IEC 62443-4-1:2018 Sikker udviklingslivscyklus for produkter inden for industriel automation

Sikker udviklingslivscyklus, otte praksisområder

47 krav. Det er muligt at blive certificeret efter denne standard hos et akkrediteret certificeringsorgan. Udgave 07/2026.

IEC 62443-4-1 kan der certificeres efter, men genstanden er usædvanlig: det, der certificeres, er udviklingsprocessen hos en navngiven udviklingsorganisation, altså en konkret dokumenteret udgave af den sikre livscyklus. Hverken et produkt eller en person bliver certificeret. Vejene er ISASecure SDLA og IECEE CB Scheme. Efter den nuværende retstilstand medfører et sådant certifikat ingen formodning om overensstemmelse med EU Cyber Resilience Act. Forveksl den ikke med IEC 62443-4-2, som stiller krav til selve komponenten. Denne liste er et arbejdsredskab til selvevaluering, ikke et bevis.

Virksomhed	Dato	Udfyldt af

5 Praksisområde 1: Sikkerhedsstyring (SM) 13

SM-1 **Der findes en fastlagt livscyklus for produktudvikling, som bærer sikkerheden gennem hver fase, fra den første idé til udfasning af produktet, og det er denne livscyklus, der faktisk følges i det daglige arbejde.** Dokument

Det taler for: Procesbeskrivelse eller arbejdsinstruktion, der angiver faserne, leverancerne per fase og overleveringspunkterne, sammen med dokumentation fra et igangværende projekt, der viser, at faserne reelt blev gennemarbejdet. En lille virksomhed klarer sig med en side per fase plus en tjekliste i sagssystemet; det afgørende er, at den dokumenterede proces og det daglige arbejde stemmer overens.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-2 **Hver opgave i den sikre udviklingslivscyklus har en udpeget ansvarlig, og denne fordeling er kendt af de involverede.** Dokument

Det taler for: Matrix over roller og ansvar, der kobler hvert procestrin til en navngiven rolle, suppleret med den aktuelle bemanding af rollerne. Med kun en håndfuld personer er en tabel med rolle, opgave og person tilstrækkelig; det vigtige er stedfortræderordningen ved ferie og sygdom.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-3 **Det er sporbart fastlagt, hvilke produkter, varianter, frigivelser og komponenter der er omfattet af den sikre udviklingslivscyklus, og hvilke der ikke er.** Dokument

Det taler for: Liste over de omfattede produkter og versionstilstande med en begrundelse for, hvad der regnes med, og hvad der holdes udenfor, vedligeholdt ved hver ny frigivelse. I praksis fungerer en kolonne i produktoversigten godt, med ja eller nej per række plus en sætning som begrundelse.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-4 **De personer, der påtager sig sikkerhedsopgaver, har den faglige kompetence, opgaverne kræver, og kompetencen opbygges og holdes aktuel på en bevidst måde.**

Det taler for: Kompetenceprofil per sikkerhedsrolle, registreringer over kvalifikationer, uddannelsesplan og registreringer over deltagelse, suppleret med en oversigt over hullerne. Små virksomheder dokumenterer dette med kursusbeviser, deltagelse i konferencer eller webinarer og en kort årlig gennemgang af, hvem der lukker hvilket hul hvornår, og køber ekstern ekspertise ind, hvor det er nødvendigt.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-5 **Anvendelsesområdet for den sikre udviklingslivscyklus er afgrænset og angiver de lokationer, organisatoriske enheder, leverandørbidrag og udviklingsmiljøer, der indgår, sammen med grænserne for anvendelsesområdet.** Dokument

Det taler for: Beskrivelse af anvendelsesområdet, der dækker lokationer, teams, outsourcede dele og systemer, plus en skitse over de eksterne grænseflader. Den, der udvikler på en enkelt lokation, dokumenterer dette i nogle få sætninger og nævner udtrykkeligt, hvad der ligger udenfor, for eksempel eksternt udviklede moduler eller hosting hos tredjepart.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-6 **For hvert element, der leveres til brugerne, altså software, firmware, konfigurationer og medfølgende filer, er en integritetskontrol mulig, så modtagerne kan opdage en ubemærket ændring.**

Det taler for: Signaturer eller offentliggjorte kontrolsummer per leverancepakke, en beskrivelse af metoden og et eksempel fra en reel frigivelse, sammen med en vejledning til kunden i, hvordan kontrollen udføres. For små teams er en signeret kontrolsumfil ved siden af downloadet plus et afsnit i frigivelsesnoterne nok.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-7 **Udviklings-, bygge- og testmiljøerne er beskyttet mod uautoriseret adgang og mod manipulation af kildekode, byggeværktøjer og artefakter.**

Det taler for: Koncept for adgangsstyring til repositoriet, byggeserveren og testsystemerne, adgangslister med datoen for den seneste gennemgang, registreringer af sikkerhedsrelevante ændringer og dokumentation for, at adgang til drift og udvikling er adskilt. Uden en intern IT-afdeling rækker tofaktorlogin, en beskyttet hovedgren med obligatorisk gennemgang og en gennemgang hvert halve år af, hvem der stadig har adgang.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-8 **Private nøgler, der bruges til at signere leverancer, er beskyttet mod videregivelse og misbrug, og brugen af dem er begrænset til autoriserede personer og systemer.**

Det taler for: Beskrivelse af opbevaring, adgang, fornyelse og tilbagekaldelse af nøgler, dokumentation for beskyttet opbevaring, for eksempel et hardwaretoken eller en nøglestyringstjeneste, plus registreringer af signeringerne. En lille virksomhed opbevarer signeringsnøglen på et hardwaretoken, dokumenterer de to personer med adgang og har en procedure klar til tabssituationen.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-9 **For indkøbte eller overtagne komponenter, herunder open source-software, er sikkerhedsforventningerne til leverandøren fastlagt, og de anvendes ved udvælgelsen.** Dokument

Det taler for: Sikkerhedskrav i leverandørspecifikationer eller kontrakter, udvælgelseskriterier for tredjepartskomponenter, en fortegnelse over alle tredjepartskomponenter med version og kilde, plus vurderingen af, om leverandøren opfylder forventningerne. Uden en indkøbsafdeling er en vedligeholdt komponentliste tilstrækkelig, når den har en kolonne, der viser, om leverandørens sikkerhedsopdateringer og indberetningskanaler er kontrolleret.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-10 **Komponenter, som en tredjepart udvikler på bestilling, er underlagt de samme sikkerhedskrav som intern udvikling, og overholdelsen verificeres.**

Det taler for: Indkøbsordre eller kontraktdokumenter, der angiver de krævede sikkerhedsforpligtelser, dokumentation fra leverandøren om de anvendte arbejdsmåder, registreringer fra godkendelsen og resultater af virksomhedens egne kontroller af det leverede. Uden budget til audit rækker et kontraktligt tilsagn, fremsendelse af leverandørens testresultater og en enkelt egen stikprøve inden godkendelsen.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-11 **Sikkerhedsrelevante fund fra alle kilder, altså test, gennemgange, brugerindberetninger og meddelelser fra tredjepart, registreres, vurderes for deres konsekvens, tildeles en ansvarlig og en frist og følges til afslutning.** Dokument

Det taler for: Fejl- eller sagssystem med en særlig markering af sikkerhedsemner, og per post vurderingen af konsekvensen, den ansvarlige, fristen og afslutningsnotatet, plus en oversigt over åbne punkter. Et lille team bruger en mærkat i det eksisterende sagssystem og et fast punkt på dagsordenen til ugemødet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-12 **Inden et produkt frigives, verificeres og dokumenteres det, at de planlagte trin i den sikre udviklingslivscyklus faktisk blev gennemført, og at de tilhørende registreringer blev udarbejdet.** Dokument

Det taler for: Frigivelsesgennemgang per frigivelse holdt op mod procestrinnene, henvisninger til de enkelte registreringer og en dokumenteret frigivelsesbeslutning med dato og underskrift. I praksis fungerer en frigivelsestjekliste godt, som ikke tillader forsendelse uden fuldstændige flueben; åbne punkter begrundes og får en dato.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SM-13 **Den sikre udviklingslivscyklus bliver selv regelmæssigt udfordret og forbedret ud fra erfaringer fra hændelser, testresultater, kundetilbagemeldinger og trusselsbilledet.**

Det taler for: Registreringer fra gennemgangen af processen, for eksempel ledelsens evaluering eller et tilbageblik, med de procesændringer den udløste, deres gennemførelsesstatus og en henvisning til grundårsagen. Den, der bruger standardens modenhedsniveauer, registrerer den aktuelle tilstand og målet per praksisområde; modenhedsniveau 4 kræver netop denne dokumentation for løbende forbedring. For en lille virksomhed er et møde om året med referat og tre konkrete forbedringer nok.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

6 Praksisområde 2: Specifikation af sikkerhedskrav (SR) 5

SR-1 **Den tilsigtede produktkontekst er beskrevet: forventet driftsmiljø, de sikkerhedsforanstaltninger, der forudsættes leveret af dette miljø, tilsigtede brugergrupper og roller, antagne tillidsgrænser og de anvendelser, som produktet udtrykkeligt ikke er beregnet til.** Dokument

Det taler for: En beskrivelse af produktets sikkerhedskontekst, enten som et selvstændigt dokument eller som et fast afsnit i produktspecifikationen, der dækker netværksmiljøet, de antagne eksterne beskyttelser, for eksempel en firewall eller fysisk adgangsstyring, en liste over roller og en udtrykkelig liste over anvendelser uden for anvendelsesområdet. En lille virksomhed holder dette på to sider, tilføjer en enkel skitse af anlægsmiljøet og lader produktejeren datere og godkende det.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR-2 **Der findes en trusselsmodel for produktet, som kortlægger datastrømme, grænseflader, tillidsgrænser og angrebsveje, navngiver de trusler, der følger heraf, og deres mulige konsekvens, og tildeler modforanstaltninger. Den gennemgås og opdateres ved relevante ændringer og mindst en gang per produktfrigivelse, og åbne punkter følges, indtil de er lukket.** Dokument

Det taler for: Trusselsmodel med et dataflowdiagram, en trusselsliste per grænseflade, tildelte modforanstaltninger og status på åbne punkter, plus en revisionshistorik med dato og forfatter. En lille virksomhed kan arbejde ud fra en tabel per grænseflade med kolonner for, hvad der kan gå galt der, hvor slemt det ville være, hvad der gøres ved det, og hvem der gennemgår det.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR-3 **Sikkerhedskravene til produktet er fastlagt og dokumenteret. De dækker resultaterne af trusselsmodellen, den beskrevne sikkerhedskontekst for produktet, gældende juridiske og kontraktlige forpligtelser og det tilstræbte sikkerhedsniveau, og de omfatter de sikkerhedsfunktioner, produktet selv skal levere.** Dokument

Det taler for: Kravliste eller værktøj til kravstyring med en entydig identifikator per krav, kilden til hver post, for eksempel en trussel, en kundekontrakt eller en juridisk forpligtelse, og det tilstræbte sikkerhedsniveau. En lille virksomhed kører dette som en enkelt tabel med en fast ID-kolonne, som verifikation og test senere kobler sig på.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR-4 **Hvert enkelt sikkerhedskrav er formuleret, så det er entydigt, uden modsigelser, testbart og sporbart til en bestemt produktfunktion eller grænseflade, og det bærer de oplysninger, der senere skal bruges til at verificere det uden yderligere afklaring.**

Det taler for: En stikprøve fra kravlisten, der for hvert krav viser et målbart acceptkriterium og den berørte funktion eller grænseflade, sammen med koblingen mellem krav og testtilfælde. En lille virksomhed kontrollerer dette med en fast formuleringsskabelon og kontrolspørgsmålet, om der kan skrives et testtilfælde ud fra kravet uden at spørge tilbage.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR-5 **Sikkerhedskravene gennemgås, inden de bruges i design og implementering, med inddragelse af de berørte parter, for eksempel udvikling, test, produktejerskab og, hvor det er nyttigt, salg eller kunden. Gennemgangen dækker fuldstændighed i forhold til trusselsmodellen og produktets sikkerhedskontekst, korrekthed og testbarhed. Fund registreres og følges til afslutning.**

