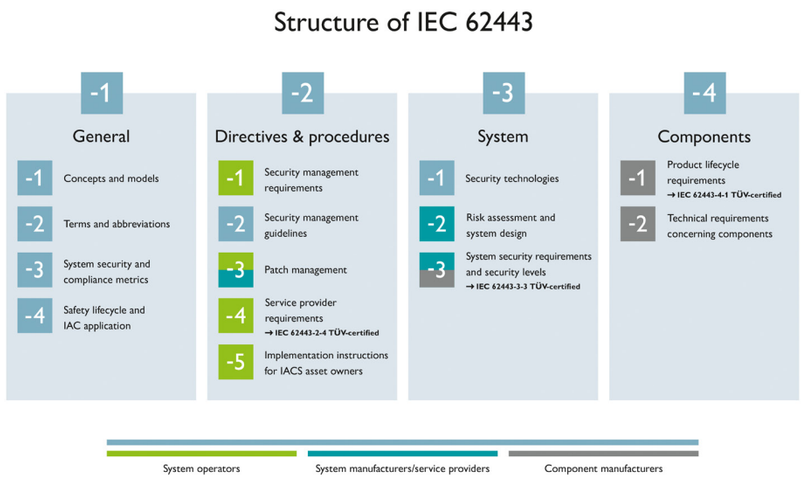
Security-by-design beskytter aktiver mod den konstant stigende cyber trussel.



IEC 62443 fastlægger kravene for systemoperatører, systemintegratorer og komponentproducenter.

Akut behov for handling for alle parter

Udvidelse af lovkrav ved implementering af cyber security

Digitalisering og sammenkobling af produktions-, produkt- og kundedata er afgørende faktorer for at øge virksomheders værditilvækst og dermed grundlaget for den økonomiske udvikling i globale regioner. EU-kommissionen har indset dette og publicerede EU Cyber security Strategy tilbage i december 2020. Den strategi definerer kravene hvad angår robusthed og angrebsblokering for komponent- og systemproducenter såvel som for alle større produktionsvirksomheder. Som førende standard er de internationale IEC 62443 standarder målrettet mod implementering af security-by-design i produkter og systemer.

På den ene side øger de nødvendige digitaliseringstiltag angrebsområdet for cyberangreb. På den anden side bliver angriberne og deres metoder stadig mere professionelle. Cyber security fokuserer derfor på at sikre virksomheders værdiskabelse og individuelle sikkerhedsmål. Det omfatter beskyttelse af know-how, f.eks. udviklingsresultater eller kontraktbetingelser samt overholdelse af lovkrav, der relaterer sig til databeskyttelse.

I produktionsvirksomheder er evnen til at producere og levere af kæmpe betydning. Udover de specifikke skader fra et angreb er der andre skader, som ofte undervurderes. F.eks. fører cyberangreb ofte til imagetab, fordi de kan påvirke, hvor tillidsfulde kunder, partnere, investorer og offentligheden er i den påvirkede virksomhed. Lovkrav til realisering af cyber security har længe eksisteret for kritisk infrastruktur. Med introduktionen af NIS 2 udvider EU disse lovkrav til at omfatte mange flere virksomheder.

Implementering i automationssektoren

State of the art inden for cyber security viser sig at være introduktionen af et sikkerhedssystem til information (Information Security Management System ISMS) i henhold til ISO 27001/2 i IT, som udvides i retning af OT (Operational Technology). ISMS omfatter organisationskrav og tekniske krav. Ved hjælp af IEC 62443-2-1 kan de tekniske krav henvises til tiltag i OT-miljøet, det industrielle automationskontrolsystem (IACS). Disse tiltag omfatter følgende:

- Konfigurering og segmentering af netværk
- Beskyttelse af data ved lagring og overførsel
- Godkendelse af brugere
- Overvågning og registrering af bruger- og systemhandlinger
- Sikkerhed for de anvendte komponenter
- Konfiguration, updatering, back-up og gendannelse
- Organisationskrav til håndtering af system

De specifikke tiltag for IACS-miljøet adresseres i IEC 62443 standarderne for de forskellige layers:

- Komponneter: IEC 62443-4-1 “Secure product development lifecycle requirements” og IEC 62443-4-2 “Technical security requirements for IACS components”
- System: IEC 62443-3-3 “System security requirements and security levels”
- Operatører: IEC 62443-2-1 “Establishing an industrial automation and control system security program”, IEC 62443-2-3 “Patch management in the IACS environment” og IEC 62443-2-4 “Security program requirements for IACS service providers”

