IEC 62443-3-3:2013 Systemkrav på säkerhet i industriell automation

Sju grundläggande krav, 51 systemkrav

100 krav. Det går att certifiera sig mot denna standard hos ett ackrediterat certifieringsorgan. Utgåva 07/2026.

IEC 62443-3-3 går att certifiera mot, och det som certifieras är ett system, inte en organisation och inte en person. Vägarna är ISASecure SSA och IECEE CB Scheme. Den som vill certifiera organisationen behöver 62443-2-1 eller 2-4, den som avser komponenten behöver 62443-4-2. Denna lista innehåller de 51 systemkraven och de 49 kravförstärkningarna. Vilka av dem som gäller beror på den säkerhetsnivå som eftersträvas: 38 från SL 1, 60 från SL 2, 90 från SL 3, alla 100 vid SL 4. Ingen kravförstärkning gäller redan vid SL 1. Denna lista är ett arbetsstöd för egenkontroll, inte ett bevis.

Företag	Datum	Upprättad av

5 FR 1: Vem eller vad begär åtkomst, och är det verkligen den som uppges 24

SR 1.1 **Mänskliga användare identifieras och deras identitet verifieras innan de får åtkomst, vid varje punkt där de kan styra eller konfigurera automationssystemet. Detta omfattar operatörspaneler vid maskinen, åtkomst för projektering och nättjänster.**

Vad som styrker det: Förteckning över alla inloggningspunkter i systemet, alltså HMI, kontrollrum, programmeringsåtkomst till PLC, switch, VPN och klient för fjärrunderhåll, var och en med det autentiseringssätt som används där. Därtill ett konfigurationsutdrag eller en skärmbild av inloggningsskärmen per enhetsklass. En liten verksamhet börjar med en tabell per enhet, kolumner: enhet, gränssnitt, autentisering finns ja eller nej, motivering vid nej. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.1 RE 1 **Varje mänsklig användare arbetar under en egen identitetsbeteckning som är tilldelad enbart den personen. Gemensamma konton och skiftkonton är avstängda, kvarvarande undantag är motiverade var för sig och kompletterade med ytterligare åtgärder.**

Vad som styrker det: Kontoexport per system med koppling mellan identitetsbeteckning och person, undantagslista med motivering och kompenserande åtgärd, till exempel en kamera eller en närvarojournal vid operatörsplatsen. Denna rad är en kravförstärkning och därför aldrig obligatorisk vid SL 1, den krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.1 RE 2 **Den som loggar in från ett nät som inte är betrott, till exempel från internet eller via en förbindelse för fjärrunderhåll, styrker sin identitet med minst två oberoende faktorer.**

Vad som styrker det: Konfiguration av fjärråtkomsten med andra faktorn aktiverad, ett exempel på en inloggningslogg som visar båda faktorerna, samt utlämningslistan över tokens eller appregistreringar. En liten verksamhet använder den andra faktorn i den befintliga VPN-gatewayen eller en autentiseringsapp, vilket inte kostar något utöver tiden för uppsättning. Kravförstärkning, krävs från SL 3 och uppåt, inte vid SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.1 RE 3 **Styrkandet av identiteten med två oberoende faktorer gäller inte bara åtkomst utifrån, utan varje inloggning av en mänsklig användare, även inloggningar inne i det nät som klassats som betrott.**

Vad som styrker det: Utdrag ur policyn för den centrala autentiseringstjänsten som visar att den andra faktorn genomdrivs utan undantag för något nät, samt stickprov på inloggningsloggar från kontrollrummet och operatörspanelen. Kravförstärkning, krävs först från SL 4 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.2 **Inte bara människor utan även programvaruprocesser och enheter autentiserar sig mot systemet innan de får utbyta data eller använda tjänster. Detta omfattar kopplingar mellan styrenheter, dataförbindelser till överordnade system och diagnosverktyg.**

Vad som styrker det: En lista över maskinella förbindelser med källa, mål, protokoll och den autentiseringsuppgift som används i varje fall, till exempel certifikat, tjänstekonto eller förutdelad nyckel. Därtill ett konfigurationsutdrag för en koppling som gör autentiseringen synlig. Krävs från SL 2 och uppåt, krävs inte vid SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.2 RE 1 **Varje programvaruprocess och varje enhet uppträder med en egen unik identitetsbeteckning. Gemensamt använda tjänstekonton eller en enda systemgemensam nyckel för många enheter används inte.** Dokument

Vad som styrker det: Sammanställning av enhet mot identitetsbeteckning eller certifikatets serienummer som visar att ingen identitetsbeteckning förekommer två gånger. Kravförstärkning, krävs från SL 3 och uppåt och ingår därför inte i SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.3 **Konton styrs under hela sin livscykel: skapande, ändring av behörigheter, avstängning vid avgång och borttagning är reglerade och stöds av de system som berörs. Detta omfattar användarkonton, tjänstekonton och nödkonton.** Dokument

Vad som styrker det: Kontoregister med typ, innehavare, syfte och status, samt bevis för anställningar och avgångar, till exempel en undertecknad överlämning eller ett ärende som visar avstängningen med datum. En återkommande genomgång av kontona är lämplig, och i en liten verksamhet räcker en årlig avstämning av kontolistan mot personallistan. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.3 RE 1 **Kontohanteringen löper enhetligt över alla komponenter i systemet, så att en avstängning på ett ställe inte förblir verkningslös i enskilda enheter.**

Vad som styrker det: Bevis för den centrala kataloganslutningen, till exempel katalogtjänst eller RADIUS, med en lista över de anslutna komponenterna och en uttrycklig lista över de enheter som inte går att ansluta tillsammans med deras ersättningsrutin. Testprotokoll för en avstängning som slår igenom på alla anslutna system. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.4 **Identitetsbeteckningar tilldelas efter fasta regler, kopplas entydigt till en person, en enhet eller en roll, tas ur bruk när de inte längre används och tilldelas aldrig senare en annan innehavare.**

Vad som styrker det: Namnregel för identitetsbeteckningar, till exempel efternamn och initial eller anläggningskod och nummer, samt historiken över beteckningar som tagits ur bruk, av vilken det framgår att de inte återanvänds. En liten verksamhet har en enda löpande lista med tilldelningsdatum och avvecklingsdatum. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.5 **Autentiseringsmedel som lösenord, nycklar, certifikat och tokens lämnas ut ordnat, byts vid misstanke om röjande och spärras vid behov. Levererade standardkonton och fabrikslösenord är ändrade före driftsättningen.**

Vad som styrker det: Utlämningslista över tokens och certifikat med mottagare och datum, bevis för byten och spärrar, samt en driftsättningschecklista per enhet med punkten fabrikslösenord ändrat, avprickad. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.5 RE 1 **Autentiseringsuppgifterna för programvaruprocesser ligger inte som en läsbar fil på lagringsmediet, utan i ett hårdvarubaserat lagringsutrymme som hindrar att den hemliga delen läses ut.**

Vad som styrker det: Typbevis för den säkerhetskomponent som används, till exempel TPM, secure element eller HSM, med ett konfigurationsutdrag som styrker att nyckeln lagras inne i komponenten. En inköpshandling eller ett datablad räcker som typbevis. Kravförstärkning, krävs från SL 3 och uppåt, krävs inte vid SL 1 och SL 2.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.6 **Trådlös åtkomst till systemet, till exempel WLAN, radiofjärrkontroller eller diagnos via Bluetooth, går att använda först efter identifiering och autentisering av både användare och enhet, och hanteras medvetet.**

