

safetywijzer²⁰²⁶

15^E
EDITIE

Aftellen richting nieuwe Machineverordening

SPONSORED BY:



BECKHOFF

Bihl
+ Wiedemann

EUCHNER
More than safety.

FESTO

fortop

kader
framework for positive change

PILZ
THE SPIRIT OF SAFETY

SICK
Sensor Intelligence.

SIEMENS

TCPM INGENIEURS
& ADVISEURS

POWERED BY:

ab
AANDEVEN & BESTUUR

constructeur

engineersonline.nl

MYbusinessmedia

Geharmoniseerde normen

DE BRUG TUSSEN WET EN PRAKTIJK

Geharmoniseerde normen zijn in de machineveiligheid veel meer dan technische achtergrondinformatie. Ze vormen de schakel tussen open wettelijke eisen en concrete ontwerpkeuzes, risicobeoordeling en conformiteitsonderbouwing. Met de overstap van de Machinerichtlijn naar de Machineverordening wordt dat belang alleen maar groter.

TEKST & BEELD: NEN

Iedereen weet dat een machine veilig moet zijn. Maar tussen die ogenschijnlijk eenvoudige constatering en een technisch verdedigbare oplossing ligt een wereld van keuzes, afwegingen en onderbouwingen. Precies daar spelen geharmoniseerde normen hun rol. Ze maken Europese veiligheidsdoelen werkbaar in de praktijk en geven structuur aan ontwerp, beoordeling en documentatie. Juist nu de overgang naar de Machineverordening dichterbij komt, is het goed om opnieuw scherp te krijgen wat geharmoniseerde normen zijn, wat ze betekenen en waarom normcommissiewerk hier belangrijk aan bijdraagt.

Niet bij de norm, maar de vraag erachter

Wie met machineveiligheid bezig is, weet dat de echte uitdaging zelden zit in het formuleren van het doel. Natuurlijk moet een machine veilig zijn. Natuurlijk moeten risico's worden beheerst. Natuurlijk moet aan de wet worden voldaan. De ingewikkelde vraag is hoe je dat in de praktijk overtuigend, reproduceerbaar en technisch verdedigbaar organiseert. Precies daar komt het belang van geharmoniseerde normen naar voren. Zij vormen in de machineveiligheid de schakel tussen open wettelijke eisen en concrete ontwerp- en beoordelingspraktijk.

Voor dit artikel is ook gekeken vanuit de praktijk van normontwikkeling, met Patricia Visser, consultant normontwikkeling bij NEN. Dat is inhoudelijk logisch. Want wie het begrip 'geharmoniseerde norm' goed wil uitleggen, ontkomt niet aan de wereld erachter: de systematiek van normen, de status

van publicaties, de relatie met Europese wetgeving en het werk in normcommissies waarin technische afspraken worden ontwikkeld, gevolgd en aangescherpt.

De wet bepaalt het doel, de norm helpt bij de route

De kern van het Europese systeem is bewust niet dichtgeregeld. De huidige Machinerichtlijn 2006/42/EG en de opvolgende Machineverordening (EU) 2023/1230 leggen essentiële gezondheids- en veiligheidseisen vast, maar schrijven niet elk technisch detail voor. Dat is geen omissie, maar een principiële keuze. De wet bepaalt welk veiligheidsniveau moet worden bereikt; de technische uitwerking blijft voor een belangrijk deel aan de praktijk, mits die uitwerking aantoonbaar voldoet aan de relevante eisen.

Die aanpak heeft duidelijke voordelen. Ze laat ruimte voor technologische ontwikkeling, verschillende ontwerp oplossingen en sectorspecifieke toepassingen. Maar ze vraagt ook om een gedeelde technische taal. Want wie alleen weet dat een risico moet worden gereduceerd, weet nog niet automatisch hoe dat het best gebeurt. Geharmoniseerde normen vervullen precies daar hun rol. Zij vertalen open wettelijke eisen naar technische afspraken die in de praktijk houvast bieden aan fabrikanten, integratoren, beoordelaars en toezichthouders.

Wanneer wordt een norm 'geharmoniseerd'?

Een norm is niet vanzelf geharmoniseerd. Die status ontstaat pas wanneer de referentie van de norm is



Patricia Visser is Consultant normontwikkeling bij NEN.

gepubliceerd in het Publicatieblad van de Europese Unie. Dat is het juridische kantelpunt. Vanaf dat moment kan toepassing van de norm leiden tot een vermoeden van overeenstemming met de essentiële eisen die door die norm worden afgedekt. Dat is iets anders dan zeggen dat de norm zelf wet is. De wet staat in de richtlijn of verordening. De norm biedt een erkende technische route om te onderbouwen dat aan die wet is voldaan. Dat onderscheid is belangrijk, juist omdat het in de praktijk nog vaak door elkaar loopt. Wie een geharmoniseerde norm toepast, volgt dus geen wettekst, maar gebruikt een technisch instrument met juridische betekenis.

Patricia: “De wet zegt dus welk veiligheidsniveau je moet bereiken. De norm helpt om dat te vertalen naar ontwerpkeuzes, afschermingen, veiligheidsafstanden en onderbouwing. Daarmee wordt een abstracte eis praktisch werkbaar.”

Het normenlandschap: van A tot C

Binnen het domein van machineveiligheid is de technische uitwerking georganiseerd in de bekende structuur van A-, B- en C-normen. Die indeling is voor vakgenoten vaak vertrouwd, maar verdient wel toelichting. Juist deze opbouw maakt duidelijk hoe algemene veiligheidsprincipes worden vertaald naar concrete maatregelen en uiteindelijk naar specifieke machines.

De NEN-EN-ISO 12100 vormt daarbij het logi-

WANNEER IS EEN NORM EEN GEHARMONISEERDE NORM?

Een norm is pas een geharmoniseerde norm wanneer de referentie ervan is gepubliceerd in het Publicatieblad van de Europese Unie.

Dat betekent in de praktijk:

- de norm krijgt een bijzondere juridische status;
- toepassing kan leiden tot een vermoeden van overeenstemming met relevante essentiële eisen;
- de norm is daarmee nog steeds geen wet, maar wel een belangrijk juridisch en technisch hulpmiddel;
- de fabrikant blijft verantwoordelijk voor de volledige conformiteitsonderbouwing.

sche vertrekpunt. De centrale positie van deze norm wordt ook verklaard door de manier waarop zij tot stand komt. Via de Vienna Agreement ontwikkelen ISO en CEN zulke basisnormen in één gezamenlijk traject. Europese normen moeten vervolgens nationaal worden overgenomen, waardoor deze A-norm in Nederland verschijnt als NEN-EN-ISO 12100. Vanuit die gemeenschappelijke basis worden B- en C-normen verder uitgewerkt.

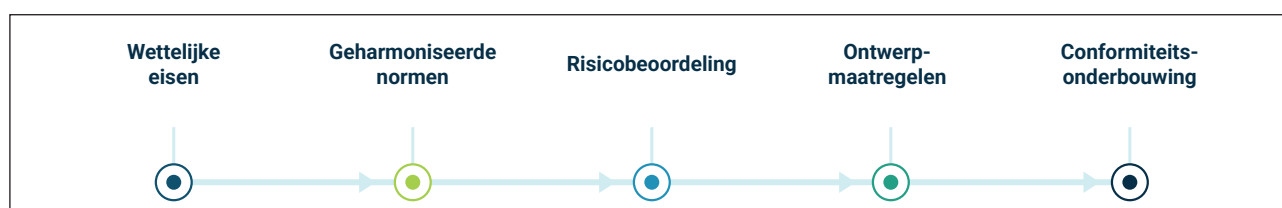
NEN-EN-ISO 12100 beschrijft de algemene ontwerpmethodologie voor machineveiligheid en de uitgangspunten van risicobeoordeling en risicoreductie. Eerst worden de grenzen van de machine bepaald. Daarna volgt de inventarisatie van gevaren, inclusief redelijkerwijs voorzienbaar verkeerd gebruik. Pas daarna komt de vraag welke risicoreducerende maatregelen passend zijn en in welke volgorde die moeten worden toegepast.

