Wat kunt u verwachten van de nieuwe machine(producten)verordening (2021/0105)

Meer aandacht voor cyber security en validatie van veiligheidsfuncties

PILZ
THE SPIRIT OF SAFETY

Even voorstellen

Edwin Buisman CMSE®, CECE, CEFS

Safety consultant

- Begeleiding CE-markering
- Veiligheidsconcepten en besturingen,
- Faalkansrekenen,
- Pragmatische aanpak van veiligheid en werkbaarheid,
- Veiligheid van robots

Actief in onder andere:

- Infrastructuur,
- Industrie,
- Farmacie en voedingsmiddelenindustrie

Trainer

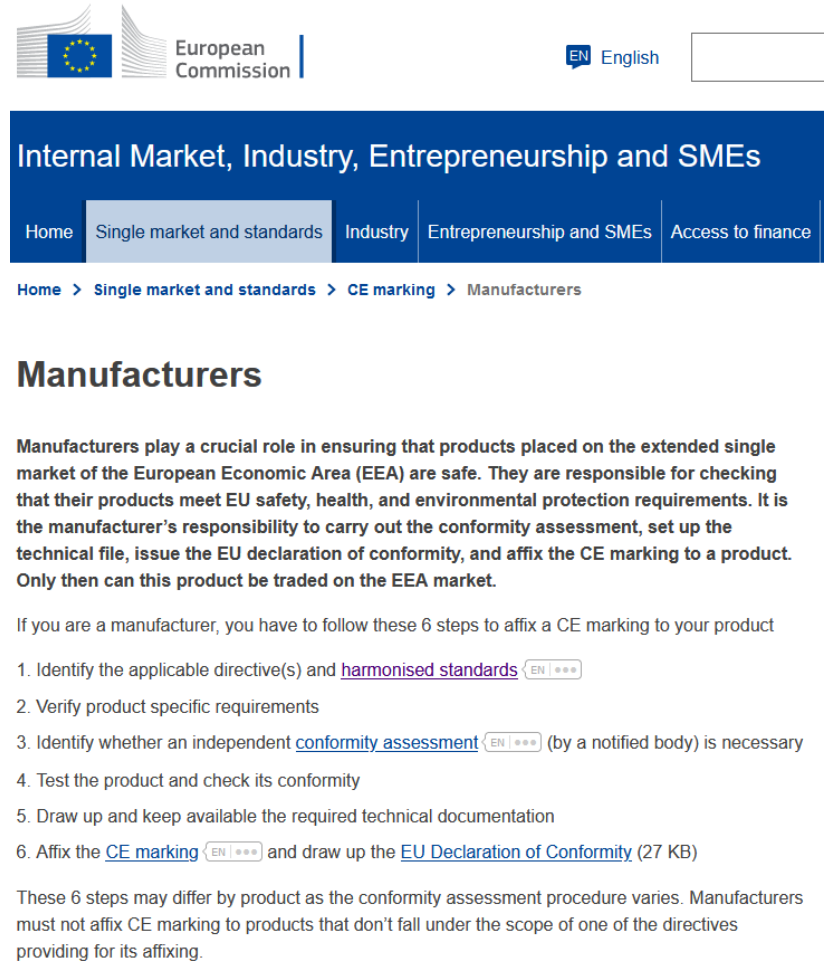
- Internationaal trainer CMSE®, CECE, CEFS
- Ontwikkeling/doceren van diverse machineveiligheid gerelateerde trainingen

Inleiding wetgeving

De CE markering

Gevolg van één of meer productrichtlijnen of productverordeningen Voor specifieke typen producten

https://single-market-economy.ec.europa.eu/single-market/ce-marking/manufacturers_en



European Commission

English

Internal Market, Industry, Entrepreneurship and SMEs

Home | Single market and standards | Industry | Entrepreneurship and SMEs | Access to finance

Home > Single market and standards > CE marking > Manufacturers

Manufacturers

Manufacturers play a crucial role in ensuring that products placed on the extended single market of the European Economic Area (EEA) are safe. They are responsible for checking that their products meet EU safety, health, and environmental protection requirements. It is the manufacturer's responsibility to carry out the conformity assessment, set up the technical file, issue the EU declaration of conformity, and affix the CE marking to a product. Only then can this product be traded on the EEA market.

If you are a manufacturer, you have to follow these 6 steps to affix a CE marking to your product