Vad som styrker det: Förteckning över alla trådlösa förbindelser med syfte, räckvidd och krypteringsmetod, konfigurationsutdrag för accesspunkten och listan över godkända slutenheter. En liten verksamhet dokumenterar dessutom vilka trådlösa gränssnitt i enheterna som medvetet stängts av. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.6 RE 1 **Varje trådlös åtkomst går att knyta entydigt till en bestämd användare eller en bestämd enhet, en gemensam nätnyckel för alla deltagare räcker inte.**

Vad som styrker det: Bevis för en metod med individuella autentiseringsuppgifter, till exempel företagsgemensam WLAN-inloggning mot en katalog eller certifikat per enhet, samt en anslutningslogg som visar den enskilda identitetsbeteckningen. Kravförstärkning, krävs från SL 2 och uppåt och därför inte vid SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.7 **Där lösenord används går deras minsta styrka att ställa in, till exempel minsta längd och krävda teckentyper, och de inställda värdena är verksamma för alla berörda konton.**

Vad som styrker det: Konfigurationsutdrag för lösenordspolicyn per system med de värden som faktiskt är satta, till exempel längd >= 10 tecken och minst tre teckentyper, samt en lista över de system som tekniskt inte klarar denna inställning tillsammans med deras kompenserande åtgärd. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.7 RE 1 **För mänskliga användare gäller dessutom regler för hur lösenord skapas och hur länge de lever: återanvändning av tidigare lösenord förhindras och giltigheten är tidsbegränsad.**

Vad som styrker det: Konfigurationsutdrag som visar lösenordshistoriken, till exempel att återanvändning av de fem senaste lösenorden är spärrad, och den inställda längsta giltigheten. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.7 RE 2 **Begränsningen av lösenordens livslängd gäller inte bara personer utan alla konton, alltså även tjänstekonton, underhållskonton och enhetskonton.**

Vad som styrker det: Bytesplan för tekniska konton med senaste och nästa bytesdatum per konto, samt bevis för bytena, till exempel en ändringslogg eller ett ärende. Kravförstärkning, krävs först från SL 4 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.8 **Där certifikat används kommer de från en ordnad certifikathantering med fastställda regler för ansökan, utfärdande, giltighetstid, förnyelse och spärr.** Dokument

Vad som styrker det: Certifikatpolicy eller en kort skriftlig regel med ansvar, giltighetstider och spärrväg, samt en förteckning över utfärdade certifikat med utgångsdatum. En liten verksamhet har en tabell med certifikat, enhet, utgångsdatum och påminnelsedatum, vilket förhindrar tyst anläggningsstillestånd på grund av utgångna certifikat. Krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 1.9 **När nyckelpar används för autentisering validerar systemet certifikatet fullständigt: förtroendekedja, giltighetstid, spärrstatus och bevis för att motparten verkligen innehar den privata nyckeln. Kopplingen mellan certifikat och konto är entydig.**

Vad som styrker det: Konfigurationsutdrag med aktiverad spärrkontroll, till exempel CRL eller OCSP, testprotokoll för en avvisad inloggning med utgånget eller spärrat certifikat, samt kopplingstabellen certifikat mot konto. Krävs från SL 3 och uppåt, krävs inte vid SL 1 och SL 2.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.9 RE 1 **De privata nycklarna ligger uteslutande i ett hårdvarubaserat lagringsutrymme som de inte går att läsa ut ur, och de används också där inne.**

Vad som styrker det: Datablad eller certifieringsbevis för den säkerhetskomponent som används och ett konfigurationsutdrag som visar att nyckeln skapas inne i komponenten, så att den privata nyckeln aldrig lämnar den. Kravförstärkning, krävs först från SL 4 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.10 **Under inloggningen röjer systemet ingen information som går att utnyttja. Inmatade lösenord visas dolt och felmeddelanden avslöjar inte om det var identitetsbeteckningen eller lösenordet som var fel.**

Vad som styrker det: Skärmbild av inloggningsskärmen med maskerad inmatning och en skärmbild av felmeddelandet efter ett misslyckat försök. För enheter som tekniskt inte klarar detta, till exempel äldre operatörspaneler, en kort notering om den kompenserande åtgärden, till exempel begränsat fysiskt tillträde till uppställningsplatsen. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.11 **Antalet inloggningsförsök i följd som misslyckas är begränsat och reaktionen på det går att ställa in, till exempel en tidsbegränsad spärr. Den valda reaktionen hindrar inte den säkerhetsinriktade manövreringen av anläggningen.**

Vad som styrker det: Konfigurationsutdrag med gränsvärdet, till exempel spärr efter <= 5 misslyckade försök, och spärrtiden, samt en kort bedömning av varför spärren inte blockerar nöddrift eller en säker nedkörning av anläggningen. Vid operatörsplatser med säkerhetsfunktion är en tidsspärr att föredra framför en varaktig kontospärr. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.12 **Före inloggningen går det att visa en användningsanvisning som pekar på reglerna för användning och övervakning av systemet. Text och visning går att ställa in av tillgångsägaren.**

Vad som styrker det: Skärmbild av den visade anvisningstexten och den godkända lydelsen med datum för godkännandet. Små verksamheter stämmer kort av lydelsen med skyddsombudet eller med ledningen, ett stycke räcker. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.13 **Åtkomst från nät som inte är betrodda, till exempel fjärrunderhåll av leverantörer, är begränsad till fastställda vägar, övervakas och går att avbryta när som helst.**

Vad som styrker det: Förteckning över fjärråtkomstvägarna med syfte, motpart, kontaktperson och den väg som används, samt anslutningsloggar och bevis för möjligheten att koppla ifrån, till exempel en nyckelbrytare, en brandväggsregel eller en router för fjärrunderhåll som går att stänga av. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 1.13 RE 1 **Varje enskild session från ett nät som inte är betrott godkänns uttryckligen av en ansvarig person innan förbindelsen upprättas, en varaktigt öppen förbindelse räcker inte.**

Vad som styrker det: Godkännandenoteringar per session för fjärrunderhåll med tidpunkt, anledning, godkännande person och varaktighet, tekniskt till exempel via en nyckelbrytare vid åtkomstroutern eller via en godkännandeportal. I en liten verksamhet räcker en journal för fjärrunderhåll vid elskåpet som underhållsteknikern prickar av för varje session. Kravförstärkning, krävs från SL 2 och uppåt och därför aldrig vid SL 1.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

6 FR 2: Användningskontroll (behörigheter, sessioner, loggposter) 24

SR 2.1 **Systemet genomdriver de tilldelade behörigheterna tekniskt: varje inloggad person, varje enhet och varje programvaruprocess får exakt den åtkomst som tilldelats, och försök därutöver avvisas.**

Vad som styrker det: Ett behörighetskoncept med koppling mellan konton och rättigheter, samt en skärmbild eller ett konfigurationsutdrag per styrsystem, HMI och projekteringsstation som visar de aktiva behörigheterna. Därtill ett testprotokoll där ett konto med låg behörighet försöker utföra en spärrad åtgärd och avvisas. Krävs från SL 1. En liten verksamhet klarar sig med två eller tre roller, till exempel drift, underhåll och projektering, och dokumenterar dem på en sida.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.1 RE 1 **Genomdrivandet av behörigheterna gäller inte bara mänskliga operatörer utan lika mycket programvaruprocesser och enheter som når systemet på egen hand.**