Juist dat methodische denken voorkomt dat veiligheid wordt teruggebracht tot een verzameling losse voorzieningen zonder onderliggende analyse. Daarin schuilt de kracht van deze A-norm: zij dwingt tot gestructureerd denken voordat oplossingen worden gekozen.

Naar concrete veiligheidsmaatregelen

Na deze algemene methodiek komen de B-normen in beeld. Die behandelen veiligheidsaspecten of veiligheidsvoorzieningen die over meerdere machinecategorieën heen relevant zijn. Denk aan afscher-

Geharmoniseerde normen verbinden open wettelijke eisen met concrete ontwerpkeuzes, risicobeoordeling en conformiteitsonderbouwing.



EKS2

Digitale toegangscontrole en
selectie van veilige bedrijfsmodus
– flexibel en eenvoudig

- ▶ Gebruiksvriendelijke LED-indicator voor snelle diagnose
- ▶ PROFINET-aansluitingen met geïntegreerde RT-switch voor snelle integratie
- ▶ Hygiënisch ontwerp met beschermingsgraad IP69
- ▶ Selectie van veilige bedrijfsmodus (MSO) op het hoogste niveau PL e via 1-oo-n veiligheidsuitgangen

EUCHNER
More than safety.

PROFI
NET

INDUSTRY4
READY



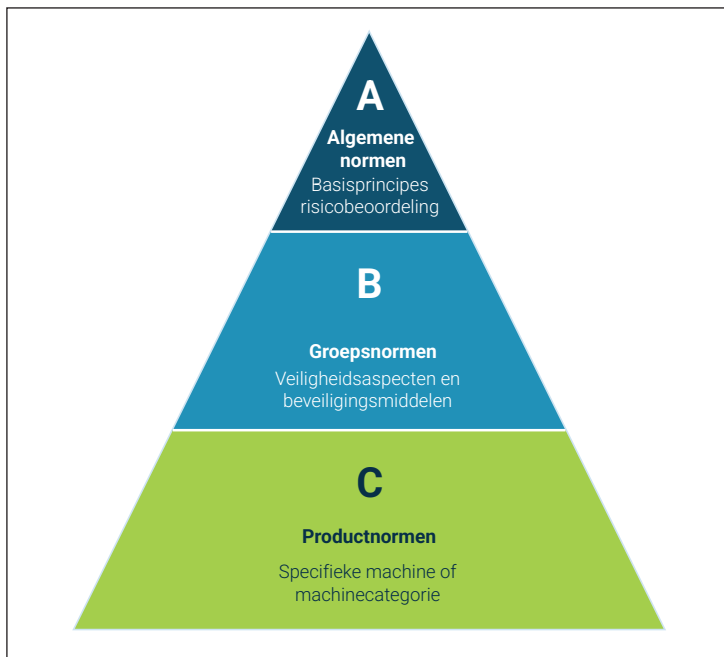
EUCHNER (BENELUX) BV | VISSCHERSBUURT 23 | 3356 AE PAPENDRECHT | +31 (0)78 615 47 66 | INFO@EUCHNER.NL

OT-systemen zijn gebouwd voor betrouwbaarheid,

niet voor cybersecurity.

Kader helpt je OT-systemen veilig te maken. Kijk op kader.nl voor meer informatie.

kader



mingen, veiligheidsafstanden, functionele veiligheid, hygiënisch ontwerp of de samenbouw van machines. Daarmee slaan B-normen een brug tussen de algemene ontwerplogica en de technische uitwerking in concrete situaties.

Daarna volgen de C-normen, die zich richten op een specifieke machine of machinecategorie. Daarin zit hun grote praktische waarde. Ze sluiten direct aan op herkenbare toepassingen en bijbehorende risico's. Bovendien geldt dat een C-norm voor een bepaalde machinecategorie in beginsel voorrang heeft als zij op een punt afwijkt van een A- of B-norm. Zo wordt voorkomen dat algemene uitgangspunten te grof worden toegepast op situaties waarvoor veel specifiekere afspraken bestaan.

Patricia: "De kracht van dit systeem zit in de opbouw. Je begint bij de veiligheidsfilosofie, werkt via specifieke veiligheidsaspecten naar de machinecategorie en komt zo tot een samenhangende onderbouwing. Het gaat bijna nooit om één norm, maar om de juiste combinatie."

Machineveiligheid is geen afvinklijst

Die combinatiegedachte is belangrijker dan ze op het eerste gezicht lijkt. In de praktijk leeft soms nog het idee dat machineveiligheid neerkomt op het vinden van de juiste norm en het vervolgens afwerken van een lijst eisen. Dat beeld is te simpel.

Wie alleen een detailnorm toepast zonder de onderliggende risicobeoordeling goed te doorlopen, kan technisch keurige maatregelen nemen die toch slecht aansluiten op het werkelijke risicoprofiel. Andersom blijft een puur abstracte benadering te mager als concrete veiligheidsfuncties, afschermingen of gebruikssituaties precieze uitwerking vragen.

Goede normtoepassing vraagt dus samenhang, niet alleen documentkennis.

In de machineveiligheid bouwen A-, B- en C-normen op elkaar voort: van algemene methodiek naar veiligheidsaspecten en machine-specifieke uitwerking.

Normen bieden structuur, maar vervangen het professionele oordeel niet. De fabrikant blijft verantwoordelijk voor de risicobeoordeling, de technische documentatie, de gebruiksinstructies en uiteindelijk voor de veiligheid van de machine als geheel. Een norm kan veel houvast geven, maar neemt de verantwoordelijkheid niet over.

Breedte van het vakgebied

Wat op de commissietafel ligt, zegt veel over het vakgebied. Dat zie je ook terug in het werk van normcommissies. Op de agenda staat zelden slechts één bekende basisnorm. Juist de samenhang tussen verschillende normen laat zien hoe breed het werkveld van machineveiligheid is. In de praktijk komen bijvoorbeeld onderwerpen langs als NEN-EN-ISO 14159, NEN-EN-ISO 11161, NEN-EN 12895 en normen in de NEN-EN-ISO 13849-reeks.

Die reeks is niet zozeer interessant omdat het indrukwekkend klinkt om met normnummers te strooien. Ze laat zien hoe breed machineveiligheid in werkelijkheid is: van ontwerpmethodiek en hygiënische of geïntegreerde machineconcepten tot specifieke technische eisen en veiligheidsgerelateerde besturingsfuncties. Daarmee maakt normcommissiewerk zichtbaar dat machineveiligheid geen los document is, maar een netwerk van onderling verbonden keuzes.

