie en authenticatie van zowel gebruiker als apparaat, en wordt bewust beheerd.

Waarvan je het vaststelt: Inventarisatie van alle draadloze verbindingen met doel, bereik en versleutelingsmethode, configuratie-uittreksel van het toegangspunt en de lijst van goedgekeurde eindapparaten. Een kleine organisatie documenteert daarnaast welke draadloze interfaces op apparaten bewust zijn uitgeschakeld. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.6 RE 1 Elke draadloze toegang moet herleidbaar zijn tot één specifieke gebruiker of één specifiek apparaat, een gedeelde netwerksleutel voor alle deelnemers is niet voldoende.

Waarvan je het vaststelt: Bewijs van een methode met individuele credentials, bijvoorbeeld enterprise-WLAN-authenticatie tegen een directory of certificaten per apparaat, plus een verbindingslogboek dat de individuele identificatie toont. Eisverbetering, vereist vanaf SL 2 en dus niet bij SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.7 Overall waar wachtwoorden worden gebruikt, kan de minimale sterkte ervan worden geconfigureerd, bijvoorbeeld minimale lengte en vereiste tekentypes, en de geconfigureerde waarden gelden voor alle betrokken accounts.

Waarvan je het vaststelt: Configuratie-uittreksel van het wachtwoordbeleid per systeem met de daadwerkelijk ingestelde waarden, bijvoorbeeld lengte ≥ 10 tekens en minstens drie tekentypes, plus een lijst van de systemen die deze instelling technisch niet kunnen ondersteunen, samen met hun compenserende maatregel. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.7 RE 1 Voor menselijke gebruikers gelden aanvullende regels voor het genereren en de geldigheidsduur van wachtwoorden: hergebruik van eerdere wachtwoorden wordt voorkomen en de geldigheid is in de tijd beperkt.

Waarvan je het vaststelt: Configuratie-uittreksel dat de wachtwoordhistorie toont, bijvoorbeeld hergebruik van de laatste vijf wachtwoorden geblokkeerd, en de geconfigureerde maximale geldigheid. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.7 RE 2 De beperking van de wachtwoordgeldigheid geldt niet alleen voor mensen, maar voor alle accounts, inclusief service-, onderhouds- en apparaataccounts.

Waarvan je het vaststelt: Rotatieschema voor technische accounts met de laatste en de volgende wijzigingsdatum per account, plus bewijs van de wijzigingen, bijvoorbeeld een wijzigingsregistratie of een ticket. Eisverbetering, pas vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.8

Waar certificaten worden gebruikt, komen ze uit een geordend certificaatbeheer met vastgelegde regels voor aanvraag, uitgifte, geldigheidsduur, vernieuwing en intrekking.[Document](#)

Waarvan je het vaststelt: Certificaatbeleid of een korte schriftelijke regel die verantwoordelijkheid, geldigheidsduur en het intrekkingstraject vastlegt, plus een inventarisatie van de uitgegeven certificaten met hun vervaldata. Een kleine organisatie houdt een tabel bij met certificaat, apparaat, vervaldatum en herinneringsdatum, wat stille productiestilstand door verlopen certificaten voorkomt. Vereist vanaf SL 2.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.9

Wanneer sleutelparen worden gebruikt voor authenticatie, valideert het systeem het certificaat volledig: vertrouwensketen, geldigheidsduur, intrekkingstatus en bewijs dat de tegenpartij daadwerkelijk de private sleutel bezit. De koppeling tussen certificaat en account is ondubbelzinnig.

Waarvan je het vaststelt: Configuratie-uitreksel met intrekkingsscontrole ingeschakeld, bijvoorbeeld CRL of OCSP, testregistratie van een geweigerde aanmelding met een verlopen of ingetrokken certificaat, plus de koppelingstabel van certificaat naar account. Vereist vanaf SL 3, niet vereist bij SL 1 en SL 2.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.9 RE 1

Private sleutels bevinden zich uitsluitend in hardware-ondersteunde opslag waaruit ze niet kunnen worden uitgelezen, en worden ook binnen die opslag gebruikt.

Waarvan je het vaststelt: Datasheet of certificeringsbewijs van het gebruikte beveiligingscomponent en een configuratie-uitreksel dat aantoont dat de sleutel binnen het component wordt gegenereerd, zodat de private sleutel het nooit verlaat. Eisverbetering, pas vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.10

Tijdens het aanmelden onthult het systeem geen informatie die kan worden misbruikt. Ingevoerde wachtwoorden worden gemaskeerd en foutmeldingen laten niet zien of de identificatie of het wachtwoord onjuist was.

Waarvan je het vaststelt: Scherm afbeelding van het aanmeldscherm met gemaskeerde invoer en een scherm afbeelding van de foutmelding na een mislukte poging. Voor apparaten die dit technisch niet kunnen, bijvoorbeeld oudere operatorpanelen, een korte notitie toevoegen over de compenserende maatregel, bijvoorbeeld beperkte fysieke toegang tot de installatielocatie. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.11

Het aantal opeenvolgende mislukte aanmeldpogingen is beperkt en de reactie daarop is configureerbaar, bijvoorbeeld een tijdelijke blokkering. De gekozen reactie belemmert de veiligheidsgerelateerde werking van de installatie niet.

Waarvan je het vaststelt: Configuratie-uitreksel met de drempelwaarde, bijvoorbeeld blokkering na <= 5 mislukte pogingen, en de blokkeringsduur, plus een korte beoordeling waarom de blokkering de noodbediening of een veilige stillegging van de installatie niet belemmert. Bij operatorstations met een veiligheidsfunctie heeft een tijdgebonden blokkering de voorkeur boven een permanente accountvergrendeling. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.12

Vóór het aanmelden kan een gebruiksmelding worden getoond die verwijst naar de regels voor gebruik en monitoring van het systeem. Tekst en weergave zijn configureerbaar door de asset-eigenaar.

Waarvan je het vaststelt: Scherm afbeelding van de getoonde meldingstekst en de goedgekeurde formulering met de goedkeuringsdatum. Kleine organisaties stemmen de formulering kort af met de personeelsvertegenwoordiging of met de directie, één alinea is voldoende. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 1.13 Toegang vanuit niet-vertrouwde netwerken, bijvoorbeeld onderhoud op afstand door leveranciers, is beperkt tot vastgelegde paden, wordt gemonitord en kan op elk moment worden onderbroken.

Waarvan je het vaststelt: Inventarisatie van de paden voor toegang op afstand met doel, externe partij, contactpersoon en het gebruikte pad, plus verbindingslogboeken en bewijs van de mogelijkheid tot verbreken, bijvoorbeeld een sleutelschakelaar, een firewallregel of een router voor onderhoud op afstand die kan worden uitgeschakeld. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 1.13 RE 1 Elke afzonderlijke sessie vanuit een niet-vertrouwd netwerk wordt expliciet goedgekeurd door een verantwoordelijke persoon voordat de verbinding tot stand komt, een permanent open verbinding is niet voldoende.