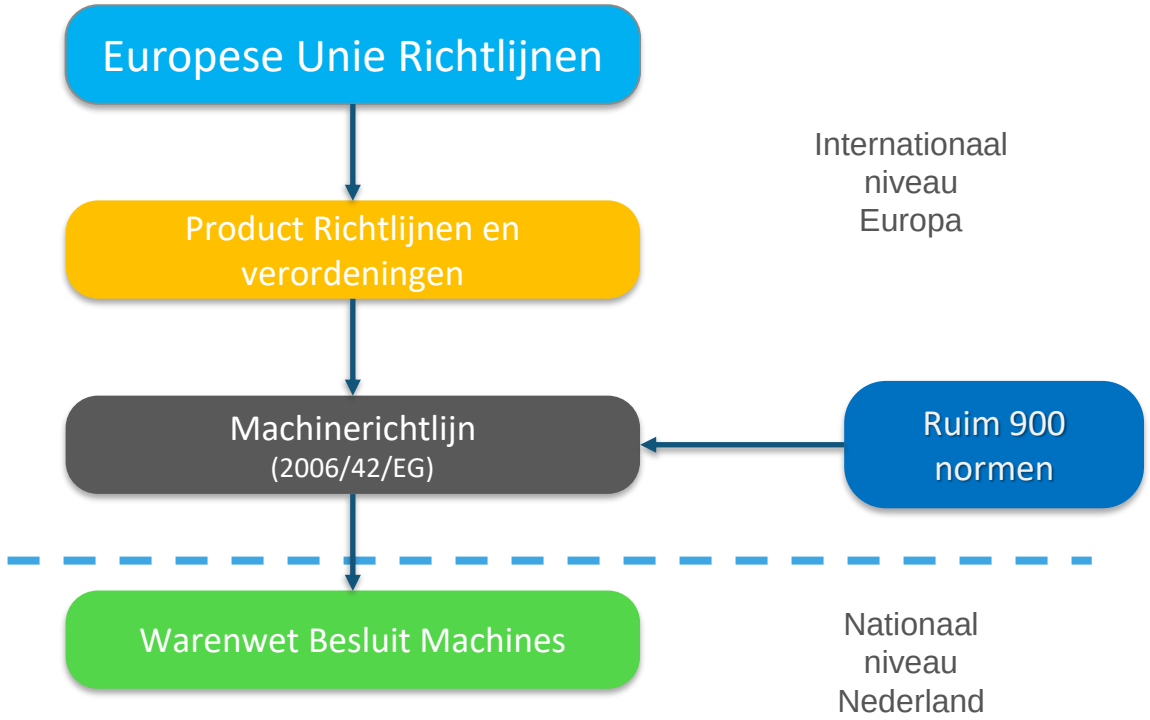
1. Identify the applicable directive(s) and harmonised standards
2. Verify product specific requirements
3. Identify whether an independent conformity assessment (by a notified body) is necessary
4. Test the product and check its conformity
5. Draw up and keep available the required technical documentation
6. Affix the CE marking and draw up the EU Declaration of Conformity (27 KB)

These 6 steps may differ by product as the conformity assessment procedure varies. Manufacturers must not affix CE marking to products that don't fall under the scope of one of the directives providing for its affixing.

Let op: deze presentatie maakt gebruikt van openbare informatie, maar de tekst van de Machine(producten)verordening is op het moment van maken van de presentatie nog niet definitief.

Huidige situatie

Machinerichtlijn (2004/42/EG)

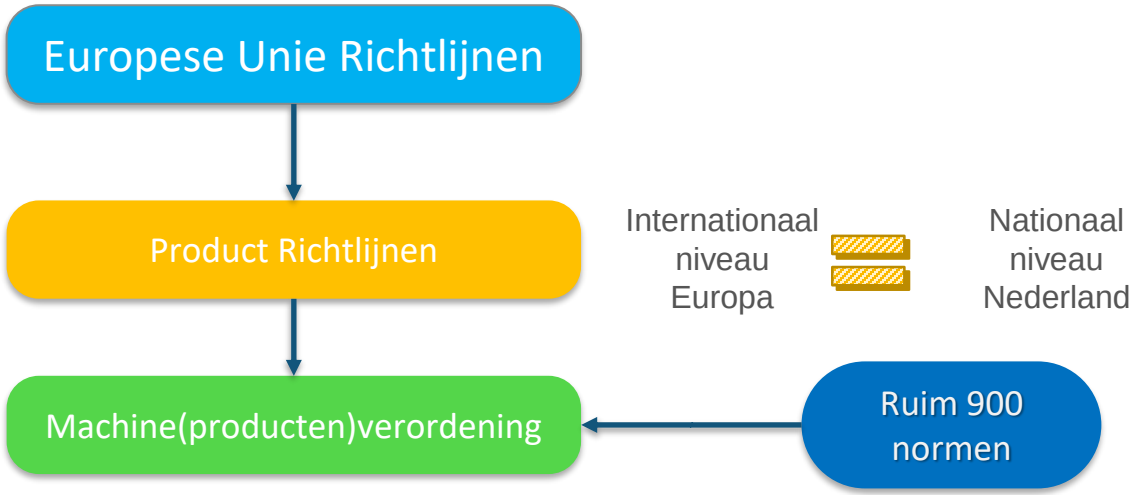


Verplichting fabrikant:

- Risicobeoordeling
- Toetsing van Essentiële Veiligheids en Gezondheids eisen
- Samenstellen Technisch Dossier
- Opstellen gebruikershandleiding
- Conformiteit/inbouwverklaring
- De CE markering plaatsen

Vanaf 2023:

Machine(producten)verordening (2021/0105)



Er verandert niets aan de verplichtingen van de fabrikant!

Machine(producten)verordening (2021/0105)

Wat gaat er veranderen?

