Machineverordening

Regelgeving (cybersecurity) nader beschouwd

Paul Hoogerkamp c.s.

koninklijke metaalunie

Inleiding

- Veranderingen door de Machineverordening,
- Een drietal artikelen nader beschouwd,
- AMT trackbot casus,
- STRIDE nader beschouwd,
- Cyberrisicobeoordeling (prEN 50742 ← → EN-ISO 12100),
- Wvttk.

Even vooraf: Fabrikant / Eigen gebruik

Artikel 3.18 (Machineverordening)

Fabrikant: elke natuurlijke of rechtspersoon die:

a) producten die binnen het toepassingsgebied van deze verordening vallen, vervaardigt of deze producten laat ontwerpen of vervaardigen, en die die producten onder zijn of haar eigen naam of merk in de handel brengt; of

b) producten die binnen het toepassingsgebied van deze verordening vallen, voor eigen gebruik vervaardigt en in bedrijf stelt;

Artikel 3.18 ‘in brokjes’

a. producten die binnen het toepassingsgebied van deze verordening vallen,
   - vervaardigt of
   - laat ontwerpen of
   - laat vervaardigen,

   EN

   - die die producten onder zijn of haar eigen naam of
   - merk in de handel brengt;

(of)

b. producten die binnen het toepassingsgebied van deze verordening vallen, voor eigen gebruik
   - vervaardigt

   EN

   - in bedrijf stelt,

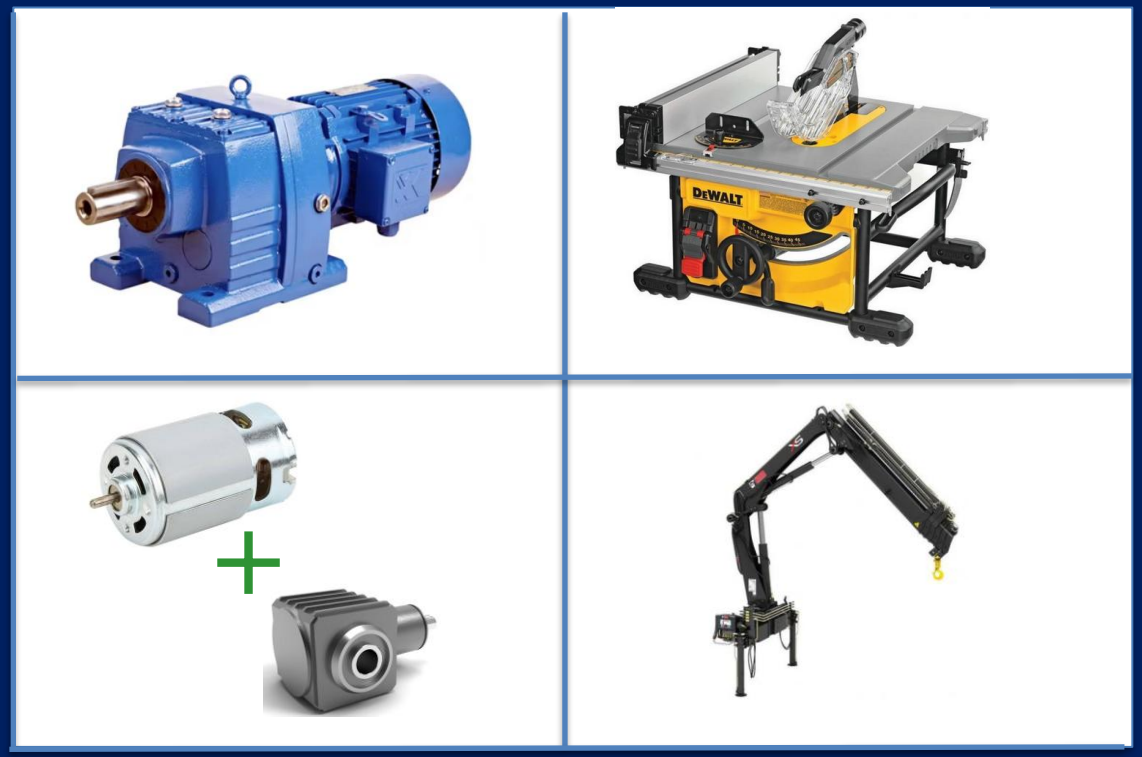
koninklijke metaalunie

Spreektaal & juridisch begrip

Voltooide machines. (af fabriek)

Spraakgebruik
Vaktaal/jargon

Niet voltooide machines. (deellevering)



Niet-voltooide machines. Voltooide machines.