Det taler for: Registrering fra gennemgangen med dato, deltagere og deres roller, den gennemgåede version af kravene, en liste over fund med en ansvarlig og afslutningsstatus samt et godkendelsesnotat. En lille virksomhed håndterer dette som en gennemgang mellem to personer fra udvikling og test, med en kort registrering og en godkendelseslinje i kravlisten.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

7 Praksisområde 3: Sikkerhed indbygget i designet (SD) 4

SD-1 **Hvert produkt har en designbeskrivelse, der fastholder de sikkerhedsrelevante dele af arkitekturen: hvilke komponenter der findes, hvordan de kommunikerer indbyrdes, hvor tillidsgrænserne går, hvilke eksterne grænseflader der er eksponeret, og med hvilke mekanismer de tidligere fastlagte sikkerhedskrav realiseres i designet.** Dokument

Det taler for: Arkitekturdokument eller designspecifikation med et diagram, der viser komponenter, datastrømme og tillidsgrænser, plus en koblingstabel fra hvert sikkerhedskrav til det designelement, der realiserer det. En lille leverandør klarer sig med et vedligeholdt diagram plus to eller tre siders forklaring; det afgørende er, at det er versionsstyret i repositoriet og opdateres, hver gang arkitekturen ændres.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SD-2 **Designet analyseres systematisk for trusler. Analysen navngiver angriberes mål, de berørte tillidsgrænser og grænseflader, de trusler, der følger heraf, sammen med deres vurdering, og de modforanstaltninger, der er truffet i designet. Den gentages, hver gang arkitektur eller miljø ændres væsentligt, og identificerede trusler følges, indtil der er truffet en beslutning om hver enkelt.** Dokument

Det taler for: Trusselsmodel per produkt eller per større frigivelse, for eksempel en tabel med kolonner for trussel, berørt grænseflade, vurdering, modforanstaltning og status, sammen med referatet fra modelleringsmødet med deltagere og dato. Et lille team modellerer pragmatisk i en workshop på to til tre timer langs arkitekturdiagrammet og noterer åbne punkter som sager, så dokumentationen for opfølgningen opstår uden ekstra arbejde.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SD-3 **Designet følger påviseligt anerkendte principper for sikkert design, blandt andet færrest mulige rettigheder, mindst mulig angrebsflade, forsvar i dybden, sikre standardindstillinger, sikker tilstand ved fejl og sikkerhedsmekanismer, der er så enkle og verificerbare som muligt. Anvendelsen af disse principper er synlig i designet og begrundet.**

Det taler for: Et afsnit i designbeskrivelsen eller en intern designretningslinje, der navngiver principperne, plus konkret dokumentation per princip i produktet, for eksempel rettighedsmatrixen for tjenesterne, listen over åbne porte med begrundelse, standardindstillingerne ved levering eller den dokumenterede fejlhåndtering. En lille leverandør bruger en kort tjekliste over disse principper som fast punkt i designgennemgangen og arkiverer det udfyldte skema sammen med designet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SD-4 **Designet gennemgås af kvalificerede fagfæller, inden implementeringen begynder. Gennemgangen dækker fuldstændighed i forhold til sikkerhedskravene, korrektheden og virkningen af sikkerhedsmekanismerne og resultaterne af trusselsanalysen. Personer med tilstrækkelig sikkerhedskompetence deltager, fund registreres og følges til afslutning.** Dokument

Det taler for: Registrering fra gennemgangen med dato, den gennemgåede genstand med angivelse af version, deltagere og deres roller, liste over fund med status og frigivelsesbeslutningen. Et lille team hænger gennemgangen på pull requesten til designdokumenterne og efterlader fundene som kommentarer med et afslutningsnotat, hvilket dokumenterer opfølgningen uden yderligere værktøjer. Mangler sikkerhedskompetencen internt, er en ekstern fagperson hyret på timebasis til de kritiske design den pragmatiske vej.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

8 Praksisområde 4: Sikker implementering (SI) 2

SI-1 **Der findes en fastlagt proces for at verificere den faktiske implementering op mod det sikre design: gennemgangen bekræfter, at de beskyttelsesforanstaltninger, designet forudser, reelt findes og er virksomme i koden, at forsvar i dybden er bevaret, og at der ikke er indført nye sårbarheder under implementeringen. Gennemgangen udføres af passende kvalificeret personale, og fundne afvigelser registreres og følges til afslutning.**

Det taler for: En skriftlig procedure for gennemgang af implementeringen sammen med registreringer per komponent eller frigivelse: det gennemgåede modul, henvisningen til designdokumentet, datoen, den ansvarlige for gennemgangen, fundene og deres afklaringsstatus. Egnet dokumentation er blandt andet gennemgange i pull requests med en obligatorisk sikkerhedstjekliste, resultater af statisk kodeanalyse med en dokumenteret vurdering af hvert træf og referater fra gennemgangsmøder. Et lille team dækker dette med fireøjneprincippet, en gennemgangsskabelon i repositoriet, hvor hver designforanstaltning afkrydses enkeltvis, og en sag per åbent fund. Det afgørende er, at den, der har skrevet koden, aldrig er den, der gennemgår netop den kode.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SI-2 **Bindende regler for sikker kodning gælder for alt sikkerhedsrelevant udviklingsarbejde og dækker som minimum undgåelse af kendte usikre konstruktioner og funktioner, håndteringen af input og fejl, styringen af hukommelse og ressourcer og brugen af afprøvet sikkerhedskode frem for selvskrevne implementeringer. Reglerne gælder per anvendt programmeringssprog, er kendt af alle udviklere og opdateres, når der er behov, for eksempel når nye angrebsmønstre eller nye værktøjer dukker op.** Dokument

Det taler for: En godkendt standard for sikker kodning med versionsstatus, anvendelsesområde per sprog og godkendelsesdato, suppleret med dokumentation for, at den virker i det daglige arbejde: konfigurationen af lintere og analyseværktøjer i repositoriet, en byggeregel, der synliggør overtrædelser, og deltagerlisten fra orienteringen. Små virksomheder skriver ikke en standard fra bunden; de gør et etableret offentligt regelsæt bindende, tilføjer en kort liste over egne supplerende regler og forankrer kontrollen i pipelinen, så overholdelsen påvises automatisk.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9 Praksisområde 5: Test til verifikation og validering af sikkerheden (SVV) 5

SVV-1 **Hvert sikkerhedsrelevant produktkrav har mindst et testtilfælde tilknyttet, som viser, at beskyttelsesfunktionen virker som tilsigtet i normal drift, at den opfører sig som specificeret ved ugyldigt input eller misbrug, og at de standardindstillinger, produktet leveres med, svarer til den sikre tilstand. Udførelse og resultat registreres for hver testet softwareversion.** Dokument

Det taler for: En sporbarhedsmatrix, der forbinder krav med testtilfælde og resultat, plus testregistreringer med dato, den testede version eller det testede build og navnet på den, der udførte testen. En lille leverandør tilføjer blot en kolonne med testtilfældets ID i kravlisten og arkiverer logudskriften fra den automatiske testkørsel i byggepipelinen som en fil knyttet til den pågældende version.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SVV-2 **De modforanstaltninger, der stammer fra trusselsmodellen, testes målrettet for at bekræfte, at de faktisk lukker den antagne angrebsvej. Der testes mod de identificerede trusler, ikke kun mod forventet, korrekt brug, og åbne punkter føres ind i fejlhåndteringsprocessen.**

Det taler for: Testtilfælde, der henviser direkte til posterne i trusselsmodellen, for eksempel et misbrugsscenarie per trussels-ID med den forventede forsvarsadfærd, sammen med registreringerne fra kørslerne. Uden tungt maskineri rækker det at tilføje en kolonne i trusselsmodellen med henvisning til testtilfældet og datoen for den seneste vellykkede kontrol.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SVV-3 **Produktet undersøges systematisk for sårbarheder inden frigivelsen. Omfanget dækker som minimum: undersøgelse af de eksternt tilgængelige grænseflader og tjenester, test med fejlformet og tilfældigt muteret input, gennemgang af de anvendte tredjepartskomponenter op mod kendte indberettede sårbarheder og en kontrol for kendte svaghedsklasser i leverandørens egen kode. Fund registreres sammen med deres vurdering.** Dokument

Det taler for: Rapporter fra de anvendte værktøjer med værktøjets navn, version og datastatus for sårbarhedsdatabasen, registreringer fra fuzzing, en liste over tredjepartskomponenter med datoen for den seneste sammenligning og listen over fund med vurdering og beslutning. En lille leverandør kombinerer gratis standardværktøjer, en afhængighedsscanning og en scanning af porte og tjenester mod det installerede produkt og lægger resultaterne per frigivelse i en enkelt mappe.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SVV-4 **Frigivelseskandidaten udsættes for et angrebsforsøg under realistiske forhold, som aktivt forsøger at omgå beskyttelsesmekanismerne i stedet for blot at afprøve dem. Omfang, rammebetingelser og grænser for testen aftales på forhånd, og de fundne svagheder håndteres og følges som fejl.**

Det taler for: Aftalen eller testordren med angivelse af omfang og testmiljø, en rapport om fremgangsmåden, de udnyttede svagheder og deres vurdering, plus posterne i fejl- eller sagssystemet med dokumentation for udbedring eller for en begrundet risikoaccept. Små leverandører køber typisk denne test eksternt inden for et afgrænset tidsbudget eller lader den udføre af en person, der ikke har udviklet produktet.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SVV-5 **Testpersonalets uafhængighed er fastlagt og passer til det tilstræbte modenhedsniveau. Den, der har udviklet en komponent, frigiver den ikke alene på grundlag af sin egen test, og efterhånden som modenhedsniveauet stiger, ligger testen hos en organisatorisk adskilt enhed eller en ekstern part. Den faktiske fordeling er sporbar for hver test.**

Det taler for: En rollebeskrivelse i udviklingsprocessen, der viser adskillelsen af udvikling og test, plus for hver testkørsel eller testrapport det registrerede navn og den registrerede rolle på den, der udførte testen. En virksomhed med to personer håndterer dette med gensidig gennemgang og et dokumenteret notat om fireøjneprincippet og henter en ekstern person ind til den dybdegående sikkerhedstest.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

10 Praksisområde 6: Håndtering af sikkerhedsfejl (DM) 6

DM-1 **Der findes en fastlagt kanal, hvor indberetninger om sikkerhedssvagheder i produktet modtages og registreres fra alle retninger: fra udviklingsteamet selv, fra test og gennemgange, fra kunder og integratorer, fra eksterne indberettere og fra sikkerhedsmeddelelser om anvendte tredjepartskomponenter og open source-komponenter. Indberetningskanalen kan findes af eksterne parter, og hver indberetning registreres med modtagelsesdato og kilde.** Dokument

Det taler for: En beskrivelse af indberetningskanalen, det offentligt tilgængelige kontaktpunkt (en sikkerhedsside, en security.txt-fil eller en postkasse som security@) og modtageregistret med dato, kilde og en kort beskrivelse for hver indberetning. En lille virksomhed kan klare sig med en fælles postkasse og et enkelt regneark eller en mærkat i sagssystemet, så længe hver indberetning ender der, også dem, der rejses i den interne udviklerchat.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

DM-2 **Hver indkommen indberetning visiteres og undersøges for at afgøre, om den er sikkerhedsrelevant, og hvilke produkter, versioner og komponenter den berører. Indberetninger, der viser sig ikke at være sikkerhedsrelevante eller ikke at gælde, lukkes også med en angivet begrundelse i stedet for at blive kasseret i stilhed.**