De volgende zaken veranderen:

- Verduidelijking van diverse rollen van marktpartijen zoals importeur en distributeur en fabrikant
- Conformiteitsbeoordelingsprocedures aangepast aan alle huidige productrichtlijn (CAP’s)
- Verduidelijking van de substantiële wijziging
- Aandacht voor kunstmatige intelligentie in machines
- Verplichte maatregelen tegen manipulatie van veiligheidsfuncties
- Eisen met betrekking Cyber security

Lay-out van de bijlagen

- Lay-out van de bijlagen
  - Essentiële Veiligheids- en gezondheidseisen Bijlage I wordt Bijlage III
  - Verklaring van overeenstemming: Bijlage II wordt Bijlage V
  - CE-Markering: Bijlage III wordt Artikel 19
  - Hoog risico machines: Bijlage IV wordt Bijlage I
  - Opbouw van het technisch Dossier van bijlage VII (A en B) wordt IV (A en B)

  Met name gedaan om het ontwikkelproces meer te volgen.

Verschillende marktdeelnemers uitgewerkt

De volgende rollen van marktdeelnemers zijn uitgewerkt:

- “**Importeur**”:

In de Unie gevestigde natuurlijke of rechtspersoon die machineproducten uit een derde land in de Unie in de handel brengt;

- “**Distributeur**”:

Andere natuurlijke persoon of rechtspersoon in de toeleveringsketen dan de fabrikant of de importeur, die een machineproduct op de markt aanbiedt;

- “**Fabrikant**”:

Elke natuurlijke persoon of rechtspersoon die machineproducten produceert of machineproducten laat ontwerpen of produceren, en die die machineproducten onder zijn eigen naam of merk in de handel brengt of die machineproducten voor eigen gebruik ontwerpt en bouwt;

Conformiteit Beoordelings Procedure (CAP’s)

CAP Modules

Systeem van CAP modules

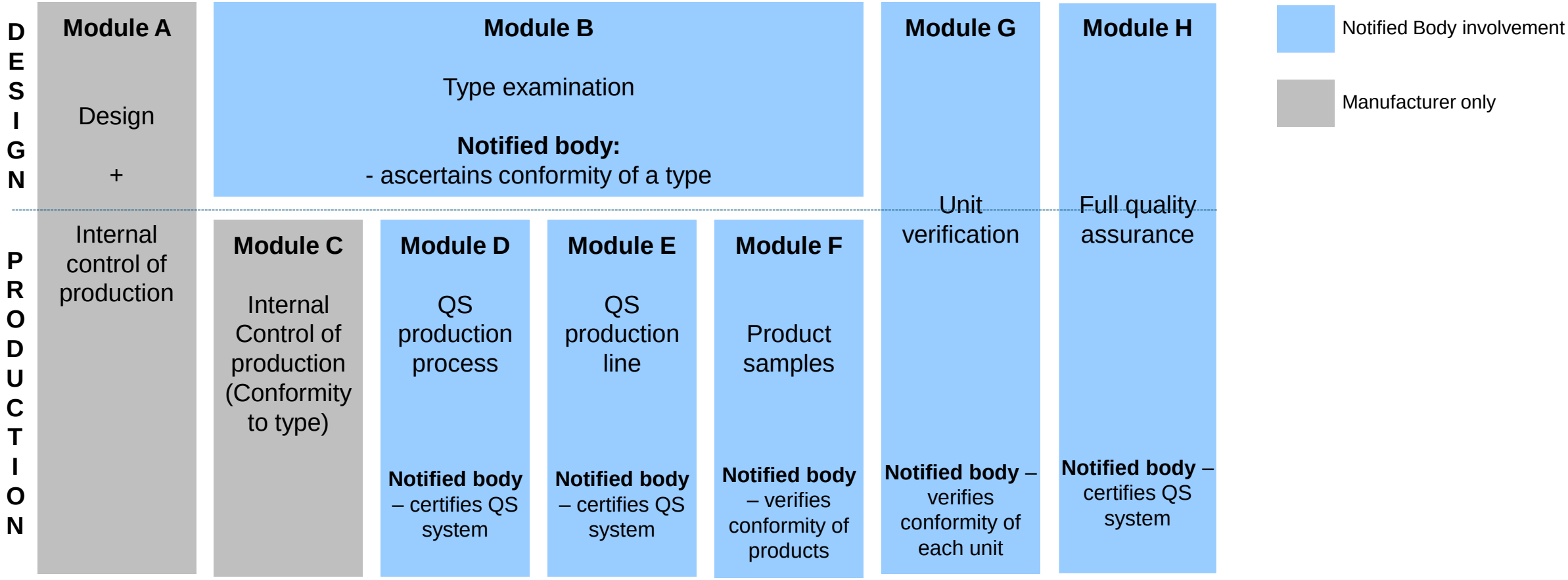
- 8 modules bepalen de verantwoordelijkheid van de fabrikant en de mate van betrokkenheid van conformiteitsbeoordelingsinstanties (d.w.z. aangemelde instanties).
- In sommige gevallen (bv. massaproductie) kan het CAP worden opgesplitst in 2 stappen:
  - Ontwerpbeoordeling
  - Productiebeoordeling
- In deze scenario's zal het CAP uit twee modules bestaan
- De conformiteitsinstantie die voor elke module wordt gebruikt, kan variëren
- In gevallen waarin er geen EU-type onderzoek is, wordt het CAP uitgevoerd met één enkele module die zowel de ontwerp- als de productiefase omvat.