Waarvan je het vaststelt: Goedkeuringsregistraties per sessie voor onderhoud op afstand met tijdstip, reden, goedkeurende persoon en duur, technisch bijvoorbeeld via een sleutelschakelaar bij de toegangsrouter of via een goedkeuringsportaal. Bij een kleine organisatie volstaat een logboek voor onderhoud op afstand bij de schakelkast, per sessie afgetekend door de onderhoudstechnicus. Eisverbetering, vereist vanaf SL 2 en dus nooit bij SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

6 FR 2: Gebruikscontrole (rechten, sessies, auditregistraties)

24

SR 2.1 Het systeem handhaaft technisch de toegekende rechten: elke aangemelde persoon, elk apparaat en elk softwareproces krijgt precies de toegang die eraan is toegewezen, en elke poging die daarbuiten gaat, wordt geweigerd.

Waarvan je het vaststelt: Een rechtenconcept dat accounts aan permissies koppelt, plus een schermafbeelding of configuratie-uittreksel per besturingssysteem, HMI en engineeringstation dat de actieve rechten toont. Daarnaast een testregistratie waarin een account met weinig rechten een geblokkeerde actie probeert en wordt geweigerd. Vereist vanaf SL 1. Een kleine organisatie werkt met twee of drie rollen, bijvoorbeeld bedienen, onderhouden, ontwerpen, en documenteert deze op één pagina.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.1 RE 1 Handhaving van rechten geldt niet alleen voor menselijke operators, maar evenzeer voor softwareprocessen en apparaten die zelfstandig toegang tot het systeem krijgen.

Waarvan je het vaststelt: Een lijst van technische en service-accounts, bijvoorbeeld OPC UA-clients, historian-verbindingen, back-updiensten, elk met de toegewezen rechtenset. Een uittreksel uit het rechtenbeheer dat aantoont dat deze accounts niet met beheerdersrechten draaien. Eisverbetering, vereist vanaf SL 2, niet bij SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.1 RE 2 Rechten worden niet per persoon afzonderlijk toegekend maar via rollen, en de koppeling van rol aan toegestane acties wordt traceerbaar vastgelegd.
[Document](#)

Waarvan je het vaststelt: Een rol- en rechtenmatrix als tabel: de rijen zijn de rollen, de kolommen de acties zoals setpoint wijzigen, programma downloaden, alarm bevestigen, account aanmaken. Plus de lijst die persoon aan rol koppelt. Eisverbetering, vereist vanaf SL 2. Een bijgehouden rekenblad met een wijzigingsdatum is volledig voldoende als bewijs.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.1 RE 3 Voor strikt afgebakende uitzonderingsgevallen kan een bevoegde toezichthouder een rechtenbeperking voor een beperkte periode opheffen, en elke dergelijke uitzondering wordt vastgelegd in het audittraject.

Waarvan je het vaststelt: Een procedurebeschrijving voor de uitzonderingsgoedkeuring die vastlegt wie deze mag verlenen en hoe lang ze geldig blijft, plus auditregistraties van reeds verleende uitzonderingen, ontleend aan het systeemlogboek. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.1 RE 4 Bijzonder kritieke ingrepen vereisen goedkeuring van twee onafhankelijke bevoegde personen voordat de actie wordt uitgevoerd.

Waaraan je het vaststelt: Een lijst van de acties die aan dubbele goedkeuring onderworpen zijn, bijvoorbeeld het wijzigen van veiligheidsparameters of het downloaden van een nieuw besturingsprogramma, samen met configuratiebewijs en auditregistraties die beide goedkeurders vermelden. Eisverbetering, pas vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.2 Het gebruik van draadloze verbindingen in het automatiseringsnetwerk is gebonden aan een expliciete autorisatie, en alleen goedgekeurde deelnemers mogen gegevens uitwisselen of draadloos ingrijpen.

Waaraan je het vaststelt: Een inventarisatie van alle draadloze verbindingen, bijvoorbeeld WLAN-toegangspunten, Bluetooth-koppelingen, mobiele routers, elk met hun doel en hun goedgekeurde deelnemers. Plus de toegangscontroleconfiguratie bij het toegangspunt. Vereist vanaf SL 1. Wie geen draadloze verbinding in het procesnetwerk gebruikt, verklaart dit precies zo schriftelijk en onderbouwt dit met een configuratieovername die draadloos uitgeschakeld toont.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.2 RE 1 Niet-geautoriseerde draadloze apparaten in de nabijheid van het automatiseringsnetwerk worden gedetecteerd en gemeld.

Waaraan je het vaststelt: Een registratie van draadloze monitoring of van een periodieke draadloze scan met datum, resultatenlijst en een notitie bij elk onbekend apparaat. Het meldingstraject naar de verantwoordelijke functie wordt genoemd. Eisverbetering, vereist vanaf SL 2, niet bij SL 1. Een kleine organisatie kan een driemaandelijkse scan uitvoeren met een laptop en het resultaat als registratie archiveren.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.3 Het gebruik van draagbare en mobiele apparaten in het systeem, bijvoorbeeld servicelaptops, USB-opslag of tablets, is geregeld door regels en technisch beperkt tot expliciet goedgekeurde apparaten.

Waaraan je het vaststelt: Het regelstelsel voor apparaatgebruik, een lijst van goedgekeurde serviceapparaten met hun identificaties, en bewijs van de technische beperking, bijvoorbeeld USB-poorten op HMI en engineeringstation uitgeschakeld of beperkt tot specifieke apparaten. Vereist vanaf SL 1. Een kleine organisatie werkt met twee gelabelde servicesticks die alleen op één overdrachtsstation worden beschreven.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.3 RE 1 Vóór aansluiting wordt de beveiligingsstatus van een draagbaar of mobiel apparaat gecontroleerd, en apparaten die niet aan de eisen voldoen, wordt de toegang geweigerd.

Waaraan je het vaststelt: De controlecriteria voor de apparaatstatus, bijvoorbeeld actuele malwarebescherming en patchniveau, plus controleregistraties per serviceapparaat en bewijs van de technische handhaving, bijvoorbeeld via een overdrachtsstation of een netwerktoegangscontrole. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.4 Voor mobiele code die op het systeem wordt uitgevoerd, bijvoorbeeld scripts in operatorinterfaces of actieve inhoud in rapporten, is vastgelegd welke types zijn toegestaan, en de uitvoering van niet-toegestane types wordt verhinderd.[Document](#)

Waaraan je het vaststelt: Een definitie van welke mobiele code op welke systemen is toegestaan, plus configuratiebewijs van de beperking, bijvoorbeeld scriptuitvoering in de HMI-browser uitgeschakeld, macro's in evaluatiebestanden geblokkeerd. Vereist vanaf SL 1. Een definitie van één pagina die de drie of vier gevallen dekt die daadwerkelijk voorkomen, is voldoende.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.4 RE 1 Voordat mobiele code wordt uitgevoerd, wordt geverifieerd dat deze van de verwachte bron komt en niet is gewijzigd.