Vad som styrker det: En lista över tekniska konton och tjänstekonton, till exempel klienter för OPC UA, anslutningar till historikdatabaser och tjänster för säkerhetskopiering, var och en med sin tilldelade uppsättning behörigheter. Ett utdrag ur behörighetshanteringen som visar att dessa konton inte körs med administratörsrättigheter. Kravförstärkning, krävs från SL 2, inte vid SL 1.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.1 RE 2 **Behörigheter tilldelas inte personer en och en utan via roller, och kopplingen från roll till tillåtna åtgärder är dokumenterad på ett spårbart sätt.** Dokument

Vad som styrker det: En matris över roller och behörigheter som tabell: raderna är rollerna, kolumnerna åtgärderna som ändra börvärde, ladda program, kvittera larm och skapa konto. Därtill listan som kopplar person till roll. Kravförstärkning, krävs från SL 2. Ett underhållet kalkylblad med ändringsdatum räcker fullt ut som bevis.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.1 RE 3 **I snävt avgränsade undantagsfall kan en behörig arbetsledare tillfälligt häva en behörighetsbegränsning, och varje sådan hävning dokumenteras i loggen över säkerhetsrelevanta händelser.**

Vad som styrker det: En rutinbeskrivning för undantagsgodkännandet med uppgift om vem som får ge det och hur länge det gäller, samt loggposter för redan givna hävningar hämtade ur systemloggen. Kravförstärkning, krävs från SL 3.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.1 RE 4 **Särskilt kritiska ingrepp kräver godkännande av två av varandra oberoende behöriga personer innan åtgärden utförs.**

Vad som styrker det: En lista över de åtgärder som omfattas av tvåpersonsgodkännande, till exempel ändring av säkerhetsparametrar eller inladdning av ett nytt styrprogram, tillsammans med konfigurationsbevis och loggposter som namnger båda godkännarna. Kravförstärkning, krävs först från SL 4.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.2 **Användningen av trådlösa förbindelser i automationsnätet är knuten till en uttrycklig behörighet, och endast godkända deltagare får utbyta data eller ingripa över radio.**

Vad som styrker det: En förteckning över alla trådlösa förbindelser, till exempel accesspunkter för WLAN, Bluetooth-kopplingar och mobilnätsroutrar, var och en med sitt syfte och sina godkända deltagare. Därtill konfigurationen av behörighetsstyrningen vid accesspunkten. Krävs från SL 1. Den som inte driver någon trådlös förbindelse i processnätet dokumenterar just det skriftligt och styrker det med en konfigurationsvy som visar att radio är avstängd.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.2 RE 1 **Obehöriga trådlösa enheter i närheten av automationsnätet upptäcks och rapporteras.**

Vad som styrker det: Ett redovisande dokument från den trådlösa övervakningen eller en återkommande radioskanning med datum, resultatlista och notering om varje okänd enhet. Rapportvägen till ansvarig funktion är namngiven. Kravförstärkning, krävs från SL 2, inte vid SL 1. En liten verksamhet kan göra en skanning per kvartal med en bärbar dator och lägga resultatet till handlingarna som redovisande dokument.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.3 **Användningen av bärbara och mobila enheter mot systemet, till exempel servicedatorer, USB-minnen eller surfplattor, är reglerad och tekniskt begränsad till uttryckligen tillåtna enheter.**

Vad som styrker det: Regelverket för enhetsanvändning, en lista över tillåtna serviceenheter med deras identitetsbeteckningar, och bevis för den tekniska spärren, till exempel att USB-portarna på HMI och projekteringsstation är avstängda eller begränsade till bestämda enheter. Krävs från SL 1. En liten verksamhet arbetar med två märkta serviceminnen som det endast skrivs till vid en enda slussdator.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.3 RE 1 **Före anslutning kontrolleras säkerhetstillståndet hos en bärbar eller mobil enhet, och enheter som inte uppfyller kraven hindras från åtkomst.**

Vad som styrker det: Kontrollkriterierna för enhetens tillstånd, till exempel aktuellt skydd mot skadlig kod och nivå på säkerhetsuppdateringar, samt kontrollprotokoll per serviceenhet och bevis för den tekniska tillämpningen, till exempel via en slussdator eller en behörighetsstyrning i nätet. Kravförstärkning, krävs från SL 3.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.4 **För mobil kod som körs på systemet, till exempel skript i operatörsgränssnitt eller aktivt innehåll i rapporter, är det fastställt vilka slag som är tillåtna, och slag som inte är tillåtna hindras från att köras.** Dokument

Vad som styrker det: En fastställd uppgift om vilken mobil kod som är tillåten på vilka system, samt konfigurationsbevis för spärren, till exempel att skriptkörning i webbläsaren på HMI är avstängd och att makron i utvärderingsfiler är blockerade. Krävs från SL 1. En fastställd uppgift på en sida med de tre eller fyra fall som faktiskt finns räcker.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.4 RE 1 **Innan mobil kod körs verifieras att den kommer från den förväntade källan och är oförändrad.**

Vad som styrker det: Konfigurationsbevis för signaturkontrollen eller kontrollsummekontrollen, samt ett testprotokoll där manipulerad eller osignerad kod avvisas. Kravförstärkning, krävs från SL 3.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.5 **En session låses efter en fastställd tid utan manöverhandling och släpps upp igen först efter förnyad autentisering, utan att visningen av säkerhetsrelevant processinformation går förlorad.**

Vad som styrker det: Ett konfigurationsutdrag med den inställda låstiden per arbetsplats, samt en motivering för arbetsplatser i ständigt bemannade kontrollrum där låsningen medvetet är inställd annorlunda. Krävs från SL 1. Visuellt bevis: en skärmbild av låsskärmen med larmraden fortfarande synlig.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 2.6 **Sessioner på distans avslutas efter en fastställd tid utan aktivitet eller på begäran av den driftansvarige, så att ingen öppen fjärrförbindelse blir kvar obevakad.**

Vad som styrker det: Konfigurationen av fjärråtkomsten med sin tidsgräns för overksamhet, loggposter för avslutade fjärrsessioner, och beskrivningen av hur den driftansvarige omedelbart kan bryta ett pågående fjärrunderhåll, till exempel via en nyckelbrytare eller ett godkännande per session. Krävs från SL 2, inte vid SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.7 **Antalet samtidigt öppna sessioner per konto eller roll är begränsat, och inloggningsförsök därutöver avvisas.**

Vad som styrker det: Ett konfigurationsutdrag med den fastställda övre gränsen per roll, till exempel <= 1 samtidig session för konton för projektering, samt ett testprotokoll för det avvisade andra inloggningsförsöket. Krävs från SL 3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.8 **Säkerhetsrelevanta händelser loggas, och varje post anger minst tidpunkt, källa, utlösande konto, händelsens art och resultat.** Dokument