Toepasselijke CE-richtlijnen bepalen de mogelijke modules voor het product

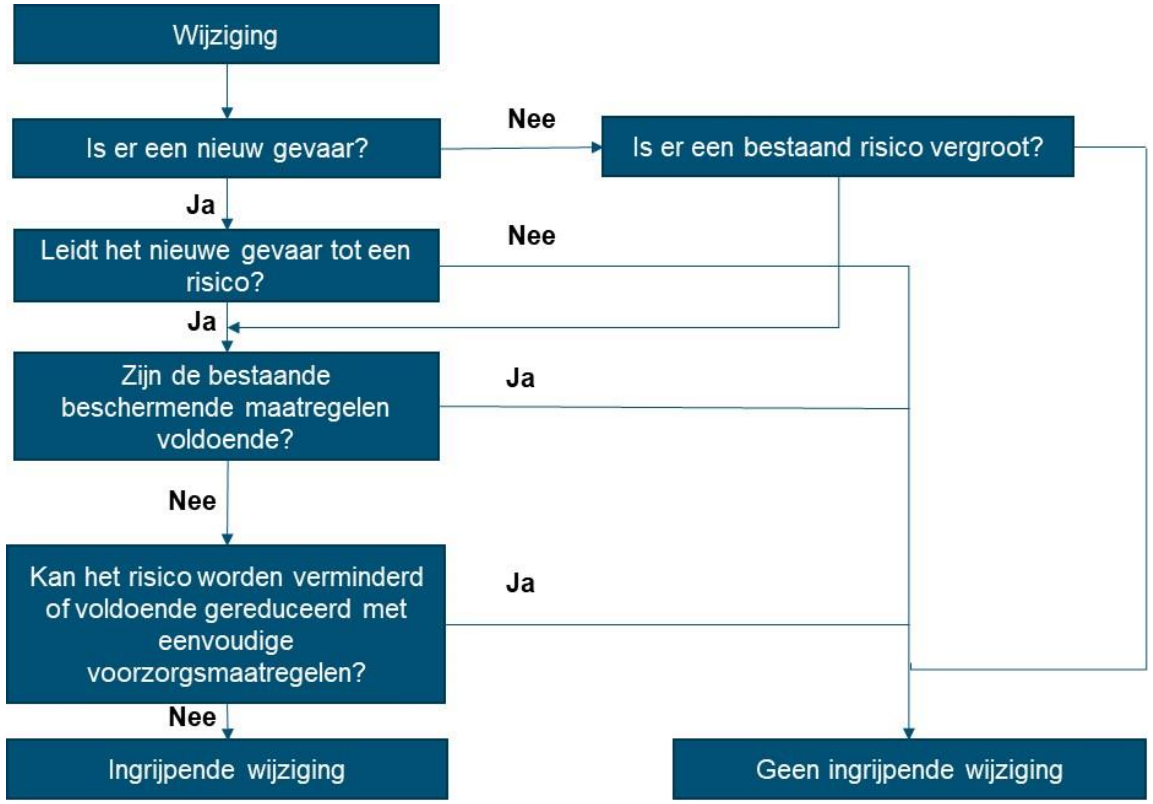
Conformiteit Beoordelings Procedure

CAP Modules

Conformity assessment procedures of the new approach: the modules



De ingrijpende wijziging



"ingrijpende wijziging":

- *niet door de fabrikant voorziene fysieke of digitale wijziging van een machineproduct nadat dat machineproduct in de handel is gebracht of in gebruik is gesteld als gevolg waarvan de overeenstemming van het machineproduct met de relevante essentiële gezondheids- en veiligheidseisen in het gedrang kan komen;*