Waaraan je het vaststelt: Configuratiebewijs van de handtekeningverificatie of controlesomcontrole, plus een testregistratie waarin gemanipuleerde of ongesigneerde code wordt geweigerd. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.5 Een sessie wordt vergrendeld na een vastgelegde periode zonder operatorhandeling en wordt pas weer vrijgegeven na hernieuwde authenticatie, zonder dat de weergave van veiligheidsrelevante procesinformatie verloren gaat.

Waaraan je het vaststelt: Een configuratie-uittreksel met de geconfigureerde vergrendelingstijd per werkstation, plus een motivering voor werkstations in permanent bemande controlekamers waar de vergrendeling bewust anders is ingesteld. Vereist vanaf SL 1. Visueel bewijs: een schermafbeelding van het vergrendelscherm met de alarmregel nog zichtbaar.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.6 Sessies op afstand worden beëindigd na een vastgelegde periode zonder activiteit of op verzoek van de operator, zodat er geen open verbinding op afstand onbeheerd blijft.

Waaraan je het vaststelt: De configuratie van de toegang op afstand met de inactiviteitslimiet, auditregistraties van beëindigde sessies op afstand, en een beschrijving van hoe de operator een lopende sessie voor onderhoud op afstand onmiddellijk kan verbreken, bijvoorbeeld via een sleutelschakelaar of een vrijgave per sessie. Vereist vanaf SL 2, niet bij SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.7 Het aantal gelijktijdige sessies per account of rol is beperkt, en aanmeldpogingen boven die limiet worden geweigerd.

Waaraan je het vaststelt: Een configuratie-uittreksel met de vastgelegde bovengrens per rol, bijvoorbeeld ≤ 1 gelijktijdige sessie voor engineering-accounts, plus een testregistratie van de geweigerde tweede aanmeldpoging. Vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.8 Beveiligingsrelevante gebeurtenissen worden geregistreerd, en elke vermelding noemt minstens het tijdstip, de bron, het veroorzakende account, het type gebeurtenis en de uitkomst.[Document](#)

Waaraan je het vaststelt: Een definitie van de te registreren gebeurtenistypes, bijvoorbeeld aanmelding, mislukte aanmelding, wijziging van rechten, programmawijziging, configuratiewijziging, plus een echt uittreksel van het auditlogboek dat de genoemde velden toont. Vereist vanaf SL 1. Een kleine organisatie verzamelt de logboeken van besturingssysteem, HMI en firewall in één map met een vaste bewaartermijn.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.8 RE 1 De auditregistraties van de afzonderlijke onderdelen worden op één centraal punt samengebracht en vormen één systeembreed geheel dat in samenhang kan worden geëvalueerd.

Waaraan je het vaststelt: Een architectuurschets van de logverzameling die alle aangesloten bronnen toont, plus een evaluatie die gebeurtenissen van minstens twee onderdelen op één tijdlijn plaatst. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.9 Er is voldoende opslag voor de auditregistraties zodat gebeurtenissen gedurende de vastgelegde bewaartermijn behouden blijven en niet onbedoeld worden overschreven.

Waaraan je het vaststelt: Een berekening of schatting van de opslagbehoefte op basis van het dagelijkse logvolume vermenigvuldigd met de bewaartermijn, plus de geconfigureerde opslagcapaciteit en de archiveringsregel. Vereist vanaf SL 1. In de praktijk volstaat een dagelijkse kopie naar een aparte opslaglocatie met een gedocumenteerde bewaartermijn.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 2.9 RE 1 Wanneer een vastgelegde vuldrempel van de auditopslag wordt bereikt, gaat er een waarschuwing naar de verantwoordelijke functie voordat de opslagcapaciteit volledig is verbruikt.

Waaraan je het vaststelt: Een configuratie-uittreksel van de drempelwaarde, bijvoorbeeld een waarschuwing vanaf ≥ 80 procent gebruik, plus een voorbeeld van de geactiveerde melding en de ontvangerslijst. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.10 Als de auditregistratie faalt of de auditopslag vol raakt, reageert het systeem op een vooraf vastgelegde manier en wordt de verantwoordelijke functie geïnformeerd, zonder de veilige werking van de installatie in gevaar te brengen.

Waaraan je het vaststelt: De vastgelegde reactie per storingsgeval, bijvoorbeeld oudere vermeldingen overschrijven en een melding genereren in plaats van de installatie stil te leggen, met een motivering vanuit procesoogpunt. Bewijs via een geactiveerde testmelding en de bijbehorende auditvermelding. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.11 Elke auditregistratie draagt een tijdstempel van een genoemde tijdbron, zodat gebeurtenissen van verschillende onderdelen ten opzichte van elkaar in volgorde kunnen worden geplaatst.

Waaraan je het vaststelt: Een opgave van de gebruikte tijdbron per onderdeel en een loguittreksel met een zichtbaar tijdstempel inclusief tijdzone. Vereist vanaf SL 2, niet bij SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.11 RE 1 De klokken van alle betrokken onderdelen zijn gesynchroniseerd met een gemeenschappelijke tijdbron zodat de afwijking binnen een vastgelegde grens blijft.

Waaraan je het vaststelt: De configuratie van de tijdsynchronisatie, bijvoorbeeld NTP-server en synchronisatie-interval, plus een controleregistratie met de gemeten afwijking per onderdeel ten opzichte van de vastgelegde grens, bijvoorbeeld ≤ 1 seconde. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.11 RE 2 De tijdbron zelf is beschermd tegen manipulatie, en een onaannemelijke of gewijzigde tijdreferentie wordt gedetecteerd en gemeld.

Waaraan je het vaststelt: Een beschrijving van hoe de tijdbron wordt beschermd, bijvoorbeeld geauthenticeerde tijdsynchronisatie, beperking tot een interne bron, monitoring op tijdsprongen, plus meldingen of auditregistraties van een gedetecteerde afwijking. Eisverbetering, pas vereist vanaf SL 4.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.12 Voor vastgelegde kritieke acties kan achteraf zonder twijfel worden vastgesteld wie ze heeft veroorzaakt, zodat de handelende persoon niet geloofwaardig kan ontkennen dit te hebben gedaan.

[Document](#)

Waaraan je het vaststelt: Een lijst van de acties waarop dit bewijs betrekking heeft, bijvoorbeeld receptwijziging, batchvrijgave, wijziging van grenswaarden, plus de bijbehorende registraties met een unieke persoonsidentificatie en bewijs dat groepsaccounts voor deze acties zijn uitgesloten. Vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 2.12 RE 1 De onweerlegbare toewijzing van de handelende persoon geldt niet alleen voor geselecteerde kritieke acties, maar voor alle gebruikers en alle acties die zij veroorzaken.

Waaraan je het vaststelt: Bewijs dat elk account aan één persoon is gebonden en dat er geen gedeelde aanmeldingen meer bestaan, plus een loguittreksel van willekeurige acties waarin steeds een unieke persoonsidentificatie voorkomt. Eisverbetering, pas vereist vanaf SL 4.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

7 FR 3: Systeemintegriteit, bescherming van gegevens, software en sessies tegen ongeautoriseerde wijziging

19

SR 3.1 Het besturingssysteem detecteert wanneer informatie is gewijzigd tijdens transport over een communicatiekanaal, en doet dit zowel voor besturingsgegevens als voor configuratiegegevens en beheerverkeer. De bescherming geldt ook voor verbindingen die het systeem verlaten of niet-vertrouwde netwerksegmenten doorkruisen.