Juridisch begrip

Software!?

wat is er zo nieuw?

Risk assessment: zelf-ontwikkeling, cybersecurity, o.a.:

- 1.1.2e: Testen van veiligheidsfuncties,
- 1.1.6 f+g: Zelf-ontwikkeling,
- 1.1.9: Cybersecurity,
- 1.2.1 a+f: Besturing / zelf-ontwikkeling / leren, cybersecurity,
- 1.3.7 lid 4: In omgeving (samen)werken met machine (bijv. Cobots),
- 1.6.2 lid 2: Bevrijden van personen,
- 1.7.4..: Digitale gebruiksaanwijzing + emmissiegegevens vermelding (artikel 10 ev.).
- e.v. diverse artikelen in hoofdstuk 2 t/m 6 (niet nader beschouwd)

Machines


RAILROAD
UNIEKE MACHINES VOOR OP EN RONDOM HET SPOOR
AMT Rail Road ontwikkelt, produceert en levert unieke oplossingen voor op en rondom het spoor. De machines worden samen met u ontwikkeld en vervolgens gebouwd naar uw wensen, eisen en gestelde wet- en regelgeving.
Apeldoorn
Apeldoorn Verbindt
& AMT
Duurzaam Verbonden
AMT
RAILROAD
ZAGRO

Casus (Schroeftrackbot)

AMT

koninklijke metaalunie

Machineverordening?

Deze verordening is niet van toepassing op (artikel 2.2.e):

- middelen voor vervoer door de lucht, over het water en via het spoor, met uitzondering van machines die op die vervoermiddelen zijn gemonteerd.

Nu focus op het machinedeel van de trackbot en de extra eisen ten opzichte van de huidige Machinerichtlijn.

‘samenstel’ van (deel)machines

Hardware en software elementen

- Robot programmeren (software)
- Sensoren koppelen, programmeren.
- Starten / stoppen van o.a.:
  - Schroefmachine
  - Trackbot (op spoor)
  - ..

  Hoe om te gaan met de regelgeving voor de cybersecurity?

Cybersecurity Bijlage III. 1.1.9

- De machine of het verwante product moet zodanig ontworpen en gebouwd zijn dat de verbinding ervan met een ander apparaat, via een functie van het aangesloten apparaat zelf of via een apparaat op afstand dat communiceert met de machine of het verwante product, niet tot een gevaarlijke situatie leidt.

verwante producten:
- verwisselbare uitrustingsstukken,
- veiligheidscomponenten,
- hijs- en hefgereedschappen,
- kettingen, kabels en banden,
- verwijderbare mechanische overbrengingssystemen.

Nu: tekst in brokjes en voor de eenvoud weglaten van het zinsdeel: ‘of het verwante product’.

koninklijke metaalunie

zin in brokjes!

De machine moet zodanig ontworpen en gebouwd zijn dat:

- de verbinding ervan met een ander apparaat,
  (of)
- via een functie van het aangesloten apparaat zelf
  of
- via een apparaat op afstand dat communiceert met de machine,

niet tot een gevaarlijke situatie leidt.

Apparaat kan zijn: machine, besturingspaneel, smartphone, camera, e.d.

Vervolg 1.1.9

- Een hardwarecomponent die een signaal of gegevens uitzendt die relevant zijn voor aansluiting op of toegang tot software die van essentieel belang is voor de overeenstemming van de machine met de relevante essentiële veiligheids- en gezondheidseisen, moet zodanig ontworpen zijn dat deze afdoende beschermd is tegen al dan niet opzettelijke corruptie.

  De machine moet bewijzen verzamelen van al dan niet rechtmatige ingrepen in de bovenvermelde hardwarecomponent indien deze relevant zijn voor de aansluiting op of de toegang tot software die van essentieel belang is voor de overeenstemming van de machine.

Wederom in brokjes

Een hardwarecomponent die een signaal of gegevens uitzendt die relevant zijn voor aansluiting op of toegang tot software die:

- van essentieel belang is voor de overeenstemming van de machine met de relevante essentiële veiligheids- en gezondheidseisen,

moet zodanig ontworpen zijn dat deze afdoende beschermd is tegen al dan niet opzettelijke corruptie.