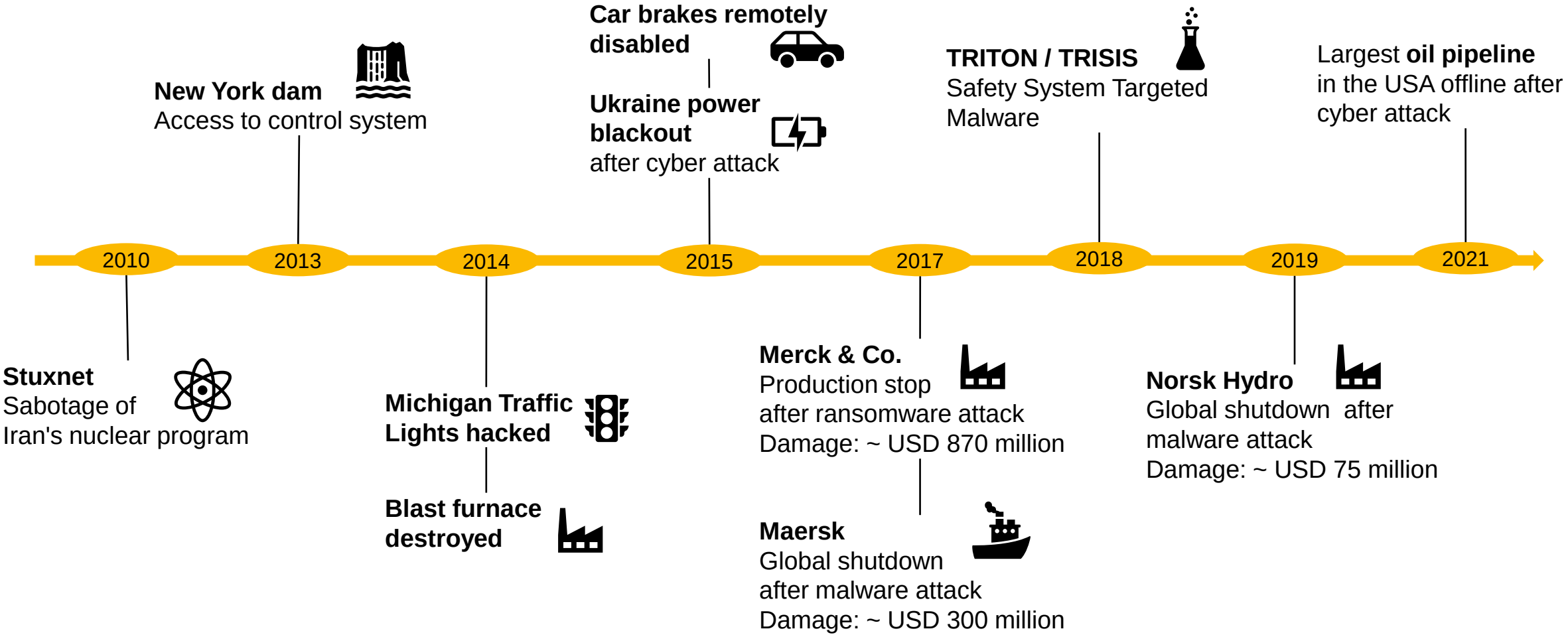
- Hiervoor zijn diverse stroomschema's beschikbaar

- Probleem hierbij is vaak beschikbaarheid van technische informatie uit het Technisch Dossier.

*Tip: Zoek met een zoekmachine op: "**werkinstructie beoordelen gewijzigde machines arbeidsinspectie**"*

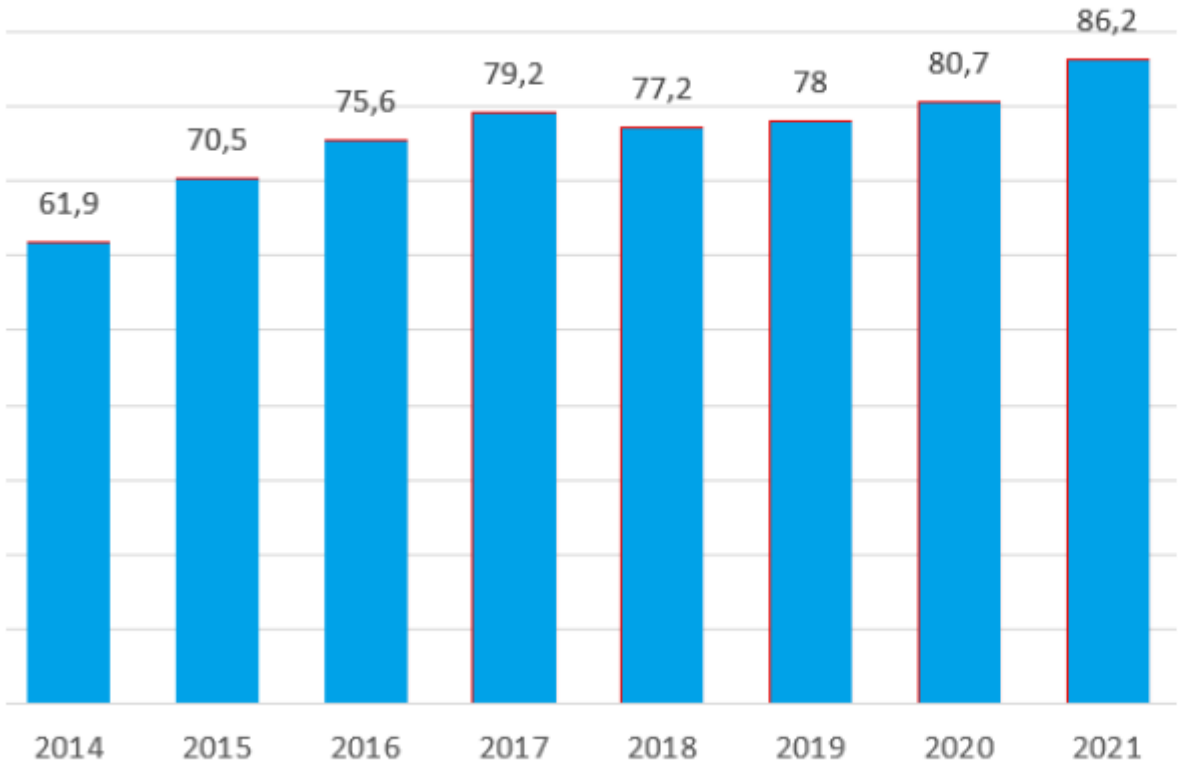
Cyber Security?