Waaraan je het vaststelt: Een netwerk- en protocoloverzicht dat aangeeft welk kanaal welk integriteitsmechanisme gebruikt (controlesom, message authentication code, gesigneerde telegrammen), een configuratie-uittreksel van de beveiligingsinstellingen van de veldbus of OPC UA, en een testregistratie die toont dat een gemanipuleerd telegram aantoonbaar werd geweigerd. Een kleine organisatie legt dit vast in een tabel per verbinding met de kolommen bron, bestemming, protocol en integriteitsmechanisme, en toont de werking eenmalig aan met een verkeersopname. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.1 RE 1 Integriteitsbescherming tijdens transport steunt op cryptografische mechanismen, zodat een opzettelijke manipulatie door een aanvalleur met eigen middelen niet onopgemerkt kan blijven. Een eenvoudige controlesom tegen transmissiefouten is hier niet voldoende.

Waaraan je het vaststelt: Een lijst van de gebruikte cryptografische mechanismen en sleutellengtes per kanaal, een verwijzing naar het onderliggende sleutelbeheer, en configuratie-uittreksels (bijvoorbeeld TLS-cipher suites, OPC UA SecurityPolicy, IPsec-profielen). Kleine organisaties vertrouwen op de veilige standaardprofielen van hun controllers en archiveren een schermafbeelding van de actieve instelling. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.2 Er zijn beschermingsmechanismen tegen kwaadaardige code aanwezig die voorkomen dat ongewenste programmacode op systeemonderdelen wordt uitgevoerd en die elke detectie melden. De mechanismen worden zo gekozen dat ze de beoogde werking van de installatie niet verstoren, en ze worden actueel gehouden.

Waaraan je het vaststelt: Een overzicht per onderdeel van welk mechanisme van toepassing is (antivirus, applicatie-whitelisting, gehard besturingssysteem zonder uitvoeringsrechten), bewijs dat handtekeningen of whitelists worden bijgewerkt, en meldingen van het beschermingssysteem. Waar antivirus niet haalbaar is, bijvoorbeeld op een controller, wordt de compenserende maatregel met motivering vastgelegd. Kleine organisaties komen ver met whitelisting op de operator-pc en een schriftelijke regel voor USB-media. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.2 RE 1 Bescherming tegen kwaadaardige code werkt bovendien op de toegangs- en uitgangspunten van de installatie, waar gegevens binnenkomen of vertrekken, en niet alleen op de eindapparaten zelf.

Waaraan je het vaststelt: Een lijst van alle toegangs- en uitgangspunten (toegang voor onderhoud op afstand, gateway voor gegevensoverdracht, verwisselbare media, overdracht naar het kantoor netwerk, e-mailtraject voor programmaversies) met het daar werkzame scanmechanisme, plus registraties van de gecontroleerde overdrachten. Kleine organisaties richten één overdracht-pc met virusscan in als gateway en leggen dit vast in een werkinstructie. Eisverbetering, vereist vanaf SL 2.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.2 RE 2 De beschermingsmechanismen tegen kwaadaardige code worden vanuit één centraal punt beheerd, updates worden centraal verspreid, en detecties worden op één plek verzameld voor evaluatie.

Waaraan je het vaststelt: De configuratie van de centrale beheerconsole, een rapport over de updatestatus van alle aangesloten onderdelen, en een evaluatie van gemelde detecties over een periode. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.3

De beveiligingsfuncties van het systeem worden op geplande intervallen en na wijzigingen geverifieerd om te bevestigen dat ze daadwerkelijk werken. De tests worden zo gepland dat ze de werking van de installatie niet in gevaar brengen, en de resultaten worden vastgelegd.

[Document](#)

Waaraan je het vaststelt: Een testplan dat het testobject, het interval en het tijdvenster vermeldt, samen met de testregistraties met datum, tester, verwacht gedrag en waargenomen gedrag. Nuttige afzonderlijke tests zijn: een aanmelding met een uitgeschakeld account mislukt, de antivirus reageert op een testbestand, toegang voor onderhoud op afstand is onbereikbaar zonder vrijgave. Kleine organisaties koppelen het testen aan de toch al geplande onderhoudsstop en werken een vaste checklist af. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.3 RE 1 Verificatie van de beveiligingsfuncties verloopt met geautomatiseerde middelen, zodat ze zonder handmatige inspanning herhaalbaar is en een consistent resultaat oplevert.

Waaraan je het vaststelt: De scripts of testtools samen met hun schema, hun uitvoerbestanden, en een vergelijking van meerdere runs waaruit blijkt dat afwijkingen worden gedetecteerd. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.3 RE 2 Verificatie van de beveiligingsfuncties is ook mogelijk tijdens normaal bedrijf, zonder de installatie te hoeven stopzetten of in een bijzondere toestand te brengen.

Waaraan je het vaststelt: Een beschrijving van de testprocedure met bewijs dat deze geen nadelig effect heeft op het proces, bijvoorbeeld een analyse van de impact op cyclustijden en netwerkbelasting, plus testregistraties uit het productieve bedrijf. Eisverbetering, vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.4 Ongeautoriseerde wijzigingen aan software, firmware en opgeslagen informatie worden gedetecteerd. Dit geldt evenzeer voor besturingsprogramma's, parametersets, recepten en configuratiebestanden.

Waaraan je het vaststelt: Een inventarisatie van de te beschermen versies met opgeslagen controlewaarden of handtekeningen, de resultaten van de integriteitsvergelijkingen, en de gedocumenteerde afstemming met de versie in versiebeheer. Kleine organisaties bewaren de vrijgegeven programmaversie samen met de controlesom op een schrijfbeveiligde locatie en vergelijken bij verdenking of na onderhoud. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.4 RE 1 Als een schending van de integriteit van software of informatie wordt gedetecteerd, meldt het systeem dit automatisch aan een verantwoordelijk punt, zonder dat iemand er actief naar hoeft te zoeken.

Waaraan je het vaststelt: De configuratie van de meldingstrajecten (alarm in de controlekamer, e-mail, bericht naar het monitorsysteem), een ontvangerslijst met vervangingsregelingen, en minstens één testalarm met een gedocumenteerde reactietijd. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.5 Invoer die het systeem accepteert vanuit procesgegevens, interfaces of gebruikersinterfaces wordt gecontroleerd op toegestane syntax, toegestaan waardebereik en toegestane lengte voordat ze wordt verwerkt. Ongeldige invoer leidt niet tot ongecontroleerd gedrag.

Waaraan je het vaststelt: Een specificatie van de grenzen en formaten per invoer, uittreksels uit de validatielogica in de controller of applicatie, en testgevallen met opzettelijk ongeldige invoer (een te grote waarde, een verkeerd datatype, een te lange tekenreeks) samen met het gedocumenteerde gedrag van het systeem. Kleine organisaties leggen de plausibiliteitsgrenzen per meetpunt vast in een tabel en verifiëren deze tijdens de inbedrijfstelling. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.6 Voor het geval van een storing is vastgelegd welke toestand de uitgangen naar de installatie aannemen, en het systeem neemt precies die toestand aan. De vastgelegde toestand is afgestemd op de functionele veiligheid van de installatie.