Brontekst … *adequately protected against accidental or intentional corruption.*

…. afdoende beschermd is tegen onopzettelijke of opzettelijke corruptie.

Cybersecurity Bijlage III. 1.2.1a+f

De besturingssystemen moeten zodanig ontworpen en gebouwd zijn dat:

a) zij, gezien de omstandigheden en de risico's, bestand zijn tegen de voorziene bedrijfsbelasting en tegen al dan niet voorziene invloeden van buitenaf, met inbegrip van redelijkerwijs voorzienbare kwaadwillige pogingen van derden die tot een gevaarlijke situatie leiden;

Cybersecurity Bijlage III. 1.2.1a+f

De besturingssystemen moeten zodanig ontworpen en gebouwd zijn dat:

f) het traceringslogboek de gegevens die bij een ingreep zijn gegenereerd, en de versies van veiligheidssoftware die zijn geüpload nadat de machine in de handel is gebracht of in bedrijf is gesteld, registreert en gedurende vijf jaar na het uploaden ter beschikking stelt, uitsluitend om de overeenstemming van de machine met deze bijlage aan te tonen, indien een nationale bevoegde autoriteit daar een met redenen omkleed verzoek toe doet.

Cyberbeveiliging.. een benadering

- Overdonderd met een berg wet- en normteksten,
- Ondertekenen van een stuk papier,
- Plakken van een CE sticker…

en hopen dat er niets fout gaat en

niemand de technische documentatie en de traceringslogboeken opvraagt.

koninklijke metaalunie

Cybersecurity: iets nieuws?

- Inbreuk op het bedoelde functioneren van een machine
- Hardware (afschermen, afsluiten, toegang voor bevoegden..)
- Software (afschermen?)

Damage control with STRIDE?

Nieuwe? richtlijnen voor ontwerp van de Boeing 787:

- Beperk toegang tot gevoelige systemen,
- Verbeter de beveiliging door compartimentering,
- Beveiligingsproblemen aanpakken,
- Focus op cyberbeveiliging.

koninklijke metaalunie

STRIDE nader beschouwd

- Spoofing (Identiteitsvervalsing):
  Ongeautoriseerde toegang door gebruiker of systeem.
- Tampering (Manipulatie):
  Het onrechtmatig wijzigen van data of bestanden.
- Repudiation (Ontkenning):
  Handelingen uitvoeren zonder dat er sporen zijn om de actie aan de dader te koppelen.
- Information disclosure (Informatielek):
  Onbevoegde toegang tot gevoelige data.
- Denial of service (Dienstenweigering):
  Systemen of netwerken verstoren of onbereikbaar maken voor legitieme gebruikers.
- Elevation of privilege (Rechtenverhoging):
  Toegangsrechten verkrijgen die men normaal gesproken niet heeft.

Alledaagse vergelijkingen

Hardware

- Identiteitsfraude
- Onrechtmatig wijzigen
- Dader onvindbaar
- Onbevoegd toegang
- Onklaar maken
- Toegangsrechten ‘verkrijgen’

Voorbeeld(en)

- Wateropnemer, nepagent ..
- Zegel verbreken en ..
- Geen sporen (vingerafdruk, DNA)
- Inbraak (diefstal en/of spioneren)
- Bewakingscamera af(p)lakken
- Lopersleutel(s) misbruiken
- ..

wat is nieuw?

Software	Voorbeeld(en)
• Identiteitsfraude	• Via valse e-mail inloggen
• Onrechtmatig wijzigen	• Rapportcijfer in dbase vervangen
• Dader onvindbaar	• Geen (code) sporen achterlaten
• Onbevoegd toegang	• Informatielekken uitbuiten
• Onklaar maken	• DDOS aanval, Ransomware, e.d.
• Toegangsrechten verkrijgen	• Password / Pincode misbruiken
• ..	• ..

Hard-software vergelijking

Hardware

- Geen open deuren
- Speciale sloten/sleutels
- Persoon gecodeerde id’s (pas/druppel)
- Bewakingscamera
- Hindernissen aanbrengen
- …

Software

- Geen open contacten (USB, bus, ..)
- Wachtwoord (dongel,..)
- Sensoren (zie EN-ISO 14119)
- CRC code e.d.
- Gelaagde toegang (‘air-gap’)
- ..