Vad som styrker det: En fastställd uppgift om vilka händelseslag som loggas, till exempel inloggning, misslyckad inloggning, behörighetsändring, programändring och konfigurationsändring, samt ett verkligt utdrag ur loggfilen som visar de nämnda fälten. Krävs från SL 1. En liten verksamhet samlar loggarna från styrsystem, HMI och brandvägg i en mapp med fast bevarandetid.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.8 RE 1 **Loggarna från de enskilda komponenterna löper samman på ett centralt ställe och bildar ett gemensamt redovisande dokument som går att utvärdera systemövergripande.**

Vad som styrker det: En arkitekturskiss över logginsamlingen med alla anslutna källor, samt en utvärdering som placerar händelser från minst två komponenter på en gemensam tidslinje. Kravförstärkning, krävs från SL 3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.9 **För loggningen finns tillräckligt lagringsutrymme, så att händelser bevaras under den fastställda bevarandetiden och inte skrivs över oavsiktligt.**

Vad som styrker det: En beräkning eller uppskattning av lagringsbehovet ur daglig loggvolym gånger bevarandetid, samt den inställda lagringsstorleken och regeln för arkivering. Krävs från SL 1. I praktiken räcker en daglig kopiering till en separat lagringsplats med dokumenterad bevarandetid.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.9 RE 1 **När en fastställd fyllnadsgräns för loggutrymmet nås går en varning till ansvarig funktion innan lagringsutrymmet är helt förbrukat.**

Vad som styrker det: Ett konfigurationsutdrag för gränsvärdet, till exempel varning från >= 80 procent beläggning, samt ett exempel på det utlösta meddelandet och mottagarlistan. Kravförstärkning, krävs från SL 3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.10 **Faller loggningen bort eller blir loggutrymmet fullt reagerar systemet på ett i förväg fastställt sätt och ansvarig funktion informeras, utan att den säkra driften av anläggningen äventyras.**

Vad som styrker det: Den fastställda reaktionen per felfall, till exempel att äldre poster skrivs över och en anmälan går ut i stället för att anläggningen stoppas, med en motivering ur processens synvinkel. Bevis genom ett utlöst testmeddelande och den tillhörande loggposten. Krävs från SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.11 **Varje loggpost bär en tidsstämpel från en namngiven tidskälla, så att händelser från olika komponenter går att ordna tidsmässigt i förhållande till varandra.**

Vad som styrker det: Uppgift om vilken tidskälla som används per komponent och ett loggutdrag med synlig tidsstämpel inklusive tidszon. Krävs från SL 2, inte vid SL 1.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.11 RE 1 **Klockorna i alla deltagande komponenter synkroniseras mot en gemensam tidskälla så att avvikelsen håller sig inom en fastställd gräns.**

Vad som styrker det: Konfigurationen av tidssynkroniseringen, till exempel NTP-server och synkroniseringsintervall, samt ett kontrollprotokoll med den uppmätta avvikelsen per komponent mot den fastställda gränsen, till exempel <= 1 sekund. Kravförstärkning, krävs från SL 3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.11 RE 2 **Tidskällan själv är skyddad mot manipulation, och en orimlig eller ändrad tidsreferens upptäcks och rapporteras.**

Vad som styrker det: En beskrivning av hur tidskällan säkras, till exempel autentiserad tidssynkronisering, begränsning till en intern källa och övervakning av tidshopp, samt meddelanden eller loggposter från en upptäckt avvikelse. Kravförstärkning, krävs först från SL 4.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.12 **För fastställda kritiska handlingar går det att i efterhand tveklöst belägga vem som utlöste dem, så att den handlande personen inte trovärdigt kan förneka det.** Dokument

Vad som styrker det: En lista över de handlingar som detta bevis gäller för, till exempel receptändring, frisläppande av en sats och ändring av gränsvärden, samt de tillhörande redovisande dokumenten med entydig personbeteckning och bevis för att gruppkonton är uteslutna för dessa handlingar. Krävs från SL 3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 2.12 RE 1 **Den tveklösa kopplingen till den handlande personen gäller inte bara utvalda kritiska handlingar utan alla användare och alla åtgärder som de utlöser.**

Vad som styrker det: Bevis för att varje konto är personbundet och att inga gemensamma inloggningar finns kvar, samt ett loggutdrag för godtyckliga åtgärder där en entydig personbeteckning står genomgående. Kravförstärkning, krävs först från SL 4.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7 FR 3: Systemintegritet, skydd av data, programvara och sessioner mot obehörig ändring 19

SR 3.1 **Automationssystemet upptäcker när information har ändrats under överföring via en kommunikationskanal, och det gäller styrdata, konfigurationsdata och administrationstrafik lika. Skyddet omfattar även förbindelser som lämnar systemet eller passerar nätsegment som inte är betrodda.**

Vad som styrker det: En översikt över nät och protokoll med uppgift om vilken kanal som använder vilken integritetsmekanism (kontrollsumma, message authentication code, signerade telegram), ett konfigurationsutdrag för säkerhetsinställningarna i fältbussen eller OPC UA, och ett testprotokoll som visar att ett manipulerat telegram bevisligen förkastades. En liten verksamhet dokumenterar detta i en tabell per förbindelse med kolumnerna källa, mål, protokoll och integritetsmekanism, och styrker verkan en gång med en infångad trafikmängd. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.1 RE 1 **Integritetsskyddet under överföring vilar på kryptografiska metoder, så att en riktad manipulation från en angripare med egna medel inte förblir oupptäckt. En enkel kontrollsumma mot överföringsfel räcker inte här.**

Vad som styrker det: En lista över de kryptografiska metoder och nyckellängder som används per kanal, en hänvisning till den underliggande nyckelhanteringen, och konfigurationsutdrag (till exempel chiffersviter för TLS, SecurityPolicy för OPC UA och profiler för IPsec). Små verksamheter använder de säkra fabriksprofilerna i sina styrenheter och lägger en skärmbild av den aktiva inställningen till handlingarna. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.2 **Det finns skyddsmekanismer mot skadlig kod som hindrar att oönskad programkod körs på systemkomponenter och som rapporterar varje fynd. Mekanismerna är valda så att de inte stör anläggningens avsedda drift, och de hålls aktuella.**

Vad som styrker det: En översikt per komponent över vilken mekanism som griper in (virusskydd, vitlistning av program, härdat operativsystem utan körrättigheter), bevis för att signaturer eller vitlistor uppdateras, och meddelanden från skyddssystemet. Där virusskydd inte är möjligt, till exempel på en styrenhet, dokumenteras den kompenserande åtgärden med sin motivering. Små verksamheter klarar sig väl med vitlistning på operatörsdatorn och en skriftlig regel för USB-medier. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.2 RE 1 **Skyddet mot skadlig kod griper dessutom in vid de punkter där data kommer in i eller lämnar anläggningen, och inte bara i slutenheterna själva.**

Vad som styrker det: En lista över alla punkter där data kommer in eller lämnar (åtkomst för fjärrunderhåll, gateway för dataöverföring, flyttbara medier, överlämning till kontorsnätet, e-postvägen för programversioner) med den avsökning som är verksam vid var och en, samt redovisande dokument över de överlämningar som kontrollerats. Små verksamheter sätter upp en enda överlämningsdator med virusavsökning som sluss och dokumenterar detta i en arbetsinstruktion. Kravförstärkning, krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.2 RE 2 **Skyddsmekanismerna mot skadlig kod styrs från ett centralt ställe, uppdateringar fördelas centralt, och fynd samlas på ett ställe för utvärdering.**