Waarvan je het vaststelt: Een definitie per uitgang of uitgangsgroep (waarde vasthouden, vastgelegde vervangwaarde, veilige stilstoestand) met een motivering uit de risicobeoordeling, een configuratie-uittreksel van de controller, en bewijs uit een storingstest, bijvoorbeeld een kabelbreuk of communicatieverlies, dat het verwachte gedrag toont. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.7 Het systeem behandelt foutsituaties zodanig dat de bediening onder controle blijft en geen informatie wordt vrijgegeven die een aanvaller zou helpen. Foutmeldingen die aan operators worden getoond, blijven beknopt, terwijl de technische details alleen naar de interne registraties gaan.

Waarvan je het vaststelt: Een overzicht van de foutklassen met het per klasse voorziene systeemgedrag, voorbeelden van de getoonde meldingen vergeleken met de bijbehorende interne logvermeldingen, en testbewijs dat geen bestandspaden, accountnamen, database-uitvoer of versiegegevens op de operatorinterface verschijnen. Vereist vanaf SL 1.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.8 Actieve sessies zijn beschermd tegen kaping en tegen het injecteren van vreemde berichten. Een sessie eindigt na afmelding of na een vastgelegde periode zonder activiteit, en kan daarna niet worden hergebruikt.

Waarvan je het vaststelt: De configuratie van het sessiebeheer met de geconfigureerde limieten voor inactiviteitstijd en maximale duur, bewijs van het mechanisme dat beschermt tegen het herhalen van berichten, en een testregistratie waarin een onderschepte sessie na afmelding niet meer werkt. Vereist vanaf SL 2.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.8 RE 1 Sessie-identificaties verliezen hun geldigheid wanneer de sessie eindigt en worden niet opnieuw door het systeem geaccepteerd, ook niet wanneer ze opnieuw van buitenaf worden aangeboden.

Waarvan je het vaststelt: Een configuratie-uittreksel van het sessiebeheer met betrekking tot ongeldigmaking, plus een testregistratie waarin een eerder geldige identificatie na afmelding opnieuw wordt verzonden en door het systeem wordt geweigerd. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.8 RE 2 Voor elke nieuwe sessie wordt een unieke, eenmalig te gebruiken identificatie gegenereerd. Identificaties worden niet hergebruikt tussen sessies, gebruikers of apparaten.

Waarvan je het vaststelt: Een beschrijving van de generatieprocedure en bewijs uit het logboek of een verkeersopname dat meerdere opeenvolgende aanmeldingen verschillende identificaties krijgen. Eisverbetering, vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.8 RE 3 Sessie-identificaties worden gegenereerd met erkende willekeurige mechanismen, zodat ze noch kunnen worden geraden noch kunnen worden afgeleid van voorgaande identificaties.

Waarvan je het vaststelt: Een opgave van de gebruikte randomgenerator en zijn entropiebron, een leveranciersverklaring of testrapport hierover, en een statistische evaluatie van een steekproef van gegenereerde identificaties. Eisverbetering, vereist vanaf SL 4.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 3.9

De beveiligingsgerelateerde registraties en de tools die worden gebruikt om ze te evalueren, zijn beschermd tegen ongeautoriseerde toegang, wijziging en verwijdering. De kring van personen die registraties mogen wijzigen of verwijderen, blijft beperkt en is benoemd.

[Document](#)

Waaraan je het vaststelt: Een autorisatieconcept voor de loggegevens met naamgebonden toewijzing, de configuratie van doorsturen naar een apart logsysteem, bewaartermijnen, en testbewijs dat een gewone operator geen vermeldingen kan verwijderen. Kleine organisaties sturen de logs door naar een apart apparaat waartoe de installatie-operators geen schrijftoegang hebben. Vereist vanaf SL 2.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 3.9 RE 1

De beveiligingsgerelateerde registraties worden bovendien opgeslagen op een medium dat latere overschrijving uitsluit, zodat een eenmaal geschreven vermelding niet meer kan worden gewijzigd, ook niet met beheerdersrechten.

[Document](#)

Waaraan je het vaststelt: Een beschrijving van de gebruikte opslag (write-once-medium, manipulatiebestendig archief, doorlopend uitgebreide handtekeningketen), bewijs van een mislukte poging om een vermelding te wijzigen, en de regel voor het bewaren en opvragen van de media. Eisverbetering, vereist vanaf SL 3.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

8 FR 4: Vertrouwelijkheid van gegevens

6

SR 4.1

Het automatiseringssysteem beschermt vertrouwelijke informatie tegen ongeautoriseerde openbaarmaking, zowel tijdens transport als in opgeslagen toestand. Er is vastgelegd welke gegevens als vertrouwelijk gelden, bijvoorbeeld recepten, parametersets, credentials, configuratiebestanden of diagnosegegevens met een persoonsreferentie.

[Document](#)

Waaraan je het vaststelt: Een lijst van de te beschermen gegevenstypes, met vermelding van waar ze worden bewaard en hoe ze worden verzonden, plus de specifieke beschermingsmaatregel voor elke vermelding, bijvoorbeeld een versleutelde verbinding, een versleuteld opslagmedium of een beperkte share. Een kleine organisatie werkt met een tabel van één pagina: gegevenstype, waar het zich bevindt, wie het mag zien, wat het beschermt. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 4.1 RE 1

Voor informatie die over niet-vertrouwde netwerken reist of buiten de beschermde omgeving wordt opgeslagen, wordt vertrouwelijkheid technisch afgedwongen in plaats van louter organisatorisch beloofd.

Waaraan je het vaststelt: Een configuratie-uitreksel van de gebruikte transport- of opslagversleuteling, bijvoorbeeld het VPN-profiel voor onderhoud op afstand, de TLS-instellingen van de interface van het besturingssysteem, of de versleuteling van de back-upmedia. Een gedateerde schermafbeelding van de actieve instelling is voldoende als bewijs. Vereist vanaf SL 2, niet vanaf SL 1, omdat dit een eisverbetering is.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 4.1 RE 2

Vertrouwelijkheid wordt ook afgedwongen op de grenzen tussen zones, zodat informatie niet in leesbare vorm zichtbaar wordt wanneer ze van de ene zone naar de andere overgaat.

Waaraan je het vaststelt: Een zone- en kanaalplan dat aangeeft welke overgangen zijn versleuteld, samen met de configuratie van het grenscomponent zoals een gateway, firewall of datadiode. Een verkeersopname of testregistratie die toont dat er geen leesbare gegevens op de grens verschijnen. Vereist vanaf SL 4.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 4.2

Er is vastgelegd hoe vertrouwelijke informatie betrouwbaar wordt verwijderd wanneer apparaten buiten gebruik worden gesteld, van eigenaar wisselen, ter reparatie gaan of worden hergebruikt, zodat er geen leesbare restgegevens achterblijven.