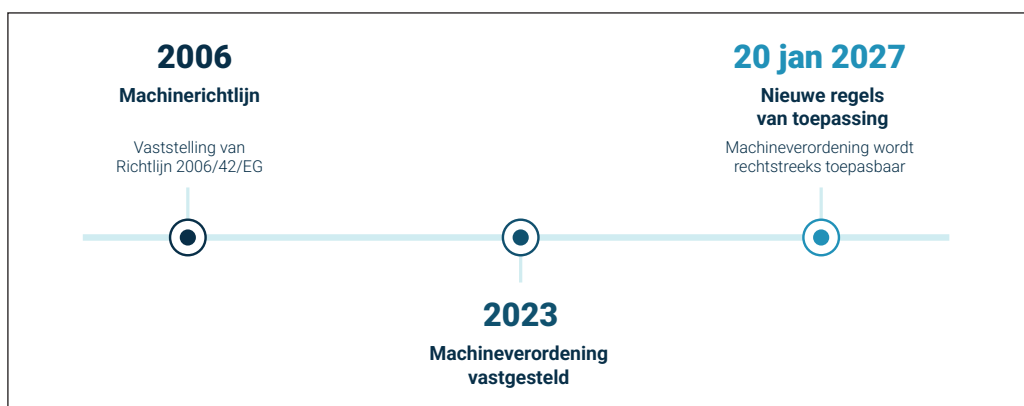
Niet alleen de inhoud telt

Een tweede punt dat in de praktijk vaak wordt onderschat, is de actualiteit van normen. Niet alleen de inhoud van een norm is relevant, maar ook de actuele juridische status. Een norm kan technisch bruikbaar zijn, maar alleen een norm waarvan de referentie in het Publicatieblad is gepubliceerd, heeft de status van geharmoniseerde norm.

Dat betekent dat bedrijven niet alleen moeten vragen welke norm technisch passend is, maar ook welke status die norm op dat moment heeft. Is de referentie gepubliceerd, beperkt, vervangen of ingetrokken? Dat is geen juridisch detail voor aan de zijlijn. In een conformiteitsdossier, audit of markttoezichtkwestie kan die status een groot verschil maken. Juist daarom is normstrategie geen taak die je pas aan het eind van een traject oppakt. Ze raakt ontwerp, verificatie, documentatie en markttoegang tegelijk. Wie te laat naar de status van normen kijkt, loopt achter de feiten aan.

Sneller 2027 dan gedacht

Tegen die achtergrond krijgt de overgang van de



De Machineverordening (EU) 2023/1230 wordt van toepassing op 20 januari 2027 en vervangt dan de Machinerichtlijn 2006/42/EG.

Machinerichtlijn naar de Machineverordening extra gewicht. De verordening is al vastgesteld, maar wordt vanaf 20 januari 2027 van toepassing. Tot die datum blijft de Machinerichtlijn het primaire kader. Daarna geldt de verordening rechtstreeks in alle lidstaten van de EU. Het verschil tussen een richtlijn en een verordening is meer dan een andere titel. Een richtlijn vereist nationale omzetting; een verordening werkt rechtstreeks. Daarmee beoogt de EU meer uniformiteit in toepassing en handhaving. Tegelijk is de Machineverordening inhoudelijk ook een actualisering. Zij sluit beter aan op een praktijk waarin machines vaker via het internet verbonden zijn, software-updates relevanter worden en digitale documentatie een grotere rol speelt. Dat betekent niet dat het hele systeem opnieuw wordt uitgevonden. De basisstructuur van essentiële eisen plus vrijwillige geharmoniseerde normen blijft overeind. Maar de context verandert wel degelijk, en daarmee ook de relevantie van goede normkennis. Patricia: “De stap naar de Machineverordening verandert niet het hele systeem, maar hij maakt wel zichtbaar dat machineveiligheid allang niet meer alleen over klassieke mechanica en elektronica gaat. Software, connectiviteit en digitale informatievoorziening tellen steeds nadrukkelijker mee.”

Wie mee wil praten

Wie wil meepraten over veiligheid, moet ook naar normcommissies kijken. Juist daarom is het begrip

geharmoniseerde normen richting 2027 geen administratief onderwerp, maar een strategisch thema. Bedrijven die machines ontwerpen, bouwen, integreren of beoordelen, moeten niet alleen weten wat de wet zegt, maar ook hoe normen helpen om die wet technisch werkbaar te maken. Dat vraagt inzicht in de A/B/C-structuur, in de actuele status van normen en in de manier waarop normontwikkeling meebeweegt met technologische veranderingen. Daarmee wordt ook het belang van normcommissies concreet. Normen ontstaan niet vanzelf en ook niet in een technisch luchtdelige. Zij komen tot stand in commissies en werkgroepen waar veiligheid, uitvoerbaarheid, innovatie en praktijkervaring met elkaar worden verbonden. Juist daar krijgt de praktijk invloed op de technische spelregels van morgen. Voor Nederland speelt NEN daarin een centrale rol. Voor professionals in machineveiligheid zijn normcommissies daarom niet alleen relevant om het eindresultaat te volgen en te begrijpen hoe dat tot stand komt, maar ook om mee te denken en mee te schrijven aan EN-ISO-normen. Patricia: “In normcommissies komt de praktijk echt aan tafel. Daar zie je hoe technische eisen worden gewogen, waar uitvoerbaarheid schuurt met ambitie en hoe veiligheid uiteindelijk in hanteerbare afspraken wordt omgezet.”

Gereedschap voor de praktijk

Voor lezers van Constructeur is het helder. Geharmoniseerde normen zijn geen papieren aanhangsel van Europese regelgeving en ook geen vrijblijvende technische naslag. Zij vormen de werkbare verbinding tussen open wettelijke eisen en concrete ontwerp- en beoordelingspraktijk. Ze helpen om risico's systematisch te benaderen, maatregelen te onderbouwen en conformiteit sterker neer te zetten. Maar ze vragen wel om actualiteit, samenhang en begrip van hun echte status. Wie dat onderschat, ziet normen vooral als verplicht nummer. Wie het goed begrijpt, ziet dat zij juist een van de belangrijkste instrumenten zijn om machineveiligheid technisch én juridisch beheersbaar te maken. ●

WAT VERANDERT ER OP 20 JANUARI 2027?

Op 20 januari 2027 wordt de Machineverordening (EU) 2023/1230 van toepassing en vervangt de Machinerichtlijn 2006/42/EG.

Dat betekent onder meer:

- het kader geldt dan rechtstreeks in alle EU-lidstaten;
- er komt meer nadruk op de actuele technologische praktijk, zoals software, connectiviteit en digitale documentatie;
- de rol van geharmoniseerde normen blijft belangrijk als technische route naar onderbouwing van conformiteit.

WWW.NEN.NL

Safety-componenten

DE MACHINEVERORDENING EN DE NIEUWE CYBER RESILIENCE ACT (CRA)

De toenemende digitalisering van industriële machines heeft voor een fundamentele verandering gezorgd over wat men verstaat onder “veilige” apparatuur. De EU-Machinerichtlijn is vervangen door de nieuwe EU-Machineverordening (EU) 2023/1230, die vanaf 20 januari 2027 van toepassing wordt en verplichte eisen introduceert op het gebied van cybersecurity, software en digitale risicobeheersing. Omdat de conformiteit van machines nu mede afhankelijk is van de beveiliging en ‘lifecycle-management’ van hun componenten, zijn onderdelen die uitsluitend aan de vroegere Machinerichtlijn voldeden, mogelijk niet langer toereikend.

MAARTEN BRAADBAART, SAFETY SERVICES LEADER | EUROPE SOUTH & WEST, SICK
MARTIN KIDMAN, SAFETY MANAGER | EUROPE SOUTH & WEST, SICK

In deze bijdrage wordt uiteengezet waarom machinebouwers en -leveranciers er verstandig aan doen nu al componenten toe te passen die aansluiten bij de EU Cyber Resilience Act, om zo *compliance-risico's* te verlagen, toekomstige conformiteit te borgen en concurrerend te blijven in een digitaliserende industriële omgeving.

Belangrijke opmerking: Deze bijdrage weerspiegelt de visie en kennis van de auteurs ten tijde van publicatie. Technologieën, normen en *best-practices* kunnen wijzigen; lezers wordt aangeraden actuele informatie zelfstandig te verifiëren.