Vad som styrker det: Konfigurationen av den centrala hanteringskonsolen, en rapport över uppdateringsstatus för alla anslutna komponenter, och en utvärdering av rapporterade fynd över en tidsperiod. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.3 **Systemets säkerhetsfunktioner verifieras med planerade intervall och efter ändringar för att bekräfta att de verkligen fungerar. Proven planeras så att de inte äventyrar anläggningens drift, och resultaten dokumenteras.** Dokument

Vad som styrker det: En provplan med provobjekt, intervall och tidsfönster, tillsammans med testprotokollen som visar datum, provare, förväntat beteende och iakttaget beteende. Nyttiga enskilda prov är: en inloggning med ett avstängt konto misslyckas, virusskyddet reagerar på en testfil, åtkomsten för fjärrunderhåll går inte att nå utan godkännande. Små verksamheter lägger provningen till det underhållsstopp som ändå är planerat och betar av en fast checklista. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.3 RE 1 **Verifieringen av säkerhetsfunktionerna löper med automatiserade medel, så att den går att upprepa utan manuellt arbete och ger ett enhetligt resultat.**

Vad som styrker det: Skripten eller provverktygen tillsammans med sitt schema, sina utdatafiler, och en jämförelse av flera körningar som visar att avvikelser upptäcks. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.3 RE 2 **Verifieringen av säkerhetsfunktionerna är möjlig även under normal drift, utan att anläggningen behöver stoppas eller sättas i ett särskilt tillstånd.**

Vad som styrker det: En beskrivning av provrutinen med bevis för att den inte har någon negativ inverkan på processen, till exempel en analys av påverkan på cykeltider och nätbelastning, samt testprotokoll hämtade från produktiv drift. Kravförstärkning, krävs från SL 4 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.4 **Obehöriga ändringar av programvara, firmware och lagrad information upptäcks. Detta gäller lika för styrprogram, parameteruppsättningar, recept och konfigurationsfiler.**

Vad som styrker det: En förteckning över de versioner som är värda att skydda med lagrade kontrollvärden eller signaturer, resultaten av integritetsjämförelserna, och den dokumenterade avstämningen mot den version som ligger i versionshanteringen. Små verksamheter lagrar den frisläppta programversionen tillsammans med sin kontrollsumma på en skrivskyddad plats och jämför vid misstanke eller efter underhåll. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.4 RE 1 **Upptäcks ett brott mot integriteten hos programvara eller information rapporterar systemet detta automatiskt till ett ansvarigt ställe, utan att någon aktivt måste leta efter det.**

Vad som styrker det: Konfigurationen av meddelandevägarna (larm i kontrollrummet, e-post, meddelande till övervakningssystemet), en mottagarlista med ersättarordning, och minst ett testlarm med dokumenterad svarstid. Kravförstärkning, krävs från SL 3 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.5 **Inmatningar som systemet tar emot från processdata, gränssnitt eller användargränssnitt kontrolleras mot tillåten syntax, tillåtet värdeområde och tillåten längd innan de bearbetas. Ogiltiga inmatningar leder inte till okontrollerat beteende.**

Vad som styrker det: En specifikation av gränser och format per inmatning, utdrag ur valideringslogiken i styrenheten eller programmet, och testfall med avsiktligt ogiltiga inmatningar (ett för stort värde, en felaktig datatyp, en överlång teckensträng) tillsammans med systemets dokumenterade beteende. Små verksamheter dokumenterar rimlighetsgränserna per mätpunkt i en tabell och verifierar dem vid driftsättningen. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.6 **För felfallet är det fastställt vilket tillstånd utgångarna till anläggningen intar, och systemet intar exakt det tillståndet. Det fastställda tillståndet är avstämt mot anläggningens funktionssäkerhet.**

Vad som styrker det: En fastställd uppgift per utgång eller utgångsgrupp (hållet värde, fastställt ersättningsvärde, säkert frånslag) med en motivering ur riskbedömningen, ett konfigurationsutdrag för styrenheten, och bevis från ett felprov, till exempel ett kabelbrott eller ett kommunikationsbortfall, som visar det förväntade beteendet. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.7 **Systemet hanterar feltillstånd så att driften förblir under kontroll och ingen information röjs som skulle hjälpa en angripare. Felmeddelanden som visas för operatörer förblir korta, medan de tekniska detaljerna går enbart till de interna loggarna.**

Vad som styrker det: En översikt över felklasserna med det systembeteende som förutses för var och en, exempel på de visade meddelandena jämförda med de motsvarande interna loggposterna, och provbevis för att inga filsökvägar, kontonamn, databasutdata eller versionsuppgifter syns i operatörsgränssnittet. Krävs från SL 1 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 3.8 **Aktiva sessioner är skyddade mot kapning och mot att främmande meddelanden förs in. En session upphör vid utloggning eller efter en fastställd tid utan aktivitet, och därefter går den inte att återanvända.**

Vad som styrker det: Konfigurationen av sessionshanteringen med de inställda gränserna för overksam tid och längsta varaktighet, bevis för den mekanism som skyddar mot återuppspelning av meddelanden, och ett testprotokoll där en avlyssnad session inte längre fungerar efter utloggning. Krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.8 RE 1 **Sessionsidentiteter förlorar sin giltighet när sessionen upphör och tas inte emot igen av systemet, inte heller när de visas upp på nytt utifrån.**

Vad som styrker det: Ett konfigurationsutdrag för sessionshanteringen som omfattar ogiltigförklaringen, samt ett testprotokoll där en tidigare giltig identitet skickas på nytt efter utloggning och avvisas av systemet. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.8 RE 2 **För varje ny session skapas en egen identitet för engångsbruk. Identiteter återanvänds inte mellan sessioner, användare eller enheter.**

Vad som styrker det: En beskrivning av framställningsrutinen och bevis ur loggen eller en infångad trafikmängd för att flera inloggningar i följd får olika identiteter. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.8 RE 3 **Sessionsidentiteter skapas med erkända slumpmetoder, så att de varken går att gissa eller härleda ur föregående identiteter.**

Vad som styrker det: Uppgift om vilken slumptalsgenerator som används och dess entropikälla, en leverantörsförsäkran eller provrapport om den, och en statistisk utvärdering av ett stickprov av skapade identiteter. Kravförstärkning, krävs från SL 4 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.9 **De säkerhetsrelaterade loggarna och de verktyg som används för att utvärdera dem är skyddade mot obehörig åtkomst, ändring och radering. Kretsen av personer som får ändra eller ta bort loggposter hålls snäv och är namngiven.** Dokument

Vad som styrker det: Ett behörighetskoncept för loggdata med namngiven tilldelning, konfigurationen av vidarebefordran till ett separat loggsystem, bevarandetider, och provbevis för att en vanlig operatör inte kan radera poster. Små verksamheter vidarebefordrar loggarna till en separat enhet som anläggningens operatörer inte har skrivbehörighet till. Krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 3.9 RE 1 **De säkerhetsrelaterade loggarna lagras dessutom på ett medium som utesluter senare överskrivning, så att en post som en gång skrivits inte längre går att ändra, inte ens med administrativa rättigheter.** Dokument

Vad som styrker det: En beskrivning av den lagring som används (medium som endast går att skriva en gång, manipulationssäkert arkiv, fortlöpande förlängd signaturkedja), bevis för ett misslyckat försök att ändra en post, och regeln för hur medierna bevaras och hämtas fram. Kravförstärkning, krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8 FR 4: Konfidentialitet för data 6