Reminder



Gevolgen van een Cyber attack

Companies that were affected by at least one successful cyber attack



1,200 qualified IT securiy decision makers and practioners questioned.
From organizations with more than 500 employees and 19 industries

Source: Cyberedge Group 2021 Cyberthreat Defense Report

Wat voor soort cyber aanvallen bestaan er?

- **Ransomware**:
  Encryptie van bedrijfs data om het bedrijf af te persen voor geld (via bijv. Bitcoin)
- **Spyware**:
  Software-gebaseerde spionage van gebruikers activiteiten of andere data
- **Andere type malware:**
  Virussen, wormen, trojans etc.
- **Manuele Hacking**
  Manipulatie van hard- of software zonder gebruik van malware
- **Distributed Denial of Service (DDoS)**
  Het versturen van vele paketten/verzoeken naar web- en/of mailservers met het doel om deze te overbelasten

Veiligheid versus beveiliging

Veiligheid

Doel: Het beschermen van mensen

Zal niet snel aangepast worden na implementatie

Beveiliging:

Doel: Het beschermen van data en machines

Moet continu gemonitored en aangepast worden

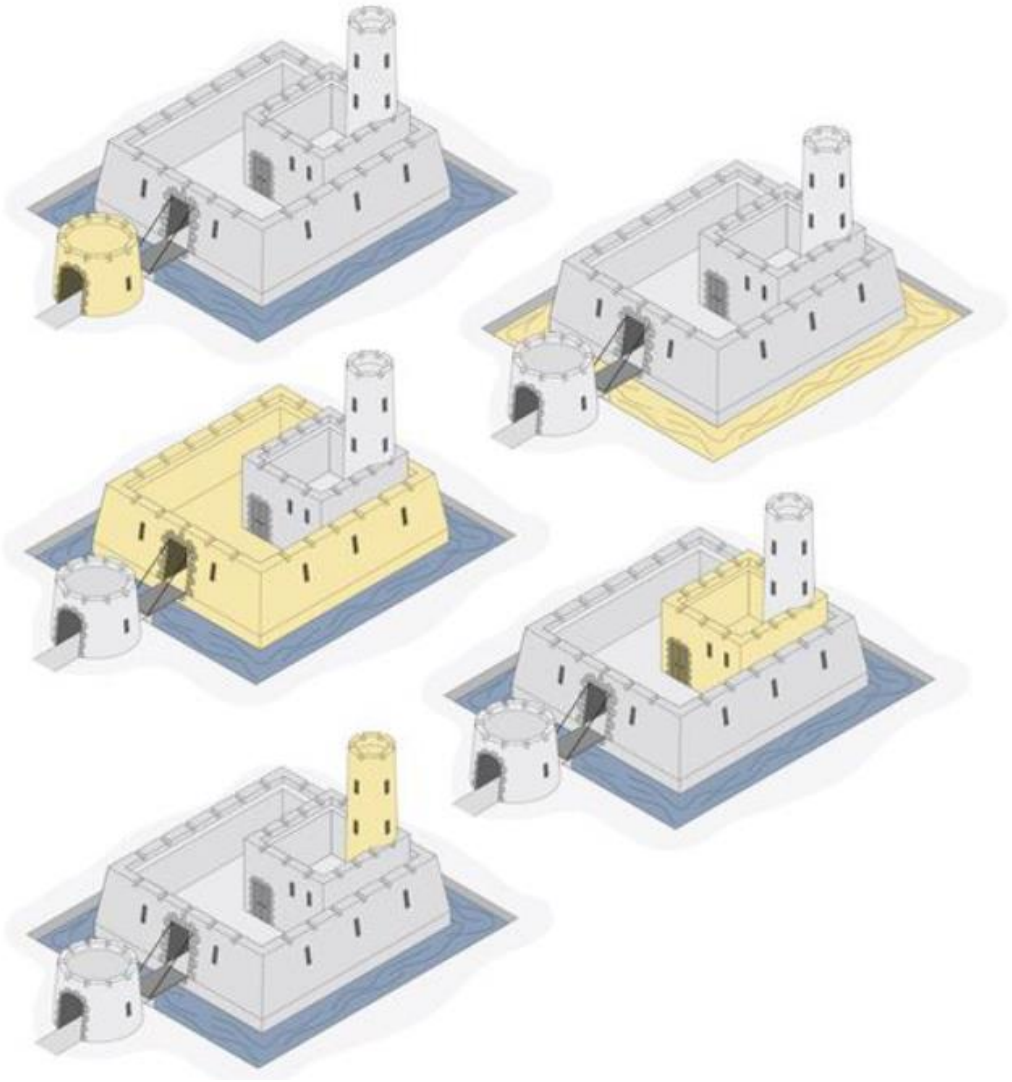
Verandert in de loop van de tijd

Cyber aanvallen

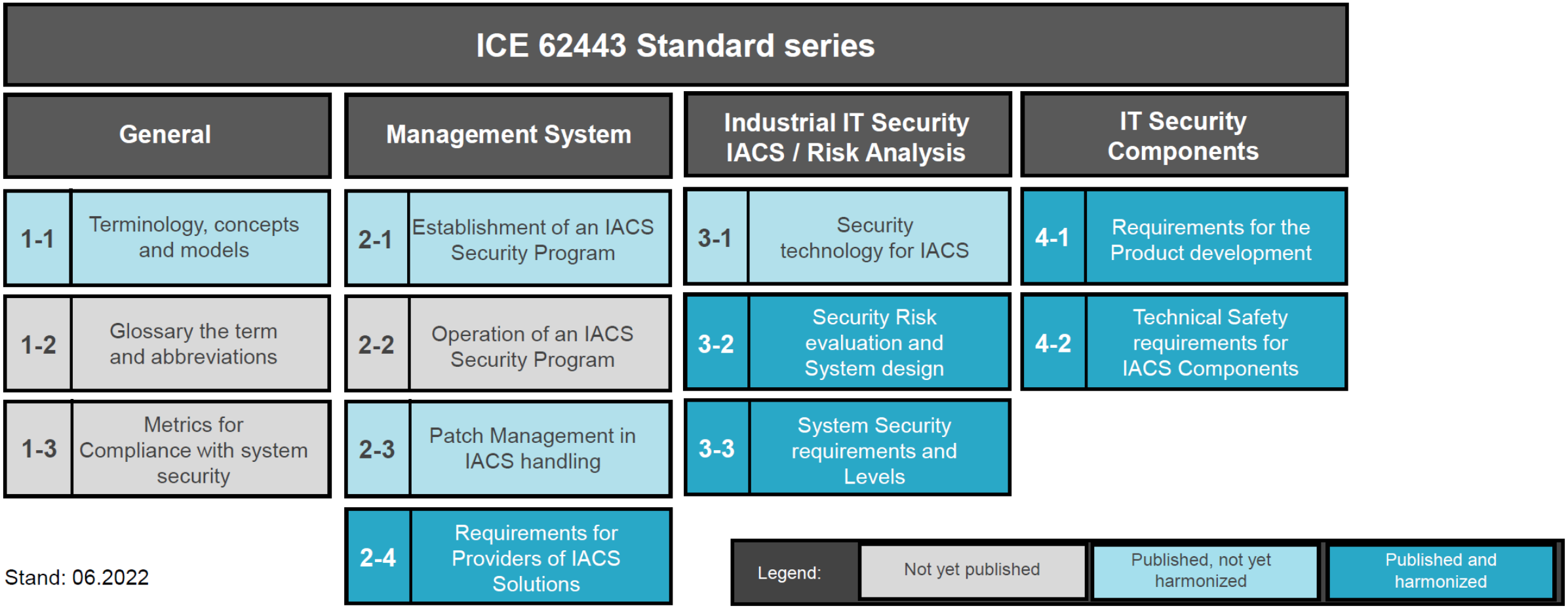
Aantal mogelijke scenarios

- Het injecteren van Malware via bijv. USB sticks of externe hardware
- Het infecteren van Malware via het inter- of intranet
- Sabotage door personen (bijv. express verkeerde configuratie laden of niet updaten)
- Sociale Engineering en Phishing
- DDoS aanvallen
- Inbreken via remote login
- Het gebruik van malifide hard- of software
- Het aanpassen van bedrijfs laptops- of telefoons