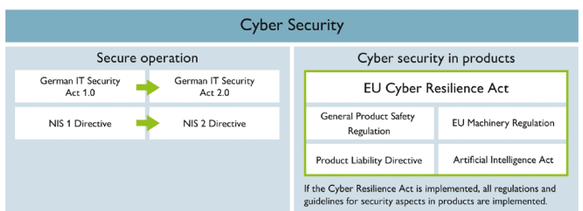
Et særligt element i IEC 62443 er den omfattende security-by-design tilgang, som spænder fra krav til betjeningsprocesser til rammebetingelser for systemer og produkter og beskriver både procesmæssige og tekniske tiltag og krav. Konceptet ”defense-in-depth” fungerer som standardens afgørende sikkerhedskoncept: ved at forskyde flere sikkerhedstiltag efter hinanden, gøres adgangen mere besværlig for angribere. F.eks. vil en angriber først skulle passre en eller flere firewalls for at komme til målet og lancere et angreb på netværket. Her skal angriberen forbi et brugerlogin og stoppes derefter af interne sikkerhedsmekanismer.

Opvurdering af reguleringer gennem NIS 2

De nævnte cyber security tiltag har tidligere kun været et lovkrav for kritisk infrastruktur. Derudover er de implementeret hos store, primært internationalt aktive, systemoperatører. Med introduktionen af EU’s NIS 2 direktiv ændrer dette sig nu væsentligt. NIS 2 (Network and Information Security) direktivet kræver, at operatører af offentlige eller private selskaber skal implementere passende sikkerhed for at beskytte deres systemer mod cyberangreb. Sammenlignet med den eksisterende NIS, udvider NIS 2 reguleringen til virksomheder med mere end 50 ansatte og mere end 100 mio. euro i omsætning. NIS 2 gælder for ”væsentlige” og ”vigtige” faciliteter i EU.

Med “væsentlige faciliteter” menes virksomheder inden for kritisk infrastruktur som elektricitet/gasproduktion, lagring og overførsel, transport på vand, vej og skinner, drikke- og spildevandsfaciliteter samt digital infrastruktur. ”Vigtige faciliteter” vælges fra en liste på 7 sektorer baseret på deres kritiske niveau for deres forretningsområde og type af service. Eksempler omfatter produktion og distribution af fødevarer og kemi og produktion af elektrisk udstyr, maskiner og køretøjer.

NIS 2 direktivet træder i kraft den 16. januar 2023 og skal overføres til national lovgivning af EU-lande. Det er imidlertid svært at overholde disse krav, hvis de anvendte produkter ikke er udviklet i overensstemmelse med security-by-design. For at imødekomme denne udfordring har EU defineret Cyber Resilience Act (CRA).



Cyber lovgivningen for sikker drift og for sikre produkter går hånd i hånd.

Udvikling af security-by-design produkter iht. med Cyber Resilience Act

CRA kræver, at producenter udvikler security-by-design produkter. Produkter, der er underlagt CRA, vil i fremtiden ikke få et CE-mærke, hvis de ikke overholder CRA krav. Der er defineret minimumskrav til implementering af sikkerhedstiltag. Afhængig af produktklassen skal disse sikkerhedstiltag påvises som led i en overensstemmelsesprøvning af bemyndigede organer, f.eks. TÜV eller af producenterne selv ved hjælp af en harmoniseret standard.

De væsentlige krav i CRA skal indfries i design, udvikling og produktion af et produkt, dvs. baseret på en sikker udviklingsproces. Kravene omfatter adgangsbeskyttelse, beskyttelse af fortrolighed,

(fortsættes næste side)

integritet og tilgængelighed og en sikker leveringstilstand. En yderligere komponent af CRA er sårbarhedsstyring og regler, der styrer den periode, hvor fabrikanter skal levere sikkerhedsopdateringer til deres produkter. Udkastet til CRS blev offentliggjort i september 2022 og er nu i en aftemningsproces. Som EU-lov behøver den ikke blive gennemført i national lovgivning og forventes derfor at blive gældende i hele EU i 2024. IEC 62443 standarderne dækker både den sikre udviklingsproces og de tekniske krav til individuelle produkter og systemer. Det følger heraf, at IEC 62443 eller en afledt sektorstandard er en lovende kandidat til en CRA-harmoniseret standard. For at overholdene kravene til sårbarhedsstyring skal alle produkter have en standard Software Bill of Material (SBOM), dvs. en liste, der beskriver alle softwarekomponenter i et produkt. Yderligere skal kendte sårbarheder gøres tilgængelige i et standardiseret, digitaliseret format som f.eks. Common Secrity Advisory Framework (CSAF). Det er den eneste måde at overholde korte deadlines for rapportering og eliminering af sårbarheder i henhold til CRA og NIS 2.