Ingrijpende verandering

De Europese Unie staat op het punt een ingrijpende verandering door te voeren in de manier waarop machines worden ontworpen, geleverd en geïntegreerd in industriële omgevingen. De EU-Machine-

verordening (EU) 2023/1230, die op 20 januari 2027 van kracht wordt, vervangt de lang bestaande Machinerichtlijn (2006/42/EC) en introduceert onder meer strengere eisen op het gebied van cybersecurity, software-lifecycle-beheer en AI-veiligheid. Voor componentfabrikanten zoals SICK, systeemintegrators en machinebouwers betekent dit niet alleen een actualisering van wetgeving, maar vooral een strategische noodzaak.

Machines die op de markt worden gebracht, moeten voldoen aan een aanzienlijk uitgebreid pakket aan eisen op het gebied van veiligheid, beveiliging en regelgeving. Hoewel veel principes uit de Machinerichtlijn blijven gelden, zorgen de nieuwe verplichtingen rondom cybersecurity en *product-lifecycle* ervoor dat componenten die uitsluitend volgens de oude regelgeving zijn ontwikkeld, mogelijk niet meer voldoen.

De Machineverordening bevat cybersecurity-eisen die moeten worden nageleefd voor alle veiligheidscomponenten. De nieuwe norm prEN 50742 geeft praktische richtlijnen over hoe hieraan voldaan kan worden.

De Cyber Resilience Act (CRA) wordt later geïntroduceerd en is van toepassing op alle digitale producten met digitale interfaces. Subsystemen en componenten met digitale elementen moeten aantoonbaar gaan voldoen aan deze CRA om een passend niveau van risicobeheer aan te tonen.

Sommige producten, zoals basisveiligheidsrelais, >

NU DOEN!

Machinebouwers zouden nu al:

- een audit moeten uitvoeren op hun huidige componentenportefeuille;
- componenten met erkende cybersecurityborging prioriteren;
- leveranciers bevragen over hun *roadmap* richting conformiteit;
- risicobeoordelingsprocessen uitbreiden met cybersecurity;
- interne QMS-processen (Quality Management System) actualiseren.



De EU-Machineverordening (EU) 2023/1230 verandert de manier waarop machines worden ontworpen, geleverd en geïntegreerd ingrijpend.

mechanische schakelaars en lichtschermen met uitsluitend OSSD-uitgangen en dus zonder digitale interfaces, blijven zodoende binnen de scope van de Machineverordening maar vallen buiten de scope van de Cyber Resilience Act.

Van Richtlijn naar Verordening

In tegenstelling tot een richtlijn geldt een verordening rechtstreeks in alle EU-lidstaten, zonder omzetting naar nationale wetgeving. Dit betekent:

- geen nationale interpretatieverschillen;
- heldere eisen voor conformiteitsbeoordeling;
- eenduidige inspectie- en markttoezichtsbevoegdheden;
- nieuwe eisen voorbij de klassieke mechanische veiligheid.

Cybersecurity is een ketenverantwoordelijkheid.



Traditioneel richtte machineveiligheid zich op risico's zoals mechanische letsels, elektrische schokken, lawaai, trillingen of ergonomische gevaren. De verordening breidt dit uit met:

- cybersecurityrisico's;
- verplicht software- en firmware-lifecycle-beheer;
- eisen voor AI-systemen in machines in lijn met de EU AI Act en de bijbehorende veiligheidseisen;
- eisen voor kwetsbaarhedenbeheer en update-mechanismen.

Het concept “veilige machine” krijgt hiermee een digitale en netwerk-gerichte dimensie.

Waarom componenten nú ‘compliant’ moeten zijn

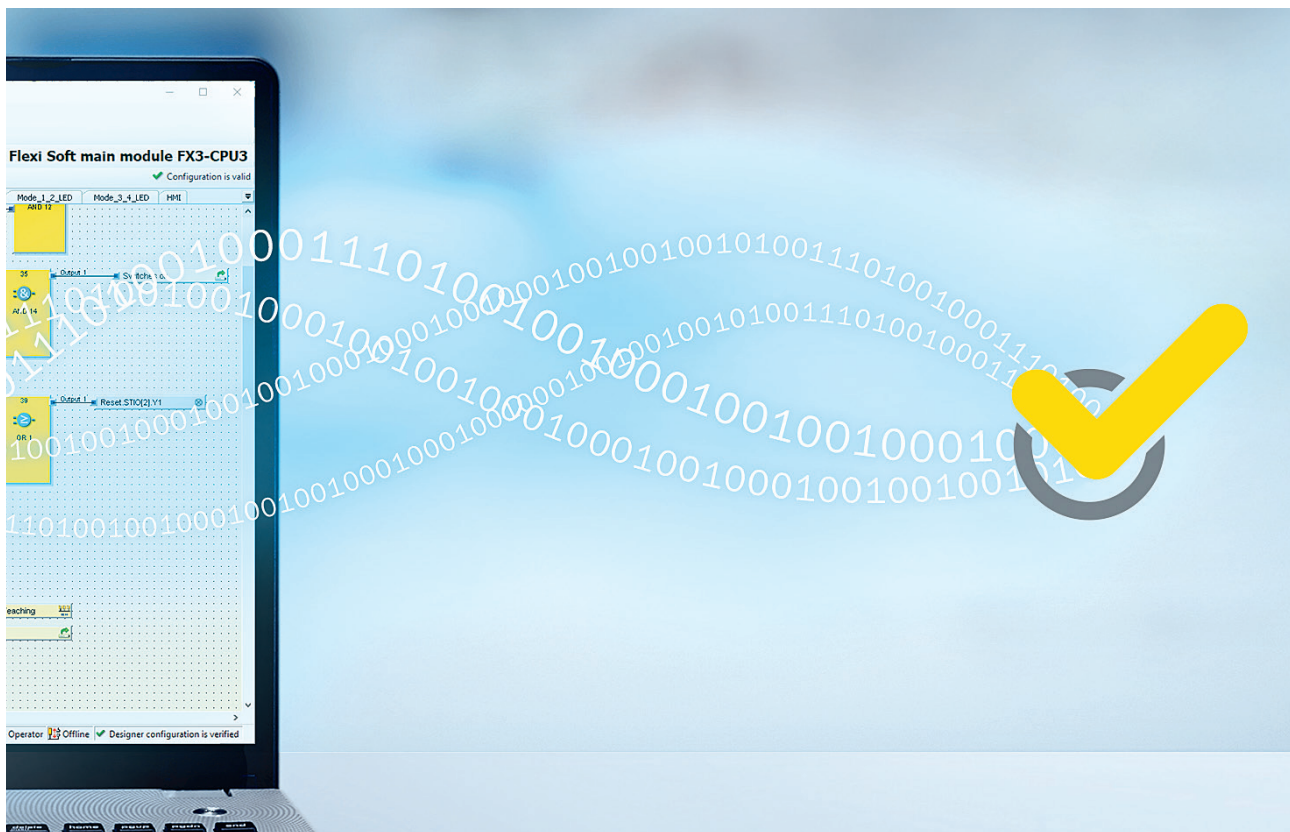
Cybersecurity is een ketenverantwoordelijkheid. De Machineverordening definieert een machine als een systeem van samenwerkende delen, waarbij elke component bijdraagt aan de veiligheid.

Integreert een machinebouwer een component met digitale interface die:

- onveilige standaardconfiguraties heeft,
- geen veilige update-mechanismen biedt,
- inloggegevens onveilig opslaat, of
- geen aantoonbare cybersecurity-borging heeft,

dan kan de conformiteit van de hele machine worden ondermijnd.