SR 4.1 **Automationssystemet skyddar konfidentiell information mot obehörigt röjande, både under överföring och i lagrat skick. Det är fastställt vilka data som räknas som konfidentiella, till exempel recept, parameteruppsättningar, autentiseringsuppgifter, konfigurationsfiler eller diagnosdata med personanknytning.** Dokument

Vad som styrker det: En lista över de datatyper som är värda att skydda, med uppgift om var de förvaras och hur de överförs, samt den konkreta skyddsåtgärden för varje post, till exempel en krypterad förbindelse, ett krypterat lagringsmedium eller en begränsad utdelad mapp. En liten verksamhet klarar sig med en tabell på en sida: datatyp, var den ligger, vem som får se den, vad som skyddar den. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 4.1 RE 1 **För information som färdas över nät som inte är betrodda eller lagras utanför den skyddade miljön genomdrivs konfidentialiteten med tekniska medel i stället för att bara utlovas i en organisatorisk regel.**

Vad som styrker det: Ett konfigurationsutdrag för den transportkryptering eller lagringskryptering som används, till exempel VPN-profilen för fjärrunderhåll, TLS-inställningarna i styrsystemets gränssnitt, eller krypteringen av medierna för säkerhetskopiering. En daterad skärmbild av den aktiva inställningen räcker som bevis. Krävs från SL 2 och uppåt, inte från SL 1, eftersom detta är en kravförstärkning.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 4.1 RE 2 **Konfidentialiteten genomdrivs även vid gränserna mellan zoner, så att information inte blir synlig i klartext när den går från en zon in i en annan.**

Vad som styrker det: En plan över zoner och conduits med markering av vilka övergångar som är krypterade, tillsammans med konfigurationen av gränskomponenten såsom en gateway, en brandvägg eller en datadiod. En infångad trafikmängd eller ett testprotokoll som visar att inga klartextdata syns vid gränsen. Krävs från SL 4 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 4.2 **Det är fastställt hur konfidentiell information avlägsnas tillförlitligt när enheter tas ur drift, byter innehavare, går ut på reparation eller återanvänds, så att inga läsbara restdata blir kvar.** Dokument

Vad som styrker det: En skriftlig rutin för urdrifttagning med raderingsmetod per enhetstyp, samt raderingsprotokoll med enhetens beteckning, datum och den person som utförde arbetet. En liten verksamhet dokumenterar detta som en rad per enhet i en gemensam lista och lägger intygen från externa avfallsentreprenörer bredvid. Krävs från SL 2 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 4.2 RE 1 **Gemensamt använda lagringsområden töms innan de tilldelas en annan användare eller process, så att innehåll från den föregående användaren inte går att läsa ut.**

Vad som styrker det: En leverantörsförsäkran eller en konfigurationsuppgift om tömningen av återanvända minnesområden och buffertar, kompletterad med ett testprotokoll från mottagningsprovning eller underhåll. Där en komponent inte klarar detta tjänar den dokumenterade kompenserande åtgärden som bevis, till exempel att enheten inte delas mellan olika roller. Krävs från SL 3 och uppåt, inte från SL 1, eftersom detta är en kravförstärkning.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 4.3 **Där kryptografi används följer algoritmerna, nyckellängderna och nyckelhanteringen erkänd god praxis, och det är fastställt hur nycklar skapas, fördelas, lagras, byts och spärras.** Dokument

Vad som styrker det: En översikt över de metoder som används per system, med algoritm, nyckellängd och giltighetstid, samt reglerna för nyckelhantering och redovisande dokument över nyckelbyten och certifikatförnyelser. Offentliga rekommendationer tjänar som måttstock, till exempel de tekniska riktlinjerna från tyska BSI. En liten verksamhet har en certifikatlista med utgångsdatum och en påminnelse >= 30 dagar före utgången. Krävs från SL 1 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9 FR 5: Begränsat dataflöde, zoner och conduits 11

SR 5.1 **Styrsystemet går att dela upp i avgränsade zoner, och trafiken mellan dessa zoner löper uteslutande via fastställda conduits. Uppdelningen följer en motivering som går att förklara, till exempel efter skyddsbehov, ansvar eller funktion hos de anläggningsdelar som berörs.** Dokument

Vad som styrker det: Nätplan med inritade zoner och conduits däremellan, en lista över zonerna med motivering för varje gräns, och konfigurationen av de avskiljande komponenterna såsom VLAN-definitioner eller gränssnitt i brandväggen. En liten verksamhet klarar sig med en skiss på en sida där kontor, maskinnät och fjärråtkomst står som tre rutor med förbindelserna däremellan, samt en skärmbild av switchens VLAN-konfiguration.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.1 RE 1 **Uppdelningen av zonerna är fysiskt utförd, alltså via egna nätkomponenter och egen kabeldragning, och vilar inte enbart på en logisk konfiguration inne i gemensamt använda enheter. Avsnitt 9.1 i denna lista, krävs från SL 2 och uppåt. Kravförstärkningar i denna standard är aldrig obligatoriska redan vid SL 1.**

Vad som styrker det: Inventarieförteckning över nätkomponenterna med uppgift om vilken switch eller router som betjänar vilken zon, foton eller skåpritning över de åtskilda fördelningarna, kabelmärkning. Små verksamheter styrker detta med två separata, tydligt märkta switchar i stället för en delad enhet och ett foto av elskåpet i anläggningsdokumentationen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.1 RE 2 **Automationsnätet går att driva oberoende av nät utanför automationen. Faller kontorets IT eller en extern anslutning bort fortsätter styrning och övervakning av anläggningen att löpa. Krävs från SL 3 och uppåt.**

Vad som styrker det: Beroendelista över de tjänster som används i automationsnätet såsom tidsserver, namnuppslagning, katalogtjänst eller licensserver, med uppgift om var var och en drivs, tillsammans med ett testprotokoll för ett frånkopplingsförsök där förbindelsen till kontorets IT drogs ur. En liten verksamhet noterar utfallet av ett sådant försök i underhållsjournalen: uppkopplingen urdragen, anläggningen fortsatte gå, endast rapporterna på kontoret saknades.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.1 RE 3 **Zoner med särskilt kritiska funktioner, till exempel säkerhetsfunktioner eller skyddsfunktioner, är avskilda från de övriga zonerna både logiskt och fysiskt. Krävs från SL 4 och uppåt.**

Vad som styrker det: Märkning av de kritiska zonerna i zonplanen med motivering av klassningen, bevis för egna nätkomponenter och egen kabeldragning för dessa zoner, konfiguration av conduits med bevis för att ingen gemensam väg finns.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.2 **Vid zongränserna styrs och övervakas trafiken och tillåts eller nekas enligt fastställda regler. Det finns ingen väg mellan två zoner som går förbi denna kontrollpunkt.**

Vad som styrker det: Exporterad regeluppsättning från brandväggen eller gränsenheten, loggar över nekade och tillåtna förbindelser, bevis för att inga sidovägar finns, till exempel genom en kontroll av ytterligare nätkort, modem eller mobilnätsroutrar i anläggningens datorer. En liten verksamhet styrker detta med regelexporten från sin enda brandvägg och en kort notering från en skyddsrond som bekräftar att ingen oplanerad router sitter i något elskåp.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.2 RE 1 **Regeluppsättningen vid zongränsen bygger på principen att allt nekas om det inte uttryckligen har tillåtits. Varje tillåtelseregel är motiverad var för sig och knuten till ett syfte. Krävs från SL 2 och uppåt.**