[Document](#)

Waaraan je het vaststelt: Een schriftelijke procedure voor buitengebruikstelling met de saneringsmethode per apparaattypen, plus wisregistraties met apparaatidentificatie, datum en de persoon die het uitvoerde. Een kleine organisatie legt dit vast als één regel per apparaat in een gedeelde lijst en archiveert de certificaten van externe verwerkingsbedrijven ernaast. Vereist vanaf SL 2.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 4.2 RE 1 Gedeelde opslaggebieden worden gewist voordat ze aan een andere gebruiker of proces worden toegewezen, zodat inhoud van de vorige gebruiker niet kan worden uitgelezen.

Waaraan je het vaststelt: Een leveranciersverklaring of configuratieregistratie over het wissen van hergebruikte geheugen- en buffergebieden, aangevuld met een testregistratie uit acceptatietest of onderhoud. Waar een onderdeel dit niet kan, dient de gedocumenteerde compenserende maatregel als bewijs, bijvoorbeeld het apparaat niet delen tussen verschillende rollen. Vereist vanaf SL 3, niet vanaf SL 1, omdat dit een eisverbetering is.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 4.3 Overal waar cryptografie wordt gebruikt, volgen algoritmes, sleutellengtes en sleutelbeheer erkende goede praktijken, en is vastgelegd hoe sleutels worden gegenereerd, verspreid, opgeslagen, geroteerd en ingetrokken.

[Document](#)

Waaraan je het vaststelt: Een overzicht van de per systeem gebruikte mechanismen, met vermelding van algoritme, sleutellengte en geldigheidsduur, plus de regels voor sleutelbeheer en registraties van sleutelrotaties en certificaatvernieuwingen. Publieke aanbevelingen dienen als maatstaf, bijvoorbeeld de technische richtlijnen van het Duitse BSI. Een kleine organisatie houdt een certificatenlijst bij met vervaldatum en een herinnering ≥ 30 dagen vóór het verstrijken. Vereist vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

9 FR 5: Beperkte gegevensstroom, zones en kanalen

11

SR 5.1 Het besturingssysteem kan worden opgedeeld in afzonderlijke zones, en verkeer tussen die zones loopt uitsluitend via vastgelegde kanalen. De indeling volgt een uitlegbare logica, bijvoorbeeld naar beschermingsbehoefte, eigendom of de functie van de betrokken installatiedelen.

[Document](#)

Waaraan je het vaststelt: Netwerkdigram dat de zones en de kanalen ertussen toont, een zonelijst met de motivering voor elke grens, en de configuratie van de scheidende onderdelen zoals VLAN-definities of firewall-interfaces. Een kleine organisatie komt uit met een schets van één pagina die kantoor, machinenetwerk en toegang op afstand als drie vakken toont met de verbindingen ertussen, plus een schermafbeelding van de VLAN-configuratie van de switch.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 5.1 RE 1 Zonescheiding wordt fysiek geïmplementeerd, dat wil zeggen via toegewijde netwerkonderdelen en toegewijde bekabeling, en steunt niet uitsluitend op logische configuratie binnen gedeelde apparaten. Paragraaf 9.1 in deze lijst, vereist vanaf SL 2. Eisverbeteringen van deze norm zijn nooit al bij SL 1 verplicht.

Waaraan je het vaststelt: Inventarisatie van netwerkonderdelen met vermelding van welke switch of router welke zone bedient, foto's of kastindeling van de gescheiden verdelingen, kabellabeling. Kleine organisaties tonen dit aan met twee gescheiden, duidelijk gelabelde switches in plaats van één gedeeld apparaat en een foto van de schakelkast in de installatiedocumentatie.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 5.1 RE 2 Het automatiseringsnetwerk kan onafhankelijk van netwerken buiten de automatisering werken. Als de kantoor-IT of een externe verbinding uitvalt, blijven besturing en monitoring van de installatie doorwerken. Vereist vanaf SL 3.

Waaraan je het vaststelt: Afhangelijkheidslijst van de binnen het automatiseringsnetwerk gebruikte diensten zoals tijdserver, naamsresolutie, directory-service of licentieserver, met vermelding van waar elk wordt gehost, samen met een testregistratie van een ontkoppelingsproef waarbij de verbinding met de kantoor-IT werd verbroken. Een kleine organisatie noteert het resultaat van zo'n proef in het onderhoudslogboek: uplink verbroken, installatie bleef doorwerken, alleen de kantoorrapportages ontbraken.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 5.1 RE 3 Zones met bijzonder kritieke functies, bijvoorbeeld veiligheids- of beschermingsfuncties, zijn zowel logisch als fysiek gescheiden van de overige zones. Vereist vanaf SL 4.

Waaraan je het vaststelt: Markering van de kritieke zones in het zonediagram met de motivering voor de classificatie, bewijs van toegewijde netwerkonderdelen en toegewijde bekabeling voor die zones, configuratie van de kanalen met bewijs dat er geen gedeeld pad bestaat.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 5.2 Op de zonegrenzen wordt verkeer gecontroleerd, gemonitord en volgens vastgelegde regels toegestaan of geweigerd. Er is geen pad tussen twee zones dat dit controlepunt omzeilt.

Waarvan je het vaststelt: Geëxporteerd regelstelsel van de firewall of het grensapparaat, logboeken van geweigerde en toegestane verbindingen, bewijs dat er geen zijpaden bestaan, bijvoorbeeld via een controle op extra netwerkkaarten, modems of mobiele routers in installatiecomputers. Een kleine organisatie toont dit aan met de regelexport van de enige firewall en een korte rondgangnotitie die bevestigt dat er geen ongeplande router in enige schakelkast staat.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.2 RE 1 Het regelstelsel op de zonegrens werkt volgens het principe dat alles wordt geweigerd tenzij het expliciet is toegestaan. Elke toestaanregel is individueel gemotiveerd en aan een doel gekoppeld. Vereist vanaf SL 2.

Waarvan je het vaststelt: Regelstelsel met een zichtbare slotregel die de rest laat vallen, en een toestaanlijst met bron, bestemming, dienst, doel en verantwoordelijke persoon per regel. Kleine organisaties houden deze lijst als een tabel met vijf kolommen naast de firewalllexport en beoordelen die eenmaal per jaar op regels die niemand meer nodig heeft.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.2 RE 2 Het automatiseringsnetwerk kan bewust van alle externe verbindingen worden afgesneden en draaiend worden gehouden in eilandmodus. De actie kan worden geactiveerd zonder de installatie te hoeven stopzetten. Vereist vanaf SL 3.

Waarvan je het vaststelt: Beschrijving van de isolatieprocedure met vermelding van wie deze mag activeren en hoe, bewijs van de technische implementatie zoals een noodregelstelsel of een gelabelde isolatieschakelaar, plus de registratie van een oefening waarin de isolatie daadwerkelijk werd uitgevoerd. Een kleine organisatie voert de oefening eenmaal per jaar uit tijdens onderhoud en noteert datum, duur en bijzonderheden.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.2 RE 3 Als het apparaat op de zonegrens uitvalt of zijn regels verliest, weigert het verkeer in plaats van het door te laten. Een storing mag geen open verbinding achterlaten. Vereist vanaf SL 4.