Det taler for: Et visiteringsnotat for hver indberetning med resultatet (sikkerhedsrelevant ja eller nej), de berørte versioner og begrundelsen for afvisning, hvor det er relevant, synligt i sagen eller i modtagelisten. Teams med få indberetninger kan gennemføre visiteringen i et kort tilbagevendende møde og notere resultatet i to sætninger per post.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

DM-3 **Bekræftede sikkerhedsfejl vurderes efter en ensartet metode: grundårsag, berørte versioner og konfigurationer, mulig konsekvens for drift og sikkerhed, udnyttelighed og alvorlighed efter en fastlagt skala. Resultatet af vurderingen registreres og er sporbart.** Dokument

Det taler for: En vurderingsregistrering eller et sæt sagsfelter for hver fejl, der dækker grundårsag, alvorlighed og den anvendte skala (for eksempel et udbredt system til vurdering af alvorlighed med en dokumenteret vektor), sammen med listen over berørte versioner. Små teams kan nøjes med en fast feltskabelon i sagssystemet plus en halv side, der beskriver skalaen og de tærskler, der udløser omgående handling.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

DM-4 **For hver vurderet sikkerhedsfejl træffes der en beslutning om håndteringen: udbedring, kompenserende foranstaltning eller en begrundet accept af risikoen. Beslutningen følger af alvorligheden, den tildeles en ansvarlig person og en frist, og fejlen følges til afslutning.** Dokument

Det taler for: En handlingsliste eller sagsstatus med ansvarlig, måldato, foranstaltningstype og et afslutningsnotat, koblet til den kodebaseline eller den frigivelse, hvor rettelsen får virkning. Accepterede restrisici kræver en kort skriftlig begrundelse, som produktejerskabet godkender. En lille virksomhed kan holde dette i en sagstavle med frister, uden yderligere værktøjer.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

DM-5 **Berørte brugere, integratorer og andre interessenter informeres om sikkerhedsfejl, så snart vurderingen tilsiger det, med angivelse af de berørte versioner, konsekvensen og den tilgængelige rettelse eller kompenserende foranstaltning. Frister og modtagerkredsen for en sådan offentliggørelse er fastlagt på forhånd, og det samme gælder fremgangsmåden ved indberetninger fra tredjepart, der selv har en frist for offentliggørelse.**

Det taler for: Offentliggjorte sikkerhedsmeddelelser med dato og versionshenvisning, distributionslisten eller abonnementskanalen og den skriftlige regel om frister og koordineret offentliggørelse. Leverandører med få kunder kan bruge en enkelt udsendelse til en vedligeholdt kundeliste plus en dateret side med sikkerhedsmeddelelser, hvis ændringer er versionsstyrede.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

DM-6 **Håndteringen af sikkerhedsfejl gennemgås med faste intervaller. Gennemgangen ser på åbne og overskredne sager, tiden fra indberetning til udbedring, tilbagevendende grundårsager og virkningen af de trufne foranstaltninger. Forbedringer af processen, der følger af gennemgangen, gennemføres, og gennemførelsen følges.** Dokument

Det taler for: Referat fra den tilbagevendende gennemgang med dato, deltagere, tal for åbne og overskredne sager og en liste over aftalte forbedringer med ansvarlig og frist. En lille virksomhed kan hænge dette punkt på et eksisterende kvartalsmøde og holde tallene og beslutningerne på en enkelt side.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

11 Praksisområde 7: Håndtering af sikkerhedsopdateringer (SUM) 5

SUM-1 **Hver sikkerhedsopdatering til produktet verificeres mod de understøttede produktversioner og driftsmiljøer, inden den frigives til kunderne, og der findes en registrering, der viser, at opdateringen lukker sårbarheden uden at forstyrre den tilsigtede produktfunktion.** Dokument

Det taler for: Testregistrering per rettelse med den testede produktversion, platformen, testtilfældene (virkning mod sårbarheden plus regression af kernefunktionerne) og frigivelsesgodkendelsen. En lille leverandør kan klare sig med en kort godkendelsespost for rettelsen i sagen: sagsnummer, verificeret af, verificeret den, resultat, med loggen fra den automatiske testkørsel vedhæftet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SUM-2 **For alle produktkomponenter, der ikke er udviklet internt (tredjepartsbiblioteker, operativsystem, runtimemiljøer), er det fastlagt og dokumenteret, hvordan deres sikkerhedsopdateringer vurderes og enten optages i produktet eller afvises med en dokumenteret begrundelse.** Dokument

Det taler for: Komponentfortegnelse over tredjepartsdelene med version og kilde, plus en vurderingspost per indberettet sårbarhed i tredjepart med beslutningen (optages, ikke berørt, dækket af en kompenserende foranstaltning) og begrundelsen. Små teams kører en automatisk afhængighedsscanning i byggeprocessen og holder beslutningerne som kommentarer til scanningsresultatet eller i en slank undtagelsesliste.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SUM-3 **For hver sikkerhedsopdatering, der udsendes, får brugerne forståelig ledsagende information: hvilke produktversioner der er berørt, hvilken sårbarhed der er rettet, hvor alvorlig den er, om der skal tages hensyn til bivirkninger eller kompenserende foranstaltninger, og hvordan opdateringen installeres.** Dokument

Det taler for: Offentliggjorte sikkerhedsmeddelelser eller frigivelsesnoter med sårbarhedens identifikator, de berørte versioner, vurderingen af alvorligheden, installationstrinnene og vejledning i at rulle tilbage til den tidligere tilstand. Små leverandører holder en enkelt offentlig side med en kronologisk liste over sikkerhedsmeddelelser og henviser til den inde fra produktet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SUM-4 **Der findes en fastlagt og manipulationsbeskyttet vej, ad hvilken brugerne henter sikkerhedsopdateringer, og en opdaterings ægthed og integritet kan verificeres hos brugeren, inden den installeres.**

Det taler for: Beskrivelse af leveringskanalen (downloadområde, opdateringsserver, fysiske medier) sammen med dens beskyttelsesforanstaltninger, plus den digitale signatur eller kontrolsum per pakke og en vejledning, der fortæller brugeren, hvordan den verificeres. Små leverandører opnår dette ved at signere på byggeserveren, offentliggøre kontrolsummen ved siden af downloadet og angive et entydigt sted, hvor den offentlige nøgle ligger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SUM-5 **Der findes fastlagte tidsmål for, hvornår sikkerhedsopdateringer stilles til rådighed, gradueret efter sårbarhedens alvorlighed; de faktisk opnåede tider følges, og et tidsmål, der overskrides, begrundes og understøttes af en midlertidig foranstaltning for brugerne.** Dokument

Det taler for: Intern specifikation med et tidsvindue per alvorlighedskategori (for eksempel kritisk <= 30 dage, høj <= 90 dage) og en opgørelse per sårbarhed: indberetningsdato, dato for frigivelse af rettelsen, forløbne dage, årsag til afvigelsen. Små leverandører holder dette som to datofelter i sårbarhedssagen og gennemgår listen en gang i kvartalet i stedet for at opbygge et særskilt målesystem.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

12 Praksisområde 8: Sikkerhedsvejledninger til idriftsættelse og drift af produktet (SG) 7

SG-1 **Hvert produkt leveres med en beskrivelse af sin strategi for forsvar i dybden: den navngiver de beskyttelseslag, der er indbygget i selve produktet, kobler dem til de trusler, de imødegår, og viser, hvilken beskyttende virkning der først opstår i samspillet mellem flere lag.** Dokument

Det taler for: Et afsnit i den leverede produktdokumentation eller et selvstændigt sikkerhedskoncept, der for hvert beskyttelseslag angiver mekanismen, den dækkede trussel og grænserne for virkningen. En lille virksomhed holder dette som en tabel på to sider: kolonne beskyttelseslag, kolonne trussel hentet fra virksomhedens egen trusselsmodel, kolonne restrisiko. En krydshenvisning til trusselsmodellen fra SR-2 er tilstrækkelig, indholdet behøver ikke at blive vedligeholdt to gange.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SG-2 **Dokumentationen navngiver de sikkerhedsforanstaltninger, produktet ikke selv leverer, men forventer af driftsmiljøet, for eksempel netværkssegmentering, foranstillede firewalls, fysisk adgangsstyring eller en ekstern tidstjeneste, og gør det klart, at det lovede sikkerhedsniveau ikke nås uden disse foranstaltninger.** Dokument

Det taler for: Et kapitel om forudsætninger for idriftsættelse i manualen eller en referencearkitekturtegning med zoner og forbindelser, hvor de foranstaltninger, anlægsejeren skal levere, er udtrykkeligt markeret. En liste over antagelser om miljøet har vist sig nyttig i praksis, afledt direkte af produktets sikkerhedskontekst og gennemlæst igen ved hver produktversion.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SG-3 **Der findes en vejledning til sikker basiskonfiguration, som lister alle sikkerhedsrelevante indstillinger, tjenester, porte og grænseflader, angiver den anbefalede tilstand ved levering og beskriver konsekvensen af at afvige fra anbefalingen.** Dokument

Det taler for: Hærdningsvejledning med en tabel over indstillinger: parameter, anbefalet værdi, virkning, bivirkning ved afvigelse. Plus listen over de tjenester og porte, der er aktive i standardkonfigurationen, med en begrundelse for, hvorfor de forbliver slået til. Et lille team holder denne tabel lige ved siden af konfigurationsfilen i repositoriet og eksporterer den til leverancedokumentationen, så den følger produktet.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SG-4 **Til den løbende drift findes en vejledning, der beskriver, hvordan produktet drives sikkert, overvåges og holdes i sin sikre tilstand, herunder sikkerhedskopiering og genetablering, logning og håndteringen af sikkerhedsrelevante hændelsesmeddelelser.** Dokument

Det taler for: Driftsvejledning med afsnit om logning, sikkerhedskopier, genstart og hændelsesmeddelelser. Som yderligere dokumentation en liste over de sikkerhedsrelevante meddelelser, produktet udsender, hver med en kort anbefalet handling, så anlægsejeren ikke behøver at tolke dem alene.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SG-5 **Dokumentationen forklarer, hvordan produktets brugerkonti, roller og rettigheder oprettes og vedligeholdes, især adskillelse af roller, ændring af standardadgangsoplysninger og fjernelse af konti, der ikke længere er nødvendige.** Dokument

Det taler for: Et kapitel om kontostyring med en oversigt over roller og de rettigheder, hver rolle har, plus en udtrykkelig bemærkning om standardadgangsoplysninger og om at ændre dem ved idriftsættelsen. En kort tjekliste til idriftsættelsen i manualen fungerer godt i praksis, en, som anlægsejeren kan krydse af og arkivere.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SG-6 **Der findes en vejledning til sikker udfasning, som beskriver den fuldstændige fjernelse af følsomme data fra produktet, for eksempel adgangsoplysninger, nøgler, konfigurationsdata og logfiler, inden enheden gives videre, genbruges eller bortskaffes.** Dokument

Det taler for: Et afsnit om udfasning, der lister hvert lagringssted for følsomme data inde i produktet og den tilhørende sletteprocedure, herunder de tilfælde, hvor sletning er teknisk umulig, og hardwaren skal destrueres fysisk. En liste over vedvarende lagre hentet fra arkitekturbeskrivelsen hjælper her, den forhindrer, at et lagringssted bliver glemt.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SG-7 **Den sikkerhedsdokumentation, der leveres til brugerne, gennemgås inden frigivelsen: den er teknisk korrekt, i overensstemmelse med den leverede produktversion, fuldstændig i forhold til det tilsigtede indhold og forståelig for den tilsigtede målgruppe, og den opdateres, hver gang produktet ændres.**

Det taler for: En registrering fra gennemgangen per dokument og produktversion med den ansvarlige for gennemgangen, dato, fund og deres afslutning, koblet til frigivelsesgodkendelsen. En lille virksomhed løser dette med fireøjneprincippet i pull requesten til dokumentationen: en udvikler kontrollerer det tekniske indhold, en anden person kontrollerer forståeligheden, og godkendelsen registreres i sagen. En version kan først sendes ud, når gennemgangen er dokumenteret.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

IEC 62443-3-3:2013 Systemkrav til sikkerheden i industriel automation

Syv grundlæggende krav, 51 systemkrav

100 krav. Det er muligt at blive certificeret efter denne standard hos et akkrediteret certificeringsorgan. Udgave 07/2026.