Vad som styrker det: Regeluppsättning med en synlig slutregel som förkastar återstoden, och en tillåtelselista med källa, mål, tjänst, syfte och ansvarig person för varje regel. Små verksamheter har denna lista som en tabell med fem kolumner vid sidan av brandväggsexporten och ser över den en gång per år och gallrar bort regler som ingen längre behöver.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.2 RE 2 **Automationsnätet går att medvetet koppla bort från alla externa förbindelser och driva vidare i ödrift. Åtgärden går att utlösa utan att anläggningen behöver stoppas. Krävs från SL 3 och uppåt.**

Vad som styrker det: Beskrivning av frånkopplingsrutinen med uppgift om vem som får utlösa den och hur, bevis för det tekniska utförandet såsom en nödregeluppsättning eller en märkt frånskiljare, samt det redovisande dokumentet från en övning där frånkopplingen verkligen genomfördes. En liten verksamhet gör övningen en gång per år i samband med underhåll och noterar datum, varaktighet och allt avvikande.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.2 RE 3 **Faller enheten vid zongränsen bort eller förlorar den sina regler nekar den trafiken i stället för att släppa igenom den. Ett bortfall får inte lämna kvar en öppen förbindelse. Krävs från SL 4 och uppåt.**

Vad som styrker det: Leverantörsförsäkran eller konfigurationsbevis för hur komponenten uppträder vid fel och vid omstart, testprotokoll för ett avsiktligt framkallat bortfall med det iakttagna resultatet, avstämning mot anläggningens riskbedömning, eftersom en gräns som nekar trafik i sig kan få följder beroende på processen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.3 **Allmänna kommunikationstjänster mellan personer såsom e-post, meddelandetjänster eller videosamtal går att förhindra på automationsenheter och inne i automationsnät. Spärrens omfattning är fastställd och motiverad.**

Vad som styrker det: Fastställd uppgift om vilka tjänster som inte är tillåtna i automationsnätet, samt det tekniska utförandet: blockerade portar och mål i regeluppsättningen, borttagna eller spärrade program på operatörsplatserna, bevis ur förteckningen över programvara i enheterna. En liten verksamhet hanterar detta med en programspärr på HMI-stationen och en regel om att utgående e-post och webbtrafik från maskinnätet nekas.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.3 RE 1 **Sådana kommunikationstjänster mellan personer är förhindrade i hela automationsnätet, inte bara delvis begränsade eller inskränkta till enskilda enheter. Krävs från SL 2 och uppåt.**

Vad som styrker det: Bevis för att spärren gäller varje enhet i zonen, till exempel genom en genomgång av installerad programvara på varje dator i zonen och ett anslutningsprov från en godtycklig dator i anläggningen. Små verksamheter styrker detta med en enhetslista där varje rad är avprickad med kontrolldatum, och en skärmbild av det misslyckade anslutningsförsöket.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 5.4 **Applikationsdata och applikationsfunktioner är uppdelade så att processer med olika skyddsbehov eller olika behörigheter inte når samma områden. Uppdelningen ligger i systemarkitekturen och överlämnas inte åt installationens tillfälligheter.**

Vad som styrker det: Översikt över applikationerna med uppgift om vilka data och tjänster de använder och vilka konton som står bakom dem, konfiguration av separata instanser, databaser, kataloger eller virtuella maskiner, och en behörighetslista per område. En liten verksamhet löser detta med separata användarkonton och separata datamappar för projektering och drift, samt en notering om vilken applikation som når vilken mapp.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

10 FR 6: Snabb reaktion på händelser 3

SR 6.1 **Loggposterna som samlas i systemet kan läsas och utvärderas av de personer och roller som är behöriga till detta utan att anläggningens löpande drift störs, och åtkomsten till dessa loggposter är i sig begränsad till behöriga användare.**

Vad som styrker det: En matris över roller och rättigheter som visar vem som får se loggdata, samt en skärmbild eller en export av en loggvy som faktiskt hämtats, försedd med tidsstämpel. Därtill en kort notering om den väg som användes för hämtningen, till exempel operatörsgränssnittet i styrenheten, en loggserver eller en filexport. Små verksamheter klarar sig med en översikt på en sida per anläggning: var loggen ligger, vem som har läsbehörighet, hur den hämtas. En provhämtning en gång per år, dokumenterad i underhållsjournalen, visar att vägen fungerar. Gäller från SL 1 och uppåt för alla säkerhetsnivåer.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 6.1 RE 1 **Loggposterna går att hämta via ett maskinellt gränssnitt så att analysverktyg kan bearbeta dem vidare utan manuell inmatning på nytt, och data lämnas i ett dokumenterat och vanligt förekommande format.**

Vad som styrker det: En beskrivning av det gränssnitt som används tillsammans med formatet, till exempel syslog, OPC UA Alarms and Conditions, en REST-fråga eller en CSV-export, samt en exempelpost och konfigurationen av det mottagande systemet. Bevis kan vara ett utdrag ur konfigurationen av SIEM eller logginsamlaren tillsammans med belägg för inkommande poster. Utan SIEM räcker en logginsamlare på en enkel server som hämtar loggarna över natten med ett skript och lagrar dem; skriptet självt och en kataloglista över de insamlade filerna är beviset. Som kravförstärkning krävs detta först från SL 3 och uppåt, inte från SL 1.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 6.2 **Säkerhetsrelevant aktivitet i systemet övervakas fortlöpande, övervakningen upptäcker angreppsförsök och missbruk och rapporterar dem skyndsamt till ett namngivet kontaktställe, och de verktyg, rapportvägar och ansvar som används för detta är fastställda.**

Vad som styrker det: En översikt över övervakningsverktygen per zon, till exempel en nätsensor, meddelanden från virusskyddet, brandväggslarm eller integritetskontroll, med uppgift om vem som tar emot larmet och inom vilken tid en reaktion förväntas. Larmkonfigurationer, en lista över larm som utlösts de senaste månaderna och noteringarna om hur de hanterats tjänar som bevis. Små verksamheter behöver inget bemannat kontrollrum dygnet runt: en gemensam brevlåda eller ärendeinkorg som samlar larmen från de befintliga systemen, samt en fast regel om att en namngiven person går igenom den varje arbetsdag, räcker och styrks genom brevlådans historik. Krävs från SL 2 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

11 FR 7: Resurstillgänglighet 13

SR 7.1 **Vid överbelastning eller avsiktliga överbelastningsangrepp håller systemet ett fastställt drifttillstånd, de väsentliga styrfunktionerna fortsätter att löpa, och bortfallet av en enskild tjänst drar inte anläggningen med sig.**

Vad som styrker det: Konfiguration av skyddsmekanismerna (hastighetsbegränsning, gränser för antalet förbindelser, styrning av broadcaststormar i switcharna), leverantörsförsäkran om beteendet under belastning, samt ett redovisande dokument från ett belastningsprov eller en verklig överbelastningshändelse med iakttagelse av styrfunktionen. Krävs från SL 1 och uppåt. En liten verksamhet täcker detta med skärmbilder av inställningarna i switch och brandvägg och en kort notering om vilken funktion som fortsatte gå under ett prov i den viktigaste cellen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.1 RE 1 **Den kommunikationslast som enskilda komponenter kan lägga in i nätet är begränsad uppåt, så att en felaktig eller komprometterad komponent inte kan översvämma nätsegmentet.**