“Defense in-depth” concept

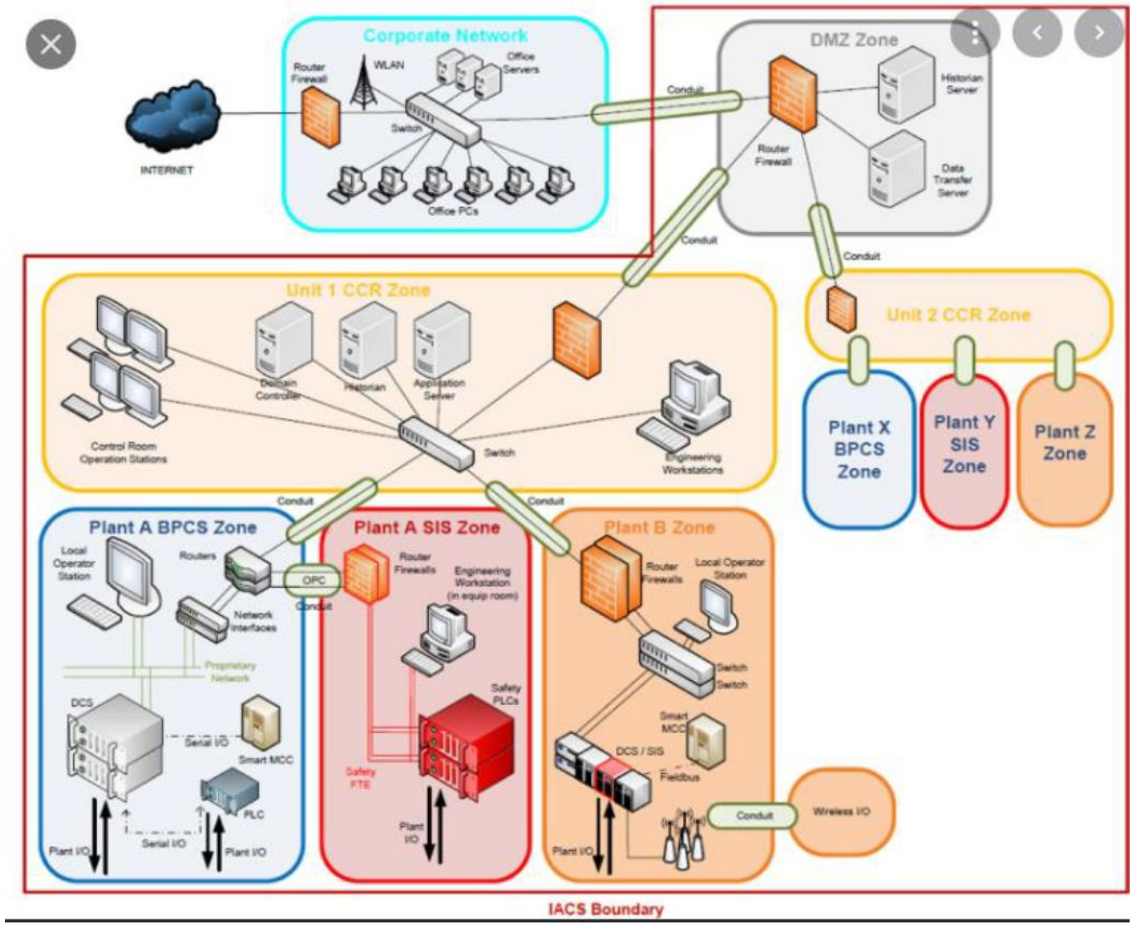


IEC 62443


ICE 62443 Standard series
General
1-1 Terminology, concepts and models
1-2 Glossary the term and abbreviations
1-3 Metrics for Compliance with system security
Management System
2-1 Establishment of an IACS Security Program
2-2 Operation of an IACS Security Program
2-3 Patch Management in IACS handling
2-4 Requirements for Providers of IACS Solutions
Industrial IT Security IACS / Risk Analysis
3-1 Security technology for IACS
3-2 Security Risk evaluation and System design
3-3 System Security requirements and Levels
IT Security Components
4-1 Requirements for the Product development
4-2 Technical Safety requirements for IACS Components
Stand: 06.2022
Legend:
Not yet published
Published, not yet harmonized
Published and harmonized

Cyber security

Zoneren en resilliance



Quick wins op het gebied van cyber security

- Zo min mogelijk verbinden met het internet indien mogelijk
- IT/OT structuur gescheiden houden waar mogelijk
- Indien scheiding niet mogelijk, bijv. de Pilz Security Brigde toepassen
- Goed authorisatie system implementeren op alle systemen
- Medewerkers inlichten en alert houden op malware/phishing/etc.
- Zorg dat programma’s en data voldoende gebackupt worden.

Kunstmatige intelligentie

Benoemd in de Machine(producten)verordening

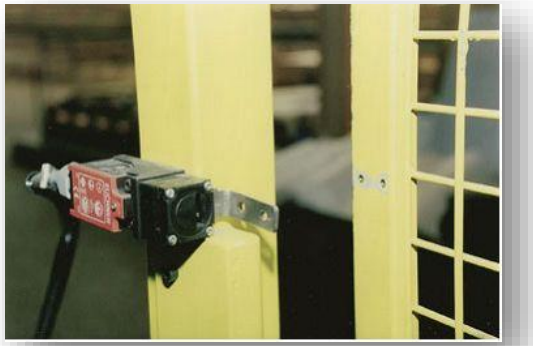
- Kunstmatige of artificiële intelligentie (AI) in machines gelijktrekken met de aanstaande AI-verordening
- Veiligheidsrisico’s van AI-systemen met een hoog risico adresseren

Beveiliging tegen corruptie

Zowel software als hardware

Essentiële eis 1.1.9 uit bijlage III van de Machine(producten)verordening

- Aansluiten van een apparaat aan een machine mag niet tot een gevaarlijke situatie leiden
- Veiligheidssensoren moeten zo ontworpen en geplaatst zodat zij niet te eenvoudig manipuleren zijn
- De machine moet bewijzen verzamelen van al dan niet rechtmatige ingrepen in de hardwarecomponent.
- Software en gegevens die van cruciaal belang zijn voor de veiligheid van de machine, moeten als zodanig herkenbaar zijn en afdoende beveiligd worden tegen al dan niet opzettelijke corruptie.
- Het machineproduct moet de in zich geïnstalleerde software die nodig is om veilig te functioneren identificeren en deze informatie te allen tijde in een gemakkelijk toegankelijke vorm kunnen verstrekken.



Bedankt voor uw aandacht

Edwin Buisman

Pilz Nederland C.V. Havenweg 22, 4131 NM Vianen

0347-320477, Info@pilz.nl, https://www.pilz.com/nl-NL

www.pilz.com


PILZ
THE SPIRIT OF SAFETY
Wir
automatisieren.
Sicher.
PILZ