Volgens Artikel 6 van de Machineverordening moeten fabrikanten passende risico-reducerende maatregelen implementeren, inclusief die tegen software-kwetsbaarheden en cybersecuritydreigingen. Cybersecurity



kan dus niet langer op het einde worden toegevoegd. Veel componenten worden al in een vroeg stadium in het ontwerp bepaald. Componentleveranciers moeten integraal deel uitmaken van de veiligheidsoplossing en zorgen dat hun producten nu al compliant zijn.

Cyber Resilience Act en componentontwerp

De EU Cyber Resilience Act stelt verplichte cybersecurity-eisen voor digitale producten en componenten die op de EU-markt worden gebracht. Hoewel de meeste certificeringprogramma's momenteel vrijwillig zijn, voorziet de Verordening in geharmoniseerde of erkende kaders voor industriële componenten en software. Het benutten van de kaders uit de Cyber Resilience Act biedt meerdere voordelen:

Met gecertificeerde componenten kan de machinebouwer zekerheid over de veiligheid traceren tot bij de componentleverancier.

1. Aantoonbare beveiligingsborging – certificering volgens erkende Europese of internationale schema's biedt vertrouwen aan klanten en toezichthouders.
2. Herhaalbare risicobeoordeling – een component met CRA-gerelateerde certificatie ondersteunt machinebouwers bij hun verplichte risicoanalyse en technische documentatie.
3. Verantwoordelijkheid in de toeleverketen – Door gecertificeerde componenten te gebruiken, kunnen machinebouwers de zekerheid over de veiligheid aantoonbaar traceren tot terug bij de componentleverancier.

Praktische gevolgen in ontwerp- en ontwikkelfase
Machinebouwers en integratoren moeten:

VERKLARING SICK (FEBRUARI 2026)

In het kader van de EU Cyber Resilience Act volgt SICK de juridische ontwikkelingen nauwgezet en implementeert het benodigde maatregelen voor bestaande en nieuwe producten. Omdat geharmoniseerde normen ter ondersteuning van de CRA nog worden ontwikkeld, kunnen op dit moment slechts beperkte bindende conformiteitsverklaringen worden afgegeven. SICK beoordeelt momenteel het volledige productportfolio en implementeert passende maatregelen. Daarnaast worden de cybersecurity-eisen voor toeleveranciers van productgerelateerde componenten geactualiseerd. Productwijzigingen die hieruit voortkomen, worden transparant gecommuniceerd.

Indien wettelijke eisen niet realiseerbaar zijn binnen een productoplossing, informeert SICK klanten tijdig via de procedure voor productuitfasering.

SICK heeft reeds proactief organisatorische en procedurele maatregelen geïmplementeerd, waaronder:

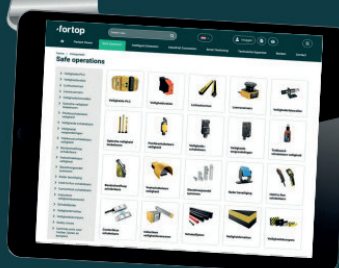
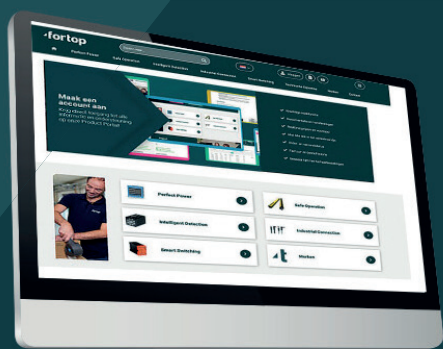
- IEC 62443-4-1:2018 (ML3) Certified Cybersecurity development process
- DIN EN ISO/IEC 17025:2018 Accredited Testing Laboratory in accordance with IEC 62443-4-2:2019
- Product Security Incident Response Team (www.sick.com/psirt)

LESS CONNECTORS MORE CONNECTION USING AS-INTERFACE



MORE-CONNECTION.COM

Optimale techniek



fortop

fortop.nl

Tel: +31 (0)38 377 2700



Ontdek onze
Product Portal



50.000+ producten



24/7 toegang



Intelligente zoek-
en filter functies



20+ topmerken



modern magazijn
voorraadhoudend



UPS 24h levering



gevestigd in 3 landen
met 4 vestigingen



8.000+ klanten



team van meer dan
50 specialisten



AuerSignal BASLER⁷ BOLD eddicy .ESCHA Janitza MAYSER REE⁸ SENSOPART .steute

-COMSYS- CONDORION DOMMIT DCEM EMU HOKUYO INXPCT MMECHAN BEGINS SENSORS SCANCOR Sinexcel

CYBERSECURITY IS NU EEN **KERNONDERDEEL VAN VEILIGHEID**. WACHTEN TOT 2027 BRENGT EEN STRATEGISCH RISICO MET ZICH MEE

- componenten selecteren met gedocumenteerde cybersecurity-risicoanalyses;
- eisen stellen aan *secure software development practices*;
- kwetsbaarhedenbeheer en updateprocessen vastleggen;
- cybersecurity opnemen in de technische documentatie;
- conformiteit aantonen via relevante normen en procedures.

Waar relevant moet de EU-conformiteitsverklaring voortaan cybersecurity-risicobeheer, software-lifecycle-beheer en AI-aspecten reflecteren. Onjuiste of onvolledige documentatie kan leiden tot non-conformiteit tijdens een conformiteitsbeoordeling.

Zakelijke meerwaarde: meer dan wetgeving

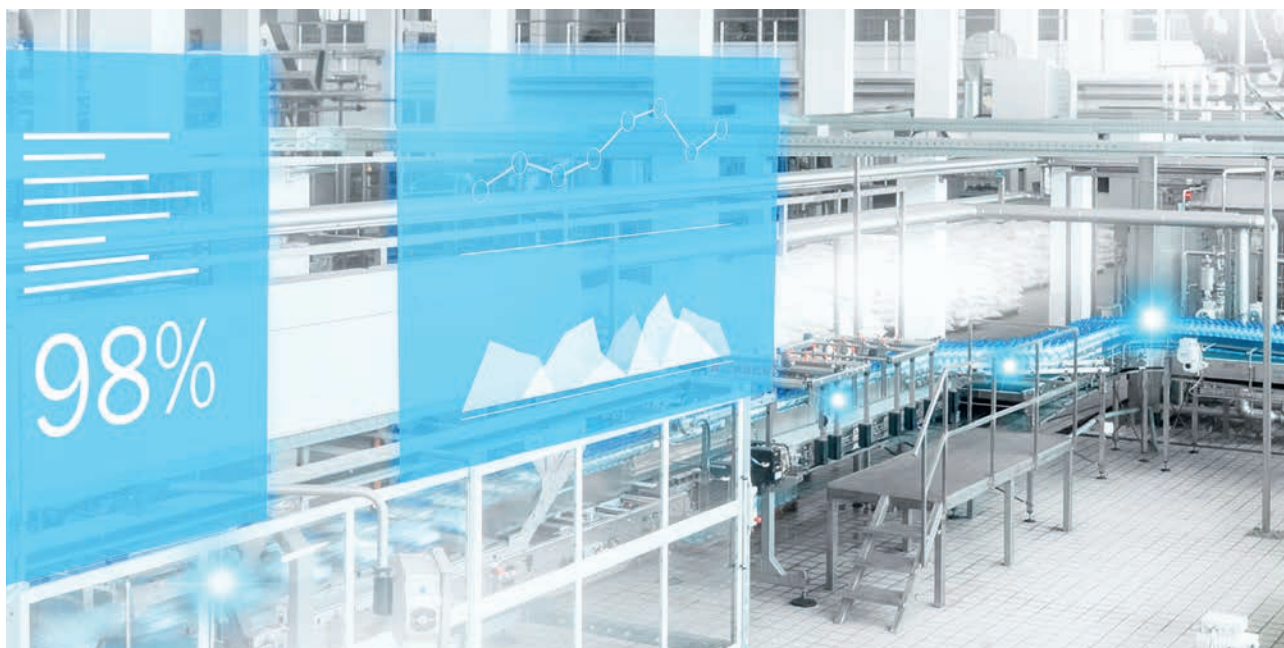
Moderne afnemers eisen steeds vaker veilige, betrouwbare machines die kunnen worden geïntegreerd in industriële IoT-ecosystemen zonder extra risico's. Leveranciers die kunnen aantonen dat hun machines voldoen aan cybersecurity-eisen, hebben een duidelijk concurrentievoordeel. Niet-conforme machines die kwetsbaar zijn voor cyberincidenten kunnen leiden tot operationele downtime, diefstal