Vad som styrker det: Gränser för bandbredd och multicast per port i nätkomponenterna, bevis för begränsningen vid varje anslutning, samt en mätning av den verkliga grundbelastningen per enhet. Krävs från SL 2 och uppåt, inte från SL 1. Utan hanterbara switchar går denna rad inte att styrka, och det är då den öppna punkten.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.1 RE 2 **En överbelastning inne i det betraktade systemet sprider sig inte till angränsande system eller nät; verkan utåt är tekniskt begränsad.**

Vad som styrker det: Regler för segmentering och filtrering vid gränserna, bevis för att utgående trafik är begränsad, samt ett testprotokoll som visar att en belastning som skapats i cellnätet inte försämrade kontorsnätet eller grannätet. Krävs från SL 3 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.2 **Användningen av processortid, arbetsminne, lagringsutrymme och nätbandbredd är begränsad så att en enskild process eller tjänst inte kan förbruka de resurser som styrningen behöver.**

Vad som styrker det: Konfiguration av resursgränserna (kvoter, processprioriteter, minnesgränser), utvärdering av beläggningsövervakningen över en representativ period, samt de gränsvärden vid vilka en varning går ut. Krävs från SL 1 och uppåt. Små verksamheter använder de inbyggda medlen i operativsystemet och en enkel övervakning med varning om diskutrymme och processorlast via e-post.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.3 **Det finns säkerhetskopior av systemkonfigurationerna, applikationsdata och programversionerna; de går att framställa utan att den löpande driften avbryts och är skyddade mot obehörig åtkomst och ändring.** Dokument

Vad som styrker det: Koncept för säkerhetskopiering med omfattning, frekvens och bevarandetid, säkerhetskopieringsloggar från de senaste körningarna, samt bevis för åtkomstskyddet av medierna (separat förvaring, kryptering, egna behörigheter). Krävs från SL 1 och uppåt. En liten verksamhet säkerhetskopierar projekt för PLC och versioner för HMI till ett krypterat medium som kopplas bort fysiskt efter kopieringen, och dokumenterar datum och version i en enkel lista.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.3 RE 1 **Säkerhetskopiornas användbarhet är verifierad; det är styrkt att ett fungerande tillstånd verkligen går att återställa från dem.**

Vad som styrker det: Redovisande dokument från ett återställningsförsök med datum, prövad kopieversion, målsystem och resultat, åtminstone för de kritiska komponenterna. Krävs från SL 2 och uppåt, inte från SL 1. Små verksamheter prövar ett program för PLC och en avbild av HMI på en reservenhet en gång per år som stickprov och dokumenterar resultatet i två meningar.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.3 RE 2 **Säkerhetskopieringen löper automatiskt enligt ett fastställt schema; en misslyckad körning upptäcks och rapporteras.**

Vad som styrker det: Schema för säkerhetskopieringsjobbet, körningsloggar utan luckor, samt bevis för felmeddelandet vid en körning som inte lyckades (larm, ärende, e-post). Krävs från SL 3 och uppåt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.4 **Efter en störning, ett bortfall eller ett angrepp går systemet att föra tillbaka till ett känt, säkert tillstånd; återställningen är övad och ansvaren är namngivna.** Dokument

Vad som styrker det: Återstartsplan för varje kritisk komponent med ordningsföljd, nödvändiga medier, kontakter och eftersträvad tid, tillsammans med det redovisande dokumentet från den senaste återställningsövningen. Krävs från SL 1 och uppåt. En liten verksamhet klarar sig med ett återstartskort på en sida per linje, förvarat i elskåpet och kontrollerat varje gång en reservdel byts.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.5 **Faller den ordinarie kraftförsörjningen bort går systemet till ett fastställt tillstånd: antingen upprätthålls försörjningen av en reservkälla eller sker en ordnad nedkörning utan att det säkra tillståndet går förlorat.**

Vad som styrker det: Bevis för dimensionering och underhåll av den avbrottsfria kraftförsörjningen eller reservkraftaggregatet, testprotokoll från det senaste batteriprovet eller belastningsprovet, samt en beskrivning av beteendet vid omkoppling och vid nätspänningens återkomst. Krävs från SL 1 och uppåt. Små verksamheter provar UPS under belastning en gång per år och dokumenterar provdatum, överbryggningstid och batteriets ålder.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.6 **Systemets inställningar för nät och säkerhet är fastlagda till ett godkänt börläge, avvikelser från detta börläge går att upptäcka, och det aktuella tillståndet går att hämta när som helst.** Dokument

Vad som styrker det: Godkänd börkonfiguration per enhetsklass (härdningsspecifikation), enheternas aktuella konfigurationstillstånd, samt resultatet av en jämförelse mellan börläge och verkligt läge med en lista över avvikelser och orsaken till var och en. Krävs från SL 1 och uppåt. En liten verksamhet lagrar konfigurationsexporterna i versionshantering och jämför dem före och efter varje ändring.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR 7.6 RE 1 **Det aktuella tillståndet för säkerhetsinställningarna går att lämna ut i maskinläsbar form så att det går att kontrollera automatiskt mot börläget.**

Vad som styrker det: Exempelutdata i ett maskinläsbart format (konfigurationsexport, strukturerad fil, gränssnittsfråga) och det skript eller verktyg som utför jämförelsen mot börläget, tillsammans med resultatrapporten från en körning. Krävs från SL 3 och uppåt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.7 **Systemet är begränsat till de funktioner som driften behöver; tjänster, portar, protokoll och gränssnitt som inte behövs är avstängda eller borttagna.**

Vad som styrker det: Lista över aktiva tjänster och öppna portar per komponent med en motivering av behovet, bevis för att de övriga är avstängda (konfiguration, resultat av en portskanning), samt en regel för USB-gränssnitt och underhållsgränssnitt. Krävs från SL 1 och uppåt. Små verksamheter kör en enkel portskanning per segment och motiverar varje öppen post på en rad.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR 7.8 **En aktuell förteckning över alla systemkomponenter med tillverkare, typ, firmware eller programvaruversion och nätadress finns tillgänglig och hålls uppdaterad vid ändringar.** Dokument

Vad som styrker det: Komponentförteckning med revideringsdatum och ansvarig, bevis för underhållet av den via ändringshistoriken, samt en jämförelse mot en nätsökning för att hitta enheter som inte är upptagna. Krävs från SL 2 och uppåt, inte från SL 1. En liten verksamhet har förteckningen som en tabell och uppdaterar den som fast regel varje gång en enhet byts och varje gång firmware uppdateras.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

Kraven är formulerade självständigt och ersätter inte standardens text. Endast originalstandarden från respektive utgivare är bindande. Denna lista är ett arbetsverktyg, inget bevis på överensstämmelse och ingen certifiering. Leanshift är inte certifierat enligt någon av dessa standarder, är inget certifieringsorgan och har ingen koppling till ISO, IEC, DIN, IATF, IAQG eller SAE. Vid tveksamhet gäller den tyska versionen av denna lista.