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 IECEE CB 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-uittreksel of een schermafbeelding 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 intrekkingsdatum. 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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 **Overal 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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

Waaraan 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, intrekkingsstatus en bewijs dat de tegenpartij daadwerkelijk de private sleutel bezit. De koppeling tussen certificaat en account is ondubbelzinnig.**

Waaraan je het vaststelt: Configuratie-uittreksel met intrekkingscontrole 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.**

Waaraan je het vaststelt: Datasheet of certificeringsbewijs van het gebruikte beveiligingscomponent en een configuratie-uittreksel 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.**

Waaraan je het vaststelt: Schermafbeelding van het aanmeldscherm met gemaskeerde invoer en een schermafbeelding 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.**

Waaraan je het vaststelt: Configuratie-uittreksel 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.**

Waaraan je het vaststelt: Schermafbeelding 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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

Waaraan 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.**

Waaraan 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 configuratieweergave 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 opslaggrootte 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 aanvaller 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 kantoornetwerk, 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 monitoringsysteem), 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.**

Waaraan je het vaststelt: Een definitie per uitgang of uitgangsgroep (waarde vasthouden, vastgelegde vervangwaarde, veilige stiltoestand) 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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-uittreksel 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 apparaattype, 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 vervaldata 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: Netwerkdiagram 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: Afhankelijkheidslijst 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.**

Waaraan 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.**

Waaraan 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 firewallexport 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan je het vaststelt: Een overzicht van de monitoringtools per zone, bijvoorbeeld een netwerksensor, antivirusmeldingen, firewallalarmen 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.**

Waaraan je het vaststelt: Configuratie van de beschermingsmechanismen (rate limiting, verbindingslimieten, 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.**

Waaraan 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.**

Waaraan 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.**

Waaraan je het vaststelt: Configuratie van de resourcelimieten (quota's, procesprioriteiten, geheugenlimieten), evaluatie van de gebruiksmonitoring 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

Waaraan 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.**

Waaraan 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.**

Waaraan je het vaststelt: Schema van de back-uptaak, 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 geoefend 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 herstelloefening. 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 belastingstest, 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: Voorbeeldуitvoer 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