Det er muligt at certificere efter IEC 62443-3-3, og det, der certificeres, er et system, ikke en organisation og ikke en person. Vejene er ISASecure SSA og IECEE CB Scheme. Den, der vil certificere organisationen, har brug for 62443-2-1 eller 2-4, den, der vil certificere komponenten, har brug for 62443-4-2. Denne liste indeholder de 51 systemkrav og de 49 kravforstærkninger. Hvilke af dem der gælder, afhænger af det sikkerhedsniveau, der stræbes efter: 38 fra SL 1, 60 fra SL 2, 90 fra SL 3, alle 100 ved SL 4. Ingen kravforstærkning gælder allerede ved SL 1. Denne liste er et arbejdsredskab til selvvurdering, ikke et bevis.

Virksomhed	Dato	Udfyldt af

5 FR 1: Hvem eller hvad beder om adgang, og er det virkelig den, det giver sig ud for at være 24

SR 1.1 Menneskelige brugere identificeres, og deres identitet verificeres, inden de får adgang, ved hvert punkt hvor de kan betjene eller konfigurere automationssystemet. Det omfatter betjeningspaneler ved maskinen, projekteringsadgange og netværkstjenester.

Det taler for: Fortegnelse over alle loginpunkter i systemet, altså HMI, kontrolrum, programmeringsadgang til PLC, switch, VPN og klient til fjernvedligeholdelse, hver med den autentificeringsmekanisme der anvendes på stedet. Dertil et konfigurationsudtræk eller et skærmbillede af loginskærmen for hver enhedsklasse. En lille virksomhed starter med en tabel for hver enhed, kolonner: enhed, grænseflade, autentificering til stede ja eller nej, begrundelse ved nej. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.1 RE 1 Hver menneskelig bruger arbejder under en individuel identifikator, der er tildelt netop den person. Fælles konti og skiftekonti er deaktiveret, og resterende undtagelser er begrundet enkeltvis og understøttet af yderligere foranstaltninger.

Det taler for: Kontoeksport for hvert system med sammenhæng mellem identifikator og person, undtagelsesliste med begrundelse og kompenserende foranstaltning, for eksempel et kamera eller en tilstedeværelsesjournal ved betjeningsstationen. Denne linje er en kravforstærkning og derfor aldrig obligatorisk ved SL 1, den kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.1 RE 2 Den, der logger på fra et netværk, der ikke er betroet, for eksempel fra internettet eller via en forbindelse til fjernvedligeholdelse, godtgør sin identitet med mindst to uafhængige faktorer.

Det taler for: Konfiguration af fjernadgangen med den anden faktor aktiveret, en eksempelregistrering af et login der viser begge faktorer, og udstedelseslisten over tokens eller appregistreringer. En lille virksomhed bruger den anden faktor i den eksisterende VPN-gateway eller en autentificeringsapp, hvilket ikke koster andet end opsætningstid. Kravforstærkning, kræves fra SL 3 og opefter, ikke ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.1 RE 3 Godtgørelsen med to uafhængige faktorer gælder ikke kun adgang udefra, men hvert login foretaget af en menneskelig bruger, herunder login inde i det netværk, der er klassificeret som betroet.

Det taler for: Politikudtræk fra den centrale autentificeringstjeneste, der viser at den anden faktor håndhæves uden undtagelse for noget netværk, samt eksempler på loginregistreringer fra kontrolrummet og betjeningspanelet. Kravforstærkning, kræves først fra SL 4 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.2 **Ikke kun mennesker, men også softwareprocesser og enheder autentificerer sig over for systemet, inden de får lov at udveksle data eller bruge tjenester. Det omfatter koblinger mellem styreenheder, dataforbindelser til overordnede systemer og diagnoseværktøjer.**

Det taler for: Liste over forbindelser mellem maskiner med kilde, destination, protokol og de anvendte legitimationsoplysninger i hvert tilfælde, for eksempel certifikat, servicekonto eller forud delt nøgle. Dertil et konfigurationsudtræk fra en kobling, der gør autentificeringen synlig. Kræves fra SL 2 og opefter, ikke krævet ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.2 RE 1 **Hver softwareproces og hver enhed fremviser sin egen entydige identifikator. Fælles servicekonti eller en enkelt nøgle, der bruges systemdækkende på mange enheder, er ikke tilladt.** Dokument

Det taler for: Sammenstilling af enhed og identifikator eller certifikatets serienummer, der viser at ingen identifikator optræder to gange. Kravforstærkning, kræves fra SL 3 og opefter og er derfor ikke en del af SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.3 **Konti styres gennem hele deres livscyklus: oprettelse, ændring af rettigheder, deaktivering ved fratrædelse og fjernelse er reguleret af regler og understøttet af de systemer, der indgår. Det omfatter brugerkonti, servicekonti og nødkonti.** Dokument

Det taler for: Kontoregister med type, ejer, formål og status samt dokumentation for tiltrædelser og fratrædelser, for eksempel en underskrevet overdragelse eller en sag, der viser deaktiveringen med dato. En tilbagevendende gennemgang af konti er tilrådelig, og i en lille virksomhed er en årlig afstemning af kontolisten mod personalelisten tilstrækkelig. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.3 RE 1 **Kontostyringen er samlet på tværs af alle systemets komponenter, så en deaktivering ét sted ikke forbliver uden virkning på enkelte enheder.**

Det taler for: Dokumentation for integrationen med det centrale katalog, for eksempel katalogtjeneste eller RADIUS, med en liste over de tilsluttede komponenter og en udtrykkelig liste over de enheder, der ikke kan tilsluttes, sammen med den alternative fremgangsmåde for dem. Testprotokol for en deaktivering, der får virkning på alle tilsluttede systemer. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.4 **Identifikatorer udstedes efter faste regler, tildeles entydigt til en person, en enhed eller en rolle, trækkes tilbage når de ikke længere bruges, og udstedes aldrig senere til en anden indehaver.**

Det taler for: Navngivningsregel for identifikatorer, for eksempel efternavn plus forbogstav eller anlægskode plus nummer, samt historikken over tilbagetrukne identifikatorer, der viser at de ikke genbruges. En lille virksomhed fører én løbende liste med udstedelsesdato og tilbagetrækningsdato. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.5 **Autentificeringsmidler som adgangskoder, nøgler, certifikater og tokens udstedes ordentligt, skiftes ved mistanke om afsløring og tilbagekaldes når det er nødvendigt. Standardkonti og fabriksadgangskoder som leveret ændres inden idriftsættelsen.**

Det taler for: Udstedelsesliste over tokens og certifikater med modtager og dato, dokumentation for ændringer og tilbagekaldelser samt en tjekliste ved idriftsættelse for hver enhed med punktet fabriksadgangskode ændret, kvitteret. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.5 RE 1 **Legitimationsoplysningerne for softwareprocesser ligger ikke som en læsbar fil på lagermediet, men i et hardwarebaseret lager, der forhindrer at den hemmelige del kan læses ud.**

Det taler for: Typedokumentation for den anvendte sikkerhedskomponent, for eksempel TPM, secure element eller HSM, med et konfigurationsudtræk der godtgør at nøglen opbevares inde i komponenten. Et købsbilag eller et datablad rækker som typedokumentation. Kravforstærkning, kræves fra SL 3 og opefter, ikke krævet ved SL 1 og SL 2.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.6 **Trådløs adgang til systemet, for eksempel WLAN, radiofjernbetjeninger eller Bluetooth-diagnose, kan først bruges efter identifikation og autentificering af både bruger og enhed, og den styres bevidst.**

Det taler for: Fortegnelse over alle trådløse forbindelser med formål, rækkevidde og krypteringsmetode, konfigurationsudtræk fra adgangspunktet og listen over godkendte slutenheder. En lille virksomhed dokumenterer desuden, hvilke trådløse grænseflader på enheder der bevidst er slået fra. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.6 RE 1 **Hver trådløs adgang kan henføres til én bestemt bruger eller én bestemt enhed, og en fælles netværksnøgle for alle deltagere er ikke tilstrækkelig.**

Det taler for: Dokumentation for en metode med individuelle legitimationsoplysninger, for eksempel WLAN-autentificering i virksomhedstilstand mod et katalog eller certifikater for hver enhed, samt en forbindelseslog der viser den individuelle identifikator. Kravforstærkning, kræves fra SL 2 og opefter og derfor ikke ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.7 **Hvor der bruges adgangskoder, kan deres mindstestyrke konfigureres, for eksempel mindste længde og krævede tegntyper, og de konfigurerede værdier får virkning for alle berørte konti.**

Det taler for: Konfigurationsudtræk for adgangskodepolitikken i hvert system med de værdier der faktisk er sat, for eksempel længde >= 10 tegn og mindst tre tegntyper, samt en liste over de systemer der teknisk ikke kan understøtte denne indstilling, sammen med deres kompenserende foranstaltning. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.7 RE 1 **For menneskelige brugere gælder yderligere regler for dannelse og levetid af adgangskoder: genbrug af tidligere adgangskoder forhindres, og gyldigheden er tidsbegrænset.**

Det taler for: Konfigurationsudtræk der viser adgangskodehistorikken, for eksempel spærring af genbrug af de sidste fem adgangskoder, og den konfigurerede maksimale gyldighed. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.7 RE 2 **Begrænsningen af adgangskoders levetid gælder ikke kun personer, men alle konti, herunder konti til service, vedligeholdelse og enheder.**

Det taler for: Rotationsplan for tekniske konti med sidste og næste ændringsdato for hver konto samt dokumentation for ændringerne, for eksempel en ændringsregistrering eller en sag. Kravforstærkning, kræves først fra SL 4 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.8 **Hvor der bruges certifikater, kommer de fra en ordentlig certifikatstyring med fastlagte regler for anmodning, udstedelse, gyldighedsperiode, fornyelse og tilbagekaldelse.** Dokument

Det taler for: Certifikatpolitik eller en kort skriftlig regel med ansvar, gyldighedsperioder og vejen til tilbagekaldelse samt en fortegnelse over de udstedte certifikater med deres udløbsdatoer. En lille virksomhed fører en tabel med certifikat, enhed, udløbsdato og påmindelsesdato, hvilket forhindrer stille anlægsstop forårsaget af udløbne certifikater. Kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.9 **Når nøglepar bruges til autentificering, validerer systemet certifikatet fuldstændigt: tillidskæden, gyldighedsperioden, tilbagekaldelsesstatus og bevis for at modparten faktisk har den private nøgle. Sammenhængen mellem certifikat og konto er entydig.**

Det taler for: Konfigurationsudtræk med tilbagekaldelseskontrol aktiveret, for eksempel CRL eller OCSP, testprotokol for et afvist login med et udløbet eller tilbagekaldt certifikat samt tabellen der knytter certifikat til konto. Kræves fra SL 3 og opefter, ikke krævet ved SL 1 og SL 2.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.9 RE 1 **Private nøgler ligger udelukkende i et hardwarebaseret lager, hvorfra de ikke kan læses ud, og de bruges også inde i dette lager.**

Det taler for: Datablad eller certificeringsdokumentation for den anvendte sikkerhedskomponent og et konfigurationsudtræk der viser at nøglen dannes inde i komponenten, så den private nøgle aldrig forlader den. Kravforstærkning, kræves først fra SL 4 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.10 **Under login afslører systemet ingen oplysninger, der kan udnyttes. Indtastede adgangskoder skjules, og fejlmeddelelser røber ikke om identifikatoren eller adgangskoden var forkert.**

Det taler for: Skærmbillede af loginskærmen med maskeret indtastning og et skærmbillede af fejlmeddelelsen efter et mislykket forsøg. For enheder der teknisk ikke kan dette, for eksempel ældre betjeningspaneler, tilføjes en kort note om den kompenserende foranstaltning, for eksempel begrænset fysisk adgang til opstillingsstedet. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.11 **Antallet af mislykkede login i træk er begrænset, og reaktionen på det kan konfigureres, for eksempel en midlertidig spærring. Den valgte reaktion hindrer ikke sikkerhedsrelateret drift af anlægget.**

Det taler for: Konfigurationsudtræk med grænseværdien, for eksempel spærring efter <= 5 mislykkede forsøg, og spærringens varighed samt en kort vurdering af hvorfor spærringen ikke blokerer nøddrift eller en sikker nedlukning af anlægget. Ved betjeningsstationer med en sikkerhedsfunktion er en tidsbegrænset spærring at foretrække frem for en permanent kontospærring. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.12 **En brugsmeddelelse kan vises inden login med henvisning til reglerne for brug og overvågning af systemet. Tekst og visning kan konfigureres af anlægsejeren.**

Det taler for: Skærmbillede af den viste meddelelsestekst og den godkendte ordlyd med datoen for godkendelsen. Små virksomheder aftaler ordlyden kort med medarbejderrepræsentationen eller med ledelsen, ét afsnit er nok. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.13 **Adgang fra netværk, der ikke er betroede, for eksempel fjernvedligeholdelse fra leverandører, er begrænset til fastlagte veje, overvåges og kan afbrydes til enhver tid.**

Det taler for: Fortegnelse over vejene til fjernadgang med formål, modpart, kontaktperson og den anvendte vej samt forbindelseslogge og dokumentation for muligheden for at afbryde, for eksempel en nøgleafbryder, en firewallregel eller en router til fjernvedligeholdelse der kan slukkes. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 1.13 RE 1 **Hver enkelt session fra et netværk, der ikke er betroet, godkendes udtrykkeligt af en ansvarlig person, inden forbindelsen etableres, og en permanent åben forbindelse er ikke tilstrækkelig.**

Det taler for: Godkendelsesregistreringer for hver session med fjernvedligeholdelse med tidspunkt, årsag, godkendende person og varighed, teknisk for eksempel via en nøgleafbryder ved adgangsrouteren eller via en godkendelsesportal. I en lille virksomhed er en logbog for fjernvedligeholdelse ved styretavlen, kvitteret af serviceteknikeren for hver session, tilstrækkelig. Kravforstærkning, kræves fra SL 2 og opefter og derfor aldrig ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

6 FR 2: Brugsstyring (rettigheder, sessioner, logregistreringer) 24

SR 2.1 **Systemet håndhæver teknisk de tildelte rettigheder: hver person der er logget på, hver enhed og hver softwareproces får præcis den adgang, der er tildelt, og ethvert forsøg derudover afvises.**

Det taler for: Et rettighedskoncept der knytter konti til rettigheder samt et skærmbillede eller konfigurationsudtræk for hvert styresystem, hver HMI og hver projekteringsstation med de aktive rettigheder. Dertil en testprotokol hvor en konto med lave rettigheder forsøger en spærret handling og bliver afvist. Kræves fra SL 1. En lille virksomhed klarer sig med to eller tre roller, for eksempel betjening, vedligeholdelse og projektering, og dokumenterer dem på én side.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.1 RE 1 **Håndhævelsen af rettigheder gælder ikke kun menneskelige operatører, men i samme grad softwareprocesser og enheder, der tilgår systemet af sig selv.**

Det taler for: En liste over tekniske konti og servicekonti, for eksempel OPC UA-klienter, forbindelser til historikdatabasen og sikkerhedskopieringstjenester, hver med sit tildelte sæt rettigheder. Et udtræk fra rettighedsstyringen der viser at disse konti ikke kører med administratorrettigheder. Kravforstærkning, kræves fra SL 2, ikke ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.1 RE 2 **Rettigheder tildeles ikke enkeltpersoner én for én, men gennem roller, og sammenhængen mellem rolle og tilladte handlinger er registreret sporbart.** Dokument

Det taler for: En matrix over roller og rettigheder som tabel: rækkerne er rollerne, kolonnerne handlingerne som at ændre setpunkt, overføre program, kvittere alarm og oprette konto. Dertil listen der knytter person til rolle. Kravforstærkning, kræves fra SL 2. Et vedligeholdt regneark med en ændringsdato er fuldt tilstrækkeligt som dokumentation.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.1 RE 3 **I snævert afgrænsede undtagelsestilfælde kan en autoriseret overordnet ophæve en rettighedsbegrænsning i en begrænset periode, og hver sådan ophævelse registreres i logsporet.**

Det taler for: En procedurebeskrivelse for undtagelsesgodkendelsen med hvem der må give den, og hvor længe den gælder, samt logregistreringer af allerede givne ophævelser, taget fra systemloggen. Kravforstærkning, kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.1 RE 4 **Særligt kritiske indgreb kræver godkendelse fra to uafhængige autoriserede personer, inden handlingen udføres.**

Det taler for: En liste over de handlinger der er underlagt dobbelt godkendelse, for eksempel ændring af sikkerhedsparametre eller overførsel af et nyt styreprogram, sammen med konfigurationsdokumentation og logregistreringer der nævner begge godkendere. Kravforstærkning, kræves først fra SL 4.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.2 **Brugen af trådløse forbindelser i automationsnetværket er knyttet til en udtrykkelig godkendelse, og kun godkendte deltagere må udveksle data eller gribe ind via luften.**

Det taler for: En fortegnelse over alle trådløse forbindelser, for eksempel WLAN-adgangspunkter, Bluetooth-parringer og mobilroutere, hver med sit formål og sine godkendte deltagere. Dertil konfigurationen af adgangsstyringen i adgangspunktet. Kræves fra SL 1. Den der ikke driver nogen trådløs forbindelse i procesnetværket, oplyser netop det skriftligt og understøtter det med en konfigurationsvisning der viser trådløs deaktiveret.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.2 RE 1 **Uautoriserede trådløse enheder i nærheden af automationsnetværket opdages og rapporteres.**

Det taler for: En registrering fra den trådløse overvågning eller en tilbagevendende trådløs scanning med dato, resultatliste og en note om hver ukendt enhed. Vejen til rapportering til den ansvarlige funktion er nævnt. Kravforstærkning, kræves fra SL 2, ikke ved SL 1. En lille virksomhed kan køre en kvartalsvis scanning med en bærbar computer og arkivere resultatet som registrering.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.3 **Brugen af bærbare og mobile enheder på systemet, for eksempel servicecomputere, USB-lagermedier eller tablets, er reguleret af regler og teknisk begrænset til udtrykkeligt godkendte enheder.**

Det taler for: Regelsættet for brug af enheder, en liste over godkendte serviceenheder med deres identifikatorer og dokumentation for den tekniske begrænsning, for eksempel USB-porte på HMI og projekteringsstation deaktiveret eller begrænset til bestemte enheder. Kræves fra SL 1. En lille virksomhed arbejder med to mærkede USB-nøgler til service, som kun skrives til ved én overførselsstation.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.3 RE 1 **Inden tilslutning bliver sikkerhedstilstanden på en bærbar eller mobil enhed kontrolleret, og enheder der ikke opfylder kravene, forhindres i at få adgang.**

Det taler for: Kriterierne for kontrol af enhedens tilstand, for eksempel aktuel beskyttelse mod skadelig kode og aktuelt rettelsesniveau, samt kontrolregistreringer for hver serviceenhed og dokumentation for den tekniske håndhævelse, for eksempel gennem en overførselsstation eller en netværksadgangskontrol. Kravforstærkning, kræves fra SL 3.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.4 **For mobil kode der udføres på systemet, for eksempel scripts i betjeningsgrænseflader eller aktivt indhold i rapporter, er det fastlagt hvilke typer der er tilladt, og typer der ikke er tilladt, forhindres i at blive udført.** Dokument

Det taler for: En fastlæggelse af hvilken mobil kode der er tilladt på hvilke systemer, samt konfigurationsdokumentation for begrænsningen, for eksempel scriptudførelse i HMI-browseren deaktiveret og makroer i evalueringsfiler spærret. Kræves fra SL 1. En fastlæggelse på én side der dækker de tre eller fire tilfælde der faktisk findes, er tilstrækkelig.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.4 RE 1 **Inden mobil kode udføres, verificeres det at den kommer fra den forventede kilde og ikke er ændret.**

Det taler for: Konfigurationsdokumentation for signaturkontrollen eller kontrolsummen samt en testprotokol hvor manipuleret eller usigneret kode afvises. Kravforstærkning, kræves fra SL 3.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.5 **En session låses efter en fastlagt periode uden betjening og frigives først igen efter fornyet autentificering, uden at visningen af sikkerhedsrelevante procesoplysninger går tabt.**

Det taler for: Et konfigurationsudtræk med den konfigurerede låsetid for hver arbejdsstation samt en begrundelse for arbejdsstationer i permanent bemandede kontrolrum, hvor låsen bevidst er sat anderledes. Kræves fra SL 1. Visuel dokumentation: et skærmbillede af låseskærmen hvor alarmlinjen stadig er synlig.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.6 **Fjernsessioner afsluttes efter en fastlagt periode uden aktivitet eller på operatørens anmodning, så ingen åben fjernforbindelse står uden opsyn.**

Det taler for: Konfigurationen af fjernadgangen med dens tidsgrænse for inaktivitet, logregistreringer af afsluttede fjernsessioner og en beskrivelse af hvordan operatøren straks kan afbryde en igangværende session med fjernvedligeholdelse, for eksempel gennem en nøgleafbryder eller en frigivelse for hver session. Kræves fra SL 2, ikke ved SL 1.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 2.7 **Antallet af samtidige sessioner for hver konto eller rolle er begrænset, og loginforsøg ud over denne grænse afvises.**

Det taler for: Et konfigurationsudtræk med den fastlagte øvre grænse for hver rolle, for eksempel <= 1 samtidig session for projekteringskonti, samt en testprotokol for det afviste andet loginforsøg. Kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.8 **Sikkerhedsrelevante hændelser registreres, og hver post angiver mindst tidspunkt, kilde, den udløsende konto, hændelsens art og resultatet.** Dokument

Det taler for: En fastlæggelse af de hændelsestyper der skal registreres, for eksempel login, mislykket login, ændring af rettigheder, programændring og konfigurationsændring, samt et ægte udtræk af logfilen der viser de nævnte felter. Kræves fra SL 1. En lille virksomhed samler loggene fra styresystem, HMI og firewall i én mappe med en fast opbevaringsperiode.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.8 RE 1 **Logregistreringerne fra de enkelte komponenter samles ét centralt sted og danner én systemdækkende registrering, der kan analyseres samlet.**

Det taler for: En arkitekturskitse over logindsamlingen med alle tilsluttede kilder samt en analyse der placerer hændelser fra mindst to komponenter på én tidslinje. Kravforstærkning, kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.9 **Der er afsat tilstrækkelig lagerplads til logregistreringerne, så hændelser bevares i hele den fastlagte opbevaringsperiode og ikke overskrives utilsigtet.**

Det taler for: En beregning eller et skøn over lagerbehovet ud fra dagligt logomfang gange opbevaringsperiode samt den konfigurerede lagerstørrelse og reglen for arkivering. Kræves fra SL 1. I praksis rækker en daglig kopi til et separat lagersted med en dokumenteret opbevaringsperiode.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.9 RE 1 **Når en fastlagt grænse for loglagerets fyldningsgrad nås, udsendes en advarsel til den ansvarlige funktion, inden lagerkapaciteten er brugt helt op.**

Det taler for: Et konfigurationsudtræk med grænseværdien, for eksempel en advarsel fra >= 80 procent udnyttelse, samt et eksempel på den udløste meddelelse og modtagerlisten. Kravforstærkning, kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.10 **Hvis logningen svigter eller loglageret løber fuldt, reagerer systemet på en på forhånd fastlagt måde, og den ansvarlige funktion informeres, uden at anlæggets sikre drift bringes i fare.**

Det taler for: Den fastlagte reaktion for hvert fejltilfælde, for eksempel overskrivning af ældre poster og en meddelelse i stedet for standsning af anlægget, med en begrundelse ud fra processen. Dokumentation gennem en udløst testmeddelelse og den tilhørende logpost. Kræves fra SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.11 **Hver logregistrering bærer et tidsstempel fra en navngivet tidskilde, så hændelser fra forskellige komponenter kan sættes i rækkefølge i forhold til hinanden.**

Det taler for: En oplysning om den anvendte tidskilde for hver komponent og et logudtræk med synligt tidsstempel inklusive tidszone. Kræves fra SL 2, ikke ved SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.11 RE 1 **Urene i alle deltagende komponenter synkroniseres mod en fælles tidskilde, så afvigelsen holder sig inden for en fastlagt grænse.**

Det taler for: Konfigurationen af tidssynkroniseringen, for eksempel NTP-server og synkroniseringsinterval, samt en kontrolregistrering med den målte afvigelse for hver komponent i forhold til den fastlagte grænse, for eksempel <= 1 sekund. Kravforstærkning, kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.11 RE 2 **Selve tidskilden er beskyttet mod manipulation, og en tidsreference der ikke er plausibel, eller som er ændret, opdages og rapporteres.**

Det taler for: En beskrivelse af hvordan tidskilden er beskyttet, for eksempel autentificeret tidssynkronisering, begrænsning til en intern kilde og overvågning for tidsspring, samt meddelelser eller logregistreringer om en opdaget afvigelse. Kravforstærkning, kræves først fra SL 4.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.12 **For fastlagte kritiske handlinger kan det bagefter fastslås uden tvivl, hvem der udløste dem, så den handlende person ikke troværdigt kan benægte at have gjort det.** Dokument

Det taler for: En liste over de handlinger denne dokumentation gælder for, for eksempel receptændring, batchfrigivelse og ændring af grænseværdier, samt de tilhørende registreringer med en entydig personidentifikator og dokumentation for at gruppekonti er udelukket for disse handlinger. Kræves fra SL 3.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 2.12 RE 1 **Den uafviselige henføring til den handlende person gælder ikke kun udvalgte kritiske handlinger, men alle brugere og alle handlinger de udløser.**

Det taler for: Dokumentation for at hver konto er knyttet til én enkelt person, og at der ikke er fælles logins tilbage, samt et logudtræk over vilkårlige handlinger hvor en entydig personidentifikator optræder hele vejen igennem. Kravforstærkning, kræves først fra SL 4.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

7 FR 3: Systemintegritet, beskyttelse af data, software og sessioner mod uautoriseret ændring 19

SR 3.1 **Styresystemet opdager når information er blevet ændret under overførsel over en kommunikationskanal, og det gælder styredata, konfigurationsdata og administrationstrafik i samme grad. Beskyttelsen omfatter også forbindelser der forlader systemet eller krydser netværkssegmenter, som ikke er betroede.**

Det taler for: En oversigt over netværk og protokoller med angivelse af hvilken kanal der bruger hvilken integritetsmekanisme (kontrolsum, message authentication code, signerede telegrammer), et konfigurationsudtræk for sikkerhedsindstillingerne i feltbussen eller OPC UA, og en testprotokol der viser at et manipuleret telegram beviseligt blev afvist. En lille virksomhed opsamler dette i en tabel for hver forbindelse med kolonnerne kilde, destination, protokol og integritetsmekanisme og dokumenterer virkningen én gang med en trafikoptagelse. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.1 RE 1 **Integritetsbeskyttelsen under overførsel bygger på kryptografiske mekanismer, så en bevidst manipulation fra en angriber med egne midler ikke kan passere uopdaget. En simpel kontrolsum mod overførselsfejl er ikke tilstrækkelig her.**

Det taler for: En liste over de kryptografiske mekanismer og nøglelængder der bruges i hver kanal, en henvisning til den underliggende nøglestyring og konfigurationsudtræk (for eksempel TLS cipher suites, OPC UA SecurityPolicy og IPsec-profiler). Små virksomheder læner sig op ad de sikre standardprofiler i deres styreenheder og arkiverer et skærmbillede af den aktive indstilling. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.2 **Der findes beskyttelsesmekanismer mod skadelig kode, som forhindrer uønsket programkode i at blive udført på systemets komponenter, og som rapporterer enhver opdagelse. Mekanismerne er valgt, så de ikke forstyrrer anlæggets tilsigtede drift, og de holdes aktuelle.**

Det taler for: En oversigt for hver komponent over hvilken mekanisme der gælder (antivirus, hvidlistning af programmer, hærdet operativsystem uden udførelsesrettigheder), dokumentation for at signaturer eller hvidlister opdateres, og alarmer fra beskyttelsessystemet. Hvor antivirus ikke er muligt, for eksempel på en styreenhed, registreres den kompenserende foranstaltning med sin begrundelse. Små virksomheder klarer sig godt med hvidlistning på betjeningscomputeren og en skriftlig regel for USB-medier. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.2 RE 1 **Beskyttelsen mod skadelig kode virker desuden ved anlæggets indgangspunkter og udgangspunkter, hvor data kommer ind eller går ud, og ikke kun på slutenhederne selv.**

Det taler for: En liste over alle indgangspunkter og udgangspunkter (adgang til fjernvedligeholdelse, gateway til dataoverførsel, flytbare medier, overdragelse til kontornetværket, mailvejen for programversioner) med den scanningsmekanisme der virker hvert sted, samt registreringer af de overdragelser der blev kontrolleret. Små virksomheder opstiller én overdragelsescomputer med virusscanning som sluse og fastholder dette i en arbejdsinstruktion. Kravforstærkning, kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.2 RE 2 **Beskyttelsesmekanismerne mod skadelig kode styres fra ét centralt sted, opdateringer fordeles centralt, og opdagelser samles ét sted til analyse.**

Det taler for: Konfigurationen af den centrale styringskonsol, en rapport om opdateringsstatus for alle tilsluttede komponenter og en analyse af rapporterede opdagelser over en periode. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.3 **Systemets sikkerhedsfunktioner verificeres med planlagte intervaller og efter ændringer for at bekræfte at de faktisk virker. Testene lægges, så de ikke bringer anlæggets drift i fare, og resultaterne registreres.** Dokument

Det taler for: En testplan med testobjekt, interval og tidsvindue sammen med testprotokollerne med dato, tester, forventet adfærd og observeret adfærd. Nyttige enkelttest er: et login med en deaktiveret konto mislykkes, antivirus reagerer på en testfil, og adgangen til fjernvedligeholdelse er ikke tilgængelig uden frigivelse. Små virksomheder lægger testen til det vedligeholdelsesstop der alligevel er planlagt, og arbejder en fast tjekliste igennem. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.3 RE 1 **Verifikationen af sikkerhedsfunktionerne kører med automatiserede midler, så den kan gentages uden manuel indsats og giver et ensartet resultat.**

Det taler for: Scripts eller testværktøjer sammen med deres tidsplan, deres uddatafiler og en sammenligning af flere kørsler der viser at afvigelser opdages. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.3 RE 2 **Verifikationen af sikkerhedsfunktionerne er også mulig under normal drift, uden at anlægget behøver at blive standset eller sat i en særlig tilstand.**

Det taler for: En beskrivelse af testproceduren med dokumentation for at den ikke påvirker processen negativt, for eksempel en analyse af virkningen på cyklustider og netværksbelastning, samt testprotokoller fra produktiv drift. Kravforstærkning, kræves fra SL 4 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.4 **Uautoriserede ændringer af software, firmware og lagret information opdages. Det gælder i samme grad styreprogrammer, parametersæt, recepter og konfigurationsfiler.**

Det taler for: En fortegnelse over de versioner der er værd at beskytte, med gemte kontrolværdier eller signaturer, resultaterne af integritetssammenligningerne og den dokumenterede afstemning med den version der ligger i versionsstyringen. Små virksomheder gemmer den frigivne programversion sammen med dens kontrolsum et skrivebeskyttet sted og sammenligner ved mistanke eller efter vedligeholdelse. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.4 RE 1 **Opdages en krænkelse af integriteten af software eller information, melder systemet det automatisk til et ansvarligt sted, uden at nogen aktivt behøver at lede efter det.**

Det taler for: Konfigurationen af meddelelsesvejene (alarm i kontrolrummet, e-mail, besked til overvågningssystemet), en modtagerliste med stedfortræderordning og mindst én testalarm med en dokumenteret svartid. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.5 **Inddata som systemet modtager fra procesdata, grænseflader eller brugergrænseflader, kontrolleres for tilladt syntaks, tilladt værdiområde og tilladt længde, inden de behandles. Ugyldige inddata fører ikke til ukontrolleret adfærd.**

Det taler for: En specifikation af grænser og formater for hvert inddata, udtræk fra valideringslogikken i styreenheden eller applikationen og testtilfælde med bevidst ugyldige inddata (en for stor værdi, en forkert datatype, en for lang tegnstreng) sammen med systemets dokumenterede adfærd. Små virksomheder registrerer plausibilitetsgrænserne for hvert målepunkt i en tabel og verificerer dem ved idriftsættelsen. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.6 **For fejltilfælde er det fastlagt hvilken tilstand udgangene til anlægget antager, og systemet antager netop den tilstand. Den fastlagte tilstand er afstemt med anlæggets funktionelle sikkerhed.**

Det taler for: En fastlæggelse for hvert udgangssignal eller hver gruppe af udgange (fastholdt værdi, fastlagt erstatningsværdi, sikker standsningstilstand) med en begrundelse fra risikovurderingen, et konfigurationsudtræk fra styreenheden og dokumentation fra en fejltest, for eksempel et kabelbrud eller tab af kommunikation, der viser den forventede adfærd. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.7 **Systemet håndterer fejltilstande, så driften forbliver under kontrol, og der ikke afsløres oplysninger, som ville hjælpe en angriber. Fejlmeddelelser til operatørerne holdes korte, mens de tekniske detaljer kun går i de interne registreringer.**

Det taler for: En oversigt over fejlklasserne med den systemadfærd der er forudset for hver af dem, eksempler på de viste meddelelser sammenholdt med de tilhørende interne logposter og testdokumentation for at ingen filstier, kontonavne, databaseuddata eller versionsdetaljer optræder på betjeningsgrænsefladen. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.8 **Aktive sessioner er beskyttet mod kapring og mod indsættelse af fremmede meddelelser. En session slutter efter udlogning eller efter en fastlagt periode uden aktivitet og kan derefter ikke genbruges.**

Det taler for: Konfigurationen af sessionsstyringen med de konfigurerede grænser for inaktiv tid og maksimal varighed, dokumentation for den mekanisme der beskytter mod genafspilning af meddelelser, og en testprotokol hvor en opfanget session ikke længere virker efter udlogning. Kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.8 RE 1 **Sessionsidentifikatorer mister deres gyldighed når sessionen slutter, og accepteres ikke igen af systemet, heller ikke når de fremvises igen udefra.**

Det taler for: Et konfigurationsudtræk fra sessionsstyringen der dækker ugyldiggørelsen, samt en testprotokol hvor en tidligere gyldig identifikator sendes igen efter udlogning og afvises af systemet. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.8 RE 2 **For hver ny session dannes en særskilt identifikator til engangsbrug. Identifikatorer genbruges ikke på tværs af sessioner, brugere eller enheder.**

Det taler for: En beskrivelse af dannelsesproceduren og dokumentation fra loggen eller en trafikoptagelse for at flere logins i træk får forskellige identifikatorer. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.8 RE 3 **Sessionsidentifikatorer dannes med anerkendte tilfældighedsmekanismer, så de hverken kan gættes eller udledes af foregående identifikatorer.**

Det taler for: En oplysning om den anvendte tilfældighedsgenerator og dens entropikilde, en leverandørerklæring eller testrapport om den og en statistisk analyse af en stikprøve af dannede identifikatorer. Kravforstærkning, kræves fra SL 4 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.9 **De sikkerhedsrelaterede registreringer og de værktøjer der bruges til at analysere dem, er beskyttet mod uautoriseret adgang, ændring og sletning. Kredsen af personer der må ændre eller fjerne registreringer, holdes snæver og er navngivet.** Dokument

Det taler for: Et rettighedskoncept for logdata med navngiven tildeling, konfigurationen af videresendelsen til et separat logsystem, opbevaringsperioder og testdokumentation for at en almindelig operatør ikke kan slette poster. Små virksomheder videresender loggene til en separat enhed, som anlæggets operatører ikke har skriveadgang til. Kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 3.9 RE 1 **De sikkerhedsrelaterede registreringer gemmes desuden på et medie, der udelukker senere overskrivning, så en post der én gang er skrevet, ikke længere kan ændres, heller ikke med administratorrettigheder.** Dokument

Det taler for: En beskrivelse af det anvendte lager (medie der kun kan skrives én gang, manipulationssikkert arkiv, løbende udvidet signaturkæde), dokumentation for et mislykket forsøg på at ændre en post og reglen for hvordan medierne opbevares og hentes frem. Kravforstærkning, kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

8 FR 4: Datafortrolighed 6

SR 4.1 **Automationssystemet beskytter fortrolig information mod uautoriseret afsløring, både under overførsel og i hvile. Det er fastlagt hvilke data der tæller som fortrolige, for eksempel recepter, parametersæt, legitimationsoplysninger, konfigurationsfiler eller diagnosedata med personhenførbarhed.** Dokument

Det taler for: En liste over de datatyper der er værd at beskytte, med angivelse af hvor de ligger, og hvordan de overføres, samt den konkrete beskyttelsesforanstaltning for hver post, for eksempel en krypteret forbindelse, et krypteret lagermedie eller en delt mappe med begrænset adgang. En lille virksomhed klarer sig med en tabel på én side: datatype, hvor den ligger, hvem der må se den, hvad der beskytter den. Kræves fra SL 1 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 4.1 RE 1 **For information der gemmes uden for det beskyttede miljø eller bevæger sig over netværk, som ikke er betroede, håndhæves fortroligheden med tekniske midler frem for blot at være lovet i en organisatorisk regel.**

Det taler for: Et konfigurationsudtræk for den transportkryptering eller lagerkryptering der er i brug, for eksempel VPN-profilen til fjernvedligeholdelse, TLS-indstillingerne for styresystemets grænseflade eller krypteringen af sikkerhedskopimedierne. Et dateret skærmbillede af den aktive indstilling er nok som dokumentation. Kræves fra SL 2 og opefter, ikke fra SL 1, fordi dette er en kravforstærkning.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 4.1 RE 2 **Fortroligheden håndhæves også ved grænserne mellem zoner, så information ikke bliver synlig i klartekst, når den krydser fra én zone ind i en anden.**

Det taler for: En plan over zoner og forbindelser der markerer hvilke overgange der er krypteret, sammen med konfigurationen af grænsekomponenten som gateway, firewall eller datadiode. En trafikoptagelse eller en testprotokol der viser at der ikke optræder klartekstdata ved grænsen. Kræves fra SL 4 og opefter.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 4.2 **Det er fastlagt hvordan fortrolig information fjernes pålideligt, når enheder tages ud af drift, skifter ejer, sendes til reparation eller genbruges, så der ikke efterlades læsbare restdata.** Dokument

Det taler for: En skriftlig procedure for udfasning med slettemetode for hver enhedstype samt sletteregistreringer med enhedens identifikation, datoen og den person der udførte det. En lille virksomhed registrerer dette som én linje for hver enhed i en fælles liste og arkiverer certifikaterne fra eksterne bortskaffelsesfirmaer sammen med den. Kræves fra SL 2 og opefter.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 4.2 RE 1 **Fælles lagerområder tømmes, inden de tildeles en anden bruger eller proces, så indhold der tilhører den forrige bruger, ikke kan læses ud.**

Det taler for: En leverandørerklæring eller konfigurationsregistrering om tømning af genbrugte hukommelsesområder og bufferområder, suppleret med en testprotokol fra afprøvning ved overtagelse eller vedligeholdelse. Hvor en komponent ikke kan dette, tjener den dokumenterede kompenserende foranstaltning som dokumentation, for eksempel at enheden ikke deles på tværs af forskellige roller. Kræves fra SL 3 og opefter, ikke fra SL 1, fordi dette er en kravforstærkning.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 4.3 **Hvor der bruges kryptografi, følger algoritmer, nøglelængder og håndtering af nøgler anerkendt god praksis, og det er fastlagt hvordan nøgler dannes, fordeles, gemmes, skiftes og tilbagekaldes.** Dokument

Det taler for: En oversigt over de anvendte mekanismer i hvert system med algoritme, nøglelængde og gyldighedsperiode samt reglerne for nøglestyring og registreringer af nøgleskift og certifikatfornyelser. Offentlige anbefalinger tjener som målestok, for eksempel de tekniske retningslinjer fra det tyske BSI. En lille virksomhed fører en certifikatliste med udløbsdatoer og en påmindelse >= 30 dage før udløb. Kræves fra SL 1 og opefter.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9 FR 5: Begrænset datastrøm, zoner og forbindelser 11

SR 5.1 **Styresystemet kan opdeles i adskilte zoner, og trafik mellem disse zoner går kun gennem fastlagte forbindelser. Opdelingen følger en begrundelse der kan forklares, for eksempel ud fra beskyttelsesbehov, ejerskab eller funktionen af de anlægsdele der indgår.** Dokument

Det taler for: Netværksdiagram med zonerne og forbindelserne mellem dem, en zoneliste med begrundelsen for hver grænse og konfigurationen af de adskillende komponenter som VLAN-definitioner eller firewallgrænseflader. En lille virksomhed klarer sig med en skitse på én side der viser kontor, maskinnetværk og fjernadgang som tre kasser med forbindelserne mellem dem, samt et skærmbillede af switchens VLAN-konfiguration.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.1 RE 1 **Adskillelsen af zonerne er udført fysisk, altså med egne netværkskomponenter og egen kabelføring, og hviler ikke alene på en logisk konfiguration inde i delte enheder. Afsnit 9.1 i denne liste, kræves fra SL 2 og opefter. Kravforstærkninger i denne standard er aldrig obligatoriske allerede ved SL 1.**

Det taler for: Fortegnelse over netværkskomponenter med angivelse af hvilken switch eller router der betjener hvilken zone, fotos eller tavletegning over de adskilte fordelinger og kabelmærkning. Små virksomheder dokumenterer dette med to separate, tydeligt mærkede switche i stedet for én fælles enhed og et foto af styretavlen i anlægsdokumentationen.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.1 RE 2 **Automationsnetværket kan drives uafhængigt af netværk uden for automationen. Svigter kontorets IT eller en ekstern forbindelse, kører styring og overvågning af anlægget videre. Kræves fra SL 3 og opefter.**

Det taler for: Afhængighedsliste over de tjenester der bruges inde i automationsnetværket, som tidsserver, navneopslag, katalogtjeneste eller licensserver, med angivelse af hvor hver enkelt er placeret, sammen med en testprotokol fra en frakoblingsprøve hvor forbindelsen til kontorets IT blev trukket ud. En lille virksomhed noterer resultatet af sådan en prøve i vedligeholdelsesjournalen: uplink trukket ud, anlægget kørte videre, kun kontorrapporterne manglede.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.1 RE 3 **Zoner med særligt kritiske funktioner, for eksempel sikkerhedsfunktioner eller beskyttelsesfunktioner, er adskilt fra de øvrige zoner både logisk og fysisk. Kræves fra SL 4 og opefter.**

Det taler for: Markering af de kritiske zoner i zonediagrammet med begrundelsen for klassificeringen, dokumentation for egne netværkskomponenter og egen kabelføring til disse zoner og konfiguration af forbindelserne med dokumentation for at der ikke findes nogen fælles vej.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.2 **Ved zonegrænserne styres og overvåges trafikken og tillades eller afvises efter fastlagte regler. Der findes ingen vej mellem to zoner, der går uden om dette kontrolpunkt.**

Det taler for: Eksporteret regelsæt fra firewallen eller grænseenheden, logge over afviste og tilladte forbindelser og dokumentation for at der ikke findes sideveje, for eksempel gennem en kontrol for ekstra netværkskort, modemer eller mobilroutere i anlæggets computere. En lille virksomhed dokumenterer dette med regeleksporten fra sin ene firewall og en kort rundgangsnote der bekræfter at der ikke sidder en uplanlagt router i nogen styretavle.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.2 RE 1 **Regelsættet ved zonegrænsen arbejder efter princippet om at alt er afvist, medmindre det udtrykkeligt er tilladt. Hver tilladelsesregel er begrundet enkeltvis og knyttet til et formål. Kræves fra SL 2 og opefter.**

Det taler for: Regelsæt med en synlig sidste regel der kasserer resten, og en tilladelsesliste med kilde, destination, tjeneste, formål og ansvarlig person for hver regel. Små virksomheder fører denne liste som en tabel med fem kolonner ved siden af firewalleksporten og gennemgår den én gang om året for regler ingen længere har brug for.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.2 RE 2 **Automationsnetværket kan bevidst afskæres fra alle eksterne forbindelser og køre videre i ødrift. Handlingen kan udløses uden at anlægget behøver at blive standset. Kræves fra SL 3 og opefter.**

Det taler for: Beskrivelse af isolationsproceduren med hvem der må udløse den, og hvordan, dokumentation for den tekniske gennemførelse som et nødregelsæt eller en mærket skilleafbryder samt registreringen af en øvelse hvor isolationen faktisk blev afprøvet. En lille virksomhed kører øvelsen én gang om året under vedligeholdelsen og noterer dato, varighed og alt usædvanligt.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.2 RE 3 **Svigter enheden ved zonegrænsen eller mister den sine regler, afviser den trafikken i stedet for at lade den passere. En fejl må ikke efterlade en åben forbindelse. Kræves fra SL 4 og opefter.**

Det taler for: Leverandørerklæring eller konfigurationsdokumentation for hvordan komponenten opfører sig ved fejl og ved genstart, testprotokol for et bevidst fremkaldt svigt med det observerede resultat og afstemning med anlæggets risikovurdering, fordi en grænse der afviser trafik, selv kan have konsekvenser afhængigt af processen.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.3 **Almindelige tjenester til kommunikation mellem personer som e-mail, beskeder eller videoopkald kan forhindres på automationsudstyr og inde i automationsnetværk. Omfanget af spærringen er fastlagt og begrundet.**

Det taler for: Fastlæggelse af hvilke tjenester der ikke er tilladt i automationsnetværket, samt den tekniske gennemførelse: spærrede porte og destinationer i regelsættet, fjernede eller spærrede programmer på betjeningsstationerne og dokumentation fra fortegnelsen over enhedernes software. En lille virksomhed håndterer dette med en programspærring på HMI-stationen og en regel om at udgående mailtrafik og webtrafik fra maskinnetværket afvises.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.3 RE 1 **Sådanne tjenester til kommunikation mellem personer forhindres i hele automationsnetværket, ikke blot begrænset delvist eller til enkelte enheder. Kræves fra SL 2 og opefter.**

Det taler for: Dokumentation for at spærringen gælder hver enhed i zonen, for eksempel gennem en gennemgang af den installerede software på hver computer i zonen og en forbindelsestest fra en vilkårlig anlægscomputer. Små virksomheder dokumenterer dette med en enhedsliste hvor hver række er kvitteret med kontroldatoen, og et skærmbillede af det mislykkede forbindelsesforsøg.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 5.4 **Applikationsdata og applikationsfunktioner er opdelt, så processer med forskelligt beskyttelsesbehov eller forskellige rettigheder ikke kan nå de samme områder. Adskillelsen er indbygget i systemarkitekturen og overlades ikke til tilfældigheder ved installationen.**

Det taler for: Oversigt over applikationerne med angivelse af hvilke data og tjenester de bruger, og hvilke konti der står bag dem, konfiguration af adskilte instanser, databaser, kataloger eller virtuelle maskiner og en rettighedsliste for hvert område. En lille virksomhed løser dette med adskilte brugerkonti og adskilte datamapper til projektering og drift samt en note om hvilken applikation der tilgår hvilken mappe.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

10 FR 6: Rettidig reaktion på hændelser 3

SR 6.1 **De logregistreringer der samles i systemet, kan læses og analyseres af de personer og roller der er autoriseret til det, uden at anlæggets løbende drift forstyrres, og adgangen til disse registreringer er selv begrænset til autoriserede brugere.**

Det taler for: En matrix over roller og rettigheder der viser hvem der må se logdata, samt et skærmbillede eller en eksport af en logvisning der faktisk er hentet, forsynet med tidsstempel. Dertil en kort note om den vej der blev brugt til hentningen, for eksempel styreenhedens betjeningsgrænseflade, en logserver eller en fileksport. Små virksomheder klarer sig med en oversigt på én side for hvert anlæg: hvor loggen ligger, hvem der har læseadgang, hvordan den hentes. En prøvehentning én gang om året, registreret i vedligeholdelsesjournalen, viser at vejen virker. Gælder fra SL 1 og opefter for alle sikkerhedsniveauer.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 6.1 RE 1 **Logregistreringerne kan hentes gennem en maskingrænseflade, så analyseværktøjer kan behandle dem videre uden manuel genindtastning, og data leveres i et dokumenteret, almindeligt anvendt format.**

Det taler for: En beskrivelse af den anvendte grænseflade sammen med formatet, for eksempel syslog, OPC UA Alarms and Conditions, en REST-forespørgsel eller en CSV-eksport, samt en eksempelregistrering og konfigurationen af det modtagende system. Dokumentationen kan være et udtræk fra konfigurationen af SIEM eller logopsamleren sammen med bevis for indgåede registreringer. Uden et SIEM rækker en logopsamler på en enkel server der henter loggene om natten med et script og gemmer dem; selve scriptet plus en mappevisning over de indsamlede filer er dokumentationen. Som forstærkning kræves dette først fra SL 3 og opefter, ikke fra SL 1.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 6.2 **Sikkerhedsrelevant aktivitet i systemet overvåges løbende, overvågningen opdager forsøg på angreb og misbrug og melder dem hurtigt til et navngivet kontaktpunkt, og de værktøjer, meldeveje og ansvar der bruges til dette, er fastlagt.**

Det taler for: En oversigt over overvågningsværktøjerne i hver zone, for eksempel en netværkssensor, antivirusalarmer, firewallalarmer eller integritetskontrol, med angivelse af hvem der modtager alarmen, og inden for hvilken tidsramme en reaktion forventes. Alarmkonfigurationer, en liste over alarmer fra de seneste måneder og noterne om håndteringen af dem tjener som dokumentation. Små virksomheder behøver ikke et døgnbemandet kontrolrum: en fælles postkasse eller sagsindbakke der samler alarmerne fra de eksisterende systemer, plus en fast regel om at en navngiven person gennemser den hver arbejdsdag, er tilstrækkelig og dokumenteres gennem postkassens historik. Kræves fra SL 2 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

11 FR 7: Ressourcernes tilgængelighed 13

SR 7.1 **Ved overbelastning eller bevidste oversvømmelsesangreb forbliver systemet i en fastlagt driftstilstand, de væsentlige styrefunktioner kører videre, og svigt af en enkelt tjeneste trækker ikke anlægget med sig.**

Det taler for: Konfiguration af beskyttelsesmekanismerne (hastighedsbegrænsning, forbindelsesgrænser, styring af broadcaststorme på switchene), leverandørudsagn om adfærd under belastning samt en registrering af en belastningstest eller af en reel overbelastningshændelse med observation af styrefunktionen. Kræves fra SL 1 og opefter. En lille virksomhed dækker dette med skærmbilleder af indstillingerne i switch og firewall og en kort note om hvilken funktion der kørte videre under en test af den vigtigste celle.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.1 RE 1 **Den kommunikationsbelastning som enkelte komponenter kan sende ind i netværket, er begrænset med et loft, så en fejlbehæftet eller kompromitteret komponent ikke kan oversvømme netværkssegmentet.**

Det taler for: Grænser for båndbredde og multicast for hver port på netværkskomponenterne, dokumentation for loftet for hver forbindelse samt en måling af den faktiske grundbelastning for hver enhed. Kræves fra SL 2 og opefter, ikke fra SL 1. Uden administrerbare switche kan denne linje ikke dokumenteres, og det er så det åbne punkt.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.1 RE 2 **En overbelastningssituation inde i det betragtede system breder sig ikke til tilstødende systemer eller netværk, og virkningen udad er teknisk indkapslet.**

Det taler for: Regler for segmentering og filtrering ved grænserne, dokumentation for at udgående trafik er begrænset med et loft, samt en testprotokol der viser at en belastning skabt i cellenetværket ikke forringede kontornetværket eller nabonetværket. Kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.2 **Brugen af behandlingstid, hukommelse, lagerplads og netværksbåndbredde er afgrænset, så en enkelt proces eller tjeneste ikke kan opbruge de ressourcer der er nødvendige for styringen.**

Det taler for: Konfiguration af ressourcegrænserne (kvoter, procesprioriteter, hukommelsesgrænser), analyse af udnyttelsesovervågningen over en repræsentativ periode samt de grænseværdier hvor en advarsel udløses. Kræves fra SL 1 og opefter. Små virksomheder bruger de indbyggede midler i operativsystemet og enkel overvågning med en advarsel om diskplads og CPU via e-mail.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.3 **Der findes sikkerhedskopier af systemkonfigurationerne, applikationsdata og programversionerne, de kan fremstilles uden at afbryde den løbende drift og er beskyttet mod uautoriseret adgang og ændring.** Dokument

Det taler for: Koncept for sikkerhedskopiering med omfang, hyppighed og opbevaringsperiode, sikkerhedskopilogge fra de seneste kørsler samt dokumentation for adgangsbeskyttelsen af sikkerhedskopimedierne (separat opbevaring, kryptering, egne rettigheder). Kræves fra SL 1 og opefter. En lille virksomhed sikkerhedskopierer PLC-projekter og HMI-versioner til et krypteret medie, der fysisk kobles fra efter sikkerhedskopieringen, og registrerer dato og version i en enkel liste.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.3 RE 1 **Sikkerhedskopiernes brugbarhed er verificeret, og det er dokumenteret at en fungerende tilstand faktisk kan genetableres ud fra dem.**

Det taler for: Registrering af en genetableringstest med dato, den afprøvede sikkerhedskopiversion, målsystem og resultat, mindst for de kritiske komponenter. Kræves fra SL 2 og opefter, ikke fra SL 1. Små virksomheder kontrollerer stikprøvevis ét PLC-program og ét HMI-systemaftryk på en reserveenhed én gang om året og registrerer resultatet i to sætninger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.3 RE 2 **Sikkerhedskopieringen kører automatisk efter en fastlagt tidsplan, og en mislykket kørsel opdages og rapporteres.**

Det taler for: Tidsplan for sikkerhedskopieringsjobbet, udførelseslogge uden huller samt dokumentation for fejlmeddelelsen ved en kørsel der ikke lykkedes (alarm, sag, mail). Kræves fra SL 3 og opefter.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.4 **Efter en forstyrrelse, et svigt eller et angreb kan systemet føres tilbage til en kendt, sikker tilstand, genetableringen er øvet, og de ansvarlige er navngivet.** Dokument

Det taler for: Genstartsplan for hver kritisk komponent med rækkefølge, nødvendige medier, kontaktpersoner og den tilstræbte tid sammen med registreringen af den seneste genetableringsøvelse. Kræves fra SL 1 og opefter. En lille virksomhed klarer sig med et genstartskort på én side for hver linje, opbevaret i styretavlen og kontrolleret hver gang en reservedel udskiftes.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.5 **Svigter den normale strømforsyning, går systemet i en fastlagt tilstand: enten opretholdes forsyningen af en nødkilde, eller der sker en ordentlig nedlukning uden tab af den sikre tilstand.**

Det taler for: Dokumentation for dimensionering og vedligeholdelse af den uafbrydelige strømforsyning eller nødgeneratoren, testprotokol fra den seneste batteritest eller belastningstest samt en beskrivelse af adfærden ved omskiftning og ved netstrømmens tilbagekomst. Kræves fra SL 1 og opefter. Små virksomheder tester UPS under belastning én gang om året og registrerer testdato, batteridriftstid og batteriets alder.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.6 **Systemets indstillinger for netværk og sikkerhed er fastlagt til en godkendt måltilstand, afvigelser fra denne måltilstand kan opdages, og den aktuelle tilstand kan hentes til enhver tid.** Dokument

Det taler for: Godkendt målkonfiguration for hver enhedsklasse (hærdningsspecifikation), enhedernes aktuelle konfigurationstilstande samt resultatet af en sammenligning af mål og faktisk tilstand med en liste over afvigelser og begrundelsen for hver af dem. Kræves fra SL 1 og opefter. En lille virksomhed gemmer konfigurationseksporterne i versionsstyring og sammenligner dem før og efter hver ændring.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

SR 7.6 RE 1 **Den aktuelle tilstand af sikkerhedsindstillingerne kan udlæses i maskinlæsbar form, så den automatisk kan kontrolleres mod måltilstanden.**

Det taler for: Eksempeluddata i et maskinlæsbart format (konfigurationseksport, struktureret fil, forespørgsel via grænseflade) og det script eller værktøj der udfører sammenligningen med måltilstanden, sammen med resultatrapporten fra én kørsel. Kræves fra SL 3 og opefter.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 7.7 **Systemet er begrænset til de funktioner der er nødvendige for driften, og tjenester, porte, protokoller og grænseflader der ikke er nødvendige, er deaktiveret eller fjernet.**

Det taler for: Liste over aktive tjenester og åbne porte for hver komponent med en begrundelse for behovet, dokumentation for at de øvrige er deaktiveret (konfiguration, resultat af portscanning) samt en regel for USB og vedligeholdelsesgrænseflader. Kræves fra SL 1 og opefter. Små virksomheder kører en enkel portscanning for hvert segment og begrunder hvert åbent punkt på én linje.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

SR 7.8 **En aktuel fortegnelse over alle systemkomponenter med fabrikat, type, firmwareversion eller softwareversion og netværksadresse foreligger og holdes opdateret ved ændringer.** Dokument

Det taler for: Komponentfortegnelse med revisionsdato og ejer, dokumentation for vedligeholdelsen via ændringshistorikken samt en sammenligning med en netværksscanning for at finde enheder der ikke er registreret. Kræves fra SL 2 og opefter, ikke fra SL 1. En lille virksomhed fører fortegnelsen som en tabel og opdaterer den som fast regel hver gang en enhed udskiftes, og hver gang firmware opdateres.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse