IEC 62443: en gjennomgang

Seks artikler gjennom den internasjonale standarden for cybersikkerhet i industrielle styringssystemer — fra grunnleggende terminologi til systemdesign, OEM-forpliktelser, NIS2-kartlegging, og en enkeltsides dokumentasjons-pakke.

Versjon 1.0.0 – 2026-05-18
DOI: 10.5281/zenodo.20276993

Seks artikler gjennom IEC 62443 — den internasjonale standarden for cybersikkerhet i industrielle styringssystemer — fra grunnleggende terminologi til systemdesign, OEM-forpliktelser, NIS2-kartlegging, og en enkeltsides dokumentasjons-pakke.

Rajesh Khanikar
ORCID: 0009-0008-8976-4491
Versjon 1.0.0 — 2026-05-18

DOI: 10.5281/zenodo.20276993 (denne versjonen)
Kanonisk: https://khanikar.com/no/series/iec-62443/

Slik siteres pakken:

> Khanikar, R. (2026). *IEC 62443: en gjennomgang* (Versjon 1.0.0). https://doi.org/10.5281/zenodo.20276993. Lisensiert under CC BY 4.0.

Denne pakken er redaksjonell veiledning for tekniske og innkjøps-rettede lesere. Den utgjør ikke juridisk, regulatorisk eller profesjonell rådgivning; forfatteren er verken advokat, revisor eller sertifiseringsorgan. Innholdet leveres uten noen form for garanti, uttrykkelig eller underforstått — ingen garanti for nøyaktighet, fullstendighet, tidsmessighet eller egnethet for noen bestemt produktlinje, noe prosjekt eller noen jurisdiksjon. Leserne må verifisere mot primærkildene — IECs publiserte standarder — og konsultere kvalifiserte fagfolk før de handler på grunnlag av noe i pakken. IEC-standardene er den kanoniske teksten; denne pakken reflekterer deres innhold på publiseringstidspunktet ovenfor, men standardene kan ha blitt endret siden. Forfatteren påtar seg intet ansvar for beslutninger, handlinger eller unnlatelser gjort i tillit til dette innholdet.

Rettelser, errata, og substansielle uenigheter tas gjerne imot på linkedin.com/in/rajeshkhanikar.

Contents

1. IEC 62443-1-x: ordene alle krangler om
2. IEC 62443-2-x: forvaltningssystemet bak et sikkert industrianlegg
3. IEC 62443-3-2 og 3-3: hva anleggseiere og integratorer må bevise
4. IEC 62443-4-1 og 4-2: hva en OEM faktisk må bevise
5. Kartlegging av IEC 62443-kontroller mot NIS2 Artikkel 21-tiltak
6. IEC 62443-bevismappe: enkeltsides versjon

IEC 62443-1-x: ordene alle krangler om

14. mai 2026 · 27 min lesetid · #compliance #security #industrial #iec-62443

To personer sto ved siden av et 33 kV-koblingsanlegg på et 220 MW solkraftverk i fjor høst, begge med samme revisjonssjekkliste, begge flytende i samme standard, og begge fullstendig forbi hverandre. Sertifiseringsorganets hovedrevisor sa at inverter-SCADA-en «trengte SL 3». Integratorens prosjektleder svarte, rolig, «vi er allerede SL 3 — komponentene er sertifisert». Anleggets OT-ingeniør, som måtte leve med det de ble enige om, stilte det eneste spørsmålet som betydde noe: «SL 3 av hva? Mål, oppnådd eller kapabilitet? For hvilken sone?»

Det er den samtalen `IEC TS 62443-1-1:2009` ble skrevet for å forhindre. Den klarer som regel ikke å forhindre den — ikke fordi standarden er dårlig, men fordi nesten ingen på et reelt anlegg faktisk har lest den. De har lest et leverandørwhitepaper som siterte den, en NIS2-kartleggingstabell som omskrev den, eller en lysarkpresentasjon som blandet den sammen med `IEC 62443-3-3`. Vokabularet driver da, revisjonen knirker, og anleggseieren betaler for misforståelsen.

Denne teksten er en sakte, deliberat gjennomgang av **Del 1**-dokumentene i ISA/IEC 62443 -serien — fundamentgruppen. Dette er dokumentene som definerer hva alle andre deler av serien mener med IACS, sone, kanal, sikkerhetsnivå, grunnkrav, essensiell funksjon, anleggseier, integrator og så videre. Hvis du allerede har lest mine gjennomganger av IEC 62443-2-x , IEC 62443-3-2 og 3-3 eller IEC 62443-4-1 og 4-2 , er dette teksten som forklarer hvorfor de andre tekstene bruker så mye tid på å være forsiktige med ordvalg.

TL;DR

`IEC 62443-1-x` er **fundament**-gruppen i IEC 62443-serien. Den eneste dokumentet i denne gruppen som for tiden er publisert som et frittstående IEC-dokument på IEC Webstore er `IEC TS 62443-1-1:2009` (en teknisk spesifikasjon, utgave 1.0, fra juli 2009) og nyere `IEC TS 62443-1-5:2023` (teknisk spesifikasjon om sikkerhetsprofiler). Delene `1-2` (hovedordliste), `1-3` (samsvarsmålinger for systemsikkerhet) og `1-4` (IACS-sikkerhetslivssyklus og bruksområder) er fortsatt under utvikling av ISA99 / IEC TC65 WG10 — de er referert gjennom serien, men du kan ikke i dag kjøpe dem som ferdige dokumenter. Det faktum alene løser overraskende mange workshop-krangler. Alt nedenfor forklarer resten.

1. Seriekartet — hvor 1-x sitter, og hvilke andre deler som avhenger av det

IEC 62443-serien er organisert, formelt, i fire dokumentgrupper. ISA99-komiteen — som ko-publiserer med IEC TC65/WG10 — beskriver dem som:

- **Generelt (1-x):** terminologien, referansemodellen, det konseptuelle stillaset. Det er her `IEC 62443-1-1` lever.
- **Retningslinjer og prosedyrer (2-x):** hva en anleggseier-organisasjon må gjøre for å drive et program. `IEC 62443-2-1:2024` er det levende ankerpunktet her; `2-3`, `2-4` og det kommende `2-2` (for tiden `IEC PAS 62443-2-2:2025`) utdyper det.
- **System (3-x):** tekniske systemnivå-krav. `IEC 62443-3-2` er risikovurderings-/soneinndelings-standarden, `IEC 62443-3-3` er katalogen over systemkrav knyttet til de syv grunnkravene.
- **Komponent (4-x):** sikker utviklingslivssyklus for produktleverandører (`IEC 62443-4-1:2018`) og komponentnivå tekniske krav (`IEC 62443-4-2:2019`).

En nyere femte gruppe, **Profiler (6-x og den planlagte 5-x-familien)**, ble lagt til etter at IEC formelt utpekte serien som en horisontal standard i 2021 — som betyr at vertikalindustri-komiteer burde referere til 62443 i stedet for å skrive sine egne. Den horisontale utpekingen er grunnen til at `IEC TS 62443-1-5:2023` finnes: den spesifiserer ordningen som sektor-spesifikke profiler skrives og aksepteres etter.

Hvert senere dokument i serien peker tilbake til `IEC 62443-1-1` for definisjoner. Når `IEC 62443-3-3` skriver «SR 1.1 Human user identification and authentication … shall be capable of … Security Level 2», er ordet «Security Level» ikke definert der. Det er definert i `1-1`. Når `IEC 62443-2-1:2024` snakker om en «anleggseier» og en «tjenesteleverandør», er disse rollene definert i `1-1`. Når `IEC 62443-4-2` vurderer en komponent til SL-C 2 for FR3, sporer betydningen av grunnkrav, kapabilitet, nivå og komponent alle tilbake til `1-1`. Hele serien henger fra denne kroken.

Det har to praktiske konsekvenser. For det første — hvis du designer et program i dag, må du eie og lese `IEC TS 62443-1-1:2009`. Ikke sammendrag av den. Den faktiske PDF-en fra IEC Webstore, publikasjon 7029 . For det andre — du må akseptere at dokumentet er seksten år gammelt og at andre utgave fortsatt skrives. Noe av språket har beveget seg videre (serien snakker om «tjenesteleverandører» og «automasjonsløsninger» med mer presisjon nå), men definisjonene av soner, kanaler, SL-T/SL-A/SL-C og de syv FR-ene i `1-1` forblir de kanoniske inntil andre utgave kommer.

2. IACS, ICS, OT, ICS-cybersikkerhet — hva standarden faktisk sier

Dette er det første folk tar feil av, og det første `IEC 62443-1-1` definerer.

IACS — Industrial Automation and Control System. Dette er 62443-fagtermen. `IEC TS 62443-1-1:2009` definerer IACS bredt: en

samling av personell, maskinvare, programvare og retningslinjer involvert i drift av en industriell prosess, og som kan påvirke eller influere dens trygge, sikre og pålitelige drift. Avgjørende — **personell og retningslinjer er innenfor IACS-grensen.** Det er ikke «nettverket». Det er ikke «kontrollerne». Det er det driftende sosio-tekniske systemet. `IEC 62443-2-1:2024` forsterker dette — omfanget arver eksplisitt «den brede definisjonen og omfanget av hva som utgjør en IACS som beskrevet i `IEC TS 62443-1-1`».

ICS — Industrial Control System. Et snevrere begrep. Generelt brukt for å betegne kontrollteknologi-undersettet — PLS-er, DCS-er, SCADA, RTU-er, HMI-er, ingeniørarbeidsstasjonene og det industrielle nettverket som binder dem sammen. I den eldre `IEC TR 62443-3-1:2009` var språket «ICS» fordi begrepet predaterer den IACS-sentrerte omformuleringen. I moderne 62443-dokumenter er det foretrukne paraplybegrepet IACS, med ICS som dukker opp som et nær-synonym i referanser til kontrollteknologi-laget.

OT — Operational Technology. Ikke et IEC 62443-begrep. OT er begrepet brukt av NIST SP 800-82 Rev. 3 (september 2023) , hvis tittel er «Guide to Operational Technology (OT) Security». NIST definerer OT som «programmerbare systemer og enheter som samhandler med det fysiske miljøet (eller styrer enheter som samhandler med det fysiske miljøet)». Revisjon 3 utvidet omfanget fra den eldre «ICS»-innrammingen av revisjon 1 og 2 fordi bygningsautomasjon, transport, fysisk adgangskontroll og miljøovervåking ikke passet behagelig under «industriell». OT er supersettet av ICS og det nærmeste eksterne begrepet til IACS, men OT inkluderer ikke personell og prosedyrer — det gjør IACS.

ICS-cybersikkerhet / OT-cybersikkerhet / IACS-sikkerhet. Brukt om hverandre i praksis. Internt i 62443 er de alle «IACS-cybersikkerhet».

Argumentet dette løser: i revisjonen jeg nevnte, var spørsmålet «er ingeniør-laptopen del av systemet?» omstridt. Integratoren argumenterte nei — det er IT, ikke en inverter. Anleggseieren argumenterte ja — den programmerer inverterne. Standarden er enig med anleggseieren. Under `IEC 62443-1-1` er ingeniør-laptopen del av IACS-en fordi den påvirker trygg, sikker og pålitelig drift. Etiketten på dens aktiva-merke fritar den ikke.

I fornybar-energi-arbeid spesifikt betyr dette noe konstant. En solparks IACS inkluderer inverter-SCADA-en, meteorologi-stasjonens datavei, beskyttelsesreléene i 33 kV-koblingsanlegget, BESS batteristyringssystemet, nettverksutstyret i transformatorstasjonen, ingeniør-laptopene som O&M-teamet plugger inn månedlig og OEM-ens fjernsupport-VPN. Ingen av disse kan argumenteres ut av omfang på grunnlag av at de er «bare IT» eller «bare sikkerhet».

3. Referansemodellen (nivå 0-5) og hvordan den forholder seg til Purdue

`IEC TS 62443-1-1:2009` legger ut en hierarkisk referansemodell brukt gjennom serien. Den er informert av Purdue Enterprise Reference Architecture (PERA) fra Purdue Universitys PLAIC-program, men er ikke identisk med den. 62443-referansemodellen definerer funksjonelle nivåer — abstrakte bånd — som beskriver hvor aktiviteter sitter i automasjonshierarkiet.

Nivåene, slik de brukes på tvers av serien:

- **Nivå 0 — Prosess.** Det fysiske utstyret under kontroll: turbiner, transformatorer, invertere, ventiler, motorer, det faktiske utstyret som gjør arbeid.
- **Nivå 1 — Grunnkontroll.** Sensorer, aktuatorer, kontrollere (PLS-er, IED-er, motorkontrollere, BMS-kontrollere). Sanntid, deterministisk.

- **Nivå 2 — Område- / overordnet kontroll.** HMI-er, lokale SCADA-frontender, anleggshistorikkens innhentingslag. Operatørvendt, fortsatt sanntid-tilstøtende.
- **Nivå 3 — Sted- / driftkontroll.** Anleggnivå-systemer: site-historian, MES-ekvivalenter, ingeniørarbeidsstasjoner, anlegg-omfattende SCADA. Fortsatt innenfor IACS.
- **Nivå 3.5 — DMZ.** Den industrielle demilitariserte sonen. Meglet datautveksling mellom drift og virksomhetens enterprise. Ikke tilstede i den opprinnelige Purdue-modellen; lagt til i industriell cybersikkerhets-praksis og behandlet av 62443 som en sonegrense.
- **Nivå 4 — Forretningsplanlegging og logistikk på stedet.** ERP, MES proper, forretningssystemer på stedsnivå.
- **Nivå 5 — Enterprise.** Bedrifts-IT.

`IEC 62443-1-1` er nøye på ett punkt som nesten alle tar feil av: **nivåer er funksjonelle, ikke topologiske.** To enheter på samme fysiske VLAN kan sitte på forskjellige referansemodell-nivåer. En PLS på nivå 1 kan være i samme rom som en historian på nivå 3. Referansemodellen forteller deg hva enheten gjør, ikke hvor Ethernet-kabelen ender.

Forholdet til Purdue er derfor «kompatibelt, ikke identisk». Purdue ga oss den hierarkiske metaforen. 62443 la til sikkerhetssone-resonnement på toppen — soner trenger ikke følge Purdue-nivåer, selv om de i de fleste velkonstruerte anlegg ender med å gjøre det av veldig gode grunner.

Hvorfor dette betyr noe for fornybar-energi-anlegg: et moderne solparksted passer sjelden inn i lærebok-Purdue-diagrammet. Inverter-produsenter sender skytilkoblet telemetri direkte ut av nivå 1-enheter. BESS-systemer kommer ofte med sin egen muromringede sky på «nivå 3-ish» uten noensinne å passere en anleggshistorian.

Vindturbiner kobler seg gjennom OEM-fjernsupport-tunneler som bygger bro mellom nivå 1 og 5 og later som om de ikke gjør det. `IEC 62443-1-1` lar deg beskrive disse arkitekturene ærlig — etter sone og kanal, med eksplisitte referansemodell-nivåer for hver funksjon — uten å tvinge inn et rent Purdue-bilde som aldri har matchet virkeligheten.

4. Soner og kanaler — og hva som teller som en sonegrense

Det enkelt mest konsekvensrike paret av definisjoner i `IEC TS 62443-1-1:2009`:

- En **sikkerhetssone** er en gruppering av logiske eller fysiske aktiva som deler felles sikkerhetskrav.
- En **kanal** er en logisk gruppering av kommunikasjonskanaler — som deler felles sikkerhetskrav — som forbinder to eller flere soner.

Tre ting følger som fanger folk.

For det første — soner grupperes etter sikkerhets-krav, ikke etter topologi eller funksjon alene. En sone er hvilket som helst sett med aktiva du kan forsvarlig argumentere trenger samme beskyttelse, samme tillit, samme overvåking, samme tilgangsregime. To fysisk separerte vindturbinarrayer på forskjellige spenninger kan være én sone hvis de deler sikkerhetskrav. Én enkelt transformatorstasjons-kontrollbygning kan inneholde tre soner (reléebeskyttelse, stasjons-SCADA, telekom-gateway) hvis de funksjonene berettiger forskjellige beskyttelsesnivåer. Tommelfingerregelen jeg bruker i revisjoner: hvis to aktiva noen gang ville berettige forskjellige kontroller på dette stedets risikoregister — er de ikke i samme sone.

For det andre — kanaler er ikke «brannmuren». En kanal er en logisk konstruksjon: settet med kommunikasjonskanaler med felles

sikkerhetsbehov som krysser en sonegrense. Brannmuren, svitsjen, datadioden eller VPN-konsentratoren er en komponent av kanalen, ikke kanalen i seg selv. Det er derfor `IEC 62443-3-3`-krav gjelder kanaler så vel som soner: en kanal har SL-mål, kapabiliteter og et eget oppnådd nivå.

For det tredje — «tillitssone» er ikke det samme som «sikkerhetssone». En tillitssone (i IT zero-trust-forstand) er en grense der identitet og policy revurderes. En 62443-sikkerhetssone er en grense der sikkerhets-krav endres. De overlapper, men er ikke synonymer. Å si «vi har zero-trustet OT-nettverket, så vi trenger ikke soner» er en kategorifeil. 62443-sone-definisjonen gjelder fortsatt; zero trust er ett mulig middel for å håndheve kanalen mellom to soner.

En praktisk sonegrense-sjekkliste for et hybrid fornybart sted:

1. Hvor endres det cyber-fysiske risikoprofilet? (f.eks. å bevege seg fra inverterkontroll til batteritermisk styring til nettbeskyttelse)
2. Hvor endres populasjonen av brukere / leverandører / tjenesteleverandører?
3. Hvor varierer regulatoriske eller kontraktuelle forpliktelser (f.eks. nettkode-mandaterte systemer vs. eieroperasjonelle systemer)?
4. Hvor endres konsekvensen av kompromittering i art (inntekstap vs. sikkerhet vs. nettstabilitet)?

Hvert bekreftende svar er en kandidat-sonegrense. Hver er, ifølge `IEC 62443-1-1`, grunnlaget for en kanal.

Dette er inngangen som IEC 62443-3-2 forbruker når den ber om et partisjonert System under Consideration (SuC) med dokumenterte soner og kanaler. Resonnementet lever i `1-1`; metodikken lever i `3-2`; kontrollkatalogen anvendt på hver sone og kanal lever i `3-3`.

5. Sikkerhetsnivåer — SL-T, SL-A, SL-C og den ofte forvirrede SL 1-4 numeriske skalaen

Dette er seksjonen som, hvis jeg skrev denne posten for kun én person, ville vært hele posten.

`IEC TS 62443-1-1:2009` definerer et Sikkerhetsnivå som et mål på tillit til at en IACS er fri for sårbarheter og fungerer på tiltenkt måte. Den definerer deretter fire numeriske bånd:

- **SL 1** — beskyttelse mot tilfeldig eller utilsiktet brudd.
- **SL 2** — beskyttelse mot tilsiktet brudd med enkle midler, lite ressurser, generiske ferdigheter og lav motivasjon.
- **SL 3** — beskyttelse mot tilsiktet brudd med sofistikerte midler, moderate ressurser, IACS-spesifikke ferdigheter og moderat motivasjon.
- **SL 4** — beskyttelse mot tilsiktet brudd med sofistikerte midler, utvidede ressurser, IACS-spesifikke ferdigheter og høy motivasjon.

Disse fire nivåene beskriver trusselaktørs-kapabilitet. De beskriver ikke, alene, et anlegg, et produkt, en sone eller en kontroll.

Det neste trinnet er der alle tar feil. Serien definerer tre typer Sikkerhetsnivå, og den numeriske skalaen (1-4) gjelder hver:

- **SL-T (Target / Mål)** — sikkerhetsnivået en bestemt sone eller kanal trenger å oppnå basert på dens risikovurdering. SL-T velges, per-sone, per-FR, av anleggseieren i konteksten av IEC 62443-3-2 . Resultatet av risikovurdering er en SL-T-vektor — sju tall, ett per grunnkrav — for hver sone og hver kanal.
- **SL-C (Capability / Kapabilitet)** — sikkerhetsnivået en komponent eller et system er i stand til å oppnå når riktig konfigurert og integrert. SL-C er hva en produktleverandør erklærer om en enhet, testet mot IEC 62443-4-2 for komponenter eller `IEC 62443-3-3` for systemer. En sertifisert PLS kan være SL-C 2

på tvers av alle syv FR-er, eller SL-C 3 for FR1 og SL-C 2 for alt annet. Sertifikatet bærer vektoren.

- **SL-A (Achieved / Oppnådd)** — sikkerhetsnivået som-bygget, som-driftet sonen eller kanalen faktisk leverer i tjeneste. SL-A måles (eller estimeres) etter design, integrasjon, idriftsetting og driftsoverlevering. Det er, i praksis, hva revisjonsbeviset ditt skal bevise.

Kjeden standarden vil at du skal gå er derfor: **SL-T (fra risiko) → velg komponenter / system med tilstrekkelig SL-C → design og drift for å levere SL-A ≥ SL-T**. Hvis SL-A faller under SL-T, må du enten akseptere restrisiko, anvende kompenserende tiltak eller endre designet.

Dette er hvorfor revisor og integrator argumenterte forbi hverandre i åpningsscenen. Integratoren sa «vi er SL 3» og mente SL-C 3 for komponentene de leverte. Revisor sa «vi trenger SL 3» og mente SL-T 3 for sonen. Ingen hadde målt SL-A. En komponent med SL-C 3 sluppet inn i en sone med SL-T 3 produserer **ikke** automatisk SL-A 3 — det avhenger av konfigurasjon, integrasjon, de omkringliggende kompenserende tiltakene, og om driftspraksisene (dekket i IEC 62443-2-1:2024) faktisk opprettholder kapabiliteten.

Tre videre feller som vokabularet fortsatt ikke fullt løser:

- **SL er per grunnkrav, ikke en enkelt skalar.** Å si «vi er SL 2» uten en vektor på tvers av FR1-FR7 er, strengt tatt, ikke en 62443-uttalelse. Standarden forventer en tuppel. I praksis rapporterer mange programmer en enkelt dominerende verdi pluss unntak; det er forsvarlig hvis unntakene er oppført.
- **IACS-omfattende SL vs sone-SL.** Det finnes ikke noe slikt som en «IACS-omfattende SL» i `IEC 62443-1-1`. SL gjelder soner og kanaler. En IACS er en samling av soner, hver med sin egen SL-T-

vektor. Et enkelttall SL for et helt anlegg er en markedsføringsartefakt.

- **Modenhetsnivå (ML 1-4) er ikke Sikkerhetsnivå.** Modenhetsnivåer dukker opp i `IEC 62443-2-4` (tjenesteleverandør-krav) og `IEC TS 62443-6-1:2024` (vurderingsmetodikken for 2-4). ML måler modenheten til en prosess. SL måler sikkerhetsnivået til en sone, kanal, system eller komponent. De er forskjellige skalaer for forskjellige ting, og er ikke utskiftbare.

6. De syv grunnkravene (FR1-FR7)

`IEC TS 62443-1-1:2009` definerer syv grunnkrav. De er kolonnene i matrisen som resten av serien fyller inn.

1. **FR1 — Identification and Authentication Control (IAC).** Hvem eller hva ber om handling, og har de bevist det?
2. **FR2 — Use Control (UC).** Har de tillatelse til å gjøre den forespurte handlingen?
3. **FR3 — System Integrity (SI).** Opprettholdes integriteten til kode, data og konfigurasjon mot tilsiktet og utilsiktet endring?
4. **FR4 — Data Confidentiality (DC).** Er informasjon i hvile og i bevegelse beskyttet mot avsløring der det kreves?
5. **FR5 — Restricted Data Flow (RDF).** Er dataflyter partisjonert langs sone- og kanalgrenser?
6. **FR6 — Timely Response to Events (TRE).** Blir sikkerhetsrelevante hendelser oppdaget, logget, varslet og respondert på i tide?
7. **FR7 — Resource Availability (RA).** Holdes essensielle funksjoner tilgjengelige under stress, angrep eller degradering?

To viktige ting om FR-ene som vokabularet fortsatt snubler folk på.

FR-er er ikke kontroller. De er mål. `IEC 62443-3-3` dekomponerer dem i systemkrav (SR) og kravsforsterkninger (RE), og IEC 62443-4-2

dekomponerer dem igjen til komponentkrav (CR). Frasen «vi er i samsvar med FR3» er meningsløs alene — hva som er meningsfullt er «vi oppfyller SR 3.1 til 3.9 på SL-C 2 i sone X, med RE for 3.4 og 3.8 anvendt». Hvis en leverandørs datablad bare sier «i samsvar med FR3» uten SR / CR-detalj og uten SL-vektor, behandle det som markedsføringskopi.

Rekkefølgen av FR-ene er ikke en prioritetsrekkefølge. FR1 er ikke «viktigere» enn FR7. I OT er det motsatte ofte tilfelle: FR7 (ressurstilgjengelighet) og FR3 (systemintegritet) overgår ofte FR4 (datakonfidensialitet) i risikoregisteret. FR-ene er en oppregning, ikke en rangering.

De syv FR-ene er også dimensjonene i hver SL-vektor. Når en integrator overlater deg en `IEC 62443-3-3`-samsvarsmatrise for et system, bør det være et 7-kolonners rutenett tastet til FR1 til FR7 med en SL-C-verdi i hver celle. Når anleggseieren utleder SL-T fra `IEC 62443-3-2`, har utgangen samme form. Grunnen til å matche former er slik at SL-C og SL-T kan sammenlignes komponent-for-komponent.

7. Roller — anleggseier, systemintegrator, produktleverandør, tjenesteleverandør

`IEC 62443-1-1` introduserer rolle-taksonomien som resten av serien operasjonaliserer. Påfølgende ISA99-arbeid og ISAGCA Quick Start Guide skjerper disse til fire hovedroller:

- **Anleggseier.** Organisasjonen som er ansvarlig for IACS-en i drift. I fornybar er dette IPP-en, energiselskapet, asset management-selskapet — den som bærer drifts- og regulatorisk ansvar for anlegget. Anleggseier-vendte krav lever primært i IEC 62443-2-1:2024 .
- **Produktleverandør.** Organisasjonen som designer, utvikler og støtter et produkt — en komponent eller et system — brukt i IACS-en. Produktleverandører adresseres av IEC 62443-4-1:2018

(utviklingsprosess-krav) og IEC 62443-4-2:2019 (komponentnivå tekniske krav) .

- **Systemintegrator.** Organisasjonen som tar produkter fra leverandører og setter dem sammen til en automasjonsløsning for en anleggseier. Integratorer adresseres av `IEC 62443-2-4:2023` (sikkerhetsprogram-krav for IACS-tjenesteleverandører) i deres integrasjons-rolle, og av IEC 62443-3-2 og 3-3 der de utfører design og verifikasjon på vegne av anleggseieren.
- **Tjenesteleverandør.** Organisasjonen som drifter, vedlikeholder, overvåker eller på andre måter betjener IACS-en etter overlevering. `IEC 62443-2-4` dekker dem også — eksplisitt skille mellom integrasjons-tjenesteleverandører og vedlikeholds-tjenesteleverandører.

Vedlikeholds-tjenesteleverandør-rollen er den som er hyppigst usynlig i fornybar-kontrakter og den som forårsaker mest smerte i år-tre-revisjoner. OEM-en som leverer deg turbinene er en produktleverandør. EPC-en som bygde vindparken er en systemintegrator. O&M-leverandøren som kommer på sted hvert kvartal — og OEM-fjernsupport-teamet bak en VPN-tunnel — er en vedlikeholds-tjenesteleverandør, og `IEC 62443-2-4`-krav gjelder dem. Hvis O&M-kontrakten din er stille om cybersikkerhets-kapabilitetskrav, har du forskjøvet modenhetsrangeringen av programmet ditt ned. Det er et `IEC 62443-2-1`-problem forårsaket av et vokabularproblem fra `1-1`.

Argumentet dette vokabularet løser: når «leverandøren» gjør fjernsupport en søndagskveld for å gjenopprette en inverter, er det en produktleverandør-handling eller en tjenesteleverandør-handling? Svaret betyr noe fordi kravsettene er forskjellige. Under `IEC 62443-1-1` er det en tjenesteleverandør-handling (de utfører driftsarbeid på den som-bygde løsningen), og kontrakten din bør reflektere `2-4`-kapabilitetskrav.

8. Essensielle funksjoner og kompenserende tiltak

To flere `IEC 62443-1-1`-begreper som alle bruker sløvt.

Essensiell funksjon. En funksjon hvis driftsstans, eller drift i degradert tilstand, kan forårsake uakseptabel konsekvens for sikkerhet, integritet eller tilgjengelighet. I et solparkanlegg inkluderer essensielle funksjoner: beskyttelse-utløsning ved 33 kV / HV-grensesnittet, BESS termisk runaway-nedstengning, primær frekvensrespons (hvis stedet leverer systemtjenester), og de sikkerhetsrelaterte kontrollene av eventuelt høyspentkoblingsanlegg. Essensiell funksjon er ikke det samme som viktig funksjon. Listen er «tap er uakseptabelt», ikke «tap er upraktisk». `IEC 62443-3-3` sier eksplisitt at visse SR-er gjelder strengere der essensielle funksjoner står på spill — for eksempel lener krav rundt tjenestenekt-toleranse seg tungt på essensiell-funksjon-konseptet.

Den praktiske konsekvensen: når du tegner sonediagrammet for IEC 62443-3-2 , må hver essensielle funksjon ende opp identifisert og sporbar til en sone. SL-T for den sonen blir deretter påvirket av konsekvensen av kompromittering av den essensielle funksjonen. En sone som bare er vert for «viktige» funksjoner kan ha en lavere SL-T enn en som er vert for essensielle funksjoner.

Kompenserende tiltak. En kontroll anvendt fordi den iboende kontrollen ikke kan implementeres eller er upraktisk. Standardens logikk er: hvis du ikke kan oppfylle en SR direkte inne i en sone, kan du anvende et kompenserende tiltak andre steder (ofte i den omkringliggende kanalen, eller med prosedyremessige midler) forutsatt at du kan argumentere for at restrisikoen er ekvivalent. Kompenserende tiltak er ikke «vi droppet det fordi det var vanskelig». De er dokumentert, begrunnet og sporbart. Et rimelig eksempel: en eldre inverter-kontroller som ikke kan håndheve sterk menneskelig-bruker-autentisering direkte (FR1 / SR 1.1) kan kompenseres med en jump host inne i kanalen, pluss en admin-

prosedyre som beviser hvilken navngitt person brukte hvilken økt — forutsatt at den kompensasjonen er dokumentert, testet og gjennomgått ved frekvensen sikkerhetsprogrammet krever.

Argumentet dette løser: når et anskaffelses-team skriver «systemet skal samsvare med `IEC 62443-3-3` SL 2 på tvers av alle FR-er uten unntak», har de skrevet et anskaffelseskrav som kanskje er umulig å tilfredsstille med feltutstyret som fysisk eksisterer. Standarden forventer unntak, forventer kompenserende tiltak, og forventer at de argumenteres på papir. Å kjøpe som om kompenserende tiltak var et tegn på svakhet snarere enn en normal utgang av design er i seg selv en feillesning av `IEC 62443-1-1`.

9. Sikkerhetslivssyklusen (fra 1-4) — vurder, design, implementer, vedlikehold

`IEC TR 62443-1-4` — IACS security lifecycle and use cases — er en teknisk rapport, fortsatt under utvikling på ISA99 / IEC TC65 WG10-nivået. Utkast har sirkulert i komiteen siden rundt 2013. Det er ment å gi en detaljert beskrivelse av den underliggende livssyklusen som resten av serien antar, med bearbeidede bruksområder. Det er ikke, per skrivende stund, et ferdig IEC-dokument på IEC Webstore . Det som er publisert — og bredt sitert — er ISAGCA Security Lifecycles-whitepaperet fra ISA's Global Cybersecurity Alliance, som fanger samme konseptuelle innhold i påvente av den formelle TR-en.

Livssyklusen serien bruker har fire brede faser:

1. **Vurder.** Risikovurdering, definisjon av SuC, soneinndeling og kanal-partisjonering, utleding av SL-T per sone og kanal per FR. Dette er hjemmet til IEC 62443-3-2 og inngangspunktet for ethvert nytt prosjekt eller større modifikasjon. IEC 62443-2-1:2024 gjør vurderingsfase-aktiviteter til et programkrav for anleggseiere.
2. **Design og implementer.** Valg av produkter og integratorer med tilstrekkelig SL-C mot SL-T, design av kompenserende tiltak,

fabrikkakseptansetest (FAT) og site-akseptansetest (SAT) inkludert cybersikkerhets-testtilfeller, idriftsetting. `IEC 62443-3-3` er designverifikasjons-referansen; IEC 62443-4-2 er komponentvalgs-referansen; `IEC 62443-2-4` er integrator-kapabilitets-referansen.

3. **Drift og vedlikehold.** Oppdateringsstyring, kontohygiene, overvåking, hendelsesrespons, periodisk re-vurdering, leverandørkjede-kontroller for vedlikeholds-tjenesteleverandører. IEC 62443-2-1:2024 er driftsfase-referansen. `IEC TR 62443-2-3:2015` dekker oppdateringsstyring.
4. **Avvikle.** Sikker håndtering av legitimasjon, konfigurasjoner, avviklede aktiva, restdata. Ofte den mest forsømte fasen. Vedlikeholdsdokumentasjonen sier «avvikle per OEM-instruksjoner» og OEM-instruksjonene er stille om cybersikkerhet.

Livssyklusen i `1-4` og ISAGCA's whitepaper er ikke lineær. Den er skjæringspunktet av tre livssykluser: produktlivssyklusen (eid av produktleverandører), automasjonsløsnings-livssyklusen (eid av integratorer) og driftslivssyklusen (eid av anleggseiere og tjenesteleverandører). Hvor de krysser hverandre er der kontrakter, bevis og overleveringer lever. Det er derfor cybersikkerhet for fornybar-energi-anlegg er så kontraktdrevet: livssyklusmodellen i `1-4` er den eneste måten å kartlegge hvem som må bevise hva til hvem ved hvilken milepæl.

Argumentet dette løser: «vi gjorde `IEC 62443-3-2` i designfasen, så vi er i samsvar». Nei — `3-2` er én aktivitet i vurderingsfasen. Livssyklusen fortsetter de neste tjue årene. Et soneinndelings-dokument fra 2024 er foreldet innen 2028 med mindre det re-valideres. Livssyklus-innrammingen i `1-4` er det som tvinger den kontinuerlige re-valideringen inn i kontrakten.

10. Målinger (1-3) — hva «samsvarsmåling» forsøker og hvorfor det er vanskelig

`IEC 62443-1-3` — System security conformance metrics (noen ganger skrevet som «compliance metrics» i eldre komiteekorrespondanse; den publiserte tittelen bruker conformance) — er under utvikling som en teknisk rapport. Dens mål: definere en metodikk for å utlede kvantitative målinger fra prosess- og tekniske krav som resten av serien spesifiserer. I klart språk — gjøre «samsvar med `3-3` SR 1.1 på SL-C 2» til et tall du kan måle, rapportere og spore.

Dette er vanskeligere enn det høres ut, og grunnene til at det er vanskelig er verdt å være ærlig om:

- **De fleste 62443-kravene er kapabilitetsuttalelser, ikke målinger.** «Systemet skal være i stand til menneskelig-bruker-identifikasjon og autentisering» er binært ved første øyekast, men kapabilitet under forskjellige driftsforhold er det ikke. Teller en kapabilitet som krever manuell konfigurasjon? Bare når konfigurert? Bare når revidert?
- **SL er ikke en måling, det er et nivå.** Å gjøre et nivå til en måling krever å bestemme hvilken andel av krav på det nivået må oppfylles, med hvilket bevis, ved hvilken frekvens. Forskjellige organisasjoner har forskjellige svar, og standarden er med rette tilbakeholden med å mandatere ett universelt svar.
- **Anleggseiere vil ha tidsserie-målinger.** «Hvordan trender vår 62443-posisjon kvartal mot kvartal?» er et helt rimelig executive-spørsmål. 62443-rammeverket, født fra ingeniør- snarere enn informasjonssikkerhets-styring, har historisk vært bedre på punkt-i-tid-samsvar enn på tidsserie-telemetri.
- **`IEC 62443-2-2` overlapper.** Protection Scheme (SPS)-arbeidet i nåværende `IEC PAS 62443-2-2:2025` introduserer sikkerhetsprogram-vurderinger (SPR) som gir et relatert men separat

målerammeverk. Forholdet mellom `1-3`-målinger og `2-2`-SPR-er har vært et aktivt område for komitéarbeid.

Inntil `1-3` lander som en publisert TR, bygger anleggseiere sine egne målinger. Rimelige valg inkluderer: prosent av soner med aktuell `3-2`-dokumentasjon; prosent av komponenter med SL-C ≥ SL-T per FR; prosent av vedlikeholds-tjenesteleverandører med dokumentert `2-4`-kapabilitet; gjennomsnittlig tid fra CVE-publikasjon til patch-verifikasjon; prosent av essensielle funksjoner med testede tilbakefall-prosedyrer. Ingen av disse er 62443-mandatert, men hver er forsvarlig og sporbar til et `1-1`-konsept.

Argumentet dette vokabularet løser: når ledelsen spør «er vi 62443-samsvarende — ja eller nei?» kan du korrekt svare «serien fungerer ikke slik». `IEC 62443-1-1` definerer ikke en enkelt binær samsvarstilstand for en IACS. Den definerer roller, kapabiliteter, nivåer og soner, som hver kan vurderes. Et 62443-program i IEC 62443-2-1 kan være konformt. En komponent kan være SL-C-sertifisert. En sone kan ha en SL-A som møter dens SL-T. Anlegget som helhet er summen av disse uttalelsene, ikke et enkelt ja/nei. Å late som annet er det som produserer den uheldige salgspitchen «vi er 62443-samsvarende» — som vanligvis er kortform for «vi selger et produkt som noen sertifiserte en gang».

11. Argumentene dette vokabularet fortsatt ikke løser

For alt som `IEC TS 62443-1-1:2009` avgjør, gjenstår mange argumenter genuint åpne. Noen handler om at verden har beveget seg videre siden 2009; noen handler om hull andre utgave er ment å lukke; noen handler om steder der standarden er intensjonelt taus.

Sky og IIoT. `IEC 62443-1-1` ble skrevet før «skyen» var et rutinemessig utplasseringsmål for industriell telemetri. Hvor sitter AWS IoT Core på referansemodellen? Er det nivå 3? Nivå 4? Nivå 5? Er OEM-ens sky en sone av IACS-en i det hele tatt, gitt at anleggseieren ikke

driver den? Den kommende `IEC TR 62443-1-6` (Application of the ISA/IEC 62443 series to the Industrial Internet of Things) er ment å adressere nøyaktig dette. Inntil den lander, håndterer anleggseiere det fra sak til sak — oftest ved å behandle sky-endepunktet som en sone eid av en tjenesteleverandør med en definert kanal til den på-sted IACS-en.

Trådløst og 5G. Samme problem. Trådløse lenker er kanaler med særegne fysisklag-trusselsmodeller. Serien rommer dem bredt, men det praktiske spørsmålet om en 5G-slice er en kanal eller en sone er uavklart i publisert tekst.

Sikkerhet-cybersikkerhet-interaksjon. `IEC 61511` (funksjonell sikkerhet) og `IEC 62443` (cybersikkerhet) overlapper eksplisitt ved det sikkerhetsinstrumenterte systemet. Der sikkerhetslivssyklusen og cybersikkerhets-livssyklusen er uenige — for eksempel på oppdatering av sikkerhets-PLS-er — forsoner standardene seg ikke perfekt. Nylig ISAGCA-arbeid og `IEC TR 63069:2019` gir delvis veiledning. Argumentet fortsetter i reelle revisjoner.

Horisontal utpeking og sektorprofiler. 2021-utpekingen av 62443 som en horisontal standard betyr at vertikalsektor-komiteer burde referere den snarere enn å omdefinere dens begreper. `IEC TS 62443-1-5:2023` formaliserer ordningen for sektorprofiler. Men innholdet i sektorprofiler for fornybar energi, vann, bygningsautomasjon, medisinsk utstyr og så videre skrives fortsatt, og betydningen av «SL-T 2» på et sykehus skiller seg materielt fra «SL-T 2» på en vindpark. Vokabularet holder; kalibreringen skiller seg.

Andre utgave av 1-1. En andre utgave har sirkulert for komitégjennomgang siden 2021. Den vil raffinere noen definisjoner, legge til ontologi-drevet presisjon (WG5TG3-konsistens-arbeidsgruppen har gjort betydelig arbeid på dette) og reflektere lærdommer fra resten av serien. Inntil den er publisert, er `IEC TS 62443-1-1:2009` den autoritative referansen, og det er en viss risiko for at

samvittighetsfulle lesere finner lokal divergens mellom 2009-teksten og nyere deler.

Mandatorisk eller ikke? `IEC 62443` er ikke, alene, en lov noe sted. Det europeiske NIS2-direktivet navngir «europeiske standarder og spesifikasjoner relevante for sikkerheten til nettverks- og informasjonssystemer» — og `IEC 62443` er bredt sitert som den mest-relevante referansen for OT-omfanget, men direktivet mandaterer ikke 62443 med dokumentnummer. Norge, hvor jeg arbeider, transponerer NIS2 med tilsvarende slingringsmonn. EU Cyber Resilience Act pålegger bindende cybersikkerhets-essensielle krav på produkter med digitale elementer; harmoniserte standarder under CRA vil lene seg tungt på 62443-4-1 og 4-2, men igjen, dokumentnummer er ikke i den juridiske teksten. For fornybar-energi-operatører i Europa er det praktiske svaret: 62443 er frivillig ved navn, men funksjonelt påkrevd av anskaffelse, forsikring, regulator-forventning og leverandørkjede-press. Se mine gjennomganger om NIS2-anvendbarhet og CRA-anvendbarhet for detaljene.

Røde flagg i samtale

En kort feltguide. Disse er frasene som, når jeg hører dem i en workshop eller en revisjon, forteller meg at den som snakker ikke nylig har lest `IEC TS 62443-1-1:2009` og sannsynligvis ikke har lest den i det hele tatt.

- **«Vi er SL 3-samsvarende.»** Samsvarende mot hva? Mål, kapabilitet eller oppnådd? For hvilken sone? For hvilke FR-er? På hvilket bevis? Uten de kvalifikatorene er det en markedsføringsfrase.
- **«Hele anlegget er SL 2.»** Det finnes ingen anlegg-omfattende SL i `IEC 62443-1-1`. SL gjelder soner og kanaler.

- **«OT og IACS er samme sak.»** De overlapper, men OT (per NIST SP 800-82r3) er et bredere begrep og ekskluderer personell- og prosess-omfanget som `IEC 62443-1-1` inkluderer i IACS. De er ikke synonymer.
- **«FR3 er en kontroll vi implementerte.»** FR3 er et grunnkrav — et mål. Kontroller er SR, RE og CR under det. Hvis noen kaller en FR en kontroll, har de hoppet over et nivå av standarden.
- **«PLS-en vår er 62443-sertifisert.»** Mot hvilken del? `4-1`? `4-2`? Ved hvilken SL-C? På tvers av hvilke FR-er? «62443-sertifisert» er ikke en spesifikasjon.
- **«Soner er bare VLAN-er.»** Soner er grupperinger etter felles sikkerhetskrav. VLAN-er er én mulig håndhevelses-mekanisme for kanalen mellom soner. De to konseptene er på forskjellige abstraksjonsnivåer.
- **«Vi trenger ikke kompenserende tiltak, vi er fullt samsvarende.»** Et 62443-design med ingen dokumenterte kompenserende tiltak på et reelt industrielt sted er nesten alltid ønsketenkning, ikke grundighet.
- **«`IEC 62443-1-1` er bare definisjoner, vi kan hoppe over den.»** Den definerer hvert begrep resten av serien hviler på. Å hoppe over den er hvordan revisjonssamtalen i åpningsscenen til denne posten skjer.
- **«Integratoren overleverte et SL-T-dokument, så vi er ferdige.»** SL-T er inngangen til design, utledet fra risiko. SL-A er hva du må måle etter idriftsetting og måle på nytt gjennom livssyklusen. SL-T alene beviser intensjon, ikke leveranse.
- **«Modenhetsnivå 3 er lik sikkerhetsnivå 3.»** De er forskjellige skalaer for forskjellige objekter. ML måler prosessmodenhet; SL måler sone-, kanal-, system- eller komponent-sikkerhet.

Hvert av disse røde flaggene peker tilbake til en seksjon av `IEC 62443-1-1`. Botemiddelet er sjelden å krangle høyere; det er å åpne

dokumentet og lese den relevante definisjonen sammen. Vokabularet, når delt, fjerner omtrent to tredjedeler av uenighetene som forbruker revisjonstid.

FAQ

Hva er IEC 62443-1-1?

`IEC TS 62443-1-1:2009` er fundament-teknisk-spesifikasjonen for IEC 62443-serien. Publisert av IEC i juli 2009 (utgave 1.0), den definerer terminologien, konseptene og referansemodellene som resten av serien bruker — inkludert IACS, soner, kanaler, sikkerhetsnivåer (SL-T, SL-A, SL-C), de syv grunnkravene (FR1-FR7) og hovedrollene (anleggseier, produktleverandør, integrator, tjenesteleverandør). Den er tilgjengelig fra IEC Webstore som publikasjon 7029 . En andre utgave har vært i komitégjennomgang ved ISA99 / IEC TC65 WG10 siden 2021.

Hva er forskjellen mellom SL-T og SL-C?

SL-T (Target / Mål) er sikkerhetsnivået en bestemt sone eller kanal trenger å oppnå, utledet fra risikovurdering under IEC 62443-3-2 . SL-T er en anleggseier-utgang: den sier «denne sonen trenger SL 3 på tvers av disse FR-ene på grunn av risikoprofilet her». **SL-C (Capability / Kapabilitet)** er sikkerhetsnivået en komponent eller et system er i stand til å oppnå når riktig konfigurert. SL-C er en produktleverandør-utgang, sertifisert mot IEC 62443-4-2 (komponenter) eller `IEC 62443-3-3` (systemer). En komponent med SL-C 3 sluppet inn i en sone med SL-T 3 leverer ikke automatisk SL-A (Oppnådd) 3 — det avhenger av konfigurasjon, integrasjon, kompenserende tiltak og driftspraksis.

Er IEC 62443 mandatorisk?

Alene, nei. `IEC 62443` er en frivillig internasjonal standardserie, ikke lovgivning. Imidlertid refereres den eller stoles på av en voksende liste av rammeverk som er bindende — EU NIS2-direktivet, EU Cyber

Resilience Act, sektorregulatorer og nasjonale transponeringer i land inkludert Norge. Anskaffelseskontrakter, forsikringskrav og leverandørkjede-forventninger siterer i økende grad spesifikke deler (vanligvis `IEC 62443-2-1`, `3-3`, `4-1` og `4-2`). Det praktiske svaret for en anleggseier i kritisk infrastruktur er: ikke mandatorisk ved navn, men veldig ofte mandatorisk gjennom tingene som er mandatoriske. Se mine poster om NIS2-anvendbarhet og CRA-anvendbarhet for hele resonnementkjeden.

Hvorfor er ikke IEC 62443-1-2 (hovedordlisten) tilgjengelig?

Fordi den, fra 2025-2026, fortsatt er under utvikling ved ISA99 / IEC TC65 WG10. ISAGCA Structuring the ISA/IEC 62443 Standards-skrivet bemerker at `1-2` «is a master glossary of terms and abbreviations used throughout the series» og at komiteen planlegger å levere den i et online-format. Inntil den publiseres som et ferdig IEC-dokument, forblir de autoritative definisjonene de gitt inne i `IEC TS 62443-1-1:2009` og inne i hver nummerert dels egen definisjonsklausul. Kryssreferanse med NIST SP 800-82 Rev. 3 er nyttig for OT/ICS-terminologi som berører, men ikke er identisk med 62443's IACS-vokabular.

Hvordan forholder soner og kanaler seg til Purdue-modellen?

Purdue Enterprise Reference Architecture (PERA) er en hierarkisk funksjonell modell — nivå 0 til 5 — som beskriver hvor aktiviteter sitter i et automasjonshierarki. `IEC 62443-1-1`'s referansemodell er informert av Purdue, men legger til sikkerhets-konseptene soner og kanaler på toppen. En sone grupperer aktiva som deler felles sikkerhetskrav; en kanal er settet med kommunikasjonskanaler mellom soner. Soner trenger ikke å være en-til-en med Purdue-nivåer, selv om de i velkonstruerte anlegg ofte er det av fornuftige ingeniørgrunner. De to modellene er komplementære, ikke konkurrerende.

Videre lesing på dette nettstedet: forvaltningssystem-synet er i IEC 62443-2-x: hva anleggseiere må bevise ; systemdesign-synet er i IEC 62443-3-2 og 3-3: hva anleggseiere og integratorer må bevise ; produktleverandør-synet er i IEC 62443-4-1 og 4-2: hva OEM-er må bevise . Les dem i hvilken rekkefølge du vil — men les denne først, fordi det er dokumentet de andre antar du allerede forstår.

IEC 62443-2-x: forvaltningssystemet bak et sikkert industrianlegg

13. mai 2026 · 23 min lesetid · #compliance #security #industrial #iec-62443

To av de andre tekstene i denne serien dekker den tekniske dimensjonen av IEC 62443. 4-1 og 4-2-artikkelen ser på hvordan en OEM beviser at produktet sitt er bygget sikkert og hva produktet faktisk kan gjøre. 3-2 og 3-3-artikkelen ser på hvordan anleggseieren dimensjonerer sikkerhetskravet til systemet sitt og hvordan systemintegratoren leverer mot det. Sammen dekker de fire standardene designet, komponentene og det leverte systemet. Det de ikke dekker — og det hele standardfamilien er ufullstendig uten — er den daglige driften. Menneskene som drifter anlegget, prosedyrene de følger, retningslinjene som styrer dem, oppdateringene som holder systemet aktuelt, og tjenesteleverandørene som kommer på stedet for å vedlikeholde det. Det er dimensjonen IEC 62443 Del 2 adresserer.

En nyttig måte å se hvorfor dette betyr noe er ved å utvide byggeanalogien fra forrige artikkel. Hvis 3-2 er arkitektens brief, 3-3 er byggeforskriften, 4-2 er kvalitetsmerket på hver komponent, og 4-1 er mursteinsfabrikkens kvalitetssystem, så er **Del 2 sykehusets forvaltningssystem**. Du kan ha de beste arkitektene, den strengeste byggeforskriften, de høyest gradede komponentene og de mest rigorøst kontrollerte produsentene, men hvis sykehuset deretter driftes med slurvete hygiene, uopplært personale, ingen revisjonsspor over hvem som gjorde hva, og intet system for tilbakekalling av defekt medisinsk utstyr, vil ingenting av det redde deg. Del 2 er det som gjør konstruksjonen betydningsfull i drift. Det er disiplinen som gjør et sikkert design om til et bærekraftig sikkert anlegg.

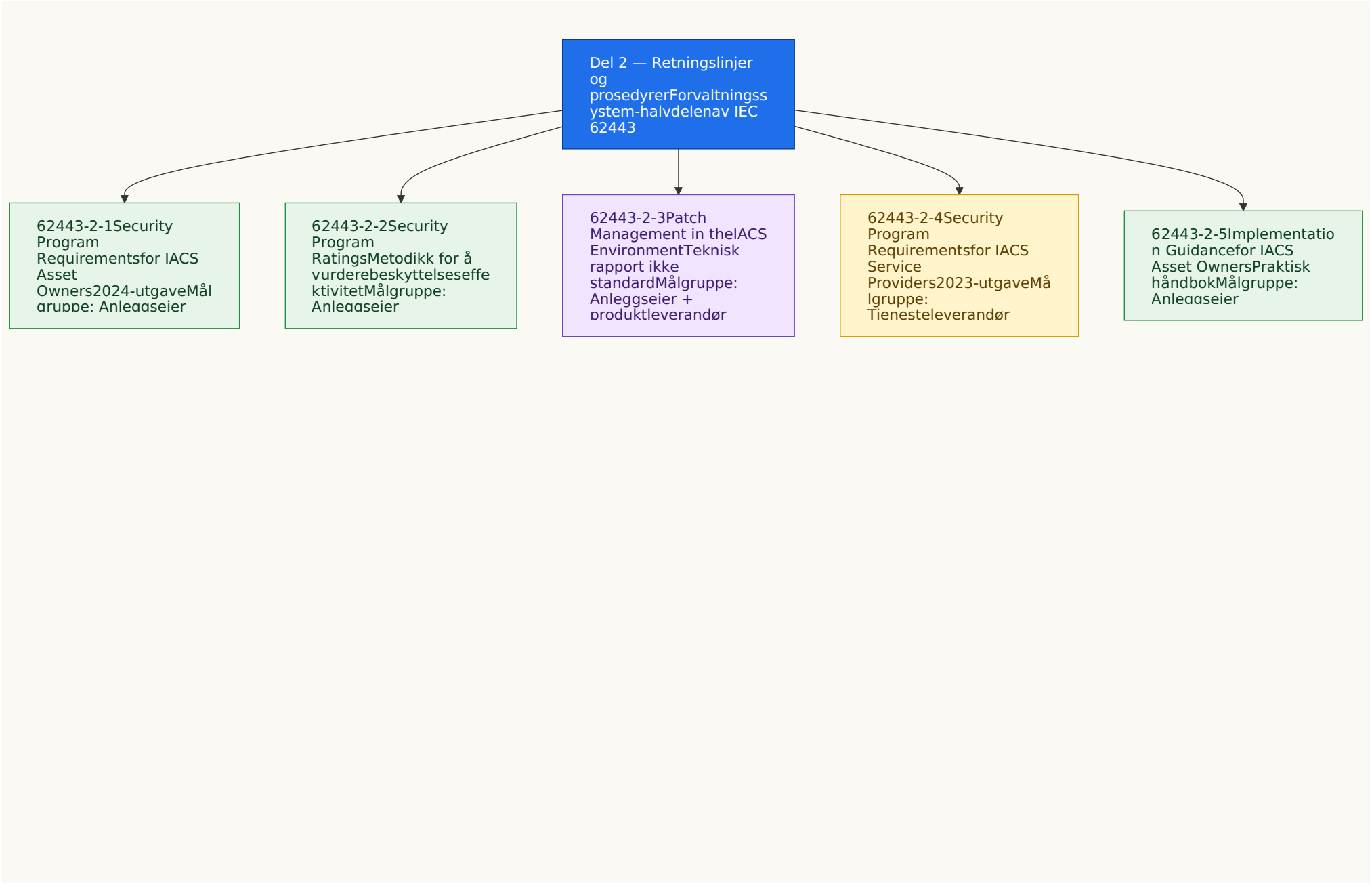
Det er fem aktive medlemmer av Del 2-familien — 2-1 til 2-5 — og de fordeler seg pent mellom to målgrupper. **Anleggseieren** er målgruppen for 2-1, 2-2 og 2-5, hvor 2-3 også berører dem. **Tjenesteleverandøren** — som standarden mener er systemintegratorer, vedlikeholdsentreprenører, managed service-leverandører og lignende tredjeparter som arbeider på eller i din IACS — er målgruppen for 2-4. Produktleverandøren dukker bare opp i Del 2 i en støtterolle (hovedsakelig i 2-3, der de må levere oppdateringsinformasjon for produktene sine i en form kundene faktisk kan bruke).

Dette blir viktig i EU-regulatorisk kontekst. Under NIS2 lander anleggseiers Artikkel 21-risikostyringsforpliktelser og Artikkel 21(2)(d) leverandørkjede-plikter direkte på territoriet 2-1 og 2-4 styrer. Under Cyber Resilience Act kobler Artikkel 14 sårbarhetsrapportering fra produktleverandøren til anleggseiers oppdateringsprogram som IEC TR 62443-2-3 kodifiserer. 2-x-standardene er det operasjonelle laget hvor EU-regulatoriske krav møter OT-virkeligheten.

Denne artikkelen jobber gjennom hver av de fem under-standardene etter tur, knytter dem deretter sammen og avsluttes med en sjekkliste for anskaffelse og revisjon.

De offisielle standardene utgis av IEC og ko-brandes av ISA. Primærkilder for hver: IEC 62443-2-1:2024 , ISA TR62443-2-2:2025 , IEC TR 62443-2-3:2015 , og IEC 62443-2-4:2015/AMD1:2018 . IEC 62443-2-5 er referert i familieoversikten på ISAs 62443-serieside .

2-x-familien i fugleperspektiv


Del 2 — Retningslinjer og prosedyrerForvaltningssystem-halvdelenav IEC 62443
62443-2-1Security Program Requirementsfor IACS Asset Owners2024-utgaveMålgruppe: Anleggseier
62443-2-2Security Program RatingsMetodikk for å vurderebeskyttelseseffektivitetMålgruppe: Anleggseier
62443-2-3Patch Management in theIACS EnvironmentTeknisk rapport ikke standardMålgruppe: Anleggseier + produktleverandør
62443-2-4Security Program Requirementsfor IACS Service Providers2023-utgaveMålgruppe: Tjenesteleverandør
62443-2-5Implementation Guidancefor IACS Asset OwnersPraktisk håndbokMålgruppe: Anleggseier

En rask orientering før vi går inn i hver i detalj. To av disse — 2-1 og 2-4 — er fulle normative standarder: de inneholder krav som en organisasjon enten oppfyller eller ikke oppfyller, og det finnes eksterne sertifiseringsordninger (mer om disse nedenfor) som kan verifisere påstanden. Én av dem — 2-3 — er en teknisk rapport, ikke en standard, som betyr at det er veiledning heller enn reviderbare krav; det er fortsatt viktig, men terskelen for «samsvar» er annerledes. Én — 2-5 — er implementeringsveiledning: den forteller deg hvordan du skal gjøre det 2-1 sier du må gjøre. Og én — 2-2 — er en relativt nylig tilføyelse som gir en måte å måle hvor godt sikkerhetsprogrammet ditt faktisk er når du har bygget det. Sammen utgjør de et sammenhengende forvaltningssystem-rammeverk.

IEC 62443-2-1: anleggseiers sikkerhetsprogram

IEC 62443-2-1, formelt med tittelen «Security program requirements for IACS asset owners», er hjørnesteinen i Del 2 og uten tvil hjørnesteinen i anleggseiers hele IEC 62443-forpliktelse. Standarden ble først utgitt i 2010 og ble vesentlig omskrevet i august 2024 som en andre utgave — en oppdatering som materielt endret strukturen på kravene og bringer standarden nærmere hvordan organisasjoner faktisk driver sikkerhetsprogrammene sine i dag.

Hva den faktisk er

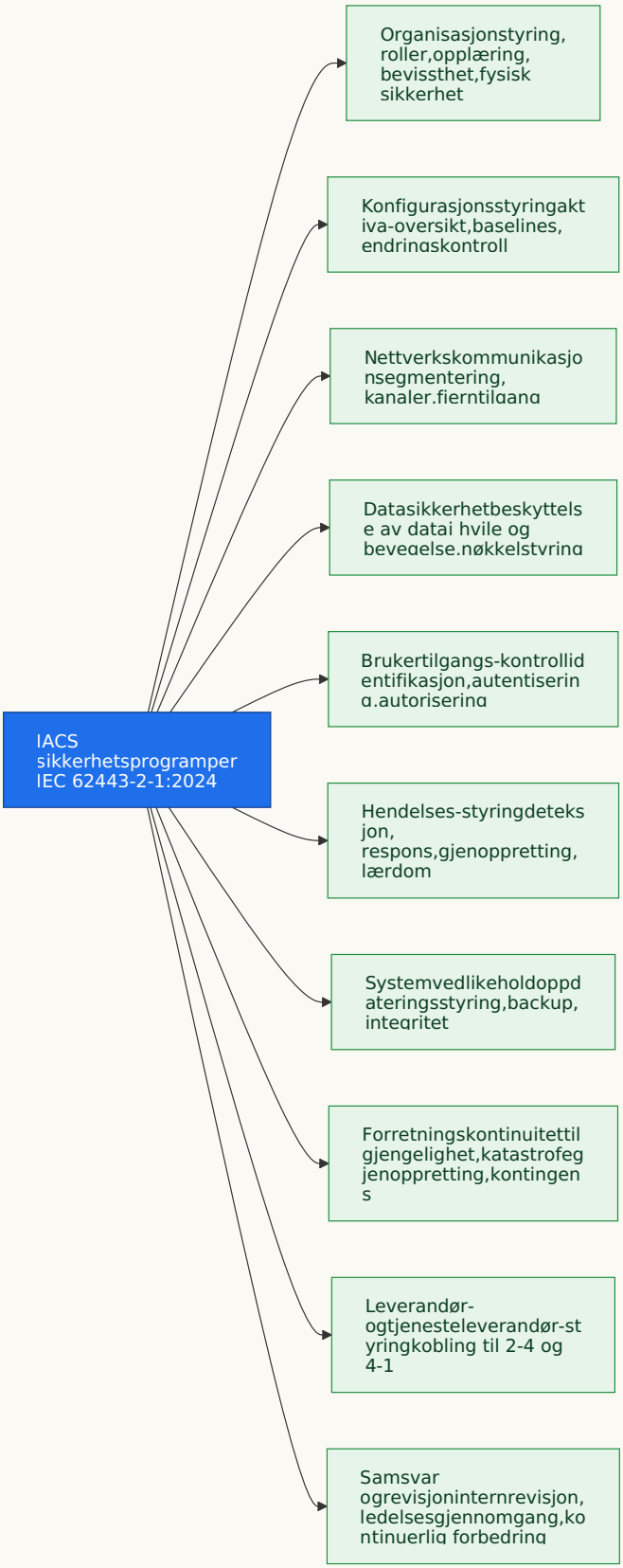
Med klart språk definerer 2-1 hva en anleggseiers **industrielle cybersikkerhetsprogram** må inneholde for å bli ansett som godt drevet. Standarden spesifiserer ikke hvordan selve IACS-en må bygges — det er jobben til 3-3 — men heller hvilke retningslinjer, prosedyrer, prosesser, opplæringsordninger, styringsstrukturer og kontinuerlige forbedringsmekanismer anleggseieren må ha pakket rundt IACS-en slik at den forblir sikker i drift. Den nærmeste analogen fra IT-verdenen er ISO/IEC 27001s Information Security Management System (ISMS), og 2024-utgaven av 2-1 gjør denne

analogien eksplisitt ved bevisst å avduplisere kravene mot ISO 27001 slik at en organisasjon som allerede har et ISMS ikke trenger å gjøre alt dobbelt.

For å returnere til sykehus-analogien er 2-1 **det kliniske styringsrammeverket** — det dokumenterte systemet som sier hvordan sykehuset ledes, hvordan kliniske beslutninger tas og gjennomgås, hvordan personalet opplæres og kredensieres, hvordan hendelser rapporteres og undersøkes, hvordan pasientsikkerhet overvåkes, hvordan risikoer spores, hvordan retningslinjer holdes aktuelle, og hvordan hele apparatet kontinuerlig forbedres. Et sykehus med solid klinisk styring kan levere trygg behandling år etter år; et sykehus uten den er én dårlig dag unna en CQC-merknad (Care Quality Commission).

Security Program Elements

2024-utgaven av 2-1 organiserer kravene sine i **Security Program Elements (SPEs)** heller enn den løsere kapittelstrukturen i 2010-utgaven. Hvert SPE er en sammenhengende gruppering av krav som adresserer en bestemt dimensjon av sikkerhetsprogrammet. De spesifikke elementnavnene og antallene i den publiserte standarden dekker den organisatoriske og styringsmessige dimensjonen, konfigurasjonsstyring, nettverkskommunikasjon, databeskyttelse, brukertilgangskontroll, hendelses- og hendelsesstyring, forretningskontinuitet, systemvedlikehold og andre operasjonelle disipliner kjent fra bredere forvaltningssystem-praksis. Hovedkategoriene en anleggseier må adressere kan visualiseres slik:



Det avgjørende konseptuelle grepet i 2024-utgaven er introduksjonen av en **modenhetsmodell** for å evaluere disse elementene. Den

ekkoer strukturen brukt i IEC 62443-4-1 for OEM-utviklingsprosesser, og 2-1-modenhetsmodellen lar en anleggseier vurderes ikke bare på om de har en retningslinje på plass, men på hvor konsekvent og effektivt de anvender den på tvers av organisasjonen. En retningslinje som eksisterer på papir, men som følges ujevnt, er på et lavere modenhetsnivå enn den samme retningslinjen påviselig håndhevet på tvers av alle steder med revisjonsbevis. Modenhetsmodellen gjør standarden mye mer nyttig som et eksternt vurderingsinstrument enn 2010-utgaven var, fordi den gir vurderere en forsvarlig skala å score mot heller enn en binær «har eller har ikke».

En annen viktig endring er hva 2-1 bevisst ikke prøver å gjøre. 2024-utgaven erkjenner at mange anleggseiere allerede driver et ISO 27001 ISMS, og heller enn å duplisere retningslinje- og prosedyre-stilaset til et ISMS, deferer den eksplisitt til ISO 27001 for det generiske informasjonssikkerhetsforvaltningsapparatet og fokuserer 2-1s krav på de IACS-spesifikke tilleggene som et ISMS ikke naturlig dekker. I praksis betyr dette at en anleggseier med et modent ISMS kan bruke 2-1 som et fokusert gap-analyseverktøy heller enn et erstatningsrammeverk, som er en betydelig innsatsbesparelse og en betydelig forbedring i klarhet.

Hva anleggseieren må bevise objektivt

En forsvarlig påstand om samsvar med IEC 62443-2-1 ser ut som en sammenhengende bevispakke som dekker hvert av Security Programme Elements på et oppgitt modenhetsnivå, med sporbarhet til operasjonell praksis. Konkret betyr dette en dokumentert IACS-sikkerhetspolitikk godkjent på passende nivå i organisasjonen, en aktuell aktiva-oversikt over IACS-systemene i omfanget, et risikoregister som lenker til CRS-en produsert under 3-2 , opplæringsregistreringer for menneskene som designer, drifter og vedlikeholder IACS-en, revisjonsrapporter som demonstrerer at retningslinjer følges i praksis, en dokumentert

hendelsesstyringsprosess med en reell historie av hendelser håndtert (eller en klar oversikt over overvåking med ingenting vesentlig å håndtere), en dokumentert endringsstyringsprosess som styrer hvordan tillegg og modifikasjoner til IACS-en godkjennes, og en ledelsesgjennomgangs-protokoll som viser at seniorledelse periodisk gjennomgår programmets effektivitet og autoriserer forbedringer.

Det finnes nå en fremvoksende tredjeparts-sertifiseringsrute for anleggseier-programmer: **ISASecure ACSSA** (Automation and Control System Security Assurance), kunngjort i 2023 og ment å dekke en operasjonell IACS på anleggseiers sted mot IEC 62443-2-1, 2-3 og de relevante delene av 3-3. ACSSA er nyere og mindre utbredt enn dens komponent-sides søsken (SDLA og CSA), men for anleggseiere i regulerte sektorer vil det sannsynligvis bli en stadig vanligere måte å bevise en 2-1-påstand. Der ACSSA ikke er i spill, er bevispakke-ruten — internrevisjonsrapporter, eksterne vurderingsrapporter fra anerkjente konsulenter, integrasjon med ISO 27001-overvåkingsrevisjoner — standardvalget. I begge tilfeller er nøkkelprinsippet det samme: en 2-1-påstand er bare så sterk som beviset bak den, og beviset må være aktuelt, organisasjonsomfattende og konsistent med hva en utenforstående faktisk ville finne hvis de tilbrakte en dag med å gå rundt på anlegget.

IEC 62443-2-2: vurdere hvor god programmet faktisk er

Hvis 2-1 forteller anleggseieren hva sikkerhetsprogrammet deres må inneholde, så adresserer **IEC 62443-2-2** det relaterte men distinkte spørsmålet: hvordan vurderer vi hvor godt programmet faktisk fungerer? Den definerer en metodikk for å produsere en Security Programme Rating — en strukturert, forsvarlig scoring av en operasjonell IACS mot kravene i standardfamilien.

Motivasjonen for dette er praktisk. En anleggseier kan dokumentere et vakkert sikkerhetsprogram på papir som svikter i drift; en annen kan ha et mindre elegant program som følges rigorøst og er ekte effektivt. Å bare se på dokumentasjonen kan ikke skille dem. 2-2 introduserer en strukturert måte å evaluere operasjonell virkelighet — hva som faktisk er konfigurert på nettverket, hva som faktisk logges og overvåkes, hva som faktisk oppdateres, hva som faktisk testes — og å produsere en rating som er sammenlignbar på tvers av steder, på tvers av forretningsenheter og over tid.

Sykehus-analogien her er **CQC-vurderingen (Care Quality Commission)** kjent for alle som har hatt å gjøre med britisk helsetjeneste. Et sykehus vurderes som Outstanding, Good, Requires Improvement eller Inadequate basert på en strukturert vurdering mot publiserte kriterier. Vurderingen er sammenlignbar på tvers av sykehus, forsvarlig overfor regulatorer og pasienter, og nyttig internt for å prioritere forbedringsarbeid. 2-2 spiller en lignende rolle for et industrisikkerhetsprogram: den produserer en vurdering som har mening utover den umiddelbare revisjonen, med kriterier som enhver informert vurderer kan reanvende.

Vurderingen er ment å brukes på flere måter. Internt hjelper den seniorledelse med å sammenligne steder mot hverandre og mot selskapets egen historiske ytelse. Eksternt gir den en måte å underbygge cybersikkerhetspåstander overfor regulatorer, forsikringsselskaper og kunder uten å måtte publisere sensitiv intern dokumentasjon. I en anskaffelses- eller M&A-kontekst gir den et forsvarlig mål på cybersikkerhetsstilling som er uavhengig av noen enkeltleverandørs produkt. Og i den fremvoksende ACSSA-sertifiseringsordningen er en 2-2-aktig vurdering implisitt i vurderingsmetodikken.

Hva en anleggseier må demonstrere for å hevde en 2-2-avledet vurdering er i hovedsak selve vurderingen, metodikken den ble

produsert med, beviset vurdert, og vurderens kompetanse. Som med 2-1 er en selv-erklært vurdering mye svakere enn en produsert av en anerkjent ekstern vurderer, og vurderingens verdi avhenger kritisk av at vurderen følger metodikken trofast — det samme poenget som gjøres om enhver sertifisering: sertifikatets troverdighet er sertifisørens troverdighet.

IEC TR 62443-2-3: å holde systemet aktuelt

IEC TR 62443-2-3 er oppdateringsstyrings-medlemmet av familien. «TR»-prefikset betyr noe: dette er en teknisk rapport heller enn en internasjonal standard. Skillet er konsekvensrikt. En teknisk rapport er informativ — den inneholder veiledning, anbefalinger og god praksis heller enn reviderbare krav. Du kan strengt tatt ikke være «ikke i samsvar med 2-3» på den måten du kan være ikke i samsvar med 2-1, fordi 2-3 ikke inneholder «skal»-klausuler å vurderes mot. Men den praktiske viktigheten av 2-3 er enorm, fordi oppdateringsstyring i en industriell kontekst er genuint vanskelig, og fraværet av et sammenhengende oppdateringsprogram er den vanligste enkelt-svakheten i en ellers godt drevet IACS.

Sykehus-analogien her er **prosedyren for vedlikehold av medisinsk utstyr og håndtering av tilbakekallinger**. Sykehusutstyr har produsent-vedlikeholdsplaner, periodiske tilbakekallinger, programvareoppdateringer og sikkerhetsvarsler. Noen av disse kan anvendes umiddelbart; noen krever at utstyret tas ut av drift, som har kliniske konsekvenser; noen krever omopplæring av personale; og noen — for veldig gammelt utstyr — må kanskje anvendes via kompenserende tiltak fordi produsenten har sluttet å utstede oppdateringer. Et sykehus som ignorerer tilbakekallinger er farlig; et sykehus som blindt anvender hver oppdatering uten testing i sin kliniske kontekst er også farlig. Disiplinen i å gjøre dette skikkelig er det 2-3 kodifiserer for det industrielle cybersikkerhets-ekvivalentet.

Hovedbidraget i 2-3 er en strukturert oversikt over hva et reelt IACS-oppdateringsstyringsprogram må adressere: de asymmetriske ansvarsforholdene mellom **produktleverandøren** (som må produsere oppdateringer, validere dem på sine produkter, og kommunisere dem i en brukbar form til sine kunder) og **anleggseieren** (som må konsumere den informasjonen, vurdere relevans i sin spesifikke driftskontekst, teste oppdateringer i et representativt miljø, planlegge anvendelse under vedlikeholdsvinduer, og verifisere at det oppdaterte systemet fortsetter å fungere riktig). 2-3 introduserer også standardiserte datastrukturer for å levere oppdateringsinformasjon — **VPatch**-konseptet er det mest omtalte eksempelet — slik at anleggseiere ikke trenger å oversette mellom hver produktleverandørs idiosynkratiske oppdateringsvarslingsformat.

For anleggseieren betyr det å demonstrere en troverdig oppdateringsstyringspraksis å vise et dokumentert program som dekker hver komponent i IACS-oversikten (inkludert, viktig, den lange halen av små innebygde enheter som er lett å overse), en prosess for å motta og triagere leverandørråd, en testet tilnærming for risikovurdering av hvert råd i den operasjonelle konteksten (fordi ikke hver CVE er like relevant for hver utplassering), bevis på oppdateringsanvendelse under planlagte vinduer med verifisering av systemoppførsel etter oppdatering, og en sammenhengende tilnærming for komponenter hvis leverandører ikke lenger utsteder oppdateringer — typisk gjennom kompenserende kontroller på nettverks- eller operasjonelt nivå.

For produktleverandøren går demonstrasjonen den andre veien. Leverandøren må vise at de produserer oppdateringer rettidig for sårbarheter som påvirker produktene deres, at de kommuniserer disse oppdateringene i en brukbar form, at oppdateringene har blitt testet i representative konfigurasjoner av produktet, og at de støtter anleggseiers testing gjennom klare utgivelsesnotater, regresjonstest-

veiledning og tilbakeruller-prosedyrer. OEM-siden av 2-3 kobler naturlig til forpliktelsene i 4-1s Praksis 7 (Security Update Management) og til EU Cyber Resilience Acts sårbarhetshåndteringskrav , så for produktleverandører som opererer i regulerte markeder blir disse forpliktelsene i økende grad bakt inn i produkt-roadmap-disiplin heller enn behandlet som et valgfritt ekstra.

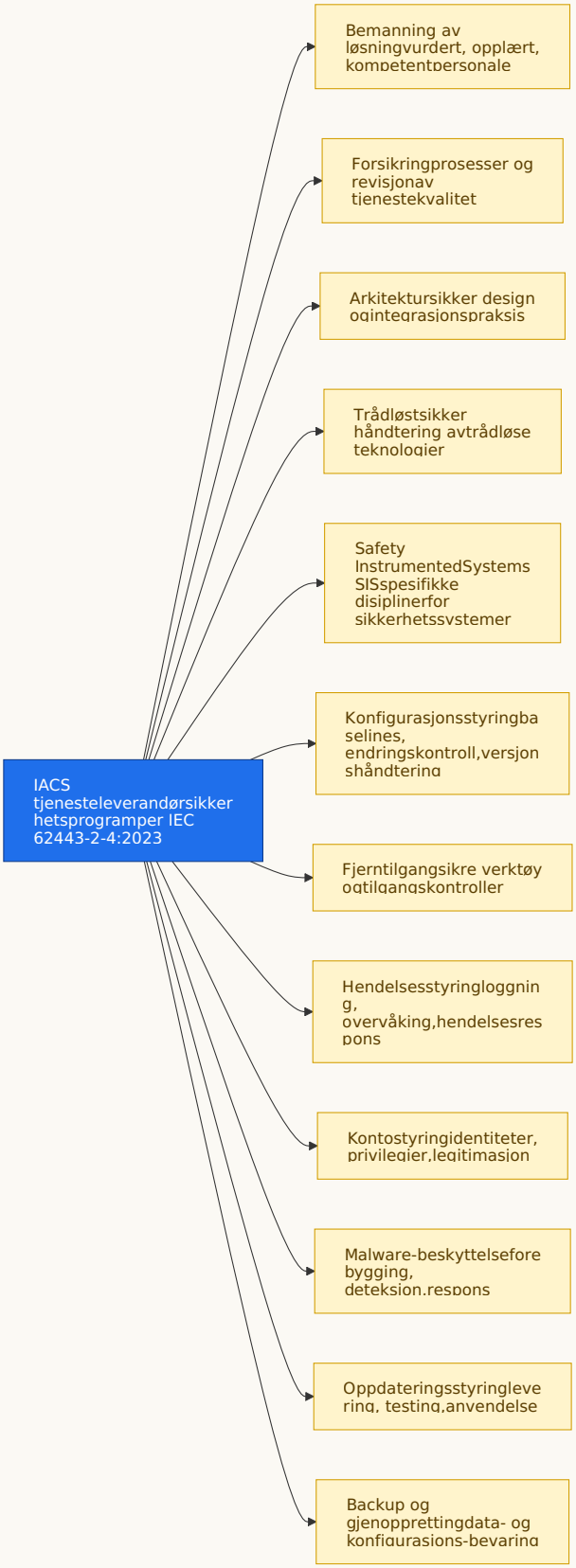
IEC 62443-2-4: tjenesteleverandørens sikkerhetsprogram

Hvis 2-1 styrer anleggseiers hus, styrer **IEC 62443-2-4** oppførselen til alle som kommer på anleggseiers sted for å designe, integrere, vedlikeholde eller drifte IACS-en. Standarden har tittelen «Security program requirements for IACS service providers», og dens nåværende utgave er 2023-andre-utgaven. «Tjenesteleverandøren» i 2-4 dekker et bredt spekter av organisasjoner: systemintegratorer (som designer og bygger det integrerte systemet per anleggseiers CRS), automasjonsentreprenører, vedlikeholdsentreprenører, managed-service-leverandører, sikkerhetstjenesteleverandører som kjører overvåking eller hendelsesrespons på vegne av anleggseier, og enhver organisasjon hvis folk har hender på anleggseiers IACS.

Sykehus-analogien her er **medisinsk-bemanningsbyråets akkrediterings- og revisjonsregime**. Et sykehus som tillater byråsykepleiere å arbeide på sine avdelinger må vite at byrået sjekker personalet sitt, opplærer dem, vedlikeholder deres profesjonelle registreringer, reviderer ytelsen deres, og selv er underlagt inspeksjon. Et sykehus som tar imot byråpersonale uten verifisering av noen av disse tingene er eksponert for klinisk risiko som ikke har noe å gjøre med hvor godt selve sykehuset er drevet. 2-4 spiller den samme rollen for tjenesteleverandører i det industrielle sikkerhetsrommet: den forteller anleggseieren hva som skal kreves av enhver som arbeider på deres IACS, og den forteller tjenesteleverandøren hva de må demonstrere for å være akseptable.

Strukturen i 2-4

2-4 organiserer kravene sine i **Functional Areas** — sammenhengende grupperinger av kapabiliteter en tjenesteleverandør må demonstrere. De viktigste Functional Areas som typisk refereres i litteraturen om standarden inkluderer følgende.



Det eksakte antallet og merkingen av Functional Areas varierer noe mellom utgaver av standarden og mellom ulike organisasjoners

sammendrag av den, men det substansielle innholdet er bredt sett stabilt: en tjenesteleverandør må ha påviselig kapabilitet på tvers av menneske-, prosess- og tekniske dimensjoner av hver aktivitet de utfører på anleggseiers IACS.

Som 4-1 for OEM-er, inkorporerer 2-4 en **modenhetsnivå-dimensjon**. En tjenesteleverandør kan vurderes på Maturity Level 1 (praksisen eksisterer, men er ad hoc), Level 2 (dokumentert og gjentakbar), Level 3 (konsekvent praktisert på tvers av organisasjonen med bevis), eller Level 4 (kontinuerlig målt og forbedret). En anleggseier som spesifiserer 2-4-samsvar i kontrakten sin bør spesifisere modenhetsnivået de krever, akkurat som de ville spesifisert en SL-T i 3-2.

Hva tjenesteleverandøren må bevise objektivt

Demonstrasjon her er veldefinert fordi det finnes en etablert tredjeparts-sertifiseringsordning. **IECEE CB-ordningen** for industriell cybersikkerhet utsteder sertifikater mot IEC 62443-2-4 gjennom akkrediterte sertifiseringsorganer, og disse sertifikatene er gjensidig anerkjent på tvers av IECEE-medlemsøkonomier. ISASecure har også drevet relevante ordninger i dette rommet på ulike tidspunkter. En tjenesteleverandør som hevder 2-4-samsvar bør kunne produsere et aktuelt tredjepartssertifikat som navngir versjonen av standarden, modenhetsnivået oppnådd per Functional Area (eller et enkelt globalt ML der det hevdes), sertifiseringsorganet, utstedelsesdatoen og utløpsdatoen — typisk tre år med overvåkingsrevisjoner i mellom.

Utover selve sertifikatet bør anleggseieren forvente at tjenesteleverandøren kan produsere det substansielle beviset som ligger til grunn for sertifikatet: opplæringsregistreringer og kompetansevurderinger for personalet som faktisk vil bli utplassert til anleggseiers sted, dokumenterte prosedyrer som dekker fjerntilgang, endringskontroll, hendelseshåndtering, oppdateringsutplassering og

konfigurasjonsstyring, bevis på internrevisjon og ledelsesgjennomgang av disse prosedyrene, og en sikkerhetshendelses-håndteringskapabilitet med en track record. Som med 4-1 betyr omfanget av sertifikatet like mye som overskriftsvurderingen: et 2-4-sertifikat som dekker en bestemt forretningsenhet, en bestemt geografi eller en bestemt tjenestelinje forteller deg om det omfanget, ikke om hele organisasjonen. Å lese omfangserklæringen nøye er det enkelt viktigste verifiseringssteget.

Der en tjenesteleverandør ikke innehar et tredjeparts 2-4-sertifikat, men hevder samsvar med standarden, bør anleggseieren be om gap-analysen som støtter påstanden, korrigerende tiltak tatt, og eventuelle internrevisjonsbevis. Selv-erklært samsvar er ikke ingenting — det kan være et springbrett — men det bærer ikke samme tyngde som en sertifisert posisjon, og anleggseieren bør gjøre en klar beslutning om de aksepterer det for den type arbeid som kontraheres.

IEC 62443-2-5: den praktiske håndboken

Det siste medlemmet av Del 2-familien, **IEC 62443-2-5**, gir implementeringsveiledning for anleggseieren. Der 2-1 sier hva en anleggseier må ha i sikkerhetsprogrammet sitt, gir 2-5 råd om hvordan man faktisk gjør det. Det er en praktisk håndbok heller enn et kravdokument, og verdien dens ligger i de bearbeidede eksemplene, malene, organisatoriske mønstrene og pragmatiske rådene den tilbyr anleggseiere som er i starten av å bygge eller modernisere sikkerhetsprogrammet sitt.

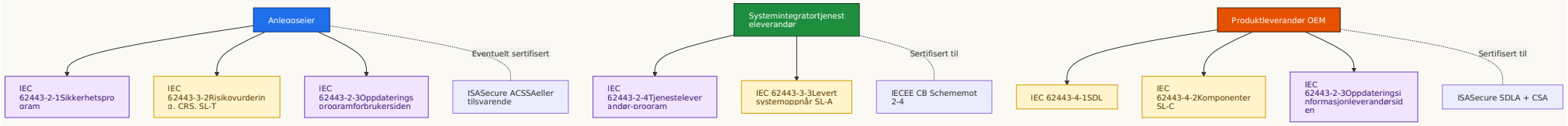
Fordi 2-5 er veiledning, genererer den ikke et «samsvars»-spørsmål på samme måte som 2-1 og 2-4. Det finnes ingen sertifisering for å være «i samsvar med 2-5»; det finnes kun spørsmålet om en anleggseier har brukt den (og lignende veiledning fra ISA, ENISA, NIST og sektor-organer) for å informere implementeringsvalgene

sine. For anleggseiere som bygger programmet sitt fra bunnen, er 2-5 et fornuftig utgangspunkt. For anleggseiere som allerede er lenger på vei, er den en nyttig sanity-sjekk.

Jeg vil ikke bruke lang tid på 2-5 fordi de substansielle forpliktelsene alle lever i dokumentene over. Men for fullstendighetens skyld bør alle som jobber seriøst med 2-1 være klar over at 2-5 eksisterer og bruke den.

Hvordan 2-x passer med resten av standardene

Det er verdt å trekke seg tilbake på dette punktet og se på hvordan Del 2 sitter ved siden av standardene dekket i de forrige artiklene. Diagrammet nedenfor viser de fire hovedpartene og standardene som styrer hver av dem, med artefaktene og sertifiseringene som flyter mellom.


Anleggseier
IEC 62443-2-1Sikkerhetsprogram
IEC 62443-3-2Risikovurdering, CRS, SL-T
IEC 62443-2-3Oppdateringsprogramforbrukersiden
Eventuelt sertifisert
ISASecure ACSSAeller tilsvarende
Systemintegratortjenesteleverandør
IEC 62443-2-4Tjenesteleverandør-program
IEC 62443-3-3Levert systemoppnår SL-A
Sertifisert til
IECEE CB Schememot 2-4
Produktleverandør OEM
IEC 62443-4-1SDL
IEC 62443-4-2Komponenter SL-C
IEC 62443-2-3Oppdateringsinformasjonleverandørsiden
Sertifisert til
ISASecure SDLA + CSA

Bildet er nå komplett. Hver part har teknisk-side-standarder (3-x og 4-x delene dekket i de forrige artiklene) og forvaltningssystem-side-standarder (2-x-delene dekket her). Hver part har minst én rute til tredjeparts-sertifisering av sitt respektive omfang. Og hvert grensesnitt mellom parter styres av en definert artefakt: CRS-en flyter fra anleggseier til integrator, SL-C-vektorene og oppdateringsinformasjonen flyter fra produktleverandør til integrator og anleggseier, det leverte systemet med sporbarhet flyter fra integrator til anleggseier, og operasjonelle praksiser på anleggseiers sted styres av anleggseiers 2-1-program med tjenesteleverandører regulert av 2-4.

En nyttig diagnostikk når man ser på et reelt industristed er å gå gjennom hvert grensesnitt i dette bildet og spørre om den tilsvarende artefakten eksisterer, om den er aktuell, og om den blir handlet på. Der noe grensesnitt mangler sin definerte artefakt, er det grensesnittet et kjedeledd uten ledd.

Vanlige fallgruver og røde flagg

Den hyppigste fallgruven i 2-1-arbeid er **å behandle det som en dokumentasjonsøvelse**. En organisasjon skriver retningslinjene, arkiverer dem i et dokumenthåndteringssystem og anser seg selv som «i samsvar» med 2-1. 2024-utgavens modenhetsmodell er spesielt designet for å motvirke denne fellen — en retningslinje som er skrevet, men ujevnt anvendt, scorer på et lavt modenhetsnivå, og en ekstern vurderer som arbeider mot standarden vil finne det ut. Det mest nyttige spørsmålet å stille av enhver 2-1-påstand er «vis meg revisjonssporet av retningslinjen i drift på tvers av alle steder de siste tolv månedene», fordi det er det som skiller en Maturity Level 1-organisasjon fra en Maturity Level 3-organisasjon.

En annen fallgruve er **å konflatere 2-1 med ISO 27001**. De to standardene overlapper, men er ikke erstatninger. ISO 27001 styrer

informasjonssikkerhet generisk; 2-1 adresserer spesifikt IACS-konteksten, inkludert de lange levetidene, legacy-komponentene, sikkerhetsinteraksjonene og operasjonelle virkelighetene som ISO 27001 ikke naturlig dekker. 2024-utgaven av 2-1 deferer bevisst til ISO 27001 for det generiske ISMS-laget, så en organisasjon med et ISMS bør ikke duplisere det stilaset, men de må legge til det IACS-spesifikke laget som 2-1 krever. En påstand om «vi er ISO 27001-sertifisert, så vi samsvarer med 2-1» er ikke, i seg selv, korrekt.

En tredje fallgruve påvirker tjenesteleverandører og deres anleggseier-kunder: **2-4-sertifikater med smalt omfang**. Et stort ingeniørselskap kan ha et 2-4-sertifikat som dekker for eksempel deres automasjons-forretningsenhet i ett land, mens selskapets markedsføringsmateriale antyder at hele organisasjonen er sertifisert. Omfangserklæringen på sertifikatet er sannheten. Når man engasjerer en tjenesteleverandør, bør anleggseieren be om en kopi av sertifikatet og lese omfanget for å verifisere at det faktiske teamet som skal utplasseres er innenfor det. Der det utplasserte teamet er fra en søsterorganisasjon eller et nylig oppkjøpt selskap, dekker omfanget kanskje ikke dem.

En fjerde fallgruve er **forvirring mellom 4-1 og 2-4**. En produktleverandør kan ha et SDLA-sertifikat mot 4-1 (som dekker deres produktutviklingsprosess), men ikke et 2-4-sertifikat (som ville dekke deres tjenesteleveranse-praksis). De to adresserer ulike omfang og ulike aktiviteter, og det ene er ikke en erstatning for det andre. En organisasjon som både produserer produkter og leverer tjenester på anleggseiers sted trenger begge sertifikatene.

En femte fallgruve er **IT-oppdateringsstyringspraksis anvendt umodifisert på OT**. IT-verdenen har veletablerte mønstre for oppdateringsutplassering — typisk raskt, automatisert, hyppig anvendt — som oversettes dårlig til industrielle miljøer hvor oppdateringer må testes i representative konfigurasjoner, planlegges

rundt produksjonsvinduer, og verifiseres for innvirkning på sanntids- og sikkerhetsoppførsler. En anleggseier hvis IACS-oppdateringsprogram drives av en IT-avdeling med IT-mønstre er i høy risiko for enten å anvende oppdateringer uten skikkelig validering eller, oftere, å anvende ingenting fordi IT-mønsteret ikke kan tilpasses. Disiplinen i TR 62443-2-3 eksisterer nøyaktig fordi OT-oppdateringsstyring er sin egen disiplin.

En sjette fallgruve, og en spesielt lumsk en, er **at legacy-systemer stille ekskluderes fra sikkerhetsprogrammet**. 2024-utgaven av 2-1 erkjenner eksplisitt at legacy-systemer uten produsentstøtte ikke kan oppfylle alle kravene direkte, og at kompenserende tiltak er det riktige svaret. Fallgruven er når legacy-systemer ekskluderes fra oversikten helt og stille aldres ut av enhver aktiv styring. Det riktige svaret er å beholde dem i programmet med deres kompenserende tiltak dokumentert og gjennomgått, ikke å droppe dem fra aktiva-registeret og håpe.

En sjekkliste for anskaffelse, revisjon og egenvurdering

Det følgende kan brukes som et kontraktsvedlegg, et internrevisjonsinstrument eller et egenvurderingsverktøy. Det er organisert etter parten som demonstrerer samsvar.

For anleggseiers egen 2-1 bevispakke

- En aktuell, styre-godkjent IACS cybersikkerhetspolitikk som refererer IEC 62443-2-1 (2024-utgaven) og identifiserer SP-elementene som dekkes.
- En dokumentert IACS aktiva-oversikt som dekker alle systemer i omfanget, inkludert legacy-systemer med deres kompenserende tiltak eksplisitt notert.
- Et risikoregister koblet til CRS-en produsert under 62443-3-2 , med regelmessig gjennomgangskadens dokumentert.

- Opplæringsregistreringer for personale med IACS-ansvar, inkludert oppfriskningssykluser og kompetansevurderinger.
- Dokumenterte prosedyrer for endringskontroll, hendelsesrespons, oppdateringsstyring (per 62443-2-3), backup og gjenoppretting, og tilgangsstyring — med driftsbevis.
- En aktuell egenvurdering eller ekstern vurdering av modenhetsnivå per SP-element, med prioriterte forbedringstiltak.
- Internrevisjonsrapporter som dekker hvert SP-element med bevis på lukkede korrigerende tiltak.
- Ledelsesgjennomgangsprotokoller som demonstrerer seniorledelses-engasjement med en definert kadens (typisk årlig).
- Der det er aktuelt, et aktuelt ISASecure ACSSA-sertifikat eller tilsvarende tredjepartsvurdering, med omfangserklæringen gjennomgått mot det faktiske operasjonelle fotavtrykket.

For anleggseiers evaluering av en tjenesteleverandørs 2-4-påstand

- Et aktuelt IECEE CB Scheme-sertifikat (eller tilsvarende) mot IEC 62443-2-4:2023, med utstedende organ, utstedelsesdato og utløpsdato tydelig oppgitt.
- En omfangserklæring på sertifikatet som eksplisitt dekker forretningsenheten, geografien og tjenestetypen relevant for kontrakten.
- En uttalelse om modenhetsnivået oppnådd per Functional Area (eller et enkelt globalt ML der det hevdes).
- Opplærings- og kompetanseregistreringer for det spesifikke personalet foreslått for utplassering til anleggseiers sted.
- Dokumenterte prosedyrer for aktivitetene tjenesteleverandøren vil utføre på anleggseiers IACS, med kobling til de sertifiserte Functional Areas.
- Bevis på tidligere ytelse på lignende oppdrag med referansekunder.

- En definert prosess for å håndtere hendelser som kan oppstå under oppdraget, med eskaleringsruter inn i anleggseiers egen hendelsesstyringsprosess under 2-1.

For anleggseiers evaluering av en produktleverandørs 2-3-bidrag

- Et dokumentert sårbarhets-avslørings- og rådgiver-program med en track record av utstedte rådgivere.
- Et definert oppdateringsleveringsformat (ideelt på linje med VPatch eller lignende maskinlesbart format) og en indikasjon på den typiske ledetiden fra sårbarhetsavsløring til oppdaterings-tilgjengelighet.
- Utgivelsesnotater og testveiledning som følger hver oppdatering, tilstrekkelig til å støtte anleggseiers egen testing.
- En definert støttelevetid per produkt med en klar slutt-på-støtte-dato, etter som anleggseieren må stole på kompenserende tiltak.
- Der det er aktuelt, påviselig kobling til leverandørens 4-1 SDLA-sertifisering (den underliggende sikre utviklingsprosessen) og 4-2 CSA-sertifisering (komponentene i omfang).

For anleggseiers evaluering av sitt eget 2-3 oppdateringsprogram

- En aktuell aktiva-oversikt som dekker hver komponent i IACS-en, med leverandør-rådgiverkanaler abonnert for hver.
- En dokumentert triage-prosess for innkommende rådgivere med risikobasert prioritering.
- Et testmiljø representativt nok til å validere oppdateringer før produksjonsutplassering.
- En planlagt oppdateringsutplassering-syklus på linje med produksjons-vedlikeholdsvinduer, med verifisering av systemoppførsel etter oppdatering.
- En dokumentert tilnærming for ikke-oppdaterbare komponenter, med kompenserende kontroller implementert og gjennomgått.

- Målepunkter som demonstrerer programmets faktiske ytelse — typisk tid-til-oppdatering etter kritikalitet, andel av rådgivere anvendt versus utsatt med begrunnelse, og trender over tid.

Der 3-x - og 4-x -standardene adresserer hva i en IACS — hva systemet må gjøre, hva komponentene må støtte, hva designet må oppnå — adresserer 2-x-standardene hvordan den drives dag for dag, år etter år, gjennom det lange driftslivet til et industrianlegg. **IEC 62443-2-1** styrer anleggseiers sikkerhetsprogram og er hjørnesteinen av familien på den operasjonelle siden. **IEC 62443-2-2** gir en måte å vurdere hvor godt det programmet faktisk fungerer. **IEC TR 62443-2-3** kodifiserer disiplinen i oppdateringsstyring for både anleggseiere og produktleverandører. **IEC 62443-2-4** styrer tjenesteleverandørene som gjør arbeid på anleggseiers sted. **IEC 62443-2-5** tilbyr praktisk implementeringsveiledning for å støtte 2-1.

Den enkelt viktigste mentale modellen å ta med seg fra denne artikkelen er at **hver part har både en teknisk-side-forpliktelse og en forvaltningssystem-side-forpliktelse under IEC 62443**, og at forsvarlig cybersikkerhet avhenger av at begge er på plass. En produktleverandør med en strålende SDL (4-1) men en kaotisk oppdaterings-rådgiverpraksis (2-3) er en halv leverandør; en systemintegrator med utmerket teknisk kapabilitet mot 3-3 men uten et sertifisert tjenesteprogram under 2-4 er en halv integrator; en anleggseier med en omhyggelig 3-2-risikovurdering, men uten et operasjonelt sikkerhetsprogram under 2-1 har bygget en bygning uten vaktmester.

Beviskjeden på tvers av hele IEC 62443 holder kun når hver part kan demonstrere sin del — med aktuelle sertifikater der de finnes, med substansielt bevis bak dem, og med en kultur av operasjonell disiplin

som holder sertifikatene meningsfulle mellom revisjoner. Standardfamilien gir deg rammeverket. Det den ikke kan gi deg er viljen til faktisk å drive ting på den måten.

IEC 62443-3-2 og 3-3: hva anleggseiere og integratorer må bevise

13. mai 2026 · 28 min lesetid · #compliance #security #industrial #iec-62443

OEM-side-teksten i denne serien tar for seg de to standardene en produktleverandør må leve med: IEC 62443-4-1 (hvordan et produkt bygges) og IEC 62443-4-2 (hva produktet faktisk kan gjøre) — for den detaljerte gjennomgangen, se IEC 62443-4-1 og 4-2: hva en OEM faktisk må bevise . De er avgjørende, men de utgjør bare halve historien. Å kjøpe sertifiserte komponenter er én ting; å gjøre dem om til et fungerende industrielt kontrollsystem som er dimensjonert riktig mot de faktiske truslene, fornuftig partisjonert mellom soner, og levert med harde bevis for at det ferdige anlegget er like sikkert som designet var ment å være — det er en annen disiplin. Den disiplinen styres av to andre deler i samme IEC 62443-familie: **IEC 62443-3-2** og **IEC 62443-3-3**.

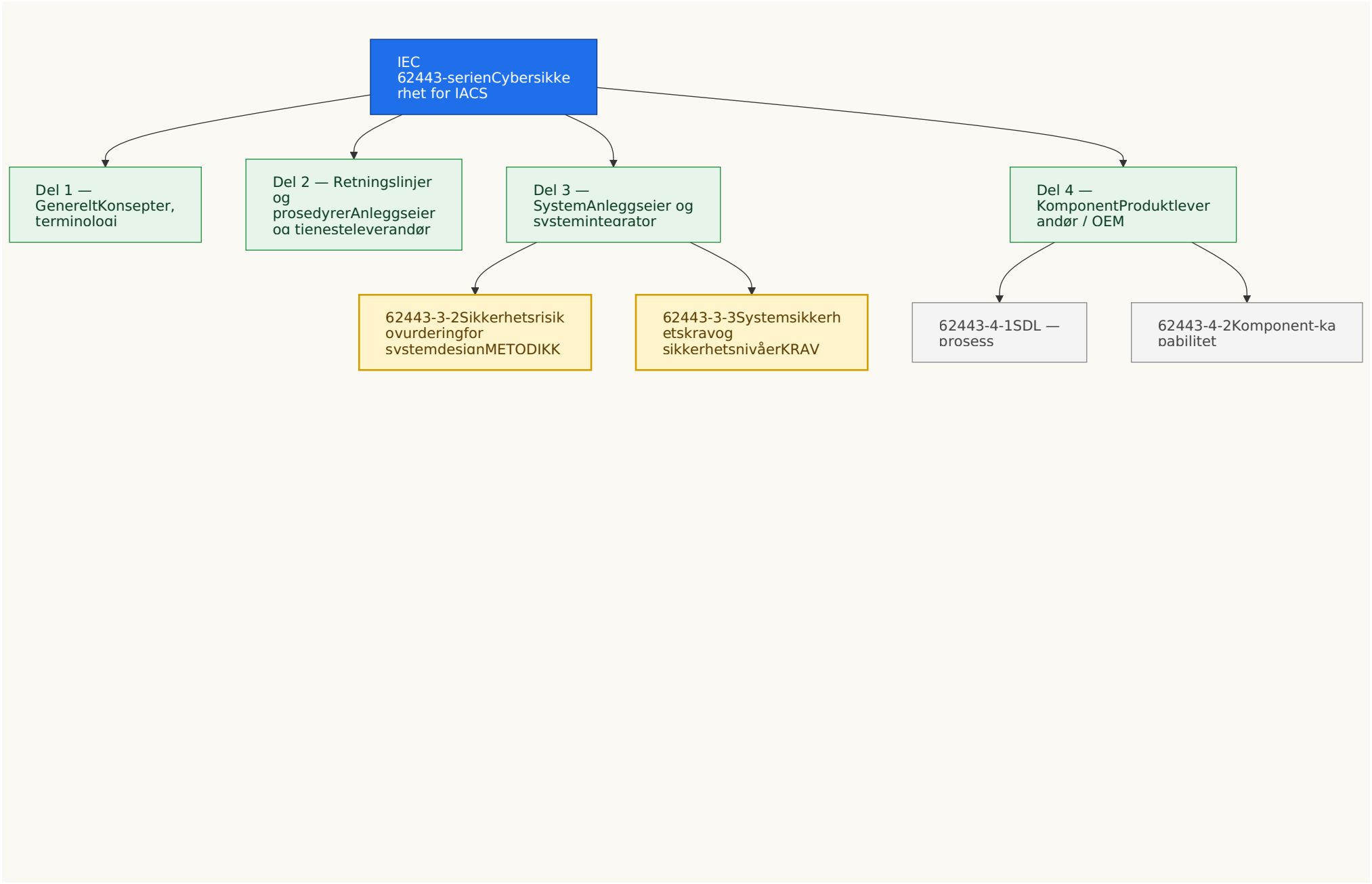
Disse to standardene sitter ett nivå over 4-1 og 4-2. De lever på **system**-laget heller enn **komponent**-laget, og de besvarer to forskjellige men tett koblede spørsmål. **IEC 62443-3-2** spør «hvordan finner jeg ut hvilket sikkerhetsnivå jeg faktisk trenger i hver del av mitt industrisystem?» **IEC 62443-3-3** spør «hvis jeg har bestemt at jeg trenger et bestemt sikkerhetsnivå i en del av systemet, hva må den delen av systemet faktisk gjøre for å levere det?» Den ene produserer kravspesifikasjonen; den andre definerer hva som teller som å oppfylle den. Sammen sitter de mellom anleggseierens risikobilde og OEM-ens sertifiserte komponenter, og dette er også hvor den EU-regulatoriske kjeden — NIS2 for anleggseier-siden, Cyber Resilience Act for produkt-siden — oftest lander i reelle anskaffelseskontrakter.

Målet er det samme som sist. Hvem som helst kan hevde «samsvar med IEC 62443»; spørsmålet som betyr noe er hva de objektivt må kunne demonstrere for å underbygge påstanden. Standardene er formelle og strukturerte nok til at svaret faktisk er kjennbart — forutsatt at du vet hva du skal spørre etter.

Du kan kjøpe de offisielle standardene fra IEC Webstore: IEC 62443-3-2:2020 og IEC 62443-3-3:2013 .

En rask orientering i IEC 62443-familien

For å se hvor 3-2 og 3-3 passer inn, hjelper det å huske den fire-nivå-formen som hele IEC 62443-serien har. Del 1 etablerer terminologi og konsepter. Del 2 dekker retningslinjer og prosedyrer, hovedsakelig for anleggseieren og deres tjenesteleverandører — dekket separat i IEC 62443-2-x: forvaltningssystemet bak et sikkert industrianlegg . Del 3 — hvor dagens to standarder lever — dekker systemnivået. Del 4 dekker de individuelle komponentene som integreres inn i systemet.


IEC 62443-serienCybersikkerhet for IACS
Del 1 — GenereltKonsepter, terminologi
Del 2 — Retningslinjer og prosedyrerAnleggseier og tjenesteleverandør
Del 3 — SystemAnleggseier og systemintegrator
Del 4 — KomponentProduktleverandør / OEM
62443-3-2Sikkerhetsrisikovurderingfor systemdesignMETODIKK
62443-3-3Systemsikkerhetskravog sikkerhetsnivåerKRAV
62443-4-1SDL — prosess
62443-4-2Komponent-kapabilitet

De to standardene i søkelyset i dag sitter klart i Del 3, og de er felles ansvar for **anleggseieren** (operatøren av anlegget) og **systemintegratoren** (ingeniørorganisasjonen som designer og bygger det integrerte systemet). OEM-ens standarder fra Del 4 er relevante her fordi komponentene de leverer må kunne kombineres til et system som oppfyller 3-3, men OEM-en er ikke selv målgruppen for 3-2 og 3-3.

Den utvidede byggeanalogien

Før vi går inn i noen av standardene i detalj, vil en analogi hjelpe — resten av artikkelen lener seg på den. Å konstruere et industrielt kontrollsystem er ikke ulikt det å konstruere et sykehus. Det er flere distinkte fag involvert, hver med sin egen disiplin, og hvert må produsere bevis tilpasset sin rolle.

IEC 62443-3-2 er arkitektens brief og konstruksjonsingeniørens beregninger. Før en eneste murstein legges, bestemmer noen hvilke laster bygningen må tåle, hvor brannskillene skal være, hva slags vinduer som trengs gitt det lokale klimaet, om operasjonsstuene trenger redundant strømforsyning, og hvordan pasientflyter skilles fra personalstrømmer. Resultatet er et sett designbeslutninger med risikobegrunnede mål knyttet til seg: denne korridoren må være et brannskille; dette rommet må ha overtrykk; denne strømmateren må ha reserve. Disse beslutningene tas av folk som er kvalifisert til å ta dem, og signeres ut av bygningens eier. De er ennå ikke en bygning — de er briefen mot hvilken bygningen vil bli konstruert.

IEC 62443-3-3 er byggeforskriften. Den er regelboka som sier: gitt hvilken type bygning du konstruerer og designvalgene som følger av det, her er de spesifikke tingene som må være sanne om den ferdige strukturen. Branndører av en viss klasse må ha gradert hengsler og selvlukkende mekanismer. Nødutganger må være av en

minimumsbredde. Operasjonsstuer i denne kategorien anlegg må ha den-og-den luftvekslingsraten. Forskriften er generisk — den kjenner ikke ditt spesifikke sykehus — men den forteller entreprenøren hva de må oppnå for å tilfredsstille designbriefen.

IEC 62443-4-2 er kvalitetsmerket på hver murstein, branndør og kursvern. Hver enkelt byggekomponent har blitt uavhengig testet og gradert. Når entreprenøren spesifiserer en branndør gradert til FD60, plukker de en dør med sertifikat på den graderingen.

IEC 62443-4-1 er mursteinsfabrikkens kvalitetsstyringssystem. Det er det som gir deg tillit til at det sertifiserte produktet på byggeplassen faktisk er det samme produktet som ble testet for kvalitetsmerket.

Sammen utgjør de fire standardene en kjede der hvert ledd har en klar eier og klare beviskrav. Anleggseieren produserer briefen (3-2). Entreprenøren bygger mot byggeforskriften (3-3) med sertifiserte komponenter (4-2) laget av kvalitetskontrollerte leverandører (4-1). Anleggseieren inspiserer, sertifiserer og drifter den ferdige bygningen. Hver overlevering er en definert artefakt, og hver part er ansvarlig for et definert omfang.

Med det bildet på plass, kommer de to standardene selv nå.

Hva IEC 62443-3-2 faktisk er

IEC 62443-3-2:2020, formelt med tittelen «Security risk assessment for system design», er **metodikkstandarden** for anleggseieren. Den forteller ikke hvordan ditt industrisystem må se ut; i stedet forteller den hvordan du selv kan finne ut det, på en strukturert og gjentakbar måte, basert på faktisk risiko i din faktiske driftskontekst.

Standardens sentrale bidrag er en arbeidsflyt — vanligvis omtalt som **Zone and Conduit Requirements (ZCR)-prosessen** — som tar en beskrivelse av systemet du har til hensikt å beskytte og produserer,

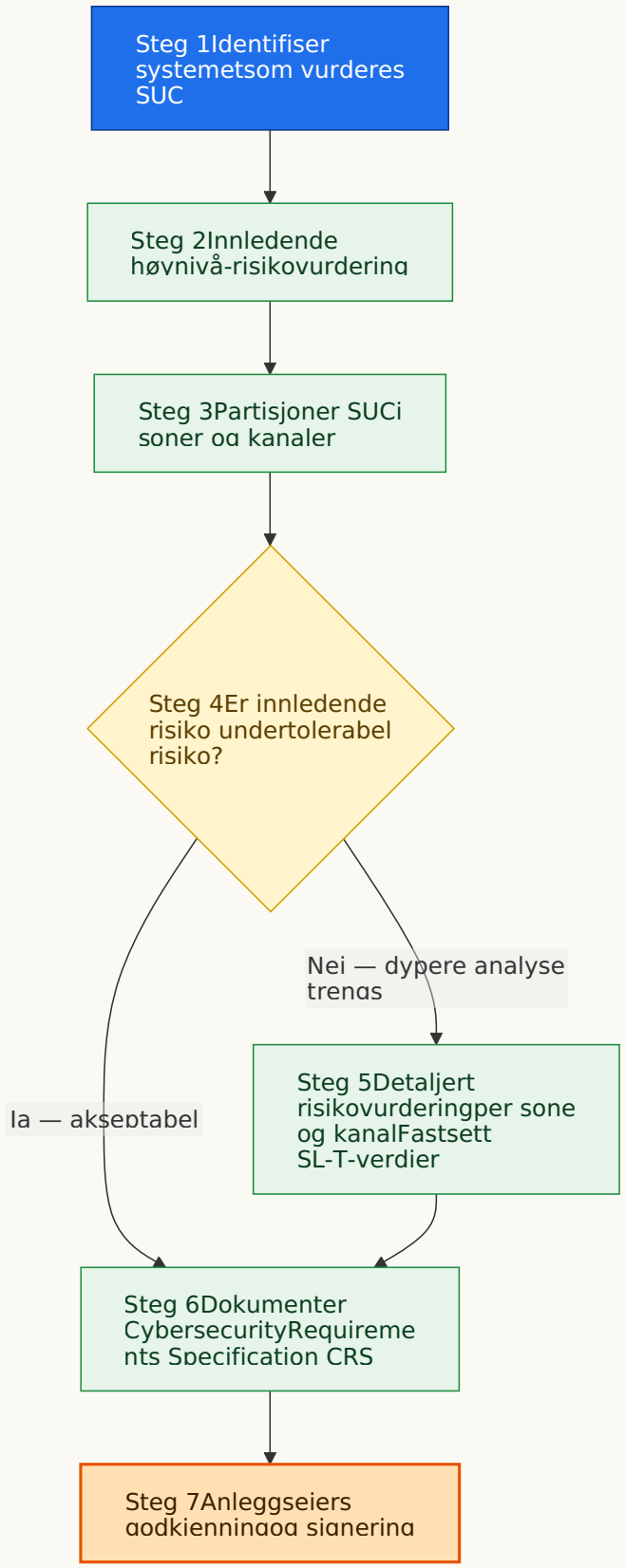
som sin utdata, et partisjonert design med **mål-sikkerhetsnivåer (Target Security Levels, SL-T)** allokert til hver del. Den utdata er den formelle inngangen til neste fase: å velge og integrere komponenter som kan oppfylle de målene, som er der IEC 62443-3-3 tar over.

Hovedmålgruppen for 3-2 er anleggseieren, selv om de nesten alltid vil engasjere ekstern hjelp. Arbeidet krever både dyp prosesskunnskap om anlegget (som anleggseieren har) og spesialisert cybersikkerhetskompetanse (som vanligvis hentes inn, ofte via en systemintegrator eller en uavhengig risikokonsulent). Det endelige ansvaret forblir likevel hos anleggseieren. Hvis en systemintegrator kjører ZCR-workshopene for deg, overfører ikke det ansvaret for det resulterende designet til dem — det overfører ansvaret for kvaliteten på analysen, men beslutningene er dine å ta og signere ut.

Hva 3-2 ikke er, er like viktig å forstå. Det er ikke en risikovurderingsmetodikk i preskriptiv forstand — den forteller deg ikke om du skal bruke en NIST SP 800-30-tilnærming, en ISO 31000-tilnærming, en HAZOP-avledet tilnærming eller noe annet. Den forteller deg hva risikometodikken din må dekke og hva den må produsere, men den overlater valget av underliggende teknikk til organisasjonen din. Dette gjør 3-2 beundringsverdig fleksibel på tvers av sektorer — prosessindustrier kan koble den inn i sin eksisterende HAZOP/LOPA-kultur, mens diskret produksjon eller energiverk kan bruke metoder mer kjent for dem — men det betyr også at «samsvar med 3-2» krever mer enn å plukke en metodikk fra hylla. Det krever å demonstrere at den valgte metodikken faktisk gjør det 3-2 krever av den.

Hva 3-2 betyr praktisk: den syv-stegs arbeidsflyten

Hjertet av IEC 62443-3-2 er en nummerert arbeidsflyt. Selv om standarden uttrykker den mer formelt, koker den i praksis ned til sju steg som flyter fra en beskrivelse av «hva vi beskytter» gjennom til «her er det dokumenterte designet med risikobegrunnede sikkerhetsnivåer».



Det første steget er å **identifisere systemet som vurderes (System Under Consideration, SUC)**. Dette høres trivielt ut, men er sjelden

det. SUC-beskrivelsen må være spesifikk nok til at hvem som helst som leser den senere — en revisor, en etterfølger, en regulator — kan forstå nøyaktig hva som ble vurdert og hva som ikke ble det. I praksis betyr dette et høynivå-arkitekturdiagram, en oversikt over hovedutstyret og programvaren i SUC, et nettverkskart, en eksplisitt uttalelse om forretnings- og sikkerhetsfunksjonene SUC støtter, en liste over eksterne grensesnitt, og en klar merknad om hva som er utenfor omfanget. En SUC som er for snevert avgrenset etterlater farlige antakelser om grensen; en SUC som er for vidt avgrenset produserer analyser som er for grove til å være nyttige.

Det andre steget er en **innledende høynivå-risikovurdering** av SUC-en som helhet. Dette er en grovkornet, kvalitativ gjennomgang som stiller det enkle spørsmålet: hvis den verste troverdige cybersikkerhetshendelsen skjedde med denne SUC, hva ville konsekvensene vært for sikkerhet, miljø, produksjon, regulatorisk stilling og inntekt? Utdata er vanligvis én enkelt «verst troverdig» risikovurdering og en indikasjon på om SUC-en som helhet rettferdiggjør den mer granulære analysen som følger. I nesten alle reelle industrielle settinger gjør den det — men å ha den innledende vurderingen på fil bygger saken for det dypere arbeidet og gir en baseline som restrisikoen senere kan sammenlignes mot.

Det tredje steget er den sentrale designhandlingen i 3-2: **å partisjonere SUC-en i soner og kanaler**. En **sone** er en gruppering av aktiva som deler samme sikkerhetskrav — typisk fordi de har lignende funksjon, lignende konsekvens av svikt, lignende tillitsnivå, eller lignende driftsmiljø. En **kanal** er den kontrollerte kommunikasjonskanalen mellom soner. Å tegne sonene og kanalene er det som gjør et udifferensiert nettverksdiagram om til en sikkerhetsbevisst arkitektur. For å fortsette byggeanalogien, er dette øyeblikket hvor arkitekten bestemmer at «disse rommene utgjør operasjonsstue-suiten, denne korridoren forbinder dem med oppvåkningsavdelingen, og svingdørene på dette punktet vil være

brannskillet». Beslutningen er konsekvensrik fordi alt nedstrøms — SL-T-allokering, komponentvalg, kanalbeskyttelsesmekanismer — flyter fra hvor du trekker disse linjene.

Det fjerde steget spør om den innledende risikoen vurdert i steg to, sett gjennom linsen av den foreslåtte partisjoneringen, allerede faller under anleggseiers tolerable risikoterskel. Hvis den gjør det — kanskje fordi SUC-en er liten, isolert og lav-konsekvens — kan prosessen gå direkte til dokumentasjon. I de fleste reelle industrielle situasjoner gjør den imidlertid ikke det, og arbeidsflyten beveger seg inn i hjertet av analysen i steg fem.

Steg fem er den **detaljerte risikovurderingen, utført per sone og per kanal**. Det er her trusler, sårbarheter og konsekvenser systematisk analyseres for hver sone og kanal ved å bruke uansett hvilken risikometodikk organisasjonen har vedtatt. Det avgjørende utfallet av dette steget er **mål-sikkerhetsnivået (SL-T)** for hver sone og kanal. SL-T uttrykkes i standardens én-til-fire-skala brukt andre steder i 62443, og — viktig — uttrykkes vanligvis per grunnkrav — så en enkelt sone kan ha en SL-T-vektor som (3, 2, 3, 2, 2, 2, 2) på tvers av FR1 til FR7. Ulike soner vil vanligvis ha ulike vektorer. En sone som inneholder det sikkerhetsinstrumenterte systemet til et raffineri, for eksempel, vil typisk kreve høyere SL-T for FR3 (System Integrity) enn ingeniørkontorets generelle IT-nettverk som sitter i en annen sone.

Steg seks er **dokumentasjon**. Utdata fra hele prosessen må fanges i en formell artefakt, konvensjonelt kalt **Cybersecurity Requirements Specification (CRS)**. CRS-en registrerer SUC-beskrivelsen, sonene og kanalene, SL-T-ene, antakelsene som er gjort (for eksempel «vi antar at bedriftens brannmur blokkerer all innkommende SMB-trafikk til kontrollnettverket»), begrensningene som er erkjent (for eksempel «den eldre PLS-familien i bruk støtter ikke multifaktorautentisering, så kompenserende kontroller anvendes

på kanalen»), og enhver restrisiko som bevisst er akseptert. CRS-en er mer enn intern dokumentasjon — den er den kontraktsmessige broen mellom anleggseier og systemintegrator. Det er det integratoren må levere mot under 3-3.

Det sjuende og siste steget er **anleggseiers godkjenning**. Standarden er eksplisitt på at anleggseieren er ansvarlig: en integrator eller konsulent kan ha produsert dokumentet, men anleggseieren må bevisst akseptere konklusjonene og restrisikoen det innebærer. I praksis betyr dette vanligvis signering på et definert seniornivå — ofte av noen i drifts- eller asset management-linjen som kan holdes ansvarlig for cybersikkerhetsstillingen ved anlegget.

Hva anleggseieren må bevise objektivt for 3-2

Når en anleggseier hevder samsvar med IEC 62443-3-2, bør de på forespørsel kunne produsere den dokumentariske oversikten over å ha gjort arbeidet skikkelig. Samsvar med 3-2 handler ikke om et sertifikat på veggen — det finnes ingen utbredt tredjepartssertifiseringsordning for anleggseier-samsvar med 3-2, slik ISASecure SDLA og CSA eksisterer for OEM-er. I stedet handler demonstrasjon om **bevispakken**.

En troverdig bevispakke begynner med **SUC-beskrivelsen** i nok detalj til at en ekstern vurderer kan spore tilbake hva som ble vurdert og hva som ble bevisst ekskludert. Den inkluderer **metodikken** som ble brukt — det eksplisitte risikovurderingsrammeverket valgt, med sine poenggivningsregler og risikoterskler. Den inkluderer **trusselkildene** som ble vurdert, ideelt med referanse til en aktuell trusselkatalog som ENISAs ICS-trusselrapporter, MITRE ATT&CK for ICS, sektorvise informasjonsdelings- og analysesentre (som E-ISAC for elektriske energiverk), eller nasjonale CSIRT-rådgivere. Den inkluderer **risikoregisteret** som resulterte fra stegene fire og fem, med hver sone og kanals risiko før kontroll og restrisiko skrevet ned.

Den inkluderer **sone- og kanaldiagrammet** selv — typisk et nettverksaktig skjema overlagt med fargede sonegrenser og merkede kanaler. Og den kulminerer i **Cybersecurity Requirements Specification**, signert ut på et passende nivå i anleggseiers organisasjon.

Standarden foreskriver ikke hvor ofte denne øvelsen må gjentas, men god praksis er å gjennomgå CRS-en når SUC-en endrer seg vesentlig, når trussellandskapet skifter betydelig, eller i en fast syklus på typisk tre til fem år. Bevis på denne gjennomgangskadensen — møtereferater, versjonskontrollerte CRS-revisjoner, en dokumentert endringskontrollprosess — er i seg selv en nyttig demonstrasjon av samsvar.

Det er en finurlighet verdt å dvele ved. Samsvar med 3-2 er ikke det samme som å ha «lav risiko» i det resulterende systemet. En anleggseier kan fullt ut samsvare med 3-2 og fortsatt bevisst akseptere relativt høy restrisiko i noen soner — forutsatt at den beslutningen er dokumentert, begrunnet av forretningskontekst, og godkjent av noen med myndighet til å gjøre det. Det 3-2 krever er bevis på å ha resonnert om det skikkelig, ikke et bestemt utfall. Standarden er prosedyremessig i ånden, ikke preskriptiv om resultater. Dette er noen ganger ubehagelig for revisorer som forventer å se en «bestått/ikke bestått»-dom, men det er det riktige designet for en standard som må tjene alt fra et avløpsrenseanlegg til et atomkraftverk.

Hva IEC 62443-3-3 faktisk er

Hvis 3-2 spør «hvilket sikkerhetsnivå trenger jeg hvor?», så spør **IEC 62443-3-3:2013** «hva må et system på et gitt sikkerhetsnivå faktisk kunne gjøre?». Den har tittelen «System security requirements and security levels», og er **kravkatalog-standarden** for systemlaget.

3-3 definerer **systemkrav (System Requirements, SRs)** gruppert under de samme syv grunnkravene som brukes andre steder i IEC 62443 — Identification and Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, og Resource Availability. Hvert SR er en kapabilitet som et integrert industrielt automasjons- og kontrollsystem må støtte, uttrykt på en måte som i stor grad er uavhengig av noen bestemt leverandørs produkter. Mange SR-er har en eller flere **kravsforsterkninger (Requirement Enhancements, REs)** som gjelder på høyere sikkerhetsnivåer — samme idé som i 4-2, der et grunnleggende SR forsterkes på SL 3 eller SL 4 med ekstra grundighet. Standarden inneholder i størrelsesorden femti pluss SR-er, med den totale tellingen som klatrer godt over hundre når REs inkluderes; den nøyaktige tellingen avhenger av hvordan du teller.

Målgruppen for 3-3 er hovedsakelig **systemintegratoren** — ingeniørorganisasjonen som tar anleggseiers CRS og gjør den om til et levert integrert system. Produktleverandøren bryr seg indirekte om 3-3 fordi komponentene deres, sertifisert til 4-2 , må kombineres på en slik måte at systemet som helhet kan oppfylle 3-3-systemnivå-kravene. Anleggseieren bryr seg fordi de må kunne verifisere at det leverte systemet faktisk oppnår det som ble spesifisert.

En nyttig mental modell er at 3-3 er til systemet det 4-2 er til komponenten. Begge standardene bruker de samme syv grunnkravene som sin organiserende ryggrad. Begge uttrykker krav på en leverandørnøytral måte. Begge graderer kravene etter sikkerhetsnivå 1 til 4. Forskjellen er integrasjonsnivået kravet gjelder på. Et 4-2-krav kan være «komponenten skal støtte unik brukerautentisering». Det tilsvarende 3-3-kravet kan være «systemet skal håndheve unik brukerautentisering på tvers av alle sine komponenter, inkludert føderering av identiteter der flere komponenter deltar i en enkelt brukersesjon, med revisjonsloggning av autentiseringshendelser som kan korreleres sentralt».

Komponenten kan være kapabel, men integrasjonen er det som gjør kapabiliteten reell.

Hva 3-3 betyr praktisk

En god måte å forstå hva 3-3 faktisk krever, er å se på noen av systemkravene gjennom linsen av hva de oversettes til for ingeniørteamet som bygger systemet.

Under grunnkrav 1 (Identification and Authentication Control) forventer 3-3 at systemet leverer unik kontoidentifikasjon på tvers av alle brukere og enheter, støtter sterke autentiseringsmekanismer passende for SL-en, og — på høyere SL-er — krever multifaktor-autentisering for sensitive operasjoner som ingeniørendringer eller modifikasjoner av sikkerhetssystemer. Praktisk betyr dette at et system på SL-T 3 ikke kan stole på delte innlogginger, generiske operatørkontoer eller hardkodede enhetspassord; identitet må være unik, sporbar og kryptografisk støttet.

Under FR 2 (Use Control) må systemet håndheve rollebasert tilgang, må begrense kjøring av mobilkode, må beskytte revisjonsinformasjon mot manipulasjon, og må støtte kontinuerlig overvåking av hvem som gjorde hva når. Dette oversettes til et system hvis ingeniørarbeidsstasjoner logger hver parameterendring til et manipulasjonsbevis revisjonsspor, hvis operatørskjermer begrenser hva en operatør kan gjøre basert på en definert rolle, og hvis programmeringsenheter ikke kan kjøre vilkårlig kode ved uhell eller ved en ondsinnet USB-pinne.

Under FR 3 (System Integrity) må systemet beskytte seg mot uautoriserte endringer av fastvare, konfigurasjon og data, både i bevegelse og i hvile. Kommunikasjonskanaler mellom soner (**kanalene** identifisert under 3-2) må beskytte meldingsintegritet, og systemet må støtte kryptografisk verifisering av programvaren og fastvaren som kjører på sine komponenter. På høyere SL-er utvider

dette seg til å inkludere kontinuerlig integritetsovervåking og automatisert deteksjon av uautoriserte endringer.

Under FR 4 (Data Confidentiality) må sensitiv informasjon i bevegelse og i hvile beskyttes. På lavere SL-er kan dette bety transportlag-kryptering for ingeniørsesjoner; på høyere SL-er inkluderer det beskyttelse av legitimasjon i lagring, kryptering av lagrede konfigurasjonsdata, og beskyttelse mot side-kanal-avsløring på delt infrastruktur.

Under FR 5 (Restricted Data Flow) må systemet operasjonelt støtte sone-og-kanal-arkitekturen som er pålagt av 3-2. Det må støtte håndheving av kanalgrensene (typisk via brannmurer, énveis-gateways eller datadioder i høyere-SL-soner), det må forhindre uautorisert lateral trafikk mellom soner, og på høyere SL-er må det inkludere mekanismer for å oppdage og varsle ved brudd på kanal-policyen.

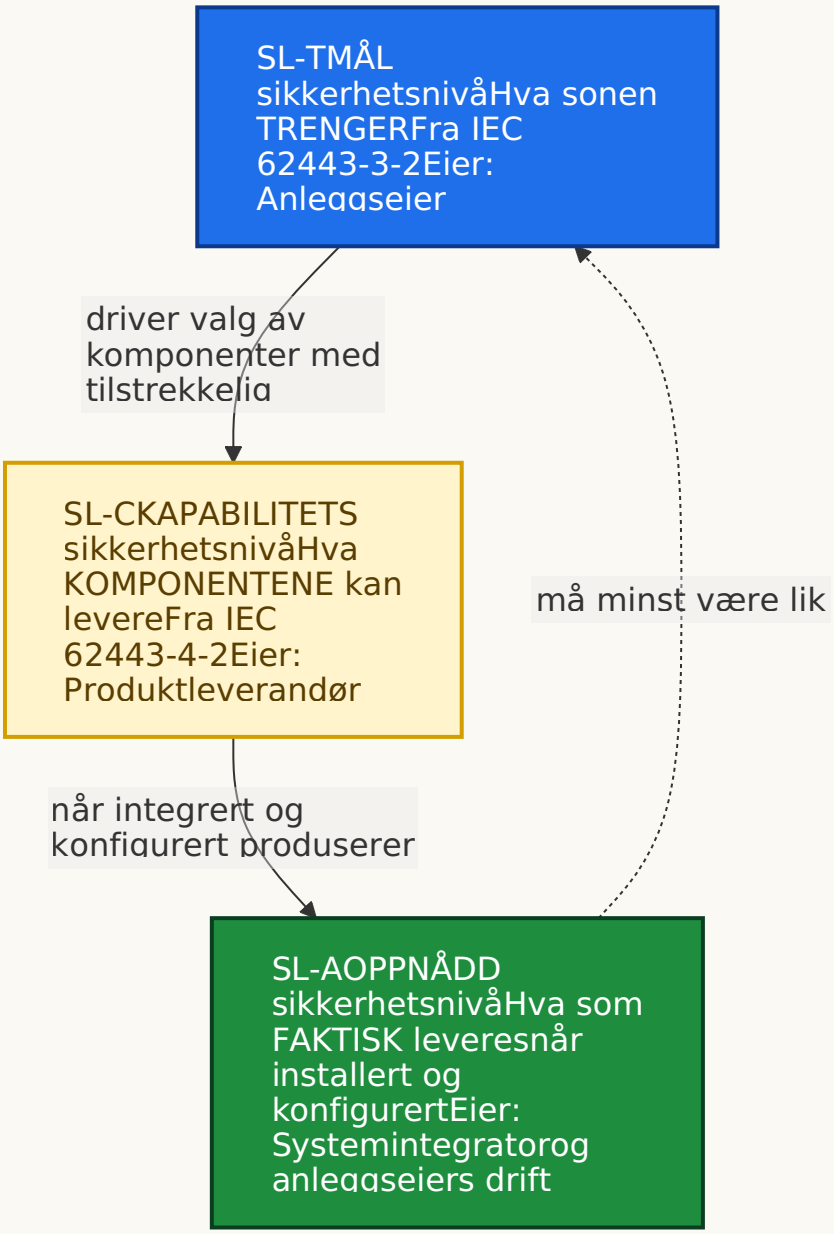
Under FR 6 (Timely Response to Events) må systemet produsere, lagre, beskytte og gjøre tilgjengelig et sammenhengende sett med sikkerhetsrelevante hendelser — logger som tillater deteksjon, undersøkelse og gjenoppretting. På høyere SL-er inkluderer dette integrasjon med Security Information and Event Management (SIEM)-systemer, evnen til å støtte nær-sanntidsvarsling, og rettsmedisinsk kvalitet på bevisbevaring.

Under FR 7 (Resource Availability) må systemet være motstandsdyktig mot tjenestenekt-forhold, må støtte sikkerhetskopiering og gjenoppretting av all kritisk konfigurasjon og data, og må kunne operere trygt når det er degradert. Dette er hvor industrispesifikke bekymringer — graceful feilmoduser, deterministisk oppførsel, prioriterte nøddrift — møter generiske krav til cybersikkerhetstilgjengelighet.

En nyttig måte å forestille seg 3-3 som helhet er som en sjekkliste av systemkapabiliteter, indeksert etter SL. På SL-T 1 er listen «beskytt mot tilfeldige eller utilsiktede brudd»; på SL-T 4 er listen «beskytt mot tilsiktede brudd med sofistikerte midler med utvidede ressurser, IACS-spesifikke ferdigheter og høy motivasjon» — bredt sett trusler i nasjonalstats-klasse. Listen over SR-er er den samme på tvers av alle fire SL-er; det som endres er dybden, grundigheten og ressursene for hver kapabilitet. Standarden er omhyggelig om dette — for hvert SR setter standardens hovedtekst SL 1-baselinen, og REs løfter den eksplisitt opp på SL 2, 3 og 4.

Det viktigste diagrammet: SL-T, SL-C og SL-A

Av alle konseptene i IEC 62443 er forholdet mellom de tre typene sikkerhetsnivå det som oftest blandes — og det som gjør mest skade når det misforstås. De tre er villedende like i sine forkortelser, og anskaffelsesdokumenter konflaterer dem rutinemessig. Å internalisere forskjellen er, etter min erfaring, det enkelt mest nyttige en kjøper eller operatør kan gjøre når de begynner å jobbe med denne standardfamilien.



SL-T, mål-sikkerhetsnivået, kommer ut av IEC 62443-3-2. Det uttrykker hva anleggseieren har bestemt er nødvendig i hver sone, basert på risikovurderingen. Det er en uttalelse om etterspørsel. Det tilhører anleggseieren.

SL-C, kapabilitets-sikkerhetsnivået, kommer ut av IEC 62443-4-2 . Det uttrykker hva et bestemt produkt teknisk er i stand til å levere når det er riktig konfigurert. Det er en uttalelse om tilbud. Det tilhører produktleverandøren.

SL-A, oppnådd sikkerhetsnivå, gjelder det leverte systemet. Det uttrykker hva det integrerte, installerte, konfigurerte og operasjonaliserte systemet faktisk gjør i det levende anlegget. Det er en uttalelse om virkelighet. Det er felles ansvar for systemintegratoren (for som-bygget) og anleggseieren (for som-driftet).

Tre regler styrer hvordan disse forholder seg, og det er regler jeg vil anbefale å lære utenat. For det første kan ingen sone oppnå en SL-A høyere enn det laveste SL-C av noen komponent som sitter i den sonen — din sone er bare så sterk som dens svakeste ledd, og en enkelt SL-C 1-komponent i en ellers SL-C 3-sone drar den oppnåelige SL-A-en tilbake til 1 for den FR-en komponenten er svak i. For det andre betyr en SL-A under SL-T-en at designet ikke har levert mot kravene; enten trengs ytterligere kompenserende kontroller (kanskje på kanalen, kanskje prosedyremessig), SL-T-en må revurderes mot revidert risikoaksept, eller restrisikoen må formelt aksepteres av anleggseieren. For det tredje er SL-C en kapabilitet, ikke en garanti: en komponent sertifisert til SL-C 3 utplassert med sikkerhetsfunksjonene slått av bidrar med ikke mer enn SL-C 1 til sonen, og den vanligste måten for en SL-A å komme til kort i forhold til en SL-T er at SL-C-kapable funksjoner forblir avskrudd i felt.

Denne tre-bokstavs-trioen er ryggraden i ethvert forsvarlig 62443-basert design. Når en leverandørbrosjyre sier «SL 3-sertifisert», er det første spørsmålet «SL-hva 3?». Når en anskaffelsesspesifikasjon sier «systemet skal være SL 2», er neste spørsmål «SL-T 2, SL-C 2 eller SL-A 2?» — fordi hvert innebærer en annen forpliktelse på en annen part. En velskrevet anbudstekst skiller dem eksplisitt: «systemet skal designes og leveres for å oppnå en SL-A på minst 2 på tvers av FR1 til FR7, med komponenter med dokumentert SL-C på minst 2, til støtte for en SL-T på 2 som bestemt i den vedlagte Cybersecurity Requirements Specification». Den ene setningen — som kombinerer alle tre SL-typene, navngir de relevante

standardene, og peker tilbake til CRS-en — fjerner mye potensiell tvetydighet.

Hva systemintegratoren må bevise objektivt for 3-3

Når en systemintegrator hevder samsvar med IEC 62443-3-3 for et levert system, bør anleggseieren forvente en sammenhengende bevispakke som sporer fra CRS-en produsert under 3-2, gjennom design- og anskaffelsesbeslutningene, til det som-bygde systemet og dets idriftsettingstester. Denne bevispakken er sjelden et enkelt dokument; den er oftere en strukturert samling artefakter som, tatt sammen, danner et reviderbart spor.

Integratoren må demonstrere **sporbarhet** mellom hver SL-T i CRS-en og systemkravene i 3-3 som har blitt anvendt i designet. For hver sone må integratoren vise hvilke SR-er på det relevante SL-et som ble vurdert, hvilke som ble implementert, hvilke som ble kompensert for via andre midler, og hvilke som formelt ble notert som ikke gjeldende med en skriftlig begrunnelse. Dette fanges vanligvis i en kravsporbarhetsmatrise som løper langs designdokumentasjonen og vedlikeholdes gjennom hele prosjektlivssyklusen. Matrisen er det enkeltdokumentet en revisor oftest vil be om først.

Integratoren må demonstrere **komponentvalgs-rasjonalet**: at komponentene som er valgt for hver sone har en SL-C minst like høy som SL-T-en for den sonen, for hvert relevante grunnkrav. Dette beviset er typisk hentet fra komponentenes egne 62443-4-2 -sertifikater (ISASecure CSA, IECEE CB Scheme, eller tilsvarende) krysshenvist med integratorens stykkliste. Der en valgt komponent ikke har tredjeparts 4-2-sertifisering, må integratoren begrunne valget og vise hvordan de tilsvarende 3-3-SR-ene oppfylles gjennom arkitektoniske eller kompenserende tiltak — kanskje ved å plassere komponenten bak en høyere-SL-gateway, ved å isolere den i en undersone, eller ved å anvende prosedyremessige kontroller.

Integratoren må demonstrere at **systemet har blitt verifisert og validert**. Dette inkluderer designgjennomganger mot SR-ene, fabrikkakseptansetesting (FAT), site-akseptansetesting (SAT), og sikkerhetsspesifikk testing som konfigurasjonsrevisjoner, sårbarhetsskanning av som-bygde systemet, og — der SL-T-en rettferdiggjør det — penetrasjonstesting av representative angrepsbaner. Testrapporter må kobles tilbake, via sporbarhetsmatrisen, til SR-ene de verifiserer. En penetrasjonstest som produserer en hundresiders rapport som ikke kan knyttes til kravene den testet, er mye mindre nyttig enn et stramt avgrenset oppdrag rettet mot SR-ene som betyr noe.

Integratoren må demonstrere at **det leverte systemet overleveres med dokumentasjonen som trengs for at anleggseieren skal kunne drifte det sikkert**. Dette betyr herdingsguider, sikkerhetskonfigurasjons-baselines, kontooversikter, dokumentasjon for logg- og SIEM-integrasjon, sikkerhetskopierings- og gjenopprettingsprosedyrer, runbooks for hendelseshåndtering skreddersydd for det spesifikke systemet, og en sikkerhetsdriftsmanual som forklarer hvordan hvert grunnkrav overvåkes og vedlikeholdes i drift. Overleveringspakken er det som gjør SL-A bærekraftig heller enn et endags-øyeblikksbilde på slutten av idriftsettingen.

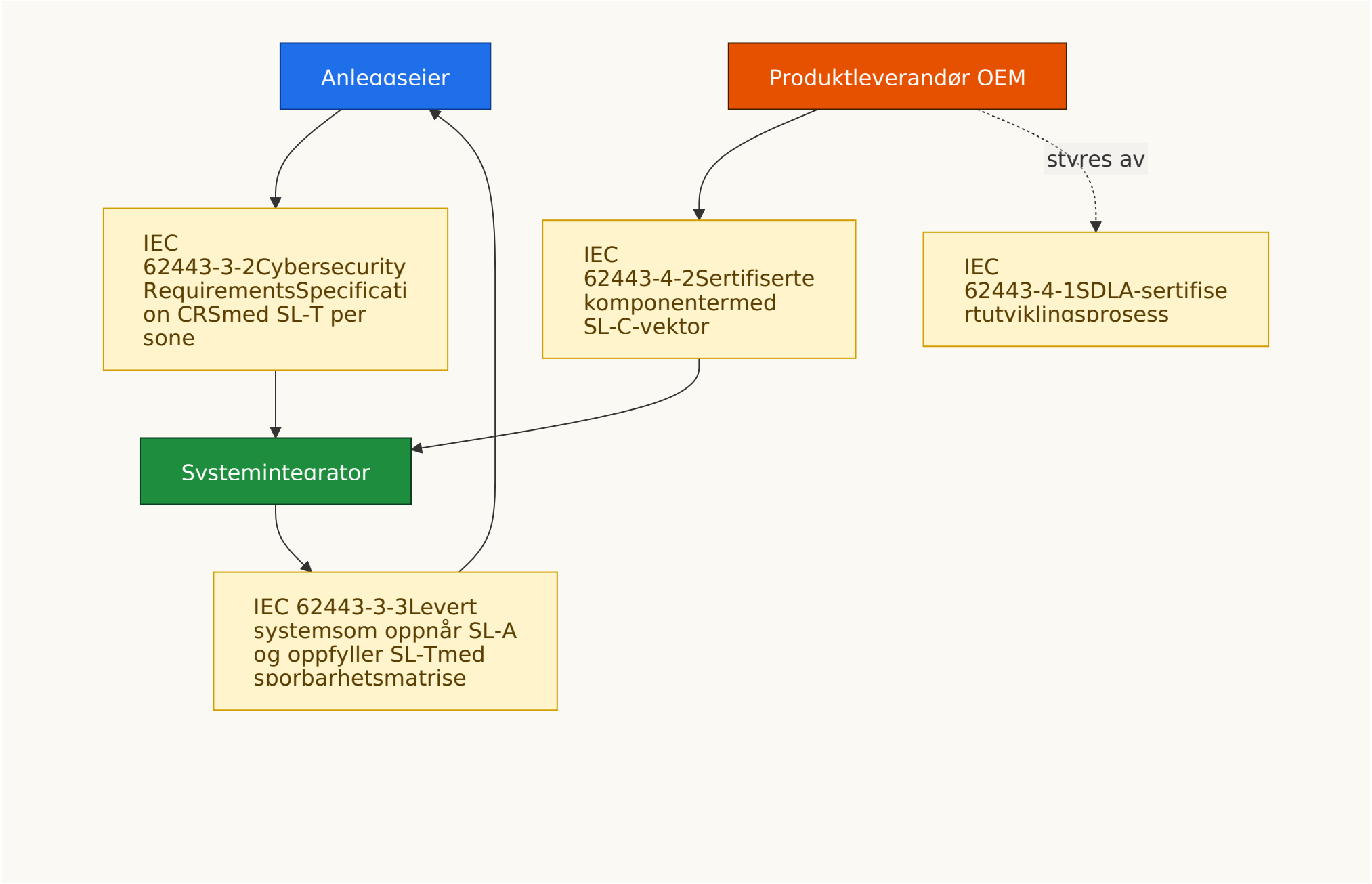
Tredjeparts-sertifiseringsruten for systemer er **ISASecure SSA** (System Security Assurance), som sertifiserer en spesifikk systemimplementasjon mot IEC 62443-3-3. Som CSA for komponenter, bærer SSA forutsetningen at leverandøren har en underliggende SDLA-sertifisert prosess for eventuelle komponenter de produserer internt. SSA er materielt mindre vanlig enn CSA, delvis fordi hver systeminstallasjon er skreddersydd, men det er det nærmeste man kommer et «kvalitetsmerke» for integrerte systemer i 62443-verdenen, og verdt å spørre etter når systemet det er snakk

om er en av leverandørens standard produkttilbud (en pakkebasert SCADA-løsning, for eksempel) heller enn en engangs-integrasjon.

Det er også en fremvoksende søsterordning — ISASecure SDA (Site Deployment Assurance) — som er ment å dekke den utplasserte installasjonen på en måte SSA ikke gjør. Per skrivende stund er SDA i ulike pilotstadier på tvers av industrien. Anleggseiere bør følge med på dette, fordi det potensielt lukker tillitsgapet mellom «det leverte systemet» (SSA) og «systemet slik det faktisk drifter på mitt anlegg» (SL-A i sin sanneste forstand).

Hvordan 3-2, 3-3, 4-1 og 4-2 alle passer sammen

En ren måte å visualisere forholdet mellom alle fire standardene er å tenke på fire parter som overlater hverandre definerte artefakter, hvor hver part er ansvarlig for et definert omfang og hver overlevering støttet av bevis som en utenforstående vurderer kan kontrollere.


Anleggseier
Produktleverandør OEM
styres av
IEC 62443-3-2Cybersecurity RequirementsSpecification CRSmed SL-T per sone
IEC 62443-4-2Sertifiserte komponentermed SL-C-vektor
IEC 62443-4-1SDLA-sertifisertutviklingsprosess
Systemintegrator
IEC 62443-3-3Levert systemsom oppnår SL-A og oppfyller SL-Tmed sporbarhetsmatrise

Anleggseieren utfører risikovurderingen under 3-2 og produserer CRS-en. Systemintegratoren tar CRS-en og leverer et system som samsvarer med 3-3, ved å bruke komponenter sertifisert til 4-2 av produktleverandører hvis utviklingsprosesser er sertifisert til 4-1. Hver part overlater den neste en definert artefakt — en CRS, en SL-C-vektor med et sertifikat, et system med sporbarhet — og hver part er ansvarlig for et definert omfang.

En nyttig test av enhver konkret utplassering er å spørre, for et hvilket som helst kontrollmål, tre spørsmål i rekkefølge: hvem eier dette, hvilken standard styrer det, og hvilket bevis dokumenterer det? Hvis noen av disse tre svarene er uskarpe, har kjeden et svakt ledd. Hvis alle tre svarene er klare, har du en forsvarlig posisjon enten du ser på det som anleggseieren, integratoren, regulatoren, eller forsikringsselskapet.

To andre deler av 62443 sitter også ved siden av disse fire. **IEC 62443-2-1** styrer anleggseiers bredere cybersikkerhets-forvaltningssystem — retningslinjene, prosedyrene, opplæringen og styringen som omslutter det tekniske arbeidet dekket i 3-2 og 3-3. **IEC 62443-2-4** styrer sikkerhetsegenskapene til tjenesteleverandører (typisk systemintegratorer og vedlikeholdsentreprenører) — menneskene, prosessene og kompetansene de bringer til ditt anlegg. Begge dekkes i detalj i IEC 62443-2-x: forvaltningssystemet bak et sikkert industrianlegg . Et komplett bilde for et enkelt industristed krever vanligvis bevis under flere av disse delene samtidig, med 3-2 og 3-3 som danner den tekniske kjernen i design- og leveringshistorien.

Det EU-regulatoriske bakteppet er også verdt å nevne her. Under NIS2 er anleggseiere innenfor omfanget av Annex I-sektorer (energi, transport, vann, produksjon osv.) pålagt å implementere leverandørkjede-sikkerhetstiltak under Artikkel 21(2)(d); en dokumentert 3-2 CRS med SL-T-allokering er den mest forsvarlige

måten å bevise at leverandørkjedekravene er risikobegrunnede heller enn vilkårlige. Under Cyber Resilience Act må industrielle produkter med digitale elementer plassert på EU-markedet oppfylle Annex I essensielle krav, som i praksis lettest bevises gjennom 4-2-sertifisering med den tilhørende 4-1-utviklingsprosessen — nøyaktig oppstrøms av kjeden som 3-3 deretter integrerer.

Vanlige fallgruver og røde flagg

Den mest hyppige fallgruven i 3-2-arbeid er å gjøre partisjoneringen før risikovurderingen. Fristelsen er enorm: ta det eksisterende nettverksdiagrammet, tegn noen bokser rundt det som allerede er segmentert på Layer 3, og kall de sonene. Dette produserer et sonekart som reflekterer historiske kablingsbeslutninger heller enn nåværende risiko, og det tenderer å under-beskytte nye høy-konsekvens-aktiva mens det over-beskytter lav-konsekvens legacy-aktiva. Risikovurderingen må drive partisjoneringen, ikke omvendt. En nyttig diagnostikk er å se på sonegrensene og spørre: er disse grensene i tråd med konsekvenskategorier, eller med VLAN-tagger? Hvis det siste, har soneinndelingen blitt gjort baklengs.

En annen vanlig fallgruve er å konflatere SL-T med SL-C i anskaffelsesdokumenter. En spesifikasjon som sier «systemet skal være SL 3» uten kvalifikasjon overlater til leverandøren å tolke om det betyr komponenter i stand til SL 3 (SL-C 3), et som-bygget system som oppnår SL 3 (SL-A 3), eller et mål drevet av risiko (SL-T 3). Disse innebærer ganske ulike kostnadsstrukturer og ganske ulike forpliktelser. Som diskutert tidligere, betaler disiplinen med å skille de tre SL-typene i anbudsspråk seg tilbake mange ganger i klarheten på den resulterende leveransen.

En tredje fallgruve er å anta at 4-2-sertifiserte komponenter automatisk gir et 3-3-samsvarende system. Det gjør de ikke. Integrasjonen betyr minst like mye som komponentene. Usikre

kanalvalg, dårlig konfigurerte autentiseringssystemer, ubeskyttede jump-verter, uovervåket loggning, delte tjenestekontoer opprettet under idriftsetting og aldri fjernet — hvilken som helst av disse kan dra et SL-C 3 komponentsett ned til en SL-A 1-virkelighet. Tilstedeværelsen av sertifiserte komponenter er nødvendig, men ikke tilstrekkelig.

Et fjerde rødt flagg er påstander om «IEC 62443-samsvarende» uten et delnummer. Standarden har mange deler, hver med en definert målgruppe. En samsvarspåstand fra en systemintegrator bør nevne 62443-3-3 (og sannsynligvis 62443-2-4 for deres tjenesteleveranse-praksis). En påstand fra en produktleverandør bør nevne 62443-4-1 og 62443-4-2 . En påstand fra en anleggseier bør nevne 62443-2-1 og 62443-3-2. Enhver påstand som ikke navngir en del er, i beste fall, upresis — og vanligvis et signal om at taleren ikke er kjent med hvordan standardfamilien er organisert.

En femte fallgruve er foreldede CRS-dokumenter. En CRS produsert for ti år siden for en SUC som siden har lagt til et nytt anlegg, to nye kontrollnettverk og en flåte fjernaksess-laptoper, er ikke lenger et troverdig dokument. Refresh-sykluser betyr noe, og bevispakken bør vise dem. En CRS uten en versjonshistorikk eller en definert gjennomgangsplan er en CRS bare i navn.

En sjette og mer subtil fallgruve er **sone-omfangs-drift**: soner som ble definert snevert under 3-2-analysen, men som gjennom anleggets levetid stille har absorbert ekstra aktiva gjennom små endringsordrer som hver virket rimelige isolert. Total-effekten er at SL-T-en opprinnelig allokert til sonen ikke lenger dekker alt i sonen. Sunn asset management-praksis — endringskontroll som eksplisitt refererer CRS-en, ny-vurdering når aktiva krysser sonegrenser — er det som forebygger dette.

En sjekkliste for anskaffelse og revisjon

Det følgende kan brukes som et kontraktsvedlegg, et leverandørspørreskjema eller en intern revisjons-sjekkliste.

For anleggseiers egen 3-2 bevispakke

- En aktuell, versjonskontrollert **System Under Consideration (SUC)-beskrivelse** med omfang eksplisitt oppgitt.
- Et eksplisitt **risikovurderings-metodikkdokument** som refererer rammeverket valgt (NIST SP 800-30, ISO 31000, sektorspesifikt eller annet) med poenggivningsregler.
- En **trusselkatalog** trukket fra troverdige kilder (ENISA, MITRE ATT&CK for ICS, sektorvise ISACs, nasjonale CSIRT-rådgivere) med oppgitt aktualitetsdato.
- Et **sone- og kanaldiagram** som viser partisjoneringen, med soner og kanaler entydig merket.
- Et **risikoregister** som fanger risiko før kontroll og restrisiko per sone og per kanal.
- En **Cybersecurity Requirements Specification (CRS)** som inneholder SL-T-vektoren for hver sone og kanal, antakelsene, begrensningene og eventuelle kompenserende tiltak som er forutsatt.
- **Anleggseiers signering** av CRS-en på et definert seniornivå, med dato.
- En **gjennomgangskadens** for CRS-en, med bevis på tidligere gjennomganger og dato for neste planlagte gjennomgang.

For systemintegrators 3-3 leveranse-bevispakke

- En **kravsporbarhetsmatrise** som kobler hver SL-T i CRS-en til spesifikke systemkrav i 62443-3-3 og til designelementene som tilfredsstiller dem.

- En **stykkliste** med hver komponents 62443-4-2-sertifikat referert (eller, der en komponent er usertifisert, en skriftlig begrunnelse og de kompenserende kontrollene som er anvendt).
- Et **designdokumentasjons-sett** som viser sone-implementasjon, kanalbeskyttelsesmekanismer, autentiseringsarkitektur, loggningsarkitektur, sikkerhetskopiering- og gjenopprettings-arkitektur, og driftsgrensesnitt.
- **FAT-rapporter (Factory Acceptance Test)** med sikkerhetsspesifikke testtilfeller koblet til SR-ene de verifiserer.
- **SAT-rapporter (Site Acceptance Test)** inkludert konfigurasjonsrevisjon, sårbarhetsskanningsutdata, og enhver penetrasjonstesting utført.
- En **overleveringspakke** inkludert herdingsguider, konfigurasjons-baselines, kontooversikter, SIEM-/loggintegrasjonsdokumentasjon, sikkerhetskopierings- og gjenopprettingsprosedyrer, og en sikkerhetsdriftsmanual.
- En **endringsstyringsprosess** for det som-bygde systemet, som definerer hvordan etterfølgende modifikasjoner vil bevare den oppnådde SL-A og hvordan CRS-en vil bli konsultert på nytt.
- Der det er aktuelt, et **ISASecure SSA-sertifikat** for systemet eller dets kjerneplattform, med omfang, nivå og gyldighetsdato.

Spørsmål til å stille en systemintegrator skriftlig

- Hvilken versjon av IEC 62443-3-3 har det foreslåtte systemet blitt designet mot?
- For hver sone i vår CRS, hva er den foreslåtte SL-C-profilen på komponentene valgt, og hvordan kartlegges den mot vår SL-T?
- Hvilke komponenter i din foreslåtte stykkliste innehar et aktuelt tredjeparts 62443-4-2-sertifikat? For hver, hva er sertifikatnummeret, utstedende organ, sertifisert fastvare-/programvareversjon, og utløpsdato?

- For enhver komponent uten tredjeparts 62443-4-2-sertifisering, hvilke kompenserende tiltak vil levere de relevante systemkravene?
- Vil leveransen inkludere en sporbarhetsmatrise som kobler SL-T til SR til designelement til verifiseringstest? Kan vi se en prøve fra et tidligere prosjekt?
- Hvilken endringsstyringsprosess vil gjelde for systemet etter overlevering, slik at modifikasjoner ikke uthuler den oppnådde SL-A?
- Er din tjenesteleveranse-praksis sertifisert eller vurdert mot IEC 62443-2-4 ?

IEC 62443-3-2 er standarden som forteller anleggseieren hvordan de skal finne ut, på en strukturert og forsvarlig måte, hvilket sikkerhetsnivå hver del av deres industrisystem faktisk trenger. **IEC 62443-3-3** er standarden som forteller systemintegratoren hva et integrert system på det sikkerhetsnivået faktisk må gjøre. Sammen sitter de mellom anleggseiers risikobilde og OEM-ens sertifiserte komponenter, og de er der beviskjeden enten henger sammen eller brister.

Behandle 3-2 som dokumentet som rettferdiggjør hele nedstrøms-programmet. En klar CRS, signert ut på riktig nivå og gjennomgått med fornuftig kadens, er den enkelt viktigste artefakten en anleggseier kan produsere — fordi det er linsen som hver påfølgende anskaffelse, hver systemoppgradering, hver sikkerhetsrevisjon og hver hendelsesrespons tolkes gjennom. Behandle 3-3 som spesifikasjonen en integrators arbeid blir bedømt mot. En sporbarhetsmatrise fra CRS gjennom til SR gjennom til verifisert testresultat er integratorens forsvar i enhver fremtidig tvist om

systemet ble levert som spesifisert. Og husk alltid at komponenter med riktig SL-C, integrert i riktige soner og kanaler, kun blir en reell SL-A når noen drifter systemet dag etter dag med sikkerhetsfunksjonene skrudd på. Standardiseringsorganer kan ikke håndheve den delen — kun god drift kan.

IEC 62443-4-1 og 4-2: hva en OEM faktisk må bevise

13. mai 2026 · 19 min lesetid · #compliance #security #industrial #iec-62443

Hvis du kjøper, spesifiserer eller drifter industrielt utstyr — en PLS, en RTU, en HMI, en industriell svitsj, en SCADA-gateway, en ingeniørarbeidsstasjon — har du nesten helt sikkert sett en leverandørbrosjyre som hevder å være «i samsvar med IEC 62443», «i tråd med 62443-4-2», eller «designet etter 62443-prinsippene». Disse formuleringene kan bety nesten hva som helst, fra en grundig revidert internasjonal sertifisering til lite annet enn ønsketenkning på et bildekort.

De to delene av standarden som nesten alltid blir nevnt er **IEC 62443-4-1** (om hvordan produktet ble bygget) og **IEC 62443-4-2** (om hva produktet kan gjøre). Denne artikkelen forklarer begge i klart språk og — viktigst av alt — angir hva en OEM må bevise objektivt for å underbygge et samsvarskrav, slik at du kan verifisere det heller enn å stole på det.

Denne teksten sitter i OEM-/produkt-hjørnet av IEC 62443-familien. Systemlaget — hvordan en anleggseier dimensjonerer sikkerhetskravet (3-2) og hvordan systemintegratoren leverer mot det (3-3) — dekkes i IEC 62443-3-2 og 3-3: hva anleggseiere og integratorer må bevise . Forvaltningssystem-laget — retningslinjene, programmene, tjenesteleverandørene og oppdateringsdisiplinen som omslutter det tekniske arbeidet — dekkes i IEC 62443-2-x: forvaltningssystemet bak et sikkert industrianlegg .

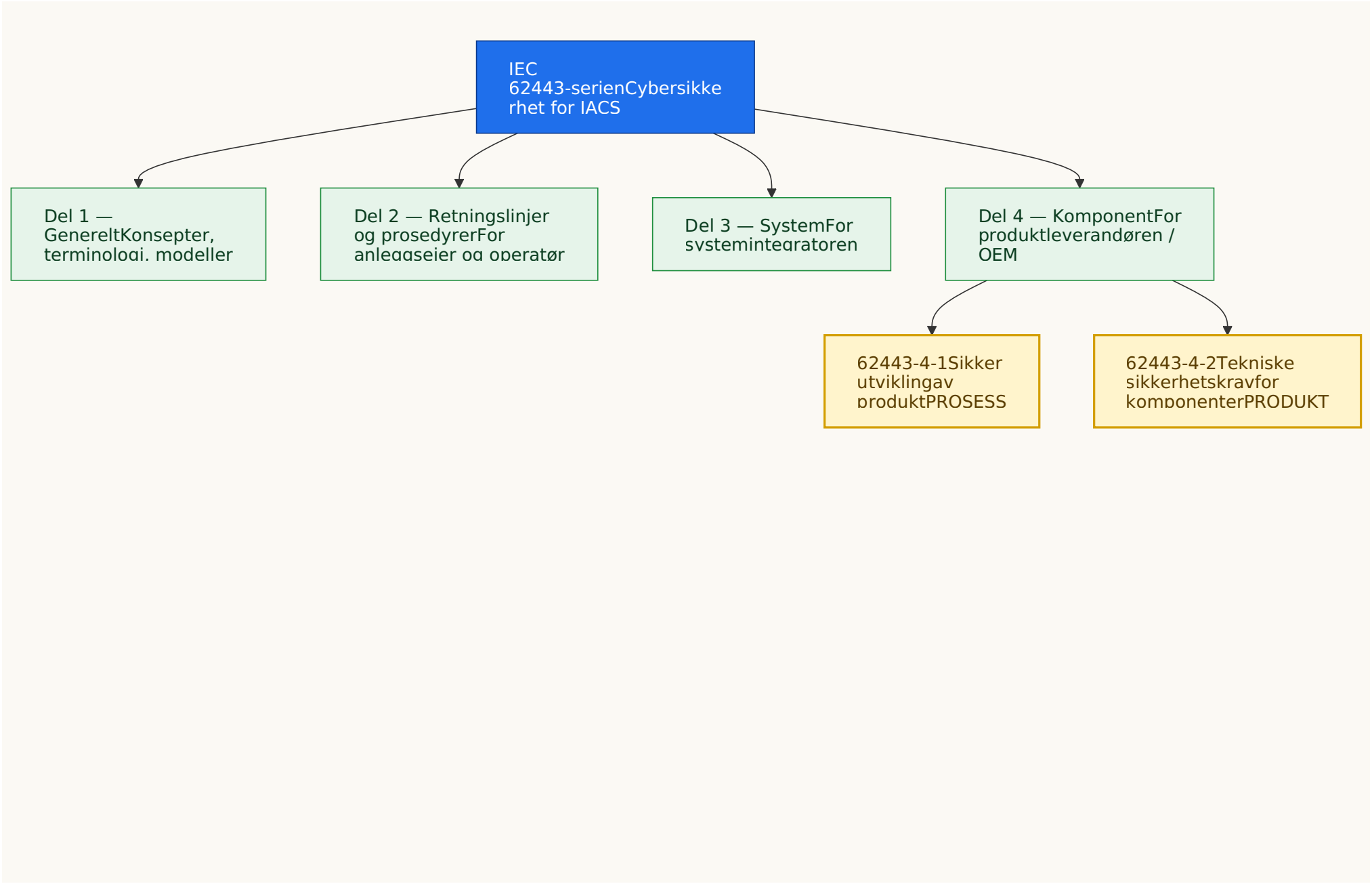
Den står også ved siden av to regulatoriske følgesvenner: spørsmålet om virksomhetens omfang, Gjelder NIS2 for ditt EU-prosjekt? , og spørsmålet om produktets omfang, Gjelder Cyber Resilience Act for

ditt produkt? . Når en industriell OEM leverer til EU, lener CRAs essensielle krav seg i økende grad på IEC 62443-4-1/4-2-bevis som det praktiske beviset, og NIS2-anleggseiere under Vedlegg I kaskaderer de samme kravene tilbake gjennom sine leverandørkontrakter. Dokumentene henvender seg til ulike publikum, men beviskjeden løper gjennom dem alle.

Du kan kjøpe de offisielle standardene fra IEC Webstore: IEC 62443-4-1:2018 og IEC 62443-4-2:2019 .

En to-minutters orientering: IEC 62443-familien

IEC 62443 er en serie standarder for cybersikkerhet i industrielle automasjons- og kontrollsystemer (IACS). Den er utgitt i fellesskap av International Electrotechnical Commission (IEC) og International Society of Automation (ISA), og er organisert i fire nivåer, hver rettet mot et ulikt publikum.


IEC 62443-serienCybersikkerhet for IACS
Del 1 — GenereltKonsepter, terminologi, modeller
Del 2 — Retningslinjer og prosedyrerFor anleggseier og operatør
Del 3 — SystemFor systemintegratoren
Del 4 — KomponentFor produktleverandøren / OEM
62443-4-1Sikker utviklingav produktPROSESS
62443-4-2Tekniske sikkerhetskravfor komponenterPRODUKT

De to vi bryr oss om her sitter begge i **Del 4 — Komponent**, og er produktleverandørens ansvar:

- **IEC 62443-4-1** regulerer **hvordan produktet utvikles** — ingeniørprosessen, menneskene, kontrollene bak kulissene.
- **IEC 62443-4-2** regulerer **hva produktet teknisk sett kan gjøre** — dets innebygde sikkerhetsfunksjoner.

Tenk på det slik: 4-1 er kjøkkenet og kokken; 4-2 er måltidet på tallerkenen. Et hygienisk kjøkken garanterer ikke et fantastisk måltid, og et tilsynelatende velsmakende måltid kan fortsatt komme fra et skittent kjøkken — derfor vil seriøse kjøpere ha forsikring om begge.

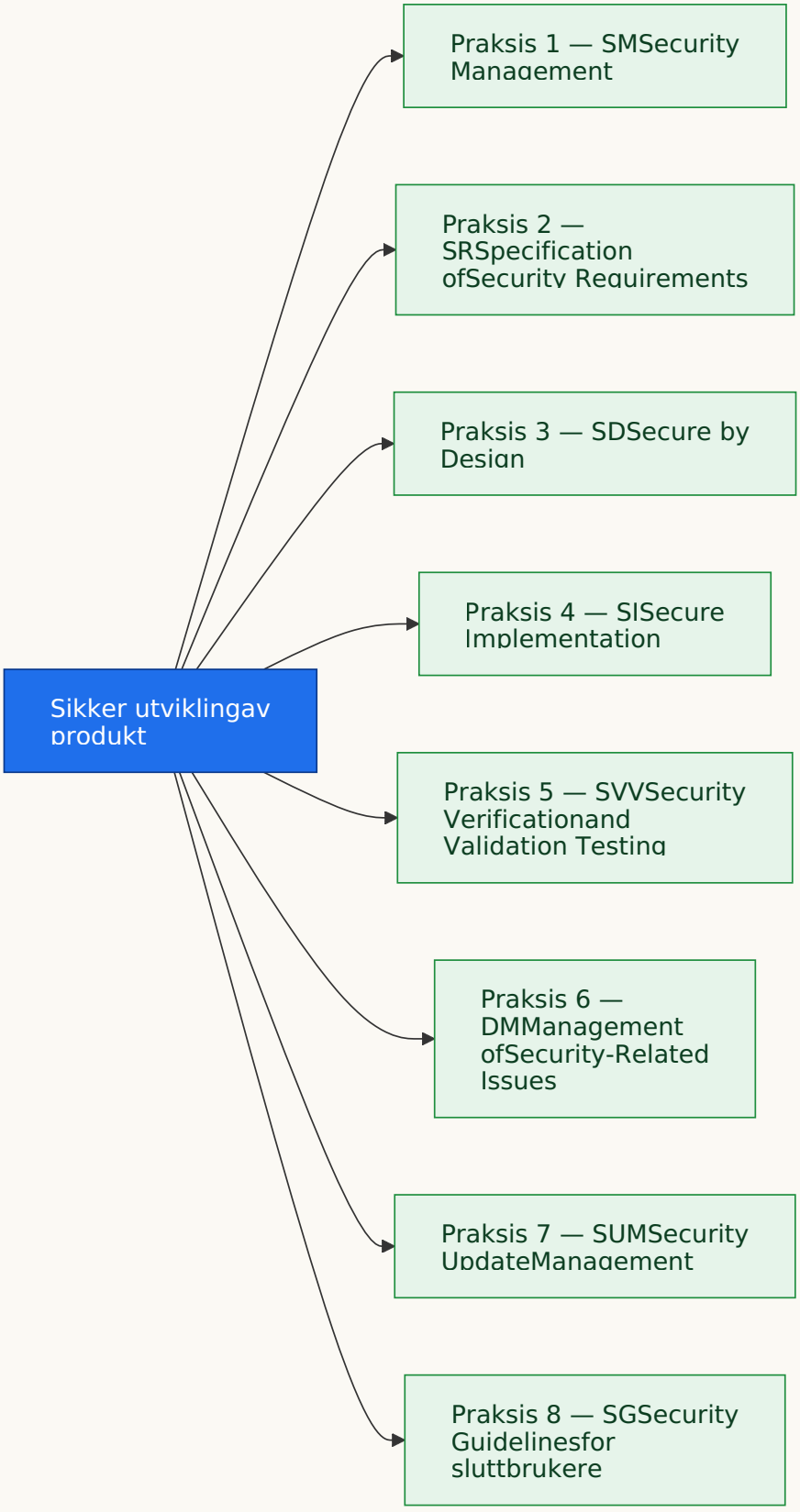
Hva IEC 62443-4-1 faktisk er

IEC 62443-4-1:2018, med tittelen «Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements», definerer en **Secure Development Lifecycle (SDL)** for industrielle produkter. Ifølge IECs egen beskrivelse dekker standarden «security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life» og gjelder utvikler og vedlikeholder av produktet, ikke integratoren eller sluttbrukeren.

Med andre ord: 4-1 er **prosessfokusert**. Den spør ikke «er fastvaren sikker?» Den spør «bygde du den på en måte som gjør sikker fastvare sannsynlig, gjentakbar og forbedrbar over tid?»

De 8 praksisene

Standarden grupperer kravene sine i åtte navngitte **praksiser**. Sammen dekker de hele buen fra opprinnelig produktidé til ende-av-støtte.



På tvers av disse åtte praksisene definerer standarden **47 toppnivå-krav**, som igjen folder ut i hundrevis av underkrav.

Sertifiseringsorganet Baker Hughes nevner dette eksplisitt i sitt offentlige whitepaper om sin egen IEC 62443-4-1 prosessvurdering: «there are a total of 47 top-level requirements, this actually consists of hundreds of sub-requirements» — og publiserer hjelpsomt sin egen poengsetting mot alle 47.

Modenhetsnivåer 1 til 4

IEC 62443-4-1 låner fra Capability Maturity Model Integration (CMMI)-tradisjonen. I stedet for å spørre «gjør dere X?» spør den «hvor godt gjør dere X?» Det er fire modenhetsnivåer (Maturity Levels, ML):

ML	Navn	Hva det betyr i klart språk
ML 1	**Initial**	Praksisen skjer, men er ad hoc og stort sett udokumentert. Ulike team kan gjøre ting forskjellig.
ML 2	**Managed**	Skrevne retningslinjer og prosedyrer finnes. Ansatte er opplært i dem. Praksisen er gjentakbar.
ML 3	**Defined (Practiced)**	Den dokumenterte praksisen følges påviselig og konsekvent på tvers av hele organisasjonen, med revisjonsbart bevis for bruk på reelle prosjekter.
ML 4	**Improving**	Organisasjonen samler målepunkter om praksisen, overvåker effektiviteten og bruker disse målepunktene påviselig til å forbedre den.

Et kritisk poeng som mange kjøpere går glipp av: under 62443-4-1 plukker du ikke «kirsebær» — for å hevde et gitt modenhetsnivå må alle relevante krav være oppfylt på det nivået. ML 2 på noen praksiser og ML 3 på andre er ikke «ML 3 totalt»; det er i beste fall ML 2 organisasjonsdekkende.

Hva 4-1 betyr praktisk for en OEM

Oversatt fra standardspråk er dette hva hver praksis betyr for menneskene som bygger produktet.

1. Security Management (SM) — «Noen har ansvaret, og det er jobben deres»

OEM-en må ha utnevnte roller for produktsikkerhet, allokert budsjett, definerte ansvarsområder, og integrert sikkerhetsaktiviteter i den formelle produktutviklingsplanen. Konfidensiell informasjon (kildekode, signeringsnøkler, trusselmodeller) må være kontrollert. Underleverandører og leverandører må holdes til samme standard.

Analogi: det er forskjellen mellom en fabrikk der noen er den navngitte HMS-ansvarlige med myndighet, opplæring og budsjett, og en der «sikkerhet» er den som tilfeldigvis tenker på det den uka.

2. Specification of Security Requirements (SR) — «Skriv ned hva 'sikker' betyr for dette produktet»

For hvert produkt (eller produktfamilie) må OEM-en produsere en skriftlig sikkerhetskontekst: hvor skal denne enheten leve, hvilke trusler står den overfor, hvilke tillitsgrenser krysser den, hvilke datastrømmer flyter inn og ut, hvilket mål-sikkerhetsnivå (SL-T) forventes? Disse kravene må godkjennes og versjonskontrolleres.

3. Secure by Design (SD) — «Bygg sikkerhet inn, ikke skru den på etterpå»

Det er her **trusselmodellering** bor. Arkitekturen og det detaljerte designet må analyseres for trusler (STRIDE, angrepstrær, eller tilsvarende), og de resulterende avbøtende tiltakene må designes inn før en linje produksjonskode er skrevet. Dybdeforsvar, minste privilegium og sikre standardinnstillinger må være eksplisitte arkitekturvalg, ikke ettertanker.

Analogi: i moderne bilbygging er deformasjonssoner, airbager og ABS designet inn i chassiset fra første skisse. Du kan ikke oppnå samme kollisjonssikkerhet ved å sveise ekstra plater på en ferdig bil på slutten av linjen. Samme logikk.

4. Secure Implementation (SI) — «Skriv koden ordentlig, og kontroller skrivingen»

Vedtatte kodestandarder (f.eks. CERT C, MISRA, SEI-veiledning), kollegafellesgjennomgang av kode, statisk applikasjonssikkerhetstesting (SAST) og regler for håndtering av usikret input. Kritisk dekker dette også **tredjeparts- og åpen kildekode-komponenter**: OEM-en må vite hva som er i produktet, hvor det kom fra og om det fortsatt støttes.

5. Security Verification and Validation Testing (SVV) — «Prøv å knekke det før noen andre gjør det»

Et dokumentert testprogram som inkluderer, som minimum: funksjonell sikkerhetstesting, **sårbarhetsskanning**, **fuzz-testing**, **penetrasjonstesting**, og **angrepsflate-analyse**. Resultatene skrives opp, defekter spores og testplanen er gjentakbar.

6. Management of Security-Related Issues (DM, defektstyring) — «Når noe blir funnet, hva skjer da?»

En dokumentert sårbarhetshåndteringsprosess: hvordan rapporter mottas (en publisert sikkerhetskontakt, helst en politikk for koordinert avsløring), hvordan de triageres, hvordan rotårsaksanalyse gjøres, hvordan rettelser produseres og spores, og hvordan kunder informeres. CVE-tildeling og en track record av CVE-håndtering er nøkkelbevis her.

7. Security Update Management (SUM) — «Oppdateringer som faktisk når feltet»

En dokumentert oppdaterings- og sikkerhetsoppdateringsprosess. Dette må dekke testing av oppdateringer før utgivelse, sikker levering (signerte oppdateringer), kundevarsling, støttetidslinjer og politikk for ende-av-liv.

8. Security Guidelines (SG) — «Fortell brukeren hvordan han skal bruke det sikkert»

Bruker-rettet dokumentasjon: herdingsveiledere, sikker konfigurasjonsveiledning, dybdeforsvars-anbefalinger, råd om kontostyring, instruksjoner for avvikling og en klar oversikt over hvilke sikkerhetsfunksjoner som finnes og hvordan de skrus på. Dette er praksisen som mest direkte kobler 4-1 til 4-2 — fordi 4-2-egenskaper kun er nyttige hvis kunden kan finne og konfigurere dem.

Hva en OEM må bevise objektivt for 4-1

Å demonstrere samsvar med IEC 62443-4-1 er sakens kjerne i OEM-ens påstand — og det bør ikke være en markedspåstand. Det bør være en posisjon OEM-en kan forsvare med dokumenter på bordet. Slik ser de dokumentene ut.

Dokumentariske og prosessuelle bevis

- En **skriftlig, versjonskontrollert Secure Development Lifecycle-politikk** som kartlegges på alle åtte praksiser og de 47 kravene.
- Et **organisasjonskart** som viser hvem som eier produktsikkerhet, med navngitte roller, opplæringsregistreringer og sikkerhetskompetanse hos nøkkelpersonell (utviklere, testere, arkitekter).
- **Sikkerhetsopplæringsregistreringer** for utviklings-, test- og produktledelsesstab — typisk oppdatert årlig.
- En **produktsikkerhetsplan** for det spesifikke produktet i omfanget, inkludert sikkerhetskonteksten, mål-SL, trusselmodell og tillitsgrenser.
- Et **trusselmodelldokument** for hvert produkt i omfanget (STRIDE, DREAD, angrepstrær eller tilsvarende) med sporbarhet inn i design og tester.

- **Sikkerhetskravs-sporbarhet** fra trusselmodellen → designbeslutninger → implementering → testtilfeller. En kjøper kan spørre: «Vis meg hvordan trussel T-17 i trusselmodellen er avdempet i designet, hvor i koden, og hvilken test som bekrefter det.»
- Skriftlige **sikre kodestandarder** som staben bruker, pluss **kodegjennomgangsregistreringer** og **statisk analyseverktøy-utdata**.
- **Software Composition Analysis (SCA)** registreringer eller en SBOM-stil oversikt over tredjeparts-/åpen kildekode-komponenter, med bevis på sårbarhetsovervåking mot dem.
- Et dokumentert **testprogram** med rapporter: sårbarhetsskanninger, fuzz-test-kampanjer, penetrasjonstest-rapporter, angrepsflate-gjennomgang.
- En **publisert sårbarhetshåndteringspolitikk og politikk for koordinert avsløring**, pluss en track record av CVE-er håndtert (tidslinjer, rådgivere, rettelser sendt).
- En **oppdaterings- og sikkerhetsoppdateringsprosedyre** med en reell historie av råd og oppdateringer.
- **Sluttbruker-sikkerhetsretningslinjer, herdingsveiledere og produktsikkerhetsråd** som OEM-en publiserer og vedlikeholder.

Tredjepartssertifisering — gullstandarden

Det mest troverdige objektive beviset er et tredjepartssertifikat utstedt av et akkreditert sertifiseringsorgan. For 62443-4-1 er de to hovedordningene:

- **ISASecure SDLA** (Security Development Lifecycle Assurance), drevet av ISA Security Compliance Institute (ISCI). Ifølge ISASecure-ordningsbeskrivelsen gjelder SDLA «applies to the development lifecycle processes of suppliers for control system products» og «certifies compliance to ISA/IEC 62443-4-1». SDLA

tilbys på fire nivåer — **SDLA Level 1, 2, 3 og 4** — som tilsvarer de fire modenhetsnivåene i standarden. Sertifisøren «evaluates the specific documented version of the organization's process to assess whether it meets the requirements stated in the SDLA specification» og «reviews representative artifacts to verify that each ISASecure SDLA requirement is being followed for products under the scope of the process».

- **IECEE CB-ordningen** for industriell cybersikkerhet, som tilbyr tilsvarende samsvarssertifikater utstedt av IECEE-anerkjente CBTL-er (Certification Body Test Laboratories). Se www.iecee.org .

To omfangsfeller å passe på

To detaljer på ethvert 4-1-sertifikat betyr mer enn overskriften:

1. **Omfanget av prosessen** — nøyaktig hvilket utviklingssted, hvilken forretningsenhet og hvilken produktlinje som dekkes. En leverandør som opererer i fem land kan kun ha ett sted sertifisert. Sertifikatet vil si det; brosjyren vanligvis ikke.
2. **Modenhetsnivået som hevdes** — og om vurdereren registrerte noen praksiser som «utenfor omfang» eller «ikke gjeldende». Baker Hughes' offentlige sertifikat, for eksempel, sier transparent at det ble vurdert til **ML 2** og at **46 av de 47** praksisene var i omfang (én ble ekskludert, med begrunnelse). Det er den slags klarhet du skal se etter og spørre etter.

Hva IEC 62443-4-2 faktisk er

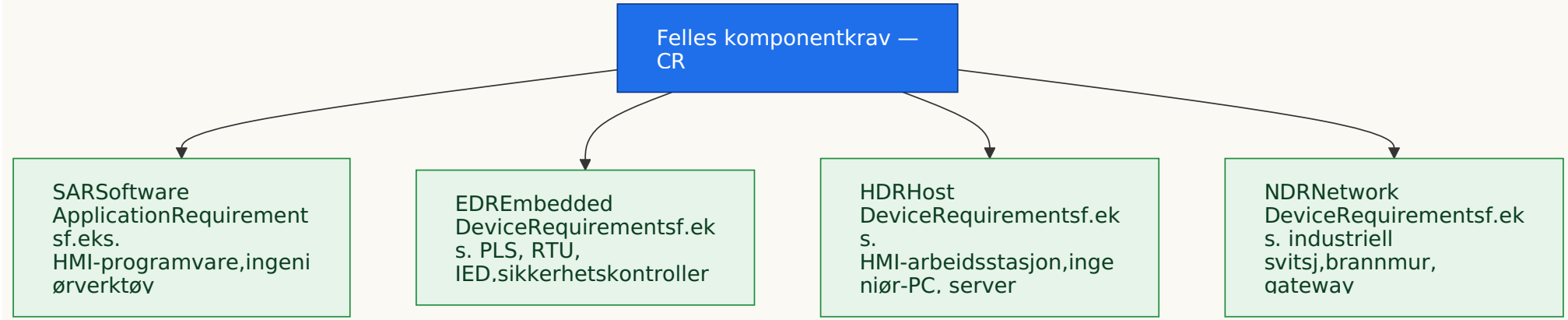
IEC 62443-4-2:2019, «Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components», definerer hva en individuell industriell **komponent** teknisk må kunne gjøre for å hevde et gitt sikkerhetsnivå. Per IECs egen omfangsuttalelse «provides detailed technical control system component requirements (CRs) associated with the seven

foundational requirements (FRs)» og definerer **kapabilitets-sikkerhetsnivå** for komponenter, **SL-C(component)**.

Der 4-1 ser på utviklingsorganisasjonen, ser **4-2 på selve produktet** — dets identifikasjonsmekanismer, tilgangskontroll, kryptografi, logging, oppdateringsmekanisme, herding, motstandsdyktighet.

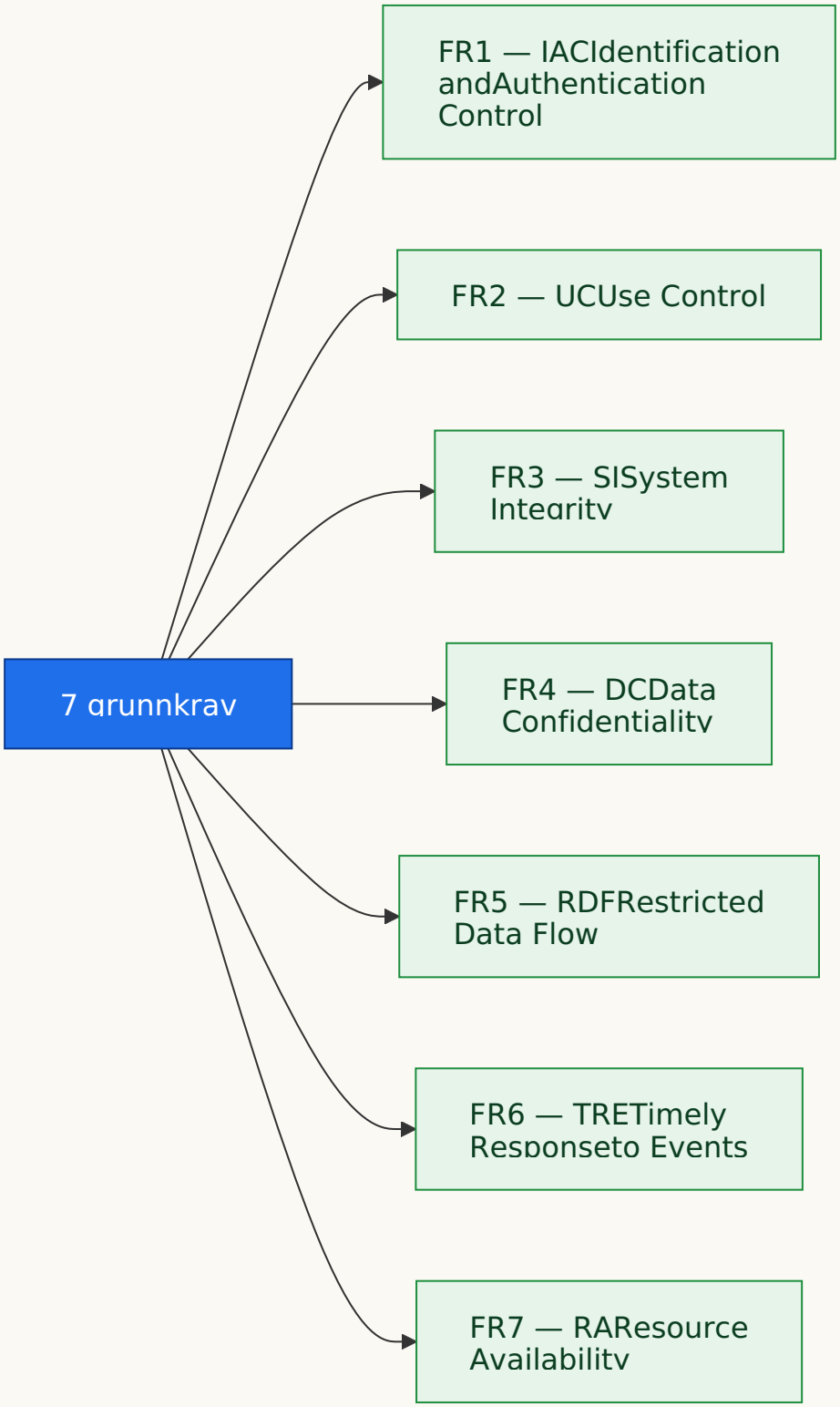
De fire komponenttypene

Standarden anerkjenner at «en PLS» og «en Windows-ingeniørarbeidsstasjon» ikke er samme dyr, og ikke alle krav gjelder likt for begge. Så krav er delt i en felles kjerne (betegnet **CR**, for Component Requirement) pluss et lag av typespesifikke krav:


Felles komponentkrav — CR
SARSoftware ApplicationRequirement sf.eks. HMI-programvare,ingeni ørverktøv
EDREmbedded DeviceRequirementsf.ek s. PLS, RTU, IED,sikkerhetskontroller
HDRHost DeviceRequirementsf.ek s. HMI-arbeidsstasjon,inge niør-PC, server
NDRNetwork DeviceRequirementsf.ek s. industriell svitsj,brannmur, gateway

De syv grunnkravene

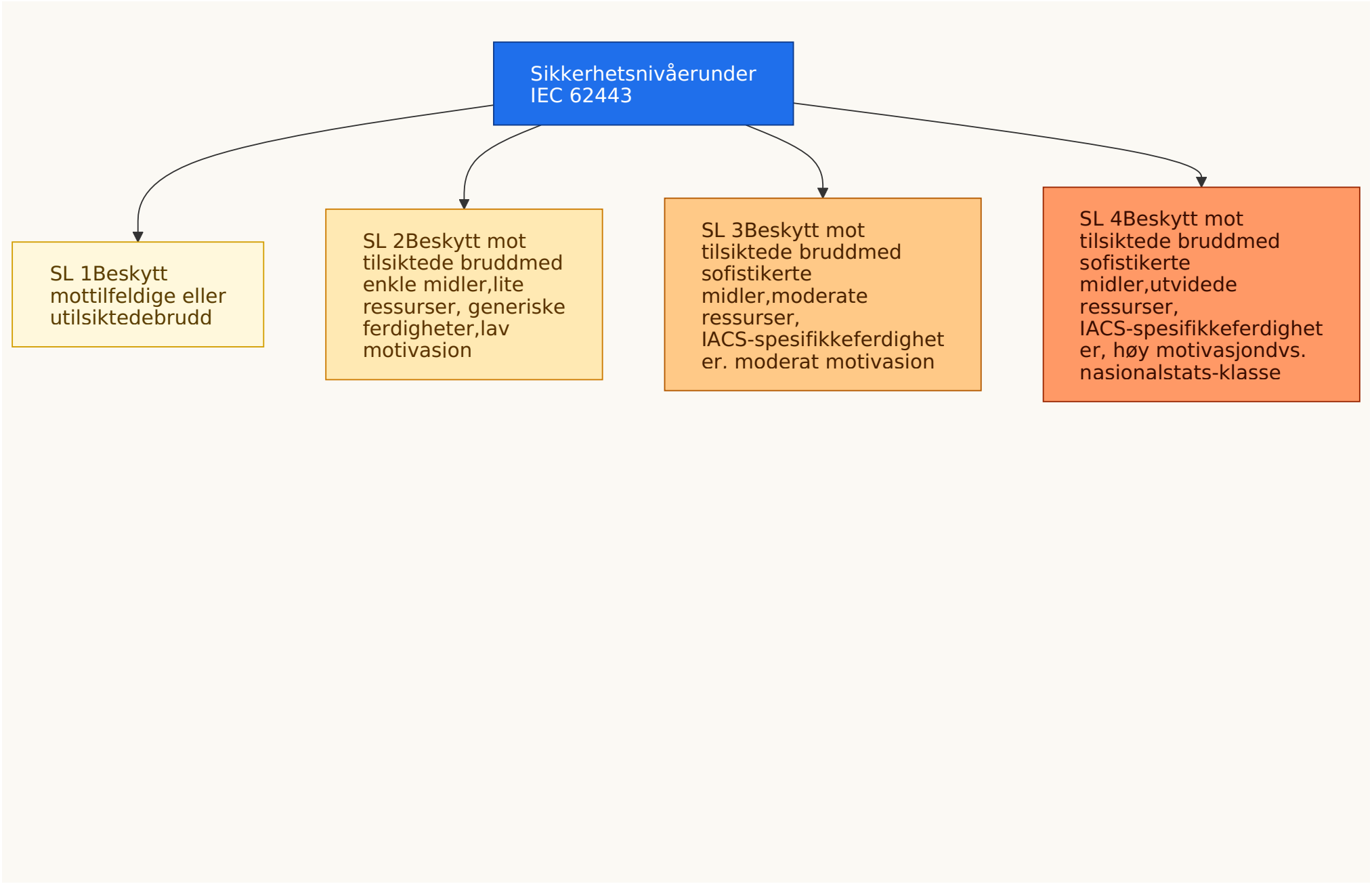
Alle krav i 4-2 er avledet fra de **syv grunnkravene (Foundational Requirements, FRs)** som ble innført helt tilbake i IEC TS 62443-1-1:



Under hvert FR sitter et antall **komponentkrav (CRs)**, som hver kan ha en eller flere **kravsforsterkninger (Requirement Enhancements, REs)** som slår inn på høyere sikkerhetsnivåer. Totalt antall CR-er er rundt **60–70** (ofte sitert som 67) før REs og komponenttypespesifikke varianter telles; det presise antallet avhenger av hvordan du teller typespesifikke EDR/HDR/NDR/SAR-regler. Noen publiserte sammendrag (som Security Compass' oversikt) refererer til «more than 140 specific cybersecurity requirements» når REs og komponentvarianter inkluderes.

Sikkerhetsnivåer 1 til 4 — gradert etter trusselmodell

Genialiteten i 4-2 er at samme krav kan gjelde med økende strenghet avhengig av hvem du forventer skal angripe deg. De fire sikkerhetsnivåene er:


Sikkerhetsnivåerunder IEC 62443
SL 1Beskytt mottilfeldige eller utilsiktedebrudd
SL 2Beskytt mot tilsiktede bruddmed enkle midler,lite ressurser, generiske ferdigheter,lav motivasion
SL 3Beskytt mot tilsiktede bruddmed sofistikerte midler,moderate ressurser, IACS-spesifikkeferdigheter. moderat motivasion
SL 4Beskytt mot tilsiktede bruddmed sofistikerte midler,utvidede ressurser, IACS-spesifikkeferdigheter, høy motivasjondvs. nasionalstats-klasse

Analogi: tenk på Euro NCAP-kollisjonstest-rangeringer for biler. En én-stjerners bil er gate-lovlig, men du vil ikke sette familien din i den på motorveien. En fem-stjerners bil er konstruert for å absorbere et alvorlig sammenstøt. SL 1 til SL 4 fungerer på samme måte: du velger nivået driftsmiljøet ditt rettferdiggjør, og du betaler (i kostnad, kompleksitet og konfigurasjonsoverhead) deretter. For de fleste generelle industrielle miljøer har ISASecure offentlig argumentert for at **SL 2 er et fornuftig minimum** for nye anskaffelser.

Hva 4-2 betyr praktisk for en OEM

Hver FR oversettes til produktegenskaper som en bruker faktisk kan se og konfigurere. Et ikke-uttømmende utvalg:

- **FR 1 – Identification & Authentication Control (IAC):** unike brukerkonti, rollebaserte identiteter, multifaktorautentisering, passordpolitikk, kontolåsning, enhet-til-enhet-autentisering med kryptografiske legitimasjoner, støtte for offentlig nøkkel-infrastruktur.
- **FR 2 – Use Control (UC):** rollebasert tilgangskontroll, sesjonsstyring, sesjonsutløp, restriksjoner på utførelse av mobil kode, USB-port-kontroll, trådløs tilgangsstyring, **revisjonsloggning** og loggbeskyttelse.
- **FR 3 – System Integrity (SI):** signert fastvare, **secure boot**, integritetsbeskyttede oppdateringer, malware-beskyttelse, input-validering, feilhåndtering som ikke lekker interne detaljer, manipulasjonsdeteksjon.
- **FR 4 – Data Confidentiality (DC):** krypterte kommunikasjoner (TLS eller tilsvarende), beskyttelse av kryptografiske nøkler, kryptering av data i hvile der det er relevant.
- **FR 5 – Restricted Data Flow (RDF):** soneinndeling, segmentering, evne til å delta i en Zones-and-Conduits-arkitektur, restriksjon av unødvendige nettverkstjenester.

- **FR 6 – Timely Response to Events (TRE):** revisjonsloggning med tilstrekkelig detalj, tidsstempling av logg, loggvideresending (f.eks. til syslog/SIEM), kroker for kontinuerlig overvåking.
- **FR 7 – Resource Availability (RA):** motstand mot tjenestenektangrep, feilsikker oppførsel, beskyttelse mot ressursuttømming, backup og gjenoppretting.

Det som endrer seg mellom SL 1 og SL 4 er essensielt grundigheten og dybden i disse mekanismene. SL 1 kan kreve «komponenten skal støtte autentisering»; SL 3 vil kreve unik per-bruker-autentisering med kryptografiske mekanismer; SL 4 vil legge til manipulasjonssikker legitimasjonslagring og motstand mot sofistikerte angrep.

Komponenttypen betyr også noe. En PLS (EDR) forventes å ha integritetsbeskyttet fastvare og en maskinvare root-of-trust; en HMI-arbeidsstasjon (HDR) forventes å støtte virksomhets-kontostyring, anti-malware og OS-herding. Krav er omfangsbestemt til det som er rimelig for enhetsklassen.

Hva en OEM må bevise objektivt for 4-2

For 4-2 er beviset **per produkt og per versjon**. Det finnes ikke noe slikt som «vårt selskap er 4-2-sertifisert» — bare «dette eksakte produktet, ved denne eksakte fastvareversjonen, oppnår SL-C n mot IEC 62443-4-2».

Hva «bra» ser ut som

- Den **spesifikke produktidentifikatoren**: modellnummer, maskinvarerevisjon, fastvare-/programvareversjon.
- En uttalelse om det **hevdede kapabilitets-sikkerhetsnivået (SL-C)** — vanligvis én SL-C-verdi per FR, noen ganger publisert som en vektor som **SL-C (2, 2, 2, 1, 2, 2, 2)** på tvers av FR1–FR7.

- En **erklæring om hvilken komponenttype** produktet er vurdert som (SAR, EDR, HDR eller NDR) — og hvis det er en sammensatt enhet, hvordan delene har blitt klassifisert.
- **Testrapporter** som viser at hvert gjeldende CR og RE er oppfylt. Uavhengige testrapporter er langt sterkere enn egenerklæringer.
- En **funksjonell sikkerhetsspesifikasjon** for sluttbrukere: hva hver sikkerhetsfunksjon gjør, hvordan man aktiverer den, og hvilke restrisikoer som gjenstår hvis den er deaktivert.
- En **herdings-/sikker konfigurasjonsveileder** som forteller integratoren nøyaktig hvordan produktet skal distribueres slik at SL-C-kravet er oppnåelig i den faktiske installasjonen.

Skillet SL-C / SL-T / SL-A — vitalt å forstå

Disse tre forkortelsene blandes konstant og forårsaker reelle innkjøpsfeil:

- **SL-C (Capability)** — hva produktet teknisk er i stand til å levere når det er riktig konfigurert. Det er dette 4-2 og ISASecure CSA sertifiserer.
- **SL-T (Target)** — hva anleggseieren har bestemt er nødvendig i en gitt sone i anlegget, basert på sin risikovurdering.
- **SL-A (Achieved)** — hva som faktisk leveres når produktet er installert, konfigurert og integrert i det levende systemet.

Et produkt kan være **SL-C 3-kapabelt** men distribueres som **SL-A 1** hvis anleggseieren skrur av funksjonene. Omvendt kan du ikke overskride din svakeste komponent: en sone bygget av SL-C 2-komponenter kan ikke oppnå SL-A 3 bare ved ønsketenkning.

Tredjepartssertifisering — gullstandarden

Hovedordningen er **ISASecure CSA (Component Security Assurance)**. Fra ISASecure CSA-100-ordningsdokumentet: CSA «focuses on the security of software applications, embedded devices,

host devices, and network devices, as defined by the ISA/IEC 62443-4-2 standard» og er «designed to certify to international standards ISA/IEC 62443-4-2 and ISA/IEC 62443-4-1». Programmet definerer **fire sertifiseringsnivåer — CSA Capability Security Level 1, 2, 3 og 4** — og sertifiseringen undersøker tre ting i tillegg til utviklingsprosessen:

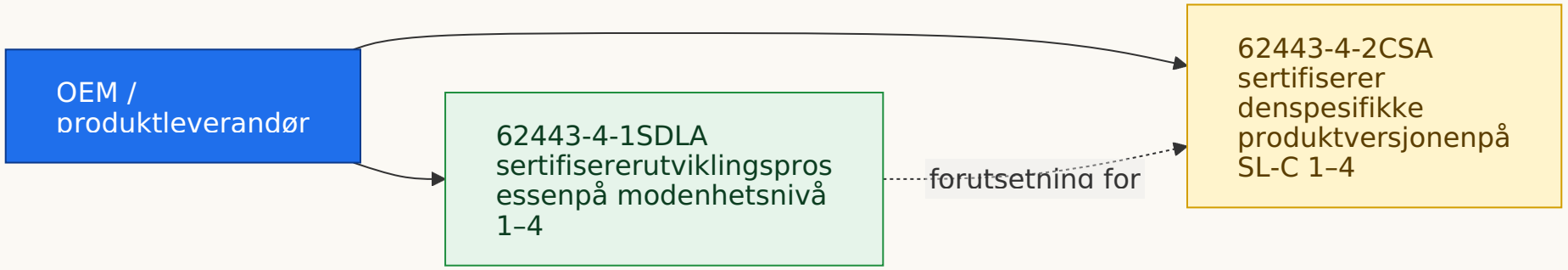
- **SDA-C (Security Development Artifacts for Components)** — utviklingsutdataene for dette produktet.
- **FSA-C (Functional Security Assessment for Components)** — sikkerhetsegenskapene produktet faktisk eksponerer.
- **VIT-C (Vulnerability Identification Testing for Components)** — skanning av produktet for kjente sårbarheter.

Kritisk krever CSA-ordningen at leverandøren **innehar en gjeldende ISASecure SDLA-sertifisering** for utviklingsprosessen. Som ISASecure SDLA-dokumentasjonen sier det: «application of ISA/IEC 62443-4-1 practices as verified by SDLA certification is intended to provide confidence that the component or system has security commensurate with its expected level of risk throughout the product's life-cycle». Kort sagt: **ingen SDLA, ingen CSA.**

Et levende register over CSA-sertifiserte komponenter vedlikeholdes på isasecure.org/end-users/iec-62443-4-2-certified-components — et godt første stopp for enhver verifiseringsøvelse. Det finnes også en IIoT-spesifikk utvidelse, **ISASecure ICSA**, for IIoT-komponenter og gatewayer, med Core- og Advanced-nivåer.

IECEE CB-ordningen utsteder også sertifikater mot 62443-4-2 og 62443-4-1, anerkjent internasjonalt mellom IECEE-medlemsorganer.

Hvordan 4-1 og 4-2 henger sammen


OEM / produktleverandør
62443-4-1SDLA sertifiserer utviklingsprosessen på modenhetsnivå 1–4
forutsetning for
62443-4-2CSA sertifiserer den spesifikke produktversjonen på SL-C 1–4

To praktiske sannheter følger:

1. Du kan i prinsippet forestille deg et 4-2-samsvar produkt fra en leverandør uten 4-1-sertifisering, men i reelle tredjepartsordninger — og i ISASecure CSA spesielt — må utviklingsprosessen også vurderes. CSA krever eksplisitt SDLA (eller tilsvarende SDLPA-C prosessvurdering) som forutsetning. Så spørsmålet å stille en leverandør er sjelden «enten 4-1 eller 4-2»; det er «vis meg begge».
2. En leverandør som kun har SDLA forteller deg at prosessen er solid, men ikke at noe bestemt produkt når et bestemt SL-C. En leverandør som hevder CSA uten underliggende SDLA gjør et krav som ikke passer sertifiseringsordningen — behandle med forsiktighet.

Det er også her den EU-regulatoriske kjeden går sammen. Under Cyber Resilience Act lener Vedlegg I essensielle krav for produkter med digitale elementer seg tungt på påviselig sikker utvikling og komponent-egenskaper — nøyaktig det 4-1 og 4-2 koder for det industrielle domenet. Og under NIS2 artikkel 21(2)(d) kaskaderer anleggseierens leverandørkjede-sikkerhetsforpliktelser kontraktsmessige krav tilbake gjennom leverandørene: i praksis ankommer det ofte OEM-en som en forespørsel om 4-1 og 4-2-bevis.

Vanlige fallgruver og røde flagg

Visse formuleringer og situasjoner i en OEMs samsvarspåstand bør få en kjøper til å bremse før kontrakten signeres.

Rødt flagg	Hvorfor det betyr noe
«Designet for å være i samsvar med 62443-4-2»	Dette er egenerklæring. Det er ikke sertifisering. Det finnes ingen uavhengig testrapport.
«I samsvar med IEC 62443» (uten delenummer)	Standarden har mange deler rettet mot ulike publikum. En leverandør «i samsvar med 62443» bør kunne navngi de spesifikke delen(e) — typisk 4-1 og/eller 4-2 for en OEM.
«I tråd med» eller **«basert på»**	Markedsføringsspråk. Det er ikke sertifisering. Be om sertifikatet.
Et krav uten en SL-C	4-2 er meningsløst uten et oppgitt SL-C. «62443-4-2-samsvar» alene forteller deg ingenting om styrke.
Uklart produktomfang	«Vårt produktsortiment er 62443-4-2-sertifisert» er nesten aldri sant — typisk er én modell på én fastvareversjon det. Krev modell og versjon.
Utdatert sertifikat	ISASecure-sertifikater har gyldighetsperioder og overvåkingsrevisjoner. Et sertifikat fra 2019 som dekker fastvare som siden har hatt 25 oppdateringer reflekterer kanskje ikke det som er i esken.
Krav om modenhetsnivå uten tredjepartsrevisjon	Egenerklært ML 3 eller ML 4 har lite vekt. ISASecure SDLA eller et IECEE-sertifikat er det troverdige artefaktet.
Forveksling med 62443-3-3 eller 62443-2-4	3-3 er en system-standard for integratorer; 2-4 er for tjenesteleverandører; 4-2 er komponent-standarden. Leverandører vifter noen ganger med et 3-3-sertifikat på et 4-2-spørsmål, eller omvendt.
«Sertifisert til SL 4» uten detalj per FR	Reelle sertifikater oppgir SL-C per FR (ofte som en vektor). Et flatt «SL 4»-krav på tvers av alt er mistenkelig.
Ingen publisert herdingsveileder eller sikkerhetsrådside	Praksisene 7 og 8 (SUM og SG) i 4-1 krever disse; deres fravær er informativt.

En kjøpers sjekkliste for anskaffelse

Bruk dette som et kontraktstillegg eller som et leverandør-spørreskjema.

Spørsmål å stille OEM-en skriftlig

1. Har selskapet et gjeldende **ISASecure SDLA**-sertifikat (eller tilsvarende IECEE 62443-4-1-sertifikat)? På hvilket

modenhetsnivå? Utstedt av hvilket sertifiseringsorgan, på hvilken dato, utløper når?

2. Hva er **omfanget** av det SDLA-sertifikatet — hvilke utviklingssteder, hvilke forretningsenheter, hvilke produktlinjer?
3. For det spesifikke produktet som tilbys, har det et **ISASecure CSA**-sertifikat (eller tilsvarende IECEE 62443-4-2-sertifikat)?
4. Hva er det **eksakte modellnummeret og fastvare-/programvareversjonen** dekket av sertifikatet?
5. Hva er det **hevdede SL-C** for hvert av de syv grunnkravene (SL-C-vektoren)?
6. Hvilken **komponenttype** har blitt sertifisert — SAR, EDR, HDR eller NDR?
7. Vennligst gi **sertifikat-PDF-en**, den **offentlige sertifiseringsrapporten** (der tilgjengelig), og **herdingsveilederen / funksjonell sikkerhetsspesifikasjon** for produktet.
8. Vennligst gi **URL-en til sårbarhetsavsløringspolitikken** og en liste over CVE-er håndtert de siste 24 månedene for denne produktfamilien.
9. Hva er **støtte- og oppdateringslevetiden** for produktet, og den dokumenterte politikken for ende-av-liv?
10. Vennligst beskriv **SBOM**-en eller tredjeparts-komponentinventaret tilgjengelig for dette produktet.

Dokumenter å kreve på fil

- SDLA / IECEE 62443-4-1-sertifikat.
- CSA / IECEE 62443-4-2-sertifikat per produkt og versjon.
- Produkt-funksjonell sikkerhetsspesifikasjon.
- Herdings-/sikker konfigurasjonsveileder.
- Sårbarhetsavsløringspolitikk.

- Eksempel-sikkerhetsråd (for å bekrefte at en reell avsløringsprosess eksisterer i praksis).

Verifiseringssteg

- Kryss-sjekk sertifikatnummeret på **ISASecure-sertifiserte produkter-registeret** på isasecure.org/end-users/iec-62443-4-2-certified-components .
- For IECEE-sertifikater, verifiser på IECEE CB-ordningens sertifikat-database på iecee.org .
- Bekreft at **sertifikatet er gyldig** og at omfangsuttalelsen matcher modellen og fastvaren du faktisk kjøper.
- Sammenlign SL-C-vektoren mot ditt eget SL-T fra risikovurderingen din.
- Be om bevis for at produktet som leveres til deg matcher den sertifiserte versjonen — oppdateringer og mindre utgivelser kan flytte produktet utenfor det sertifiserte omfanget.

IEC 62443-4-1 spør OEM-en «Er du den typen organisasjon som kan bygge sikre produkter, gjentakelig, og holde dem slik?» **IEC 62443-4-2** spør samme OEM «Har dette eksakte produktet, ved denne eksakte versjonen, de tekniske sikkerhetsfunksjonene som trengs for å motstå truslene i driftsmiljøet sitt?»

Sammen utgjør de ett av de mest grundige svarene den industrielle verden har på «hvordan vet jeg at denne OEM-en tar cybersikkerhet seriøst?» — men bare hvis du leser forbi brosjyren til sertifikatet, og forbi sertifikatet til omfanget.

Behandle dem som grunnmuren, ikke målstreken. Et sertifisert produkt, dårlig distribuert og aldri oppdatert, er ikke mer sikkert enn

et usertifisert et. Og et usertifisert produkt, uansett hvor velmenende leverandøren er, ber deg ta all forsikring på tillit.

Kartlegging av IEC 62443-kontroller mot NIS2 Artikkel 21-tiltak

14. mai 2026 · 27 min lesetid · #compliance #security #industrial #iec-62443 #nis2

Tenk deg en nordisk vindoperatør som mottar to rapporter rygg mot rygg: en IEC 62443-kapabilitetsvurdering fra et velkjent klassifikasjonsselskap, og en NIS2 gap-analyse fra et Big Four-firma. 62443-rapporten sier at virksomheten ligger komfortabelt på Sikkerhetsnivå 2 over de fleste soner, med en troverdig vei mot SL-3 på SCADA-sonen. NIS2-rapporten sier at det finnes «vesentlige mangler» i leverandørkjedestyring, hendelsesrapporteringstider og styreansvar. Samme anlegg. Samme mennesker. Samme uke.

Hvilken tar feil?

Ingen. De måler forskjellige ting — og den bærende forutsetningen under spørsmålet («hvis vi er 62443-konforme er vi NIS2-konforme») er en av de dyreste misforståelsene i operasjonell teknologi-sikkerhet i dag. Denne teksten er det lange svaret på spørsmålet: en gjennomgang tiltak for tiltak av NIS2 Artikkel 21(2)(a) til (j), kartlagt mot spesifikke klausuler i IEC 62443-serien , med en ærlig vurdering av hvor godt samsvaret faktisk er og en liste over hva en anleggseier — særlig en anleggseier innen fornybar energi — fortsatt må produsere på toppen av en 62443-bevismappe.

TL;DR

Hvis du ikke leser noe annet: **IEC 62443 og NIS2 Artikkel 21 overlapper kraftig på det tekniske kontrollnivået — grovt sett 70 % — men NIS2 legger til tre ting som IEC 62443 rett og slett ikke dekker: juridiske rapporteringsfrister for hendelser (24 timer, 72 timer, én måned), eksplisitt ansvar for styret, og et notifikasjonsregime for leverandørkjeden.** Et rent `IEC 62443-3-3`

SL-2-system vil dekke det meste av tiltakene (a), (c), (e), (g), (h), (i) og (j) på det tekniske planet, men anleggseieren må fortsatt produsere policy-artefaktene, det juridiske bevissporet og rapporteringsplaybooken oppå. Behandle 62443 som det tekniske underlaget og NIS2 Artikkel 21 pluss Kommisjonens gjennomføringsforordning (EU) 2024/2690 som styrings- og rapporteringslaget — aldri omvendt.

1. Hvorfor kartleggingen betyr noe — og forutsetningen alle gjør

I OT-sikkerhetsgjennomganger på solparker, vindparker på land, småkraftverk og nettkoblede batterilagringsanlegg (BESS) dukker én påstand opp jevnlig: «Vi går mot 62443, så vi er NIS2-konforme automatisk.»

Det er grovt sett riktig på teknisk kontrollnivå. De syv grunnkravene (FR-ene) i `IEC 62443-3-3:2013` — identifikasjons- og autentiseringskontroll, brukskontroll, systemintegritet, datakonfidensialitet, begrenset dataflyt, rettidig responsering, ressurstilgjengelighet — samsvarer rimelig godt med de tekniske søylene i NIS2 Artikkel 21(2). Hvis du kan dokumentere SL-2 over alle syv FR-er i driftsonen på en vindpark, har du bevis for en betydelig del av det Artikkel 21 forventer.

Det er feil overalt ellers. NIS2 er et EU-rettslig instrument: et direktiv som, når det er gjennomført i hver medlemsstat, skaper plikter for **juridiske personer**, for **ledelsesorganer** og for **hendelsesmeldingsstrømmer til en nasjonal CSIRT**. IEC 62443 er en frivillig teknisk standard utarbeidet av IEC TC 65/WG 10 og ISA99; standarden har ingen mening om hvorvidt du har et registrert juridisk subjekt, ingen mening om hvorvidt styret har godkjent dine risikohåndteringstiltak, og ingen forestilling om en tidlig varsling til et Computer Security Incident Response Team innen 24 timer.

En påminnelse om NIS2-omfanget før vi går videre: direktivet gjelder **vesentlige** og **viktige** enheter, med energi listet som en sektor av «høy kritikalitet» i Annex I. Produsenter av elektrisitet, systemoperatører, distribusjons- og overføringsoperatører, og — relevant for fornybarsektoren — operatører av fjernvarme, hydrogen og olje og gass faller alle innenfor virkeområdet der de oppfyller størrelsesterskelene (typisk 50+ ansatte eller EUR 10 millioner omsetning, med sektorspesifikke unntak). Jeg har gått gjennom omfanget mer detaljert i NIS2-anvendelsesteksten — les den først hvis du fortsatt undersøker om gruppen din i det hele tatt er omfattet.

2. De fem formforskjellene før vi i det hele tatt begynner å kartlegge

Før vi kartlegger en eneste kontroll, er det verdt å være ærlig om den strukturelle uoverensstemmelsen mellom de to dokumentene. Fem forskjeller i **form**, ikke innhold, forklarer det meste av friksjonen:

(i) Risikostyringsorientering versus kapabilitetsorientering. NIS2 Artikkel 21(1) er eksplisitt på at enheter «skal treffe egnede og forholdsmessige tekniske, operasjonelle og organisatoriske tiltak for å håndtere risikoene». Direktivet bryr seg om utfall. `IEC 62443-3-3` og `-4-2`, derimot, gir deg en katalog over kapabiliteter på fire sikkerhetsnivåer og lar deg velge, via `IEC 62443-3-2`-soneinndeling, hvor du skal anvende dem. 62443-revisjonen spør «leverer denne sonen SL-T?». NIS2-revisjonen spør «har du redusert risikoen for din essensielle tjeneste til et akseptabelt nivå?». Begge spørsmålene er rimelige; de er ikke det samme spørsmålet.

(ii) Tidsmessige forpliktelser. Artikkel 23 i NIS2 pålegger en tretrinns rapporteringskadens — tidlig varsel innen 24 timer, hendelsesmelding innen 72 timer, sluttrapport innen én måned — som ikke har noen tilsvarende noe sted i 62443-serien. SR 6.2

«Kontinuerlig overvåkning» sier deg å oppdage hendelser; den sier ingenting om hvem du skal ringe.

(iii) Styrets ansvar. Artikkel 20 i NIS2 gjør ledelsesorganer i vesentlige og viktige enheter **personlig** ansvarlige for å godkjenne cyberrisikohåndteringstiltakene og overvåke gjennomføringen av dem, og krever at de gjennomgår opplæring. `IEC 62443-2-1:2024` forventer toppledelsens forpliktelse — den nye strukturen med Security Programme Elements gjør det eksplisitt — men den verken kan eller pålegger personlig juridisk ansvar.

(iv) Leverandørkjedens rekkevidde. NIS2 Artikkel 21(2)(d) krever at enheter håndterer sikkerheten i «relasjonene mellom hver enhet og dens direkte leverandører eller tjenesteytere». `IEC 62443-2-4:2023` er det åpenbart nærmeste samsvaret — den spesifiserer sikkerhetsprogrammet for IACS-tjenesteleverandører — men bare anleggseieren kan kontraktsfeste det, og bare NIS2 gjør det til et juridisk anliggende å unnlate det.

(v) Frivillig versus håndhevet. IEC 62443-samsvar er noe du velger, noen ganger sertifiserer, og bruker for å vinne anbud. NIS2 er noe den nasjonale tilsynsmyndigheten — i Norges tilfelle Nasjonal sikkerhetsmyndighet (NSM) — vil til slutt revidere deg mot og bøtelegge deg for å mangle. I Norge spesifikt, per mai 2026, er dette fortsatt et bevegelig mål: gjeldende `digitalsikkerhetsloven` (LOV-2023-12-20-108) trådte i kraft 1. oktober 2025 og gjennomfører **NIS1**-regimet. NIS2 selv er ennå ikke innlemmet i EØS-avtalen og forventes gjennomført i 2026, sannsynligvis i en ny kombinert cyber/CER-lov som vil erstatte gjeldende digitalsikkerhetslov. De fem forskjellene over gjelder uansett om den norske gjennomføringen lander i juni 2026 eller desember 2026 — de er bygd inn i selve direktivet.

Med det av veien, videre til de ti tiltakene.

3. Tiltak (a) — retningslinjer for risikoanalyse og informasjonssystemsikkerhet

> «retningslinjer for risikoanalyse og informasjonssystemsikkerhet»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`, `IEC 62443-3-2:2020`.

Spesifikke klausuler. I 2024-andreutgaven av `-2-1` er Security Programme Elements (SPE-ene) som dekker dette tiltaket ORG 1 «Security programme management» og ORG 2 «Risk management». Risikovurderingsmetodikken som anleggseieren er pålagt å bruke ligger i `IEC 62443-3-2:2020` — soneinndeling og kanalinndeling av systemet under vurdering (SuC), vurdering av cyberrisiko per sone, og utledning av Target Security Level (SL-T) for hver sone og kanal. Annex A i `-3-2` gir et utarbeidet eksempel på metodikken.

Samsvar: tett. `IEC 62443-3-2` er genuint en risikostyringsmetodikk. Hvis du har gjort SuC-inndelingen for en 250 MW solpark — skilt invertkontrollsonen fra SCADA-sonen fra IT-sonen for selskapet, utledet SL-T-verdier per sone, og dokumentert restrisikoen — har du produsert nesten nøyaktig det NIS2 Artikkel 21(2)(a) ber om. ENISA Technical Implementation Guidance, publisert i juni 2025, anerkjenner eksplisitt ISO/IEC 27001 og «relevante sektorstandarder» som grunnlag for retningslinjene; `IEC 62443-3-2` er en av de relevante sektorstandardene i OT-rommet.

Hva du må vise på toppen. Tre ting. For det første, en styregodkjent skriftlig policy (ikke bare en metodikk) som sier hvordan risikoanalyse utføres, av hvem, med hvilken kadens, og hva akseptkriteriene er. For det andre, sporbarhet — risikoregisteret må vise hvilke risikoer som ble identifisert, hvilke kontroller som ble anvendt, og hvilke restrisikoer ledelsen har akseptert. For det tredje, periodisk gjennomgang — Annex 2.1 i `(EU) 2024/2690` ber om «regelmessig» gjennomgang, som ENISA-veiledningen tolker som

minst årlig. En vanlig feilmodus på et hybrid sol-pluss-BESS-anlegg er vakre 62443-sonediagrammer ved siden av et ni måneder gammelt risikoregister; mangelen, når den dukker opp, er styring, ikke ingeniørarbeid.

Spesifikt for fornybar energi. Risikobildet endrer seg når du bolter en 100 MWh BESS på et 50 MW solanlegg: en enkelt sone i SuC-inndelingen fra 2022 blir tre soner over natten. Kjør `-3-2` på nytt hver gang anleggstopologien endrer seg, og fang opp endringen i risikoregisteret som NIS2 vil ønske å lese.

4. Tiltak (b) — hendelseshåndtering

> «hendelseshåndtering»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` Foundational Requirement 6.

Spesifikke klausuler. I `-2-1:2024` er det relevante SPE-et hendelseshåndteringselementet (tidligere klausul 4.3.4.5 i 2010-utgaven; i 2024-utgaven er kravene restrukturert under et SPE som dekker identifikasjon, respons, gjenoppretting og hendelsesgjennomgang). På den tekniske siden gir `IEC 62443-3-3:2013` FR 6 «Timely response to events» — spesifikt SR 6.1 «Audit log accessibility» og SR 6.2 «Continuous monitoring» — sammen med SR 2.8 «Auditable events», SR 2.9 «Audit storage capacity», SR 2.10 «Response to audit processing failures» og SR 2.11 «Timestamps» fra FR 2. Komponentnivåspeil ligger i `IEC 62443-4-2:2019` CR 2.8 til CR 2.12 og CR 6.1, CR 6.2.

Samsvar: delvis. To halvdeler, én passer, én gjør det ikke. Deteksjon og analyse-halvdelen av hendelseshåndtering er godt dekket: 62443 gir deg loggings-, overvåknings- og forensisk kapabilitet som trengs for å vite at en hendelse har skjedd. Rapportering og ekstern kommunikasjon-halvdelen er i praksis fraværende. IEC 62443 sier

ingenting om 24-timers tidlig-varslingsplikten, ingenting om CSIRT-kontakt, ingenting om grenseoverskridende notifikasjon, og ingenting om innholdet i en sluttrapport.

Hva du må vise på toppen. En dokumentert hendelsesresponsplan som eksplisitt navngir den nasjonale CSIRT-en (i Norge, NSM via Nasjonalt cybersikkerhetssenter, NCSC), definerer utløsningskriteriene for en «vesentlig hendelse» ved bruk av tersklene i `(EU) 2024/2690` Artikkel 3 (der relevant) eller den nasjonale gjennomføringen, og tilordner navngitte roller for å utforme og sende 24-timers tidlig-varsling, 72-timers melding og én-månedssluttrapport. Planen må testes. Opptak av tabletop-øvelser som inkluderer rapporteringsstien, ikke bare den tekniske responsen, er artefaktet revisorene vil lete etter. Den kjente feilmodusen på en vindpark-tabletop er at teknikerne vet nøyaktig hvordan de skal isolere det berørte turbin-SCADA-segmentet innen en time, men ingen på vakt har NSM-portalinnloggingen eller kjenner terskeldefinisjonene. Det er gapet NIS2 vil bøtelegge deg for.

5. Tiltak (c) — virksomhetskontinuitet, sikkerhetskopiering, katastrofegjenoppretting og krisehåndtering

> «virksomhetskontinuitet, slik som sikkerhetskopiforvaltning og katastrofegjenoppretting, og krisehåndtering»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` Foundational Requirement 7.

Spesifikke klausuler. `-3-3` FR 7 «Resource availability» gir deg SR 7.1 «Denial of service protection», SR 7.2 «Resource management», SR 7.3 «Control system backup», SR 7.4 «Control system recovery and reconstitution», SR 7.5 «Emergency power» og SR 7.6 «Network and security configuration settings». Komponentnivå: `-4-2` CR 7.1 til

CR 7.6. På styringssystemsiden inneholder `-2-1:2024` krav om virksomhetskontinuitetsstyring som et SPE som dekker sikkerhetskopipolicy, gjenopprettingstesting og kontinuitetsøvelser.

Samsvar: tett (for IACS-omfang) — men med ett viktig forbehold. SR 7.3 og SR 7.4 er utmerkede: de krever ikke bare at sikkerhetskopier finnes, men at de er verifisert, at gjenoppretting til en kjent-god tilstand er oppnåelig, og at gjenopprettingsprosessen selv er dokumentert og testet. Dette går utover hva de fleste ISO 27001 sikkerhetskopikontroller krever. NIS2 Artikkel 21(2)(c) og det tilsvarende avsnittet i `(EU) 2024/2690`-anneksen (punkt 4) ber om grovt sett det samme.

Forbeholdet: 62443 har omfang IACS. Virksomhetskontinuitet under NIS2 dekker den essensielle tjenesten — for en fornybaroperatør betyr det å levere kraft til nettet, som avhenger av IACS, SCADA-bakhalen, energiledelsessystemet, leveringsgrensesnittet til TSO-en, måleledningen, og så videre. En perfekt SR 7.3/7.4-gjennomføring på vindparkens SCADA redder deg ikke hvis selskapets IT-dispatchportal er kryptert av løsepengevare. Anleggseieren trenger en kontinuitetsplan med omfang den essensielle tjenesten, der IACS-delen tilfredsstilles av 62443-kontrollene.

Hva du må vise på toppen. En dokumentert plan for virksomhetskontinuitet og katastrofegjenoppretting (BCDR) som dekker den essensielle tjenesten ende til ende; definerte gjenopprettingstidsmål (RTO) og gjenopprettingspunktmål (RPO) per kritisk prosess; offline, uforanderlige sikkerhetskopier av SCADA-konfigurasjoner, PLC-logikk og historian-data (SR 7.3-bevis); opptak av minst årlige gjenopprettingstester på representative aktiva; en krisehåndteringsprosedyre som navngir roller, eskaleringsstier og ekstern kommunikasjon. På en 200 MW vindpark på land er «vi sikkerhetskopierer SCADA-databasen nattlig» ikke nok — revisorene

vil se den siste vellykkede gjenopprettingstesten av den faktiske turbinkontrollerlogikken på en reserveenhet.

6. Tiltak (d) — leverandørkjedesikkerhet

> «leverandørkjedesikkerhet, herunder sikkerhetsrelaterte forhold knyttet til relasjonene mellom hver enhet og dens direkte leverandører eller tjenesteytere»

Primære IEC 62443-deler: `IEC 62443-2-4:2023`, `IEC 62443-4-1:2018`, `IEC 62443-2-1:2024`.

Spesifikke klausuler. `IEC 62443-2-4:2023` er sikkerhetsprogrammet for IACS-tjenesteleverandører — den definerer hva en integrator eller vedlikeholdsleverandør må gjøre på tvers av bemanning, opplæring, tjenesteomfang, herding, nettverksarkitektur, trådløst, anti-skadevare, oppdateringshåndtering, sikkerhetskopi/gjenoppretting, prosjektbemanning, sikker fjerntilgang og så videre. For produktleverandører definerer `IEC 62443-4-1:2018` kravene til Secure Product Development Lifecycle over åtte praksiser: SM (security management), SR (specification of security requirements), SD (secure by design), SI (secure implementation), SVV (security verification and validation testing), DM (management of security-related issues), SUM (security update management) og SG (security guidelines). På anleggseier-siden har `-2-1:2024` et innkjøps-/SPE som dekker leverandørvalg, kontraktssikkerhetskrav og onboarding.

Samsvar: delvis — men det sterkeste delvise i standarden. `-2-4` og `-4-1` er klart det mest direkte tekniske svaret på NIS2s leverandørkjedetiltak som finnes i noen frivillig standard i dag. Hvis du krever at vindturbin-OEM-en din opererer etter `-4-1` og at SCADA-integratoren din opererer etter `-2-4`, har du gjort det meste av den tekniske tungløftingen. Annexet til `(EU) 2024/2690` (avsnitt 5) om

leverandørkjedesikkerhet overlapper i stor grad med `-2-4`s tjenesteleverandørkrav. Den dypere gjennomgangen av `-2-4` og `-4-1` ligger i OEM-siden .

Der det kommer til kort: NIS2 forventer at anleggseieren tar et **risikobasert** syn på leverandører, inkludert ikke-IACS-leverandører (skyleverandører, IKT-utsettere, leverandører av styrte sikkerhetstjenester), tar hensyn til leverandørens egen sårbarhet for en trussel, og tar med i beregningen resultatene fra den europeiske koordinerte risikovurderingen som ENISA og NIS-samarbeidsgruppen publiserer periodisk. Ingenting av det er i `-2-4`. Videre, `-2-4` binder deg bare hvis du gjør det bindende ved kontrakt; NIS2 gjør det bindende ved lov.

Hva du må vise på toppen. En dokumentert leverandørrisikohåndteringspolicy, et lagdelt leverandørregister med risikoklassifiseringer, kontraktuelle sikkerhetsklausuler i hver relevant leverandørkontrakt (inkludert hendelsesnotifikasjonsklausuler med tidslinjer som lar deg oppfylle din egen 24-timersplikt), bevis for at kritiske leverandørers sikkerhetspåstander er gjennomgått (f.eks. et `IEC 62443-4-1` Maturity Level-sertifikat, et ISO/IEC 27001-sertifikat, en SOC 2 Type II-rapport), og kontinuerlig overvåkning. For et hybridt fornybaranlegg med tre OEM-er (turbiner, PV-invertere, BESS), tre integratorer og en ekstern SCADA-som-tjeneste-leverandør er leverandørregisteret alene ikke triviellt.

Spesifikt for fornybar energi. Dette er tiltaket der EUs Cyber Resilience Act (CRA, forordning (EU) 2024/2847) etter hvert vil gjøre deg en tjeneste. Når CRA biter inn sent i 2027, vil produktleverandører som plasserer invertere, SCADA-gatewayer og BESS-kontrollere på EU-markedet være pålagt å sende dem med dokumentert sårbarhetshåndtering, en SBOM og en

sikkerhetsoppdateringskanal — se CRA-anvendelsesteksten for detaljene. Inntil da kontraktsfester du det.

7. Tiltak (e) — sikkerhet i anskaffelse, utvikling og vedlikehold, herunder sårbarhetshåndtering og rapportering

> «sikkerhet i anskaffelse, utvikling og vedlikehold av nettverks- og informasjonssystemer, herunder sårbarhetshåndtering og rapportering»

Primære IEC 62443-deler: `IEC 62443-4-1:2018`, `IEC TR 62443-2-3:2015`, `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` FR 3.

Spesifikke klausuler. Sårbarhetshåndtering og rapportering for produktleverandører er `-4-1` praksis DM «Management of security-related issues» (DM-1 til DM-6) og praksis SUM «Security update management» (SUM-1 til SUM-5). For anleggseieren er oppdateringshåndtering dekket i `IEC TR 62443-2-3:2015`, som definerer utvekslingsformatet og prosessen mellom anleggseier og produktleverandør for sikkerhetsoppdateringer. Programvareintegritetskontroller på systemnivå er `-3-3` SR 3.4 «Software and information integrity»; på komponentnivå, `-4-2` CR 3.4. Anskaffelsespolicyen selv ligger i `-2-1:2024` under prosjektenhetens SPE.

Samsvar: tett på tekniske mekanikker, delvis på policy og rapportering. Den tekniske maskineriet for sårbarhetshåndtering — å motta en CVE-melding, vurdere anvendelighet på en spesifikk firmwareversjon, planlegge en oppdatering gjennom et vedlikeholdsvindu, verifisere integriteten til oppdateringen før installasjon — er godt spesifisert i `-4-1` DM/SUM og `IEC TR 62443-2-3`. 2024-utgaven av `-2-1` dekker likeledes oppdateringspolicy for anleggseieren.

Der det blir tynnere: NIS2 forventer en kapabilitet for **koordinert sårbarhetsrapportering** (CVD) — et sted hvor en forsker ansvarlig kan rapportere en sårbarhet i miljøet ditt, med en definert prosess for triage og bekreftelse. `IEC 62443-4-1` DM adresserer dette for produktleverandøren, men for en anleggseier som kjører tilpasset integrasjonskode eller interne ingeniørapplikasjoner ligger CVD-plikten hos deg, og standarden gir deg ikke en prosess. NIS2 forventer også at du overvåker offentlige sårbarhetskilder (ENISAs EU-sårbarhetsdatabase , nasjonale CSIRT-varsler, CISA ICS-rådgivninger) — `IEC TR 62443-2-3` nevner dette i forbifarten, men spesifiserer ikke overvåkningskadensen.

Hva du må vise på toppen. En dokumentert oppdateringshåndteringsprosedyre med SLA-er etter kritikalitet (f.eks. CVSS ≥ 9.0 oppdatert innen 30 dager etter OEM-tilgjengelighet, eller formelt risikoakseptert med kompenserende kontroller); en koordinert sårbarhetsrapporteringspolicy med en publisert kontakt (security.txt eller en security@-adresse); bevis for at du abonnerer på og triagerer varsler fra OEM-ene dine og fra minst en nasjonal CSIRT; endringshåndteringsregisteret som viser at oppdateringer er anvendt og testet. På vedlikeholdssiden, bevis for at vedlikeholdsinngrep — f.eks. en OEM-serviceingeniør som kobler til en turbinkontroller — følger sikker fjerntilgangsprosedyrer (`-2-4` SP. 05 og SP.06).

8. Tiltak (f) — retningslinjer og prosedyrer for å vurdere effektiviteten av cyberrisikohåndteringstiltak

> «retningslinjer og prosedyrer for å vurdere effektiviteten av cyberrisikohåndteringstiltak»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`.

Spesifikke klausuler. Dette tiltaket er i praksis «sjekker du at de andre tiltakene fungerer?» — ekvivalenten til ISO 27001 klausul 9.1

til 9.3 (overvåkning/måling, internrevisjon, ledelsesgjennomgang). I `-2-1:2024` dekker de relevante SPE-ene overvåkning, måling, internrevisjon og ledelsesgjennomgang av IACS-sikkerhetsprogrammet; 2024-utgaven innfører en modenhetsmodell (Maturity Levels 1 til 4) som er spesifikt utformet for å brukes som målestokken. Full gjennomgang av disse SPE-ene er i styringssystemteksten . `IEC 62443-3-3` Annex A gir deg SL-Achieved-utledningen som er den tekniske ekvivalenten.

Samsvar: tett på styringssystemnivå — men kun i 2024-utgaven. 2010-utgaven av `-2-1` var vag her; 2024-andreutgaven retter det. SPE-strukturen og modenhetsmodellen gir deg en forsvarbar metodikk for å måle effektivitet. Annexet til `(EU) 2024/2690` (punkt 7) kartlegger direkte mot dette.

Hva du må vise på toppen. Mindre enn du kanskje tror, hvis du har flyttet til `-2-1:2024`. Du trenger: et årlig internrevisjonsprogram som dekker IACS-sikkerhetsprogrammet, med dokumenterte funn og korrigerende tiltak; en plan for ledelsesgjennomgang med protokollerte beslutninger; KPI-er/målepunkter koblet til modenhetsmodellen; bevis for at målepunktene driver endring. Elementet NIS2 vil granske mest, er om ledelsen faktisk mottar og handler på gjennomgangens utdata — dette kobler direkte til Artikkel 20.

9. Tiltak (g) — grunnleggende cyberhygiene og cyberopplæring

> «grunnleggende cyberhygiene-praksis og cybersikkerhetsopplæring»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`, `IEC 62443-2-4:2023`.

Spesifikke klausuler. I `-2-1:2024` finnes det et dedikert SPE for personalsikkerhet og bevisstgjøringsopplæring — som dekker

rollebasert opplæring, oppfriskningskadens og kompetansevurdering. `-2-4:2023` speiler dette på tjenesteleverandør-siden: SP.02 «Staffing» krever at integratoren viser at personellet er opplært og vurdert. Hygiene-siden — passordregler, programvarewhitelisting, endepunktherding, sikker surfing — er implisitt i ulike `-3-3` SR-er (SR 1.7 «Strength of password-based authentication», SR 2.4 «Mobile code», SR 3.2 «Malicious code protection») og eksplisitt på komponentnivå i `-4-2`.

Samsvar: tett på arbeidsstokknivå, svakt på styrenivå. Hygienekontrollene er godt dekket. Opplæring av driftspersonell og ingeniører er godt dekket. Det IEC 62443 ikke gir deg, er **styre**-nivå-opplæringsplikten som NIS2 Artikkel 20(2) pålegger medlemmer av ledelsesorganer — den opplæringen er sui generis for direktivet.

Hva du må vise på toppen. Opplæringsregistre per individ, per rolle, med pensuminnhold kartlagt mot Artikkel 21(2)-tiltakene; oppfriskningsfrekvens (typisk årlig); et separat, dokumentert opplæringsprogram for medlemmer av ledelsesorganer som dekker deres styringsplikter under Artikkel 20 og enhetens hendelsesrapporteringsstrøm. Resultater fra phishing-simuleringer, selv om de ikke er påkrevd, er nyttige bevis. Den biten som oftest mangler i NIS2-beredskapsrevisjoner er ikke teknikeropplæringen — den har som regel pågått i årevis — men fraværet av en styrebriefing om cyberrisiko i de siste tolv månedenes styreprotokoller.

10. Tiltak (h) — kryptografi og, der det er hensiktsmessig, kryptering

> «retningslinjer og prosedyrer for bruk av kryptografi og, der det er hensiktsmessig, kryptering»

Primære IEC 62443-deler: `IEC 62443-3-3:2013` FR 4, `IEC 62443-4-2:2019`.

Spesifikke klausuler. På systemnivå: SR 3.1 «Communication integrity», SR 3.8 «Session integrity», SR 4.1 «Information confidentiality», SR 4.3 «Use of cryptography». På komponentnivå, `-4-2` CR 3.1, CR 3.8, CR 4.1, CR 4.3, pluss `-4-2` CR 1.8 «Public key infrastructure certificates» og CR 1.9 «Strength of public key-based authentication» der det er relevant. `-2-1:2024` gir SPE-et for nøkkelhåndteringspolicy. Den dypere systemsidens kontekst er i systemdesign-teksten .

Samsvar: delvis. 62443-kontrollene sier deg hva som må beskyttes (kommunikasjon, sesjoner, lagret data, autentikatorer) og at kryptografi er midlene. De er stort sett tause om hvilke algoritmer, hvilke nøkkellengder, kryptoagilitet eller post-kvante-beredskap. NIS2s Annex 2.4 i `(EU) 2024/2690` og ENISA-veiledningen forventer begge en dokumentert kryptografipolicy som navngir godkjente algoritmer, forbyr utgåtte (3DES, MD5, SHA-1, RC4), definerer nøkkellivssyklus og adresserer kryptoagilitet.

Hva du må vise på toppen. En kryptografipolicy som lister godkjente algoritmer (typisk med referanse til BSI TR-02102 , NIST SP 800-131A Rev. 2 eller ENISAs algoritmeanbefalinger); en nøkkelhåndteringsprosedyre som dekker generering, distribusjon, lagring, rotasjon og destruksjon; en oversikt over hvor kryptografi brukes i IACS-en (tenk: PROFINET Security, OPC UA-endepunkter, IPsec/VPN-tunneler tilbake til NOC-en, BESS-kontroller TLS, smartmåler-autentisering, signert firmware-verifisering); bevis for konforme konfigurasjoner. **Avgjørende: NIS2 krever ikke at du krypterer hver OT-lenke** — IEC 62443 har rett i at på en deterministisk sanntids-buss kan kryptering være feil svar. Policyen må dokumentere hvor du har bestemt at kryptering ikke er hensiktsmessig og hvorfor.

Spesifikt for fornybar energi. Inverter-til-kontroller-trafikk på et PV-anlegg, turbin-til-parkkontroller-trafikk på en vindpark, og BMS-

til-PCS-trafikk i en BESS er vanlige områder hvor båndbredde og latens driver deg vekk fra TLS. Dokumenter beslutningen; ikke lat som den ikke eksisterer.

11. Tiltak (i) — personalsikkerhet, tilgangskontroll og aktivahåndtering

> «personalsikkerhet, retningslinjer for tilgangskontroll og aktivahåndtering»

Primære IEC 62443-deler: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` FR 1 og 2, `IEC 62443-4-2:2019`.

Spesifikke klausuler. Dette tiltaket er en trio. Tilgangskontroll er `-3-3` FR 1 «Identification and authentication control» (SR 1.1 til SR 1.13) og FR 2 «Use control» (SR 2.1 til SR 2.12), med deres komponentmotstykker i `-4-2`. Aktivahåndtering ligger i `-2-1:2024` under et dedikert SPE — 2024-utgaven er mye skarpere her enn 2010-utgaven, med CM (Configuration Management)-elementer som dekker baselinjer for aktivaregister, konfigurasjonsbaselinjer og endringskontroll. Personalsikkerhet — onboarding/forflytning/avgang, screening, NDA-er, terminering — er et SPE i `-2-1:2024` (personnel security).

Samsvar: tett. Dette er trolig den reneste kartleggingen i direktivet. Hvis du har SL-2 på FR 1 og FR 2, et oppdatert IACS-aktivaregister med konfigurasjonsbaselinjer, og en SPE-konform onboarding/forflytning/avgang-prosess, har du krysset av boksene for NIS2 Artikkel 21(2)(i).

Hva du må vise på toppen. Tre artefakter. For det første, et aktivaregister som er aktuelt — revisorene vil ta stikkprøver. For en 50-turbin vindpark betyr «aktuelt» at registeret reflekterer firmwareversjonen som faktisk kjører på hver turbin, ikke versjonen som ble utrullert ved idriftsettelse. For det andre, rollebaserte

tilgangskontrollmatriser som viser hvem som har hvilken rettighet på hvilken sone, med bevis for periodisk resertifisering (NIS2 forventer minst årlig, oftere for privilegerte kontoer). For det tredje, bevis for at avgangskontoer er deaktivert raskt — en utdatert konto som tilhører en kontraktør som sluttet for to år siden, er den typen funn som dukker opp rutinemessig under tilgangs-resertifisering.

12. Tiltak (j) — flerfaktorautentisering, sikret kommunikasjon

> «bruk av flerfaktorautentisering eller løsninger for kontinuerlig autentisering, sikret tale-, video- og tekstkommunikasjon og sikret nødkommunikasjonssystemer innen enheten, der det er hensiktsmessig»

Primære IEC 62443-deler: `IEC 62443-3-3:2013` FR 1, `IEC 62443-4-2:2019`.

Spesifikke klausuler. Flerfaktorautentisering vises eksplisitt i `-3-3` SR 1.1 RE 1 «Unique identification and authentication» og er påkrevd av SL-2 og over for menneskelige brukere som aksesserer kontrollsystemet fra ikke-betrodde nettverk (SR 1.13 «Access via untrusted networks»). På komponentnivå bærer `-4-2` CR 1.1, CR 1.7, CR 1.13 de samme kravene. Sikrede kommunikasjonskanaler er FR 3 og FR 4-territorium (se tiltak (h)).

Samsvar: delvis. MFA-kartleggingen er tett ved SL-2 og over for fjerntilgang. Der samsvaret svekkes er på «sikret tale-, video- og tekstkommunikasjon og sikret nødkommunikasjonssystemer» — den kulen var åpenbart utarbeidet med telekom, offentlig administrasjon og nødetater i tankene. IEC 62443 har ingenting om herdet tale- eller radiokommunikasjon. For de fleste fornybaroperatører leses dette som «sørg for at den operasjonelle kommunikasjonen din — radio mellom transformatorstasjon og kontrollsenter, Teams eller tilsvarende brukt til operasjonell koordinering, satellitt- eller 4G/5G-

bakhal fra en fjern vindpark — bruker hensiktsmessige konfidensialitets- og integritetskontroller» og er tilfredsstilt gjennom `-3-3` FR 3/FR 4 pluss en innkjøpsbeslutning på kommunikasjonsplattformen.

Hva du må vise på toppen. MFA-håndhevingsbevis for all fjerntilgang (leverandørvedlikehold, ingeniørtilgang, SCADA-fra-laptop): eksportert konfigurasjon som viser at MFA er påkrevd, ikke valgfritt. En kontinuitetsplan for den operasjonelle kommunikasjonskanalen — hva skjer med radio-fallbacken eller satellittlenken din hvis det primære feiler. For «sikret nødkommunikasjon», en prosedyre som viser hvordan driftsteamet skal nå NSM/NCSC, OEM-en og TSO-en hvis selskapets kommunikasjonsplattform selv er kompromittert — dette er en av NIS2-pliktene som oftest fanger operatører, fordi de fleste antar at deres vanlige Teams- eller e-postkanal vil være tilgjengelig under en hendelse.

13. Der IEC 62443 har kontroller NIS2 ikke spør om eksplisitt — den omvendte kartleggingen

Det er verdt å snu spørsmålet et øyeblikk. Hvor går IEC 62443 utover NIS2 Artikkel 21?

Soneinndeling og SL-T-utledning. `IEC 62443-3-2` er fundamental for 62443-tilnærmingen, men er ikke bokstavelig navngitt i NIS2. Du vil ikke få et NIS2-funn for å unnlate å partisjonere SuC-en i soner og kanaler — forutsatt at risikovurderingen din produserer et like grundig resultat. Men hvis du har gjort `-3-2` skikkelig, har du det mest forsvarbare artefaktet for Artikkel 21(2)(a) som en OT-revisor vil be om å se. Standardens disiplin er strengere enn NIS2 strengt tatt krever.

Kapabilitets-/modenhetsmodell. Sikkerhetsnivåer (SL-C, SL-T, SL-A) på den tekniske siden og Maturity Levels 1 til 4 på

programmesiden er 62443-spesifikke konstrukter. NIS2 har ingenting tilsvarende — direktivet spør ikke «hvilken SL oppnådde du på sikkerhetssonen i vindparken din?». For intern benchmarking og for anbudsresponser til andre 62443-bevisste kjøpere betyr SL/ML noe; for NIS2-revisjonen er det støttebevis i beste fall. Terminologisporet tilbake til fundamentdokumentene er i IEC 62443-1-x fundamentteksten .

Komponentnivåsertifisering. `IEC 62443-4-2`-sertifisering av enkeltenheter (tilbudt av laboratorier akkreditert under ISASecure - eller IECEE CB -ordningene) er frivillig i 62443. NIS2 krever det ikke. De kommende europeiske cybersikkerhetssertifiseringsordningene under cybersikkerhetsforordningen og Cyber Resilience Act vil plukke dette opp — se CRA-anvendelsesteksten for hvordan `-4-2` overlapper med CRA Annex I — men per mai 2026 forblir komponentsertifisering «hyggelig å ha, ikke et må».

Utvekslingsformat for oppdateringsinformasjon. `IEC TR 62443-2-3` definerer et spesifikt XML-basert utvekslingsformat for oppdateringsmetadata mellom OEM og anleggseier. NIS2 bryr seg ikke om hvilket format du bruker, så lenge sårbarhetshåndteringen skjer; formatet selv er en 62443-finurlighet.

14. Hva NIS2 forplikter som 62443 ikke kan hjelpe med i det hele tatt

Den ærlige «fraværende»-kolonnen i kartleggingen. Dette er pliktene en 62443-revisjonsmappe ikke vil berøre, og hvor anleggseieren må bygge separate bevis fra bunnen av:

Artikkel 23 rapporteringsfrister for hendelser. 24-timers tidlig varsling, 72-timers hendelsesmelding, valgfri midlertidig rapport på forespørsel og én-månedssluttrapport er rene NIS2-plikter. Kommisjonens gjennomføringsforordning (EU) 2024/2690 av 17. oktober 2024 gir teknisk og metodologisk detalj for delmengden av

digitale infrastrukturenheter (DNS-leverandører, sky, CDN, MSP/MSSP, markedsplasser, søkemotorer, sosiale nettverk, tillitstjenesteleverandører) — energienheter er **ikke** innenfor det direkte virkeområdet, men nasjonale tilsynsmyndigheter og ENISAs Technical Implementation Guidance fra juni 2025 behandler annexet som den autoritative tolkningsveiledningen for Artikkel 21 på tvers av alle sektorer. Les det; ikke anta at det ikke gjelder for deg i ånden selv om det ikke gjelder for deg i loven.

Artikkel 24 europeisk cybersikkerhetssertifisering. NIS2 reserverer Kommisjonens mulighet til å kreve at enheter bruker IKT-produkter, -tjenester og -prosesser sertifisert under Forordning (EU) 2019/881 (cybersikkerhetsforordningen)-ordningene — EUCC (den europeiske Common Criteria-baserte ordningen vedtatt i 2024) er den første, med EUCS (skytjenester) og EU5G under utvikling. IEC 62443 er ikke, per mai 2026, en europeisk ordning; den forblir en nyttig teknisk referanse, men oppfyller ikke i seg selv noen fremtidig Artikkel 24-plikt.