Cyberrisicobeoordeling: context

- Omgeving vaststellen (grenzen)

Robot-controller

afstandssensor

(veiligheids)PLC

Boormachine

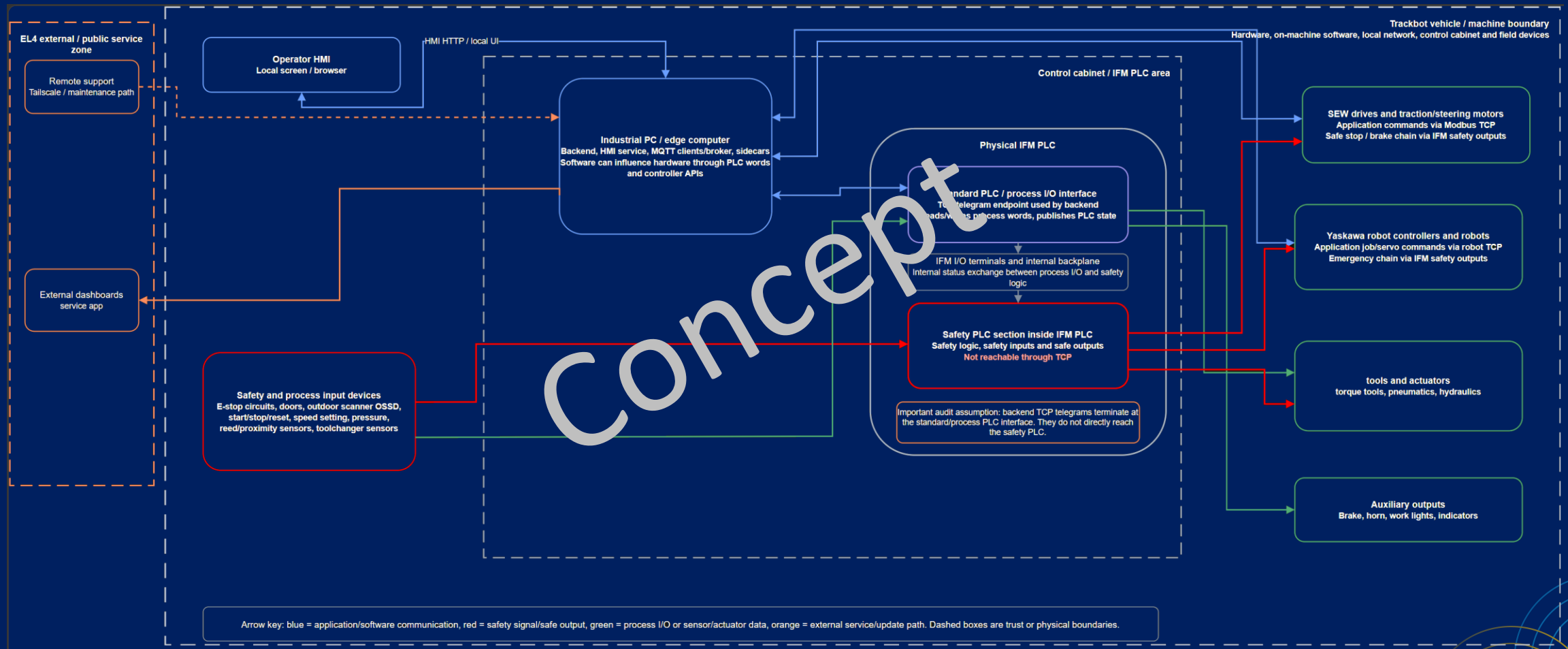
koninklijke metaalunie

Beveiligingscontext

- Beveiligingscontext overeen met wat in veiligheidsnormen het ‘beoogde gebruik’ wordt genoemd.
  - Bijvoorbeeld: ….In figuur xyxz is schematisch de samenhang van de hardware verbindingen weergegeven waarbij informatie /gegevens zouden kunnen worden verstoord….

- Leg dit vast in de gebruiksaanwijzing.

Beveiligingscontext trackbot



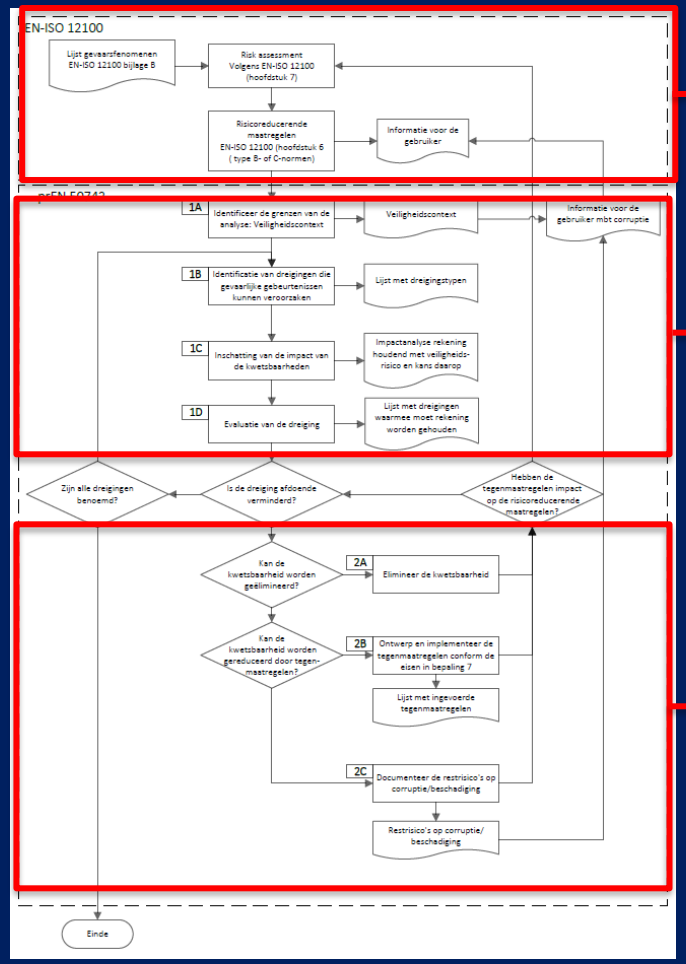
koninklijke metaalunie

Verbindingen met ‘machine’

Een verbinding (fysiek, logisch of indirect) is elke koppeling waarmee informatie kan worden uitgewisseld, bijvoorbeeld:

- wifi-verbinding,
- enkele ader/kabel,
- aders/kabel van de stroomvoorziening,
- optische verbinding,
- kaartlezer interface,
- verbinding tussen een apparaat en externe systemen:
  - gebouwnetwerken
  - clouddiensten
  - service tools

Stroomschema prEN 50742



Risicobeoordeling volgens EN-ISO 12100

Analyse

Cyberrisicobeoordeling

Maatregelen

koninklijke metaalunie

Cyberrisicobeoordeling (1)

Elementen / Veiligheidsfunctie	STRIDE categorie	TTilD	Soort bedreiging (STRIDE)	Getroffen bedrijfsmiddelen	TPID	Voorwaarden misbruik (TPID)	Toelichting	Zone (EL)
HMI webinterface en operatorbediening	S - Spoofing - Identiteitsvervalsing	TTID1.3	Ongeautoriseerde gebruikers maken gebruik van legitieme inloggegevens	Operatorcommando's, pagina-/workflowkeuze, validatie-antwoorden en machine-acties	TPID4.2	De aanvaller heeft toegang tot de HMI van het systeem	Er is momenteel geen authenticatie op de HMI	Fysieke zone
PLC-, SEW- en Yaskawa-veldbuslinks	S - Spoofing - Identiteitsvervalsing T - Tampering - Manipulatie R - Repudiation - Ontkenning I - Information Disclosure - Openbaarmaking van informatie D - Denial of Service - Dienstweigering E - Elevation of Privilege - Verhoging van bevoegdheden			IFM PLC TCP, SEW Modbus TCP, Yaskawa Motoman TCP en commandostatussen	TPID4.3	De aanvaller heeft toegang tot apparaten binnen het systeem	Repo toont raw TCP/Modbus-controllerprotocollen zonder protocol-laag authenticatie of encryptie.	Lokale zone
PLC-telegrammen en motorcommando's				PLC-telegrammen, motor-control words, stop/reset en veiligheidsgerelateerde	TPID1.2	De aanvaller heeft fysieke toegang tot de netwerkkabels	IFM-interface valideert responslengte en CRC32, gebruikt retries/timeouts en reconnects; CRC is integriteit tegen	Fysieke zone

koninklijke metaalunie

Cyberrisicobeoordeling (2)