Waarvan je het vaststelt: Leveranciersverklaring of configuratiebewijs over hoe het onderdeel zich gedraagt bij storing en bij herstart, testregistratie van een opzettelijk veroorzaakte storing met het waargenomen resultaat, afstemming met de risicobeoordeling van de installatie, omdat een grens die verkeer weigert zelf gevolgen kan hebben, afhankelijk van het proces.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.3 Algemene communicatiediensten van persoon tot persoon zoals e-mail, messaging of videobellen kunnen worden geblokkeerd op automatiseringsapparaten en binnen automatiseringsnetwerken. De omvang van de blokkade is vastgelegd en gemotiveerd.

Waarvan je het vaststelt: Definitie van welke diensten niet zijn toegestaan in het automatiseringsnetwerk, plus de technische implementatie: geblokkeerde poorten en bestemmingen in het regelstelsel, verwijderde of geblokkeerde applicaties op operatorstations, bewijs uit de software-inventarisatie van de apparaten. Een kleine organisatie lost dit op met een applicatieblokkade op het HMI-station en een regel die uitgaand mail- en webverkeer vanuit het machinenetwerk weigert.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.3 RE 1 Zulke communicatiediensten van persoon tot persoon worden in het hele automatiseringsnetwerk geblokkeerd, niet slechts gedeeltelijk beperkt of tot afzonderlijke apparaten beperkt. Vereist vanaf SL 2.

Waarvan je het vaststelt: Bewijs dat de blokkade geldt voor elk apparaat in de zone, bijvoorbeeld via een controle van de geïnstalleerde software op elke computer in de zone en een verbindingstest vanaf een willekeurige installatiecomputer. Kleine organisaties tonen dit aan met een apparatenlijst waarin elke regel is afgevinkt met de controledatum, en een schermafbeelding van de mislukte verbindingspoging.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 5.4 Applicatiegegevens en applicatiefuncties zijn opgedeeld zodat processen met verschillende beschermingsbehoeften of verschillende rechten niet bij dezelfde gebieden kunnen komen. De scheiding is ingebouwd in de systeemarchitectuur en niet overgelaten aan het toeval van de installatie.

Waarvan je het vaststelt: Overzicht van de applicaties met vermelding van welke gegevens en diensten ze gebruiken en welke accounts erachter zitten, configuratie van afzonderlijke instanties, databases, mappen of virtuele machines, en een rechtenlijst per gebied. Een kleine organisatie lost dit op met afzonderlijke gebruikersaccounts en afzonderlijke datamappen voor engineering en bediening, plus een notitie over welke applicatie welke map benadert.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

10 FR 6: Tijdige reactie op gebeurtenissen

3

SR 6.1 De in het systeem verzamelde auditregistraties kunnen worden gelezen en geëvalueerd door de daartoe bevoegde personen en rollen zonder de lopende werking van de installatie te verstoren, en de toegang tot die registraties is zelf beperkt tot geautoriseerde gebruikers.

Waarvan je het vaststelt: Een rol- en permissiematrix die toont wie loggegevens mag inzien, plus een schermafbeelding of export van een logweergave die daadwerkelijk is opgevraagd, met een tijdstempel. Voeg een korte notitie toe over de gebruikte opvraagroute, bijvoorbeeld de operatorinterface van de controller, een logserver of een bestandsexport. Kleine organisaties komen uit met een overzicht van één pagina per installatie: waar het logboek staat, wie leestoegang heeft, hoe het wordt opgevraagd. Een testopvraging eenmaal per jaar, vastgelegd in het onderhoudslogboek, toont aan dat de route werkt. Geldt vanaf SL 1 voor alle beveiligingsniveaus.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 6.1 RE 1 De auditregistraties kunnen worden opgevraagd via een machine-interface zodat analysetools ze verder kunnen verwerken zonder handmatig overtypen, en de gegevens worden geleverd in een gedocumenteerd, algemeen gebruikt formaat.

Waarvan je het vaststelt: Een beschrijving van de gebruikte interface samen met het formaat, bijvoorbeeld syslog, OPC UA Alarms and Conditions, een REST-query of een CSV-export, plus een voorbeeldregistratie en de configuratie van het ontvangende systeem. Als bewijs kan een uittreksel dienen van de SIEM- of logverzamelaarconfiguratie samen met bewijs van binnenkomende registraties. Zonder SIEM volstaat een logverzamelaar op een eenvoudige server die 's nachts via een script de logs ophaalt en opslaat; het script zelf plus een mapoverzicht van de verzamelde bestanden is het bewijs. Als verbetering is dit pas vereist vanaf SL 3, niet vanaf SL 1.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 6.2 Beveiligingsrelevante activiteit in het systeem wordt continu gemonitord, de monitoring detecteert pogingen tot aanval en misbruik en meldt deze onverwijld aan een benoemd aanspreekpunt, en de daarvoor gebruikte tools, meldingstrajecten en verantwoordelijkheden zijn vastgelegd.

Waarvan je het vaststelt: Een overzicht van de monitoringtools per zone, bijvoorbeeld een netwerksensor, antivirusmeldingen, firewallalarmeren of integriteitscontrole, met vermelding van wie de melding ontvangt en binnen welk tijdsbestek een reactie wordt verwacht. Alarmconfiguraties, een lijst van meldingen uit de afgelopen maanden en de bijbehorende afhandelingsnotities dienen als bewijs. Kleine organisaties hebben geen 24-uurs controlekamer nodig: een gedeelde mailbox of ticketinbox die de meldingen van de bestaande systemen bundelt, plus een vaste regel dat een benoemde persoon deze op elke werkdag controleert, is voldoende en wordt aangetoond via de mailboxhistorie. Vereist vanaf SL 2.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

11 FR 7: Beschikbaarheid van middelen

13

SR 7.1 Bij overbelasting of opzettelijke overstromingsaanvallen blijft het systeem in een vastgelegde bedrijfstoestand, de essentiële besturingsfuncties blijven doorwerken, en het uitvallen van één enkele dienst trekt de installatie niet mee omlaag.

Waarvan je het vaststelt: Configuratie van de beschermingsmechanismen (rate limiting, verbindingsslimieten, broadcast storm control op de switches), leveranciersverklaringen over gedrag onder belasting, plus een registratie van een belastingstest of van een echte overbelastingsgebeurtenis met observatie van de besturingsfunctie. Vereist vanaf SL 1. Een kleine organisatie dekt dit met schermafbeeldingen van de switch- en firewallinstellingen en een korte notitie over welke functie doorwerkte tijdens een test van de belangrijkste cel.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

SR 7.1 RE 1 De communicatiebelasting die afzonderlijke onderdelen in het netwerk kunnen inbrengen, is begrensd, zodat een defect of gecompromitteerd onderdeel het netwerksegment niet kan overstromen.