Sikkerhedsbetragtninger i det nye Maskindirektiv

For at beskytte mennesker og miljø mod negative konsekvenser – som kvæstelser og forurening – skal maskiner udstyret med funktionel sikker teknologi overholde Maskindirektivet 2006/42/EC. Denne standard kræver en opdatering på grund af de risici, der er forbundet med nye teknologier samt nye produktsikkerhedskrav. Derudover er det blevet tydeligt, at disse direktiver – og dermed implementering til national lov – til dels kræver forskellige regler.

I fremtiden skal der også tages højde for funktionel sikkerhed i kombination med cyber security. Disse krav har givet anledning til Maskindirektivet 2023/1230, hvor den færdige tekst blev publiceret i midten af 2023. Maskindirektivet understøtter Cyber Resilience Act, som også betragter maskiner som produkter. For maskiner med funktionel sikkerhed har Maskindirektivet dog forrang.

360o sikkerhed baseret på IEC 62443

Phoenix Contact begyndte at implementere IEC 62443 tilbage i 2017. Virksomhedens 360o sikkerhedskoncept er baseret på det ledende princip, at "sikkerhed er forankret i hele produktets og løsningens levetid".

- **Sikker udviklingsproces**
  En sikker IEC 62443-4-1 udviklingsproces er en forudsætning for designet og den samlede levetid for produkterne. Den definerer udviklingen i overensstemmelse med de etablerede cyber security metoder security-by-design og defense-in-depth men sikrer også overvågning af sårbarheder og regelmæssige sikkerhedsopdateringer.

- **Sikre produkter**
  Sikre produkter overholder IEC 62443-4-1 udviklingsprocessen og overholder kravene til funktionel sikkerhed i IEC 62443-4-2, inklusiv f.eks. denial-of-service beskyttelse, brugerstyring, fortrolighed for data i transit og lagring, logging, least-functional konfiguration. I 2021 blev PLCnext Control den første controller på markedet, der blev certificeret af TÜV Süd efter IEC 62443-4-1 ML3 og IEC 62443-4-2 SL2 Feature set. Flere sikre produkter er under udvikling eller ved at blive certificeret.

- **Sikre services**
  For at kunne diskutere, rådgive om, installere og vedligeholde sikkerhedsløsninger sammen med systemintegratorer og operatører skal medarbjdere have de nødvendige færdigheder inden for cyber security. Til det formål er det tyske datterselskab samt andre datterselkaber i Phoenix Contact gruppen IEC 62443-2-4 certificeret.

- **Sikre løsninger**
  Phoenix Contact Security Team har udviklet templates (blueprints) til forskellige løsninger og markeder og har fået dem IEC 62443-3-3 certificeret, hvor det er vurderet hensigtsmæssigt. Blueprints letter diskussioner og konceptarbejde. De understreger samtidig Phoenix Contacts ekspertise i at certificere løsninger med kunder.

Som del af et 360o sikkerhedskoncept tilbyder Phoenix Contact udover produkter og systemer også operatører og systemintegratorer IEC 62443 services i design og betjening af systemer.

- **PSIRT**
  Product Security Incidence Respons Team (PSIRT) har til opgave at reagere på potentielle sårbarheder i sikkerheden, hændelser og andre sikkerhedsrelaterede forhold i relation til Phoenix Contacts produkter, løsninger og services. PSIRT styrer afsløring, undersøgelse og intern koordination og offentliggørelse af sikkerhedsvejledninger på bekræftede sårbarheder.

Alle de nævnte certificeringer overvåges af TÜV Süd gennem årlige audits.

Overblik

NIS 2 direktivet, Cyber Resilience Act og Maskindirektivet er i øjeblikket i EU lovgivningsproces eller ved at blive omsat til national lov. Hvis de typiske overgangsperioder følges, vil alle love og standarder være fuldt gældende lov i 2026. Med tanke på deres kompleksitet er det hurtigt blevet klart, at der er et presserende behov for handling fra producenter, systemintegratorer og operatører.

Takket være sine mange års erfaring med 360° sikkerhedskoncept står Phoenix Contact godt her: udover sine produkter og systemer tilbyder virksomheden også operatører og systemintegratorer IEC 62443 services til design og betjening af systemer. "360° Industrial Security" implementeringskonceptet starter med en "Ni trin til et sikkert system" tilgang for at hjælpe systemintegratorer og operatører med at overholde kravene til security-by-design for deres specifikke løsning.

Beskyt dig mod ubudne gæster - find mere information på vores hjemmeside:

- **Industrial security**
- **IEC 62443**