Elementen / Veiligheidsfunctie	STRIDE categorie	TTilD	Soort bedreiging (STRIDE)	Getroffen bedrijfsmiddelen	TPID	Voorwaarden misbruik (TPID)	Toelichting	Zone (EL)
HMI webinterface en operatorbediening	S - Spoofing - Identiteitsvervalsing	TTID1.3	Ongeautoriseerde gebruikers maken gebruik van legitieme inloggegevens	Operatorcommando's, pagina-/workflowkeuze, validatie-antwoorden en machine-acties	TPID4.2	De aanvaller heeft toegang tot de HMI van het systeem	Er is momenteel geen authenticatie op de HMI	Fysieke zone
PLC-, SEW- en Yaskawa-veldbuslinks	T - Tampering - Manipulatie	TTID1.1	De ontvanger accepteert een valse afzender als legitiem Brute-force-aanval: met vallen en opstaan wachtwoorden, inloggegevens en versleutelingssleutels kraken Ongeautoriseerde gebruikers maken gebruik van legitieme inloggegevens				dbus- nder protocol- cryptie.	Lokale zone
PLC-telegrammen en	D - Denial of Service -	TTID2.1	Manipulatie via fysieke middelen	PLC-telegrammen, motor-control	TPID1.2	De aanvaller heeft fysieke	IFM-interface valideert responslengte	

Cyberrisicobeoordeling (3)

Getroffen bedrijfsmiddelen	TPID	Voorwaarden misbruik (TPID)	Toelichting	Zone (EL)	EL score	Gelegenheid (WoO)	WoO factor	Hack vaardigheid (AC)	AC score	Ernstgraad schade	Ernst score	AP	Aanvals-potentieel	SRSL
Operatorcommando's, pagina-/workflowkeuze, validatie-antwoorden en machine-acties	TPID4.2	De aanvaller heeft toegang tot de HMI van het systeem	Er is momenteel geen authenticatie op de HMI	Fysieke zone	2	Gelimiteerd	0,9	Behoorlijke kennis	2	schade moeilijk herstelbaar	2	3,8	AP0	SRSL0
IFM PLC TCP, SEW Modbus TCP, Yaskawa Motoman TCP en commandostatussen	TPID4.3							ıale kennis	4	schade moeilijk herstelbaar	2	8,5	AP1	SRSL1
PLC-telegrammen, motor-control words, stop/reset en veiligheidsgerelateerde statusinformatie	TPID1.2							ıale kennis	4	schade moeilijk herstelbaar	2	5,2	AP1	SRSL1
Trimble NMEA-stream, RD/WGS84-coördinaten, heading, RTK-kwaliteit en possession-navigatie	TPID1.5							gebreide kennis	1	schade moeilijk herstelbaar	2	13,8	AP2	SRSL2
Planning/balise, planning/axle_counter,	TPID1.6	De aanvaller heeft via externe netwerken logische toegang tot	ArcGIS/Atlas-integratie gebruikt externe API's en tokens; code bevat			Redelijk		Uitgebreide		schade moeilijk				

De aanvaller heeft fysieke toegang tot het netwerk
De aanvaller kan de apparatuur van de netwerkinfrastructuur manipuleren
De aanvaller heeft fysieke toegang tot de netwerkkabels
De aanvaller heeft toegang tot het draadloze netwerk
De aanvaller heeft toegang tot ongebruikte aansluitingen van aangesloten netwerkapparatuur
De aanvaller bevindt zich dicht genoeg bij / binnen het bereik van een draadloze ontvanger
De aanvaller heeft via externe netwerken logische toegang tot het netwerk
De aanvaller heeft fysieke nabijheid tot het systeem
De aanvaller beschikt over de identiteitsgegevens
De aanvaller heeft fysieke toegang tot het systeem
De aanvaller heeft toegang tot de fysieke poorten van het systeem
De aanvaller heeft toegang tot de HMI van het systeem

koninklijke metaalunie

Cyberrisicobeoordeling (4)

orm:	prEN 50742:2025 (Bijlage B)																	
	TPID	Voorwaarden misbruik (TPID)	Toelichting	Zone (EL)	EL score	Gelegenheid (WoO)	WoO factor	Hack vaardigheid (AC)	AC score	Ernstgraad schade	Ernst score	AP	Aanvals-potentieel	SRSL		Tegenmaatregelen inherent (§D Dreiging)	Mitigerend	Informatie voor gebruik	Aanvullende maatreg (rood = actie ver
	TPID4.2	De aanvaller heeft toegang tot de HMI van het systeem	Er is momenteel geen authenticatie op de HMI	Fysieke zone	2	Gelimiteerd	0,9	Behoorlijke kennis	2	schade moeilijk herstelbaar	2	3,8	AP0	SRSL0		Schakel productie-authenticatie in; gebruik operator/admin-rollen; forceer unieke accounts, sessietime-outs en Secure cookies bij HTTPS; beperk HMI-toegang tot operators.	Restrisico: huidige compose-baseline is alleen aanvaardbaar in een fysiek en logisch afgeschermde omgeving of na fabrikantbesluit.		
CP,	TPID4.3	De aanvaller heeft toegang tot apparaten binnen het systeem	Repo toont raw TCP/Modbus-controllerprotocollen zonder protocol-laag authenticatie of encryptie.	Lokale zone	5	Gelimiteerd	0,9	Minimale kennis	4	schade moeilijk herstelbaar	2	8,5	AP1	SRSL1		Plaats controllers in afgesloten kast en afgescheiden OT-netwerk; beheer switches; sta alleen bekende host-to-controller-routes toe; behoud stop-/timeout-/interlockpaden; documenteer fysieke toegangscontrole.	Restrisico: protocolbeveiliging hangt sterk af van fysieke en netwerkcompensaties van de machine-installatie.		
ol	TPID1.2	De aanvaller heeft fysieke	IFM-interface valideert responslengte en													Behoud CRC/timeout/retry checks; voorkom	Restrisico: fysieke toegang tot de		

koninklijke metaalunie

Gelegenheid maakt de dief.

Cyberrisico wordt bepaald door de:

- aanvalsmogelijkheden,
- gelegenheid,
- kennis en kunde van de aanvaller,
  en de
- ontstane schade (herstelbaar of onherstelbaar).

daaruit volgt een ‘risico-eis’ SRSL0, SRSL1, SRSL2 of SRSL3.

N.B.: SRSL: Safety-Related Security Requirement

prEN 50742 ↔ EN-ISO 12100

- Verhelpen = inherente maatregelen
  - Kwetsbaarheden moeten worden verholpen wanneer deze tot gevaarlijke situaties kunnen leiden.
- Beperken = risicoreducerende maatregelen
  - Als verhelpen niet mogelijk is, moeten kwetsbaarheden worden beperkt.
- Informeren = informatie voor de gebruiker
  - Voor alle resterende kwetsbaarheden moet de gebruikersinformatie alle nodige details bevatten over passende tegenmaatregelen.

Tegenmaatregelen

Tegenmaatregelen zijn onder andere:

- Leg kabels in een fysiek beveiligde omgeving,
- Sluit toegang(en) af,
- Gebruik netwerkapparatuur, zoals beheerde switches, routers enz., beveiligd met authenticatie,
- Gebruik versleutelde draadloze protocollen (cryptografie),
- Gebruik RJ45-poortvergrendelingen
  - Gebruik het product/machine alleen in een fysiek beveiligde omgeving,
- Beperk het zendvermogen tot een klein gebied
  - Gebruik een gerichte antenne,
- Beveilig kwetsbare onderdelen van het apparaat tegen ongeoorloofde fysieke toegang (bijv. fysiek slot, plaatsing in een afgesloten kast, uitsluitend gebruik in afgeschermde ruimtes, enz.),
- Bescherm kwetsbare poorten tegen ongeoorloofde fysieke toegang (bijv. fysiek slot, enz.).

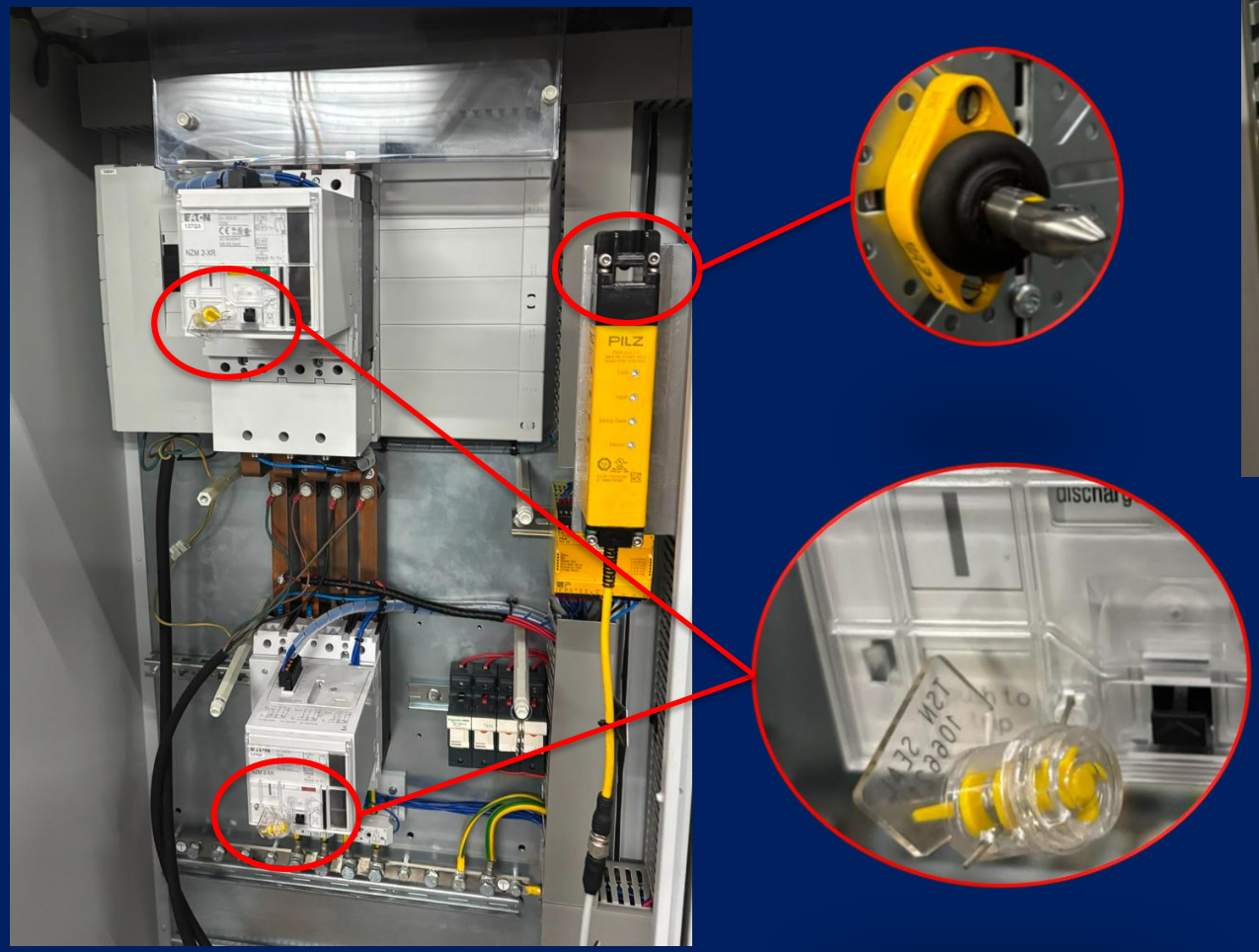
Lock-out, Tag-out, Try-out: Hobby of werk?

- Veiligstellen in vijf regels
  zie EN 50110-1→ NEN 3140/3840
- Onderhouds-, reparatie- en reinigingswerkzaamheden aan een arbeidsmiddel worden slechts uitgevoerd indien het arbeidsmiddel is uitgeschakeld **EN** drukloos of spanningsloos is gemaakt.
  (Arbobesluit Artikel 7.5-2)
- Onze gepatenteerde RLTT oplossing hiervoor.

  Veiligstellen wordt zonder menselijke tussenkomst geregeld; dus automatisch (SIL3/PLe) en cybersecure.

koninklijke metaalunie

Oplossingen



Zegelnummers uniek en gearchiveerd

koninklijke metaalunie

ff zen…

- Ten aanzien van de Cyberrisicobeoordeling:
  - denk als een ‘hacker’ maar handel oprecht.
- Ten aanzien van de richtlijnen en verordeningen:
  - lees de regelgeving aandachtig door,
  - denk in oplossingen (uitdagingen) en niet in problemen.
- Maak van cybersecurity is geen hoofdpijndossier;

Blijf kalm en ga door..

koninklijke metaalunie