Waarom je het vaststelt: Bandbreedte- en multicastlimieten per poort op de netwerkonderdelen, bewijs van de begrenzing voor elke verbinding, plus een meting van de werkelijke basislast per apparaat. Vereist vanaf SL 2, niet vanaf SL 1. Zonder managed switches kan deze regel niet worden aangetoond, en dat is dan het openstaande punt.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.1 RE 2 Een overbelastingssituatie binnen het beschouwde systeem slaat niet over naar aangrenzende systemen of netwerken; de uitwerking naar buiten is technisch ingeperkt.

Waarom je het vaststelt: Segmentatie- en filterregels op de grenzen, bewijs dat uitgaand verkeer wordt begrensd, plus een testregistratie die toont dat een in het celnetwerk opgewekte belasting het kantoornetwerk of een naburig netwerk niet aantastte. Vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.2 Het gebruik van verwerkingstijd, geheugen, opslagruimte en netwerkbandbreedte is begrensd zodat een enkel proces of dienst niet de middelen kan verbruiken die nodig zijn voor de besturing.

Waarom je het vaststelt: Configuratie van de resourcelimieten (quota's, procesprioriteiten, geheugenlimieten), evaluatie van de gebruiksmeting over een representatieve periode, plus de drempels waarbij een waarschuwing wordt gegeven. Vereist vanaf SL 1. Kleine organisaties gebruiken de ingebouwde middelen van het besturingssysteem en eenvoudige monitoring met een schijfruimte- en CPU-melding per e-mail.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.3 Er zijn back-ups van de systeemconfiguraties, applicatiegegevens en programmaversies; ze kunnen worden gemaakt zonder de lopende werking te onderbreken en zijn beschermd tegen ongeautoriseerde toegang en wijziging.[Document](#)

Waarom je het vaststelt: Back-upconcept dat omvang, frequentie en bewaartermijn dekt, back-uplogboeken van de meest recente runs, plus bewijs van de toegangsbeveiliging van de back-upmedia (aparte opslag, versleuteling, toegewezen permissies). Vereist vanaf SL 1. Een kleine organisatie zet PLC-projecten en HMI-versies terug op een versleuteld medium dat na de back-up fysiek wordt losgekoppeld, en registreert datum en versie in een eenvoudige lijst.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.3 RE 1 De bruikbaarheid van de back-ups is geverifieerd; er is aangetoond dat er daadwerkelijk een werkende toestand uit kan worden hersteld.

Waarom je het vaststelt: Registratie van een herstelproef met datum, geteste back-upversie, doelsysteem en resultaat, minstens voor de kritieke onderdelen. Vereist vanaf SL 2, niet vanaf SL 1. Kleine organisaties controleren eenmaal per jaar steekproefsgewijs één PLC-programma en één HMI-image op een reserveapparaat en leggen het resultaat in twee zinnen vast.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.3 RE 2 De back-up loopt automatisch volgens een vastgelegd schema; een mislukte run wordt gedetecteerd en gemeld.

Waarom je het vaststelt: Schema van de back-up taak, uitvoeringslogboeken zonder hiaten, plus bewijs van de foutmelding voor een run die niet slaagde (alarm, ticket, e-mail). Vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.4

Na een storing, uitval of aanval kan het systeem worden teruggebracht naar een bekende, veilige toestand; het herstel is geïnfuseerd en de verantwoordelijkheden zijn benoemd.[Document](#)

Waaraan je het vaststelt: Herstartplan voor elk kritiek onderdeel met volgorde, benodigde media, contactpersonen en streeftijd, samen met de registratie van de meest recente herstell oefening. Vereist vanaf SL 1. Een kleine organisatie komt uit met een herstartkaart van één pagina per lijn, bewaard in de schakelkast en gecontroleerd bij elke vervanging van een reserveonderdeel.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.5

Als de reguliere stroomvoorziening uitvalt, gaat het systeem naar een vastgelegde toestand: ofwel wordt de voorziening in stand gehouden door een reservebron, ofwel vindt een geordende afsluiting plaats zonder verlies van de veilige toestand.

Waaraan je het vaststelt: Dimensionerings- en onderhoudsbewijs voor de ononderbreekbare stroomvoorziening of het noodaggregaat, testregistratie van de meest recente accu- of belastingtest, plus een beschrijving van het gedrag bij omschakeling en bij het terugkeren van de netstroom. Vereist vanaf SL 1. Kleine organisaties testen de UPS eenmaal per jaar onder belasting en leggen testdatum, overbruggingstijd en acculeeftijd vast.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.6

De netwerk- en beveiligingsinstellingen van het systeem zijn vastgelegd op een goedgekeurde streeftoestand, afwijkingen van die streeftoestand zijn detecteerbaar, en de actuele toestand kan op elk moment worden opgevraagd.[Document](#)

Waaraan je het vaststelt: Goedgekeurde streefconfiguratie per apparaatklasse (hardeningsspecificatie), actuele configuratietoestanden van de apparaten, plus het resultaat van een streef-versus-actueelvergelijking met een lijst van afwijkingen en de reden voor elk. Vereist vanaf SL 1. Een kleine organisatie bewaart de configuratie-exports onder versiebeheer en vergelijkt voor en na elke wijziging.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.6 RE 1

De actuele toestand van de beveiligingsinstellingen kan machineleesbaar worden uitgevoerd zodat deze automatisch tegen de streeftoestand kan worden gecontroleerd.

Waaraan je het vaststelt: Voorbeelduitvoer in een machineleesbaar formaat (configuratie-export, gestructureerd bestand, interfacebevraging) en het script of tool dat de vergelijking met de streeftoestand uitvoert, samen met het resultaatrapport van één run. Vereist vanaf SL 3.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.7

Het systeem is beperkt tot de voor de werking benodigde functies; diensten, poorten, protocollen en interfaces die niet nodig zijn, zijn uitgeschakeld of verwijderd.

Waaraan je het vaststelt: Lijst van actieve diensten en open poorten per onderdeel met een motivering van de noodzaak, bewijs dat de overige zijn uitgeschakeld (configuratie, resultaat van poortscan), plus een regel voor USB- en onderhoudsinterfaces. Vereist vanaf SL 1. Kleine organisaties voeren een eenvoudige poortscan per segment uit en motiveren elk open item in één regel.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing

SR 7.8

Er is een actuele inventarisatie beschikbaar van alle systeemonderdelen met fabrikant, type, firmware- of softwareversie en netwerkadres, en deze wordt actueel gehouden bij wijzigingen.[Document](#)

Waaraan je het vaststelt: Onderdeleninventarisatie met revisiedatum en eigenaar, bewijs van onderhoud via de wijzigingshistorie, plus een vergelijking met een netwerkdetectie om niet-geregistreerde apparaten te vinden. Vereist vanaf SL 2, niet vanaf SL 1. Een kleine organisatie houdt de inventarisatie als tabel bij en werkt deze bij als vaste regel telkens wanneer een apparaat wordt vervangen en telkens wanneer firmware wordt bijgewerkt.

Open	In behandeling	Voldaan	Niet van toepassing
------	----------------	---------	---------------------

Bewijs / onderbouwing