van intellectueel eigendom, veiligheidsincidenten en kostbare terugroepacties. Proactieve compliance verlaagt dus zowel juridische als financiële risico's. Een geharmoniseerde verordening betekent bovendien een uniforme Europese markt, waardoor gebruik van conforme componenten marktoegang vereenvoudigt.

Conclusie

De overgang naar de EU-Machineverordening 2023/1230 is een van de grootste veranderingen in de Europese productveiligheid van de afgelopen decennia. Cybersecurity is nu een kernonderdeel van veiligheid, met directe gevolgen voor ontwerp, kwaliteitsbeheer, markttoezicht en aansprakelijkheid. Wachten tot 2027 brengt een strategisch risico met zich mee. Machineleveranciers die nu al beginnen met het integreren van cybersecurity-conforme componenten en hun ontwikkeling, documentatie en kwaliteitsprocessen afstemmen op de nieuwste EU-eisen, voldoen niet alleen tijdig aan hun wettelijke verplichtingen, maar versterken ook hun concurrentiepositie in een steeds digitaler industrieel landschap. ●

WWW.SICK.NL



Niet-conforme machines die kwetsbaar zijn voor cyberincidenten kunnen leiden tot operationele downtime, diefstal van intellectueel eigendom, veiligheidsincidenten en kostbare terugroepacties.

Praktische risico-beoordeling en -reductie

KLAAR VOOR DE TRANSITIE VAN MACHINERICHTLIJN NAAR MACHINEVERORDENING

2026 is een spannend transitiejaar voor de machinebouw. Hoewel de Machinerichtlijn 2006/42/EG nog steeds relevant is, is de nieuwe Machineverordening (EU) 2023/1230 inmiddels van kracht en wordt deze vanaf 20 januari 2027 de enige bindende wettelijke basis voor het op de markt brengen van machines in de EU.

BERT SEVERIJNEN, ADVISEUR INDUSTRIËLE VEILIGHEID, ISC-S

Voor engineers betekent dit, dat de basisprincipes van risicobeoordeling en risicoreductie — zoals vastgelegd in de A-norm EN-ISO 12100:2010 — actueler zijn dan ooit. Er zijn met de komst van de Machineverordening een aantal onderwerpen waarvoor aanvullende onderbouwing en nieuwe documentatie vereist wordt. Door ISC-S (Industrial Safety Coaching & Consulting – Severijnen) wordt een praktische aanpak voor de initiële risicobeoordeling toegepast, gebaseerd op de EN-ISO 12100:2010. In dit artikel wordt die praktische aanpak uitgelegd.

Wettelijk kader en de verplichte risicobeoordeling

Zoals inmiddels bekend verondersteld mag worden, heeft een fabrikant van machines de wettelijke plicht om uitsluitend veilige machines in de handel te brengen. Een centraal onderdeel hiervan is de CE-markering, een proces dat uit zes stappen bestaat, van het vaststellen van toepasselijke wetgeving het uitvoeren van een risicobeoordeling tot het opstellen van de EG-verklaring van overeenstemming. De initiële risicobeoordeling is als verplichting opgenomen in Bijlage I van de Machinerichtlijn en dit staat zo ook onveranderd in de Machineverordening in Bijlage III.

Door risico's in de ontwerpfase te beoordelen is ingrijpen in het ontwerp mogelijk, voordat de machine of een prototype wordt gebouwd en mogelijk ook op de markt wordt gebracht. Dit onderbouwt de ISC-S stellingname dat een goed en tijdig uitgevoerde risicobeoordeling kostenreducerend werkt: er kan worden voorkomen dat kostbare uren en materialen worden besteed aan het bouwen van een machine op basis van een ontwerp, dat achteraf niet blijkt te vol-

doen aan de veiligheids- en gezondheidseisen van de genoemde Bijlage I c.q. Bijlage III.

Als zodanig veranderen de eisen niet, maar met de komst van de nieuwe Machineverordening is er een extra focus op de technologische ontwikkelingen vooral binnen de besturingstechnologie, vanwege onder andere, cyberveiligheid en softwarematige veiligheidsfuncties.

Systematische risicoanalyse

In het begin van het ontwerpproces van een machine moet dus de initiële risicobeoordeling worden uitgevoerd op het ontwerp. Een belangrijk uitgangspunt is het uitvoeren van deze risicobeoordeling op het 'kale' ontwerp, voordat er al maatregelen zijn genomen zoals toepassen van afschermingen. Wanneer er al afschermingen worden gebruikt, dan zal een gevarenszone niet zonder meer bereikbaar zijn en in de risicobeoordeling misschien zelfs niet meer worden opgenomen, maar of de afscherming de beste maatregel is, is niet onderzocht. Volgens de EN-ISO 12100:2010 bestaat de risicobeoordeling uit een reeks logische stappen: risicoanalyse (grenzen bepalen, gevaren identificeren, inschatten van het risico) gevolgd door risico-evaluatie en zo nodig risicoreductie volgens de 3-stappenmethode, schematisch weergegeven in figuur 1 in de norm. Het gedeelte over risicobeoordeling is hier afgebeeld. In het gele vlak staan de stappen van het risicobeoordelingsproces.

Bepaling van de grenzen

Voordat een engineering-team kan beginnen, moeten de specificaties van de te ontwerpen ma- ➤



Een fabrikant van machines heeft de wettelijke plicht om uitsluitend veilige machines in de handel te brengen.

Schematische weergave van het risicoreductieproces cf. NEN-EN-ISO 12100:2010 - figuur 1
(incl. de iteratieve 3-stappenmethode)