Artikkel 25 standardiseringsreferanser. Artikkel 25 navngir ENISAs rolle i å fremme konvergens om standarder. Den pålegger ikke IEC 62443 ved nummer. Vær varsom med leverandørmarkedsføringskrav som «vi er NIS2-konforme fordi vi er 62443-konforme» — verken direktivet eller noen gjennomføringsakt trekker den ekvivalensen.

Artikkel 32 og 33 tilsynsregime og sanksjoner. Sanksjonsnivåer — opp til EUR 10 millioner eller 2 % av total verdensomspennende årsomsetning for vesentlige enheter, opp til EUR 7 millioner eller 1,4 % for viktige enheter — og tilsynsverktøykassen (inspeksjoner på stedet, ad-hoc-revisjoner, sikkerhetsskanninger, informasjonsforespørsler, bindende instrukser) er ikke noe IEC 62443 har et syn på. Anleggseieren må være klar til å være vert for en

NSM-inspeksjon på samme måte som de ville være vert for en DSB - eller Petroleumstilsynet -inspeksjon på sikkerhetssiden.

15. En praktisk bevismappe — hva man skal levere til revisjonen

Hvis du nærmer deg din første NIS2-justerte revisjon og du allerede har et aktivt IEC 62443-program, blir spørsmålet: hvilke ekstra artefakter må jeg sette sammen? Tabellen under er hva jeg ville lagt foran revisor. Venstre kolonne er NIS2-tiltaket; midten er 62443-beviset som allerede finnes; høyre er NIS2-spesifikt delta.

NIS2 Artikkel 21(2)-tiltak	62443-bevis som trolig allerede finnes	NIS2-spesifikt bevis å legge til
(a) Risikoanalyse og ISMS-policy	`-3-2` SuC-soneinndeling, SL-T-utledninger, risikoregister; `-2-1` ORG 2-registre	Styregodkjent policy-dokument; årlig gjennomgangsprotokoll; restrisiko-aksepteringslogg
(b) Hendelseshåndtering	`-3-3` FR 6 logging/overvåkningsbevis; `-2-1` IR SPE-prosedyre	Navngitt CSIRT-kontakt; 24t/72t/1mnd rapporteringsplaybook; tabletop-testlogg som dekker rapportering
(c) Virksomhetskontinuitet	SR 7.3/7.4 sikkerhetskopi- og gjenopprettingstestlogger; `-2-1` BCM SPE	Plan for essensiell tjeneste-BCDR; RTO/RPO per prosess; krisehåndteringsprosedyre med navngitte roller
(d) Leverandørkjede	`-2-4` integrator-revisjoner; `-4-1` ML-sertifikater fra OEM-er; `-2-1` innkjøps-SPE	Lagdelt leverandørregister; kontraktuelle hendelsesmeldingsklausuler; bevissthet om ENISA-koordinert risikovurdering
(e) Anskaffelse, utvikling, vedlikehold, sårbarhetshåndtering	`-4-1` DM/SUM-bevis; `IEC TR 62443-2-3` oppdateringsregistre	CVD-policy med offentlig kontakt; abonnementsliste for varselovervåkning; oppdaterings-SLA
(f) Effektivitetsvurdering	`-2-1` internrevisjons- og ledelsesgjennomgangsregistre; ML-skår	KPI-er rapportert til ledelsen; sporing av korrigerende tiltak synlig for styret
(g) Hygiene og opplæring	`-2-1` opplærings-SPE-registre; `-2-4` SP.02-registre	Artikkel 20(2)-opplæringsregistre for ledelsen; phishing-simulasjonsresultater (valgfritt)
(h) Kryptografi	`-3-3` FR 4 / `-4-2` CR 4.x designbevis	Algoritmekatalog-policy; nøkkellivssyklusprosedyre; dokumenterte ikke-anvendelighetsbeslutninger
(i) Personal, tilgang, aktivahåndtering	`-3-3` FR 1/FR 2-bevis; CM SPE aktivaregister	Periodisk tilgangs-resertifiseringslogg; onboarding/forflytning/avgang-revisjonsspor
(j) MFA og sikret kommunikasjon	SR 1.13 / CR 1.13 MFA-håndhevingsbevis	Out-of-band nødkommunikasjonsprosedyre; dokumentert MFA-unntaksprosess

16. Sammendragstabell — enkeltsides referanse

NIS2-tiltak	Primær 62443-del(er)	Sentral SR / CR / klausul	Samsvar	
(a) Risikoanalyse og retningslinjer	`-2-1:2024`, `-3-2:2020`	ORG 1, ORG 2; hele `-3-2`-metodikken	Tett	S g a
(b) Hendelseshåndtering	`-2-1:2024`, `-3-3:2013`	SR 2.8–2.11, SR 6.1–6.2; IR SPE	Delvis	C n t
(c) Virksomhetskontinuitet / DR	`-2-1:2024`, `-3-3:2013`	SR 7.1–7.6; BCM SPE	Tett (IACS-omfang)	F u k
(d) Leverandørkjede	`-2-4:2023`, `-4-1:2018`, `-2-1:2024`	Hele `-2-4`; `-4-1` SM, DM, SUM	Delvis	L k C
(e) Anskaffelse, utvikling, vedlikehold, sårbarhet	`-4-1:2018`, `IEC TR 62443-2-3:2015`, `-3-3:2013`	`-4-1` DM, SUM; SR 3.4; `TR 2-3` utveksling	Delvis	C d
(f) Effektivitetsvurdering	`-2-1:2024`	Internrevisjons- og ledelsesgjennomgangs-SPE-er; ML-modell	Tett	S k
(g) Hygiene og opplæring	`-2-1:2024`, `-2-4:2023`	Personalsikkerhet-SPE; SP.02	Tett (arbeidsstokk); løst (styret)	A d
(h) Kryptografi	`-3-3:2013`, `-4-2:2019`	SR 3.1, 3.8, 4.1, 4.3; CR 4.x	Delvis	A n
(i) Personal, tilgang, aktiva	`-2-1:2024`, `-3-3:2013`, `-4-2:2019`	FR 1, FR 2; CM SPE; personal-SPE	Tett	F n
(j) MFA og sikret kommunikasjon	`-3-3:2013`, `-4-2:2019`	SR 1.1 RE 1, SR 1.13; CR 1.13	Delvis	C n
På tvers: Art 20 ledelsesorgan	ingen	n/a	**Fraværende**	S d s
På tvers: Art 23 rapporteringsfrister	ingen	n/a	**Fraværende**	2 n
På tvers: Art 32/33 tilsyn	ingen	n/a	**Fraværende**	F d

17. Leseliste og kryssreferanser

Hvis du følger denne serien, er forutsetningslesningen IEC 62443 fundamentteksten , som setter opp konseptene og delene; styringssystem-gjennomgangen , som går dypt på `-2-1:2024`; systemdesign-teksten om `-3-2` og `-3-3`; og OEM-siden om `-4-1` og `-4-2`. På reguleringssiden er NIS2-anvendelse scoping-følgesvennen til denne teksten, og CRA-anvendelse dekker produktsiden av reguleringen som overlapper med `-4-1`/`-4-2`.

Primære regulatoriske kilder brukt gjennomgående: Direktiv (EU) 2022/2555 (NIS2) ; Kommisjonens gjennomføringsforordning (EU) 2024/2690 ; ENISA Technical Implementation Guidance fra juni 2025. Norsk gjennomføring: `digitalsikkerhetsloven` LOV-2023-12-20-108 . Standarder: IEC Webstore for 62443-serien . Kryssreferanse: NIST SP 800-82 Rev. 3 «Guide to Operational Technology (OT) Security» — nyttig som en leverandørnøytral andremening på de fleste tekniske kartleggingene over.

18. Ofte stilte spørsmål

Tilfredsstiller IEC 62443 NIS2? Ikke alene. IEC 62443 er det sterkeste tilgjengelige tekniske svaret på de fleste av NIS2 Artikkel 21s kontrollplikter og vil ta deg langt gjennom tiltak (a), (c), (e), (g), (h), (i) og (j) på det tekniske planet. Den tilfredsstiller ikke ansvaret for ledelsen i Artikkel 20, 24-timers/72-timers/én-månedsrapporteringsfristene i Artikkel 23, den europeiske sertifiseringsreferansen i Artikkel 24, eller tilsynsregimet i Artikkel 32 og 33. Behandle 62443 som det tekniske underlaget og NIS2 som styrings- og rapporteringslaget.

Hva krever NIS2 Artikkel 21? Artikkel 21(1) krever at vesentlige og viktige enheter treffer «egnede og forholdsmessige tekniske, operasjonelle og organisatoriske tiltak» for å håndtere cyberrisiko mot nettverks- og informasjonssystemene sine. Artikkel 21(2) lister

opp ti minimumstiltak: risikoanalyse-policy, hendelseshåndtering, virksomhetskontinuitet, leverandørkjedesikkerhet, anskaffelse/utvikling/vedlikehold med sårbarhetshåndtering, effektivitetsvurdering, hygiene og opplæring, kryptografi, personal/tilgang/aktivahåndtering, og MFA/sikret kommunikasjon. Kommisjonens gjennomføringsforordning (EU) 2024/2690 av 17. oktober 2024 utdyper de tekniske og metodologiske kravene — direkte bindende for digitale infrastrukturenheter og brukt som autoritativ tolkningsveiledning ellers.

Hvordan kartlegges NIS2s rapporteringsfrister for hendelser mot IEC 62443? De gjør det ikke. IEC 62443 har ingen tilsvarende tidsplikt. 24-timers tidlig varsling, 72-timers hendelsesmelding og én-månedssluttrapport under Artikkel 23 er rene NIS2-tiltak — du bygger en separat playbook for dem, navngir den nasjonale CSIRT-en (NSM/NCSC i Norge), definerer terskelene for vesentlighet, og øver ende-til-ende-strømmen minst årlig.

Er IEC 62443 obligatorisk under NIS2? Nei. Verken direktivet eller noen nåværende gjennomføringsakt navngir IEC 62443 som obligatorisk. Fortale og Artikkel 21(5) i NIS2 instruerer medlemsstatene og Kommisjonen til å fremme bruken av «europeiske og internasjonale standarder», og IEC 62443 er den dominerende slike standarden i OT — men samsvar med den er frivillig. Den kommende Cyber Resilience Act vil skape et sterkere trekk mot `-4-1` og `-4-2` for produktleverandører som plasserer enheter på EU-markedet.

Hvordan forholder Kommisjonens gjennomføringsforordning (EU) 2024/2690 seg til IEC 62443? `(EU) 2024/2690` fastsetter tekniske og metodologiske krav for de ti Artikkel 21(2)-tiltakene, med et 13-avsnitts anneks som utdyper hvert enkelt. Det formelle virkeområdet er digitale infrastruktur- og digitale leverandørenheter (DNS, sky, CDN, MSP/MSSP, markedsplasser, søkemotorer, sosiale

nettverk, tillitstjenesteleverandører), så en energioperatør er ikke juridisk bundet av det direkte. I praksis behandler tilsynsmyndigheter og ENISAs gjennomføringsveiledning fra juni 2025 annexet som referansetolkningen av Artikkel 21 på tvers av alle sektorer. IEC 62443-kontroller kartlegges rent mot de fleste anneksavsnitt — risikohåndtering, aktivahåndtering, tilgangskontroll, kryptografi, nettverkssikkerhet, sårbarhetshåndtering — og ENISAs kartleggingsregneark anerkjenner dette. Der annexet går utover IEC 62443 (juridisk-entitets styring, offentlig CVD-kontakt, leverandørregister mot ENISA-koordinerte risikovurderinger), legger anleggseieren til de manglende artefaktene på toppen av eksisterende 62443-bevis.

Hva med Norge spesifikt — når biter NIS2 faktisk inn for en norsk fornybaroperatør? Per 14. mai 2026 er svaret: ikke ennå, men snart. Den nåværende norske `digitalsikkerhetsloven` (LOV-2023-12-20-108) trådte i kraft 1. oktober 2025 og gjennomfører **NIS1**, ikke NIS2. NIS2 er ennå ikke innlemmet i EØS-avtalen, og Norge forventes å gjennomføre det i 2026, sannsynligvis gjennom en ny kombinert cyber-og-CER-lov som vil erstatte gjeldende digitalsikkerhetslov. Direktivets innholdsmessige plikter er stabile, imidlertid — Artikkel 21 og Artikkel 23 vil ikke endres mellom nå og norsk ikrafttredelse. Å bygge bevismappen som er lagt fram over, er den riktige forberedelsen i dag, og de fleste norske fornybaroperatører av en viss størrelse vil trenge den før utgangen av 2026.

Hvis du fant dette nyttig, er resten av serien lenket over; hvis du oppdager en klausulreferansefeil eller en transposisjonsoppdatering

jeg har gått glipp av, send meg en melding — korrigeringer er velkomne.

IEC 62443-bevismappe: enkeltsides versjon

15. mai 2026 · 12 min lesetid · #compliance #security #industrial #iec-62443

Tenk deg en Trinn 2-revisjon på en 120 MW solpark. Tre minutter inn spør revisor det stille spørsmålet høyt: «Det er interessant — vis meg nå beviset.» Programlederen åpner en SharePoint-mappe merket `62443_compliance`. Inni ligger elleve PDF-er. Ni er leverandørbrosjyrer med ordene «62443-klar» trykt øverst. Én er et skjermbilde av en CSV. Den ellevte er den signerte kontrakten med EPC-en. Revisor lukker laptopen, smiler høflig, ber om en kaffe, og skriver sytten avvik inn i oppfølgingsbrevet.

Denne teksten finnes for at det ikke skal skje med deg.

TL;DR

Hvis du ikke kan fremlegge et spesifikt dokument på forespørsel, er du ikke faktisk `IEC 62443`-konform — uansett hva leverandørens glansede brosjyre sier. Dette er **enkeltsides bevismappen**: en stram, meningssterk sjekkliste over artefaktene en revisor vil be om under hver av de fire nummererte gruppene i standarden (`IEC 62443-2-x`, `-3-x`, `-4-x`), pluss et lite sett tverrgående punkter. Velg pakken som matcher rollen din, skriv den ut, og gå inn i neste prosjekt med den i hånden. Den femspørsmåls selvtesten på slutten er de mest nyttige 100 ordene i teksten.

Hvem dette er for

`ISA/IEC 62443`-serien definerer fire prinsipielle roller — anleggseier, integrator, tjenesteleverandør og produktleverandør — og hver artefakt under kartlegger til en av dem. Hvis du ikke allerede har lest IEC 62443-1-x fundamentteksten , start der: rolledefinisjonene og

livssyklusmodellen for Industrial Automation and Control System (IACS) i `IEC TS 62443-1-1:2009` er stillaset alt annet henger fra.

- **Anleggseiere** (operatørene — kraftselskaper, produsenter, anleggseiere): pakken din er `-2-1` + `-3-2`.
- **Integratorer og tjenesteleverandører** (EPC-er, systemintegratorer, vedlikeholdsentreprenører): pakken din er `-2-4`.
- **Produktleverandører** (PLC-, RTU-, gateway-, HMI-, inverter-, BMS-leverandører): pakken din er `-4-1` + `-4-2`.
- **Alle** skylder de tverrgående artefaktene i avsnitt 5.

En dypere gjennomgang av hver finnes i `-2-x` styringssystemteksten , `-3-2` og `-3-3`-teksten , og `-4-1` og `-4-2`-teksten . Denne er fuskelappen.

1. Hierarkiet av 62443-bevis

Revisorer — i hvert fall de gode — tenker i tre nivåer. Det bør du også.

- **Nivå 1: policy- og prosedyredokumenter.** Hva du har til hensikt å gjøre. Charter for sikkerhetsprogrammet, risikovurderingsprosedyre, endringshåndteringspolicy. Billigst å produsere, lettest å fingere, svakest som bevis.
- **Nivå 2: opptak og operasjonelt bevis.** Hva du faktisk gjorde. Signerte protokoller, lister over opplæringsoppmøte, billetteksporter, testrapporter, oppdateringslogger, revisjonsfunn med lukkedatoer. Det er her revisjoner vinnes eller tapes.
- **Nivå 3: uavhengige sertifiseringer.** Hva en akkreditert tredjepart verifiserte. ISASecure CSA / SSA / SDLA-sertifikater, IECEE CB-ordningens testrapporter, eller akkrediterte revisjoner mot `IEC 62443-2-4` for tjenesteleverandører. Dyrest, vanskeligst å argumentere mot.

Et modent program har alle tre. Et forsvarbart program har minst Nivå 1 og 2 over hele linja, med Nivå 3 plassert under komponentene med høyest risiko. Et «brosjyre-PDF»-program har ingen av disse og flere brosjyrer.

For produktsidens Nivå 3 spesielt driver ISASecure de tre produkt-/prosessordningene som oftest siteres i anbud — `CSA` mot `IEC 62443-4-2`, `SSA` mot `IEC 62443-3-3`, og `SDLA` mot `IEC 62443-4-1` — alle under `ISO/IEC 17065` . IECEE CB-ordningen gir den parallelle internasjonale samsvarsvurderingsruten gjennom `IEC 62443` og er den de fleste europeiske kjøpere vil gjenkjenne.

2. Bevismappe for anleggseier — for `IEC 62443-2-1:2024` og `IEC 62443-3-2:2020`

2024-utgaven av `IEC 62443-2-1` erstattet det gamle Cyber Security Management System (CSMS)-språket med åtte **Security Programme Elements** (SPE-er) og la til en modenhetsmodell. Risikometodikken ligger fortsatt i `IEC 62443-3-2:2020` , som definerer systemet under vurdering (SuC), sone-og-kanaltegningen, og utledning av Target Security Level (SL-T).

Grupper beviset ditt etter SPE. Hvis en revisor ikke finner noen av følgende på forespørsel, forvent et funn.

#	Artefakt	Hva revisor vil ta stikkprøve på	Rødt flagg
1	Charter / policy-dokument for sikkerhetsprogrammet	Godkjenningssignatur, omfangsuttalelse, gjeldende IACS-anlegg	Mer enn 24 måneder gammelt uten revisjonshistorikk
2	Styre-/ledelsesprotokoll for godkjenning	Godkjenningsdato, navngitt ansvarlig leder	Godkjenneren er samme person som skrev det
3	Risikovurdering etter `IEC 62443-3-2` for hver SuC	SuC-definisjon, trussel-katalog, konsekvensvurdering	Én global risikovurdering brukt på urelaterte anlegg
4	Sone- og kanaldiagram per SuC	Versjonert tegning, aktiva-til-sone-fordeling	Ingen kanalliste, eller kanaler tegnet men ikke listet
5	SL-T-vektorutledning per sone	Per-Foundational-Requirement (FR)-vektor — syv verdier, ikke én	Et enkelt «SL 2»- eller «SL 3»-krav uten FR-oppdeling
6	Risikoregister med restrisiko-aksept	Eier, behandling, restrisikoverdi, signering	Restrisikoer akseptert av samme ingeniør som vurderte dem
7	Baseline for aktivaregister (SPE 2 — `CM 1.1`)	Maskinvare, firmwareversjoner, programvare, nettverksporter	Firmwareversjoner som ikke matcher det som faktisk kjører i felt
8	Konfigurasjonsstyringsbaselinjer	Gullbilde, prosedyre for baselineavvik	Baselinjer som er eldre enn den siste firmwareoppdateringen
9	Internrevisjonsrapporter	Omfang, funn, korrigerende tiltak, lukkedatoer	Ingen internrevisjon i de siste 12 månedene
10	Protokoll fra ledelsesgjennomgang	Inputs gjennomgått, beslutninger tatt, tiltak tildelt	Et møte uten beslutninger registrert
11	Opplæringsregistre (SPE 1)	Rollebasert opplæringsmatrise, fullføringsdatoer per person	Generiske «cyberbevissthet»-sertifikater uten OT-innhold
12	Leverandørregister (med `-2-4`-vurderingsstatus)	Siste vurderingsdato, omfang, mangler	Leverandører listet uten vurderingsdato
13	Hendelsesresponsprosedyre + øvelsesopptak		

#	Artefakt	Hva revisor vil ta stikkprøve på	Rødt flagg
		Tabletop-protokoll, post-mortem etter reelle hendelser	Prosedyren finnes, men ingen øvelse i de siste 18 månedene
14	BCDR-plan + gjenopprettingstestbevis	Siste vellykkede gjenopprettingstest, RTO/RPO oppnådd	«Sikkerhetskopi kjører nattlig» uten gjenopprettingstest registrert
15	Unntaks-/avviksregister	Hvert unntak koblet til en kompenserende kontroll og en utløpsdato	Åpne unntak uten gjennomgangsdato

Mesteparten av artefaktkartet over sitter i SPE-er 1 til 8 — organisatorisk sikkerhet, konfigurasjonsstyring, nettverks- og kommunikasjonsbeskyttelse, komponentbeskyttelse, databeskyttelse, brukertilgangskontroll, hendelses- og hendelseshåndtering, og systemintegritet og -tilgjengelighet. ISA Global Cybersecurity Alliance (ISAGCA) Quick Start Guide er den reneste gratis referansen til SPE-strukturen hvis du ikke har IEC-teksten foran deg.

3. Bevismappe for integrator og tjenesteleverandør — for `IEC 62443-2-4:2023`

`IEC 62443-2-4:2023` — utgave 2.0, publisert desember 2023 — definerer sikkerhetskapabilitetene en tjenesteleverandør tilbyr en anleggseier under integrasjon og vedlikehold, organisert i Security Programme (SP)-emner `SP.01` til `SP.12` (bemanning, assurance, arkitektur, trådløst, konfigurasjonsstyring, herding, anti-skadevare, oppdateringshåndtering, sikkerhetskopi/gjenoppretting, overvåkning, hendelseshåndtering, kontohåndtering, fjerntilgang). 2023-revisjonen konverterte mange tidligere «kapabiliteter» til påkrevde **prosesser** med dokumenterte utdata — som betyr at bevis nå er ikke-forhandlingsbart.

#	Artefakt	Kartlegger til	Rødt flagg
1	Bemannings- og kompetanseregistre	`SP.01`	Personell listet uten OT-spesifikk opplæring
2	Tjenesteomfangsdokument per kontrakt	`SP.02`	Et boilerplate-omfang gjenbrukt på urelaterte kontrakter
3	Sikker arkitektur-overleveringspakke	`SP.03`	Ingen sone/kanal-overlegg avtalt med anleggseieren
4	Trådløse konfigurasjonsopptak	`SP.04`	Trådløst brukt, men ingen deteksjonsprosess for ulovlige enheter
5	Herdingsbaselinjer anvendt per enhetsklasse	`SP.06`	Baselinjer fra en tidligere firmwaregenerasjon
6	Bevis for anti-skadevare-utrulling	`SP.07`	AV-signaturer sist oppdatert måneder før idriftsettelse
7	Oppdateringshåndteringsopptak	`SP.08`	Oppdateringer godkjent av anleggseieren, men aldri utrullet
8	Sikkerhetskopi- og gjenopprettingstestbevis	`SP.09`	Sikkerhetskopier finnes, gjenoppretting aldri testet på målmaskinvaren
9	Fjerntilgangsprosedyre + sesjonslogger	`SP.11`	Jump-host-logger som ikke registrerer kommandoer eller sesjonsvideo
10	Endringshåndteringsopptak	Tverrgående	Endringer implementert før godkjenningssignaturer

`SP.05` (assurance) og `SP.12` (hendelseshåndtering) sitter under det over som tverrgående kontroller og bør plukkes opp av den tverrgående pakken i avsnitt 5.

4. Bevismappe for produktleverandør — for `IEC 62443-4-1:2018` og `IEC 62443-4-2:2019`

`IEC 62443-4-1:2018` definerer en Secure Development Lifecycle (SDL) bygget rundt **åtte praksiser**: Security Management (`SM`), Specification of Security Requirements (`SR`), Secure by Design (`SD`), Secure Implementation (`SI`), Security Verification and Validation Testing (`SVV`), Management of Security-related Issues (`DM`), Security Update Management (`SUM`), og Security Guidelines (`SG`). `IEC`

`62443-4-2:2019` definerer så de tekniske Component Requirements (CR-ene) per Foundational Requirement, med kapabilitets-sikkerhetsnivå `SL-C 1` til `SL-C 4`.

#	Artefakt	Kartlegger til	Rødt flagg
1	SDL-policy og opplæringsregistre	`SM-1` … `SM-13`	En policy som eksisterer, men ingen utvikler er opplært mot den
2	Trusselmodell per produkt	`SR-2`	Trusselmodell skrevet én gang ved lansering, aldri oppdatert
3	Sporingsmatrise for sikkerhetskrav	`SR-1` … `SR-5`	Krav uten testcase kartlagt
4	Bevis for sikker koding (SAST, DAST)	`SI-1`, `SI-2`	Skannerapporter med kritiske funn merket «akseptert» uten begrunnelse
5	Sikkerhetstestrapport (funksjonell, fuzz, pen-test)	`SVV-1` … `SVV-5`	Ingen bevis for tester-uavhengighet
6	Sårbarhetshåndteringsprosedyre med koordinert-rapporteringskontakt (CVD)	`DM-1` … `DM-6`	Ingen `security@`-postkasse, ingen PSIRT, ingen publisert policy
7	Software Bill of Materials (SBOM) — CycloneDX eller SPDX	`SM-9`, `DM-1`	En SBOM uten versjon, uten hash, uten oppdateringskanal
8	Sikkerhetsretningslinjer / herdingsveiledning for anleggseiere	`SG-1` … `SG-7`	En «brukermanual» med ett avsnitt om sikkerhet
9	Bevis for sikkerhetsoppdateringskanal	`SUM-1` … `SUM-5`	Oppdateringer utgitt, men ingen dokumentert leveringskanal
10	End-of-life (EOL) supportpolicy	`SUM-5`, `SG-7`	EOL-datoer som flyttes stille når det passer

For `IEC 62443-4-2:2019`, legg til en per-FR testbevispakke som kartlegger hvert CR-krav til et resultat, oppsummert av en akkreditert sertifiseringsorganisasjons rapport. En ryddig måte å gjøre dette på er å vedlegge ISASecure CSA-sertifikatet pluss de underliggende Functional Security Assessment (FSA-C)- og Vulnerability Identification Testing (VIT-C)-rapportene, eller tilsvarende under IECEE CB-ordningen . For utviklingsprosess-sertifisering alene — uten et produktsertifikat — er `ISASecure SDLA` eller en IECEE `IEC`

`62443-4-1`-vurdering tilsvarende. Merk at `SDLA`-ordningen tillater en leverandør å scope ut individuelle delpraksiser, så les alltid sertifikatets omfangsuttalelse, ikke bare logoen.

5. Tverrgående artefakter

Dette er de som programmer rutinemessig glemmer — og det er de revisorene liker å spørre etter, fordi de avslører om programmet faktisk drives eller bare er skrevet ned.

1. **Risiko-akseptlogg signert av ledelsen.** Ikke en prosjektleder. Ikke en «ansvarlig ingeniør». Den ansvarlige lederen som er navngitt i SPE 1-charteret, med en dato og en restrisikoverdi.
2. **Register for kompenserende mottiltak.** Der en kontroll ikke kunne implementeres innfødt, navngis det kompenserende tiltaket, begrunnelsen dokumenteres etter `IEC TS 62443-1-1:2009`-definisjonen, og effektiviteten gjennomgås på en angitt kadens. `IEC 62443-2-1:2024` tillater eksplisitt kompenserende kontroller for eldre systemer — men bare hvis de er dokumentert.
3. **Unntaks-/avviksregister.** Hvert avvik fra en policy eller baseline, med en eier, en utløpsdato, og en kompenserende kontroll.
4. **SL-T → SL-C → SL-A sporingsmatrise per sone.** Anleggseieren utleder SL-T etter `-3-2`. Produktleverandøren publiserer SL-C etter `-4-2`. Integratoren leverer SL-A (oppnådd) i den som-bygget-konfigurasjonen. Revisorer elsker denne matrisen fordi gap faller ut av den visuelt.
5. **Versjonskontroll-logg for bevismappen.** Selve beviset trenger versjonskontroll. Hvis revisjonsmappen er «levende SharePoint» uten revisjonshistorikk, har beviset ditt ingen integritet.
6. **Tidssynkroniseringsbevis.** Ofte glemt. `IEC 62443-3-3:2013` SR 2.11 (Timestamps) krever at komponenter gir pålitelige, synkroniserte tidsstempler for revisjonsopptak. Hvis PLC-en, jump-hosten og

SIEM-klokken driver, er revisjonssporet ditt ikke juridisk brukbart. NIST SP 800-82 Rev. 3 gjør samme poeng i OT-termer.

6. Hva som IKKE teller som bevis

En kort, meningssterk rødflagg-liste. Ingen av det følgende vil overleve en revisjon alene:

- **Markedsførings-PDF-er som sier «62443-konform» uten et delnummer.** `IEC 62443` er en serie, ikke en enkelt standard. «Konform» med hvilket av de tretten-pluss dokumentene? Ved hvilket utgaveår? Mot hvilken SL? Uten det er kravet dekorativt.
- **Enkeltverdis SL-krav.** «Vi er SL 3» er meningsløst. `IEC 62443-3-3` og `-4-2` uttrykker sikkerhetsnivåer som en syv-elements vektor — én per FR (Identification & Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, Resource Availability). En vektor som `SL-C (3,2,3,1,3,2,3)` er den riktige formen.
- **Leverandørsertifikater uten en omfangsuttalelse.** `ISASecure SDLA`-sertifikatet, for eksempel, sier deg bare at prosessen ble vurdert for delpraksisene i omfang — som lovlig kan være et delsett. Les alltid omfangsannekset.
- **Samsvarsmatriser som ikke er signert, datert eller versjonskontrollert.** Et Word-dokument som er redigert av seks personer med spor-endringer av er ikke bevis; det er et rykte.
- **Testrapporter fra før den siste store firmwareoppdateringen.** En penetrasjonstest-rapport mot firmware v4.2 sertifiserer ikke v4.7. Leverandøren skylder en delta-vurdering eller en re-test.

7. Den femspørsmåls pre-revisjons-selvtesten

De mest nyttige 100 ordene i denne teksten. Kjør denne femspørsmåls testen før revisor krysser terskelen din. Hvis du ikke kan svare «ja, her er det» på alle fem, fiks det først.

1. Kan du fremlegge **SL-T-vektoren** for hver sone, utledet etter `IEC 62443-3-2`, signert i løpet av de siste 24 månedene?
2. Kan du fremlegge et **fullstendig aktivaregister** der firmwareversjonene matcher det som faktisk er utrullet på anlegget i dag?
3. Kan du fremlegge et **internrevisjonsfunn** fra de siste 12 månedene som resulterte i et korrigerende tiltak som nå er formelt lukket?
4. Kan du fremlegge bevis for at en **vedlikeholdsleverandør** er vurdert mot `IEC 62443-2-4` i den siste kontraktssyklusen?
5. Kan du fremlegge **restrisiko-akseptloggen**, signert av relevant ledelsesmedlem, datert og aktuell?

Fem «ja»-svar er ikke samsvar — men fem «nei»-svar er definitivt ikke-samsvar.

8. Hvordan bruke dette som et prosjektverktøy

Tre konkrete bruksområder, i rekkefølge etter hvor ofte hver typisk dukker opp:

- **På et nytt prosjekt.** Velg pakken som matcher rollen du spiller — eier, integrator eller leverandør — og bruk den som en leveranseliste i prosjektplanen. Hver rad blir et arbeidspakke-utfall.
- **På en revisjon.** Produser den riktige pakken og sjekk alderen på hver artefakt. Alt eldre enn 12 måneder er et spørsmål som venter

på å bli stilt; alt eldre enn 24 måneder er et funn som venter på å bli skrevet.

- **På innkjøp.** Gi leverandøren en tilpasset versjon av produktleverandør-pakken som et anbudsannekse. «Lever hvert av punkt 1–10 med budet, ellers er budet ikke-responsivt.» Denne enkle taktikken hever bunnen i leverandørresponser raskere enn noen kontraktsklausul.

Den samme logikken underbygger NIS2-kartleggingsteksten — der NIS2-direktivet (EU) 2022/2555 krever «egnede og forholdsmessige tekniske, operasjonelle og organisatoriske tiltak», er disse artefaktene som demonstrerer dem. Og for produkter plassert på EU-markedet etter desember 2027, går CRA-anvendelsesteksten gjennom hvor produktleverandør-pakken her dobler som en CRA-samsvarsmappe.

Ofte stilte spørsmål

Hva er forskjellen mellom et `-4-1`-sertifikat og et `-4-2`-sertifikat? `-4-1` sertifiserer prosessen — leverandøren har en dokumentert, revidert Secure Development Lifecycle. `-4-2` sertifiserer produktet — en spesifikk komponent, ved en spesifikk firmwareversjon, oppfyller de tekniske Component Requirements på et angitt kapabilitets-sikkerhetsnivå. Du trenger begge; en leverandør med kun `-4-2` har et testet produkt, men ingen garanti for at neste utgivelse vil bli utviklet på samme måte. En leverandør med kun `-4-1` har en ren prosess, men ingen sertifisert produkt på hylla.

Hvor lenge bør jeg oppbevare bevis? Match det lengste av: IACS-levetiden (typisk 15–25 år for et fornybaranlegg), regulatorens oppbevaringsperiode (under NIS2-gjennomføring lander dette ofte på seks år etter hendelsen), og gruppens dokumentbevaringspolicy. Tidsstemplede revisjonslogger fra `SR 2.11`-relevante systemer bør

oppbevares minst tre år på varm lagring, lenger på kald lagring. Slett aldri en artefakt mens et åpent funn refererer til den.

Trenger jeg `ISASecure` eller `IECEE CB` for å oppfylle `-4-1`? Nei. `IEC 62443-4-1`-samsvar kan være selverklært, andrepartsvurdert (av en kunde), eller tredjepartssertifisert. Selverklært bevis er akseptabelt for mange revisorer hvis det er nivå-2-grad: SBOM-er, testrapporter, sporingsmatriser, opplæringsregistre. Tredjepartssertifisering via ISASecure SDLA eller en IECEE CB-ordnings `IEC 62443-4-1`-vurdering kortslutter ganske enkelt samtalen. For produkter solgt inn i kritisk infrastruktur-anbud i Europa er tredjepart i økende grad de facto-kravet.

Hvor passer NIS2-bevis inn i denne pakken? NIS2-bevis er et supersett som forbruker 62443-pakken, ikke erstatter den. NIS2-anvendelsesteksten dekker hvem som er i omfang; NIS2-kartleggingen viser hvilke 62443-artefakter som tilfredsstiller hvilke Artikkel 21-tiltak. Praktisk: en anleggseiers `-2-1`-pakke dekker mesteparten av NIS2 Artikkel 21(2)(a)–(j); integratorens `-2-4`-pakke dekker (d) leverandørkjedesikkerhet; produktleverandørens `-4-1`/`-4-2`-pakke underbygger resten. Legg til NIS2-spesifikke punkter — 24-timers tidlig-varslingsmal, registrering hos kompetent myndighet, og attest på cyberopplæring av ledelsen — og du har en NIS2-forsvarbar posisjon bygd på et 62443-fundament.

Hvis denne sjekklisten reddet deg ett funn, har teksten betalt for seg selv. For å diskutere punkt 6 i noen av tabellene er LinkedIn veien å finne meg.