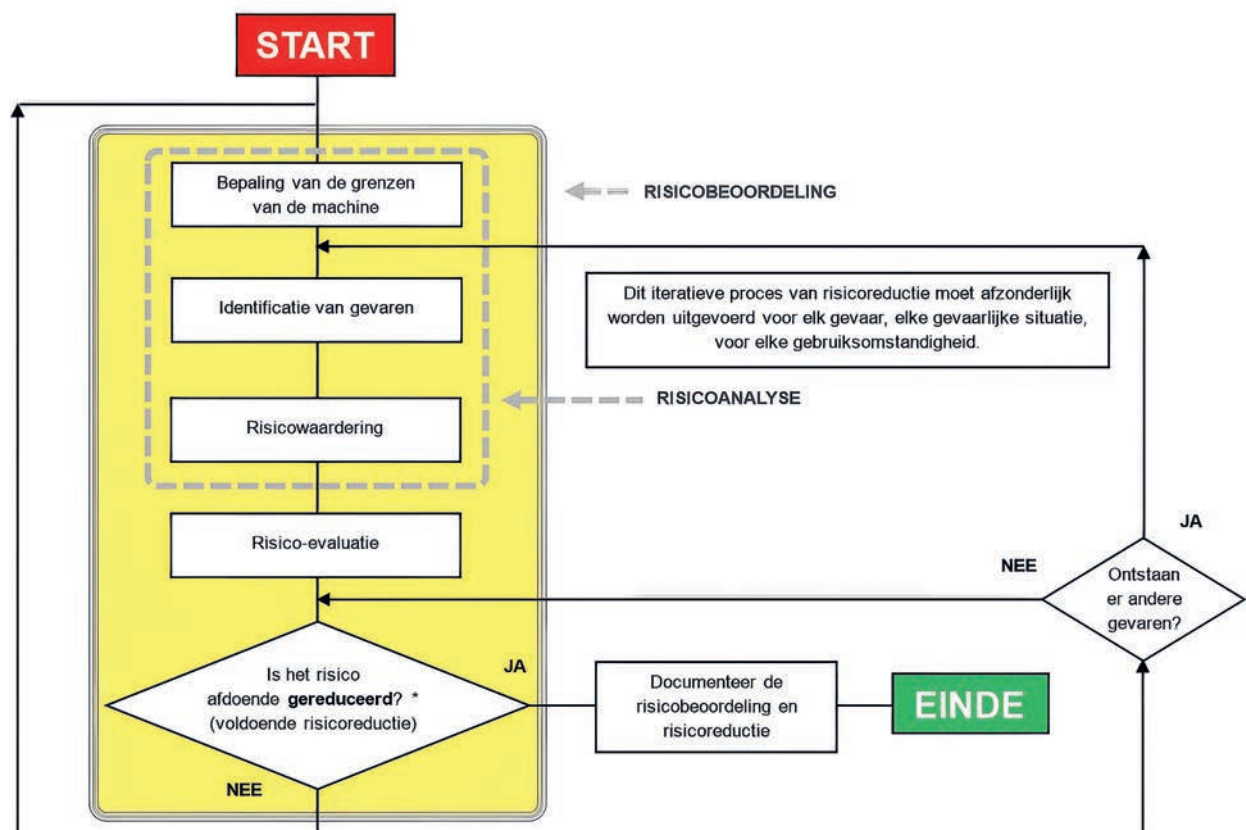


Table B.1

NEN-EN-ISO 12100:2010

No	Type of group	Examples of hazards	
		Origin ^{a)}	Potential consequences ^{b)}
1	Mechanical hazards	acceleration, deceleration angular parts approach of a moving element to a fixed part cutting parts elastic elements falling objects gravity height from the ground high pressure instability kinetic energy machinery mobility moving elements rotating elements rough, slippery surface sharp edges stored energy vacuum	being run over being thrown crushing cutting or severing drawing-in or trapping entanglement friction or abrasion impact injection shearing slipping, tripping and falling stabbing or puncture suffocation.
2	Electrical hazards	arc electromagnetic phenomena electrostatic phenomena live parts not enough distance to live parts under high voltage overload parts which have become live under fault conditions short-circuit thermal radiation	burn chemical effects effects on medical implants electrocution falling, being thrown fire projection of molten particles shock
3	Thermal hazards	explosion flame objects or materials with a high or low temperature	burn dehydration discomfort frostbite injuries by the radiation of heat sources scald
4	Noise hazards	cavitation phenomena exhausting system gas leaking at high speed manufacturing process (stamping, cutting, etc.) moving parts scraping surfaces unbalanced rotating parts whistling pneumatics worn parts	discomfort loss of awareness loss of balance permanent hearing loss stress tinnitus tiredness any other (for example, mechanical, electrical) as a
5	Vibration hazards	cavitation phenomena misalignment of moving parts mobile equipment scraping surfaces unbalanced rotating parts vibrating equipment worn parts	discomfort low-back morbidity neurological disorder osteo-articular disorder trauma of the spine vascular disorder
6	Radiation hazards	ionizing radiation source low frequency electromagnetic radiation optical radiation (infrared, visible and ultraviolet), including radio frequency electromagnetic radiation	burn damage to eyes and skin effects on reproductive capability mutation headache, insomnia, etc
7	Material/ substance hazards	aerosol biological and microbiological (viral or bacterial) agent combustible dust explosive fibre flammable fluid fume gas mist oxidizer	breathing difficulties, suffocation cancer corrosion effects on reproductive capability explosion fire infection mutation poisoning sensitization
8	Ergonomic hazards	access design or location of indicators and visual displays units design, location or identification of control devices effort flicker, dazzling, shadow, stroboscopic effect local lighting mental overload/underload posture repetitive activity visibility	discomfort fatigue musculoskeletal disorder stress any other (for example, mechanical, electrical) as a
9	Hazards associated	dust and fog electromagnetic disturbance	burn slight disease

chine vastliggen in een programma van eisen – ook scope genoemd. De specificaties in die scope zijn feitelijk de grenzen waarbinnen moet worden ontworpen. Het is dus uitermate belangrijk dat dit helder en eenduidig is voor alle deelnemers aan het ontwerptraject.

Denk dan aan grenzen zoals:

- **gebruiksgrenzen:** Wie zijn de gebruikers, (check de definitie in de Machinerichtlijn), wie 'bedient' de machine? Wat is hun opleiding en zijn er menselijke beperkingen (links- of rechtshandig, taal).
- **ruimtelijke grenzen:** Waar komt de machine te staan. Wat is benodigd aan bewegingsruimte tijdens bediening, vullen en legen, maar ook ruimte voor onderhoud, reiniging en verplaatsen.
- **tijdgrenzen:** Wat is de gebruiksduur per dag, per week, ... Wat is de verwachte technische levensduur van de machine en de veiligheidscomponenten.
- **andere grenzen:** Omgevingsfactoren zoals vochtigheid, windbelasting en de kwaliteit en specificaties van de te verwerken grondstoffen of het eindproduct.

Pas nadat de grenzen zijn vastgesteld, kan het engineering-team – zinvol – met het ontwerp starten.

Identificatie van gevaren

Zodra op basis van de scope met de grenzen een eerste ontwerp is gemaakt, is het mogelijk om te starten met de identificatie van gevaren. Voor een goed begrip van deze stap is de definitie van een gevaar relevant: een gevaar is een mogelijke bron van schade/letsel. Bijlage B.1 van de EN-ISO 12100 is een tabel met een overzicht van gevaren, onderverdeeld in 10 categorieën, waaronder mechanische, elektrische, thermische en ergonomische gevaren. In de tabel staan ook de gevolgen van blootstelling aan de diverse gevaren. De tabel lezen helpt om creatief te worden tijdens de gevariden-ificatie, waardoor vaak onverwachte details naar voren komen.

Het is essentieel om niet alleen naar de 'normale' productiefase te kijken, maar ook naar de gehele levenscyclus van de machine: van transport en installatie tot onderhoud, storing zoeken en de uiteindelijke ontmanteling. Het overzicht van de levenscyclus van een machine is opgenomen in Bijlage B.3 van de EN-ISO 12100.

Een ander belangrijk document dat de creativiteit kan stimuleren bij het identificeren van gevaren is Bijlage I van de Machinerichtlijn / Bijlage III van de Machineverordening. De essentiële eisen voor veiligheid en gezondheid hebben een relatie naar mogelijk aanwezige gevaren waar rekening mee gehouden moet worden.

Is het identificeren van gevaren in een machineontwerp moeilijk? De drempel overgaan en beginnen is

Machinerichtlijn 2006-42-EG, Bijlage I

	1. ESSENTIELE VEILIGHEIDS- EN GEZONDHEIDSEISEN
	1.1. ALGEMEEN
	1.1.1. Definities
	1.1.2. Beginselen van geïntegreerde veiligheid
	1.1.3. Materialen en producten
	1.1.4. Verlichting
	1.1.5. Ontwerp van de machine om het hanteren ervan gemakkelijker te maken
	1.1.6. Ergonomie
	1.1.7. Bedienerspost
	1.1.8. Zitplaats
	1.2. BESTURINGSSYSTEMEN
	1.2.1. Veiligheid en betrouwbaarheid van de besturingssystemen
	1.2.2. Bedieningsorganen
	1.2.3. In werking stellen
	1.2.4. Stopzetting
	1.2.4.1. Normale stopzetting
	1.2.4.2. Operationele stop
	1.2.4.3. Noodstop
	1.2.4.4. Complexe machines
	1.2.5. Keuze van de bedienings- of bedrijfsmodus
	1.2.6. Defecten in de energievoorziening
	1.3. MAATREGELEN TER BEVEILIGING TEGEN MECHANISCHE GEVAREN
	1.3.1. Risico van verlies van stabiliteit
	1.3.2. Risico van breuken tijdens het gebruik
	1.3.3. Risico's in verband met vallende of uitgeworpen voorwerpen
	1.3.4. Risico's in verband met oppervlakken, scherpe kanten, hoeken
	1.3.5. Risico's in verband met gecombineerde machines
	1.3.6. Risico's in verband met de verschillende bedrijfsomstandigheden
	1.3.7. Risico's in verband met de bewegende delen

Gedeelte van Bijlage I – Machinerichtlijn 2006/42/EG

meestal het probleem, maar de gevariden-ificatie met de genoemde hulpmiddelen moet toch voor de meesten haalbaar zijn.

Risicobeschrijving: De GELOOF-methodiek

De risicobeschrijving geeft aan waartoe een gevaar kan leiden, welk letsel kan ontstaan, onder welke omstandigheden en bij welke handelingen. Die risicobeschrijving is nodig voordat naar de stap Risicowaardering kan worden overgegaan.

Belangrijk is de termen gevaar en risico niet met elkaar te verwarren. Een gevaar is een bron van letsel/schade, terwijl een risico bestaat uit een combinatie van een gevaar en de kans hierdoor het letsel daadwerkelijk op te lopen. Een gevaar benoemen alleen - bijvoorbeeld 'een scherp mes' - biedt namelijk onvoldoende informatie voor een goede risicowaardering en voor goede keuze van eventuele risicoreductie.

De benodigde tussenstap is het opstellen van de risicobeschrijving. Daarin wordt informatie rondom het ontstaan van letsel vanwege de aanwezigheid van een gevaar en blootstelling aan dat gevaar gecombineerd. Om een risicobeschrijving zo volledig mogelijk op te kunnen stellen heeft ISC-S de GELOOF-methodiek bedacht.

>

Table B.3

NEN-EN-ISO 12100:2010

Phases of machine life cycle	Examples of tasks
Transport	Lifting Loading Packing Transportation Unloading Unpacking
Assembly and installation Commissioning	Adjustments of the machine and its components Assembly of the machine Connecting to disposal system (for example, exhaust system, waste water installation) Connecting to power supply (for example, electric power supply, compressed air) Demonstration Feeding, filling, loading of ancillary fluids (for example, lubricant, grease, glue) Fencing Fixing, anchoring Preparations for the installation (for example, foundations, vibration isolators) Running the machine without load Testing Trials with load or maximum load
Setting Teaching/programming and/or process changeover	Adjustment and setting of protective devices and other components Adjustment and setting or verification of functional parameters of the machine (for example, speed, pressure, force, travelling limits) Clamping/fastening the workpiece Feeding, filling, loading of raw material Functional test, trials Mounting or changing tools, tool-setting Programming verification Verification of the final product
Operation	Clamping/fastening the workpiece Control/inspection Driving the machine Feeding, filling, loading of raw material Manual loading/unloading Minor adjustments and setting of functional parameters of the machine (for example, speed, pressure, force, travel limits) Minor interventions during operation (for example, removing waste material, eliminating jams, local cleaning) Operating manual controls Restarting the machine after stopping/interruption Supervision Verification of the final product
Cleaning Maintenance	Adjustments Cleaning, disinfection Dismantling/removal of parts, components, devices of the machine Housekeeping Isolation and energy dissipation Lubrication Replacement of tools Replacement of worn parts Resetting Restoring fluid levels Verification of parts, components, devices of the machine
Fault-finding/ Troubleshooting	Adjustments Dismantling/removal of parts, components, devices of the machine Fault-finding Isolation and energy dissipation Recovering from control and protective devices failure Recovering from jam Repairing Replacement of parts, components, devices of the machine Rescue of trapped persons Resetting Verification of parts, components, devices of the machine
Dismantling Disabling	Disconnection and energy dissipation Dismantling Lifting Loading Packing Transportation Unloading
NOTE	These tasks can be applied to the machine or parts of it.

GELOOF staat voor:

- GEvaar - bron van het letsel,
- Letsel - gevolg, bijv. amputatie,
- Omgeving - waar gebeurt het,
- Omstandigheden - wat is de situatie, bijvoorbeeld handmatig doordrukken,
- Fase - levenscyclus, bijv. onderhoud of productie.

Dit vormt een handig ezelsbruggetje zowel bij het maken van de risicobeschrijving als voor controle achteraf.

De risicobeschrijving zoals in de werkwijze van ISC-S bestaat meestal uit één zin, die begint met 'Het risico van ...' waarna het gevaar wordt benoemd met het letsel dat het gevolg is.

Wanneer er bijzondere informatie beschikbaar is, kan dat via een aanvullende opmerking aan de risicobeschrijving worden toegevoegd. Soms kan het wat overdreven lijken, maar wees ervan overtuigd dat het na een aantal jaren ook nog duidelijk moet zijn wat met de risicobeschrijving is bedoeld. De risicobeschrijving is namelijk een essentiële stap in het gehele proces van risicobeoordeling en risicoreductie en het vergt nu eenmaal enige inspanning om te komen tot een goede beschrijving. Het toevoegen van een afbeelding met details van het ontwerp aan de risicobeschrijving maakt de situatie meestal nog beter te begrijpen. En dat is toch de bedoeling van deze stap.

Nu zullen bij een machineontwerp over het algemeen meerdere gevaren worden geïdentificeerd en dat betekent dat daarna meerdere risicobeschrijvingen zullen moeten worden opgesteld. Het heeft de voorkeur om eerst alle risicobeschrijvingen – in concept – op te stellen en daarna bij elke risicobeschrijving de Risicowaardering uit te voeren. Door dit consequent zo te doen, worden risico's die een relatie met elkaar hebben zichtbaar. Een ander verschijnsel wordt zo ook beteugeld, namelijk dat meteen geconcludeerd wordt dat er mitigerende maatregelen nodig zijn en ook vaak al gekozen wordt voor bekende maatregelen. Door het proces stapsgewijs te volgen wordt tussentijds discussiëren over maatregelen en oplossingen uitgesloten, wat de tijdsinspanning in belangrijke mate kan beperken.

Risicowaardering: 14 punts Risicograaf-methodiek

Nadat de risicobeschrijvingen zijn opgesteld komt de stap van het leggen van een maatlat naast alle risicobeschrijvingen. Door te kwantificeren ontstaat inzicht in de noodzaak en prioriteit voor eventuele risicoreductie.

Om meerdere redenen is het wenselijk om de risicobeoordeling als team-exercitie uit te voeren. Vanuit verschillende invalshoeken, met inbreng van meerdere personen met ieder een eigen expertise >



Om het verschil aan te geven een voorbeeld:

Een slechte omschrijving van het risico is: 'Het mes van de robotmaaier kan worden aangeraakt'.

Een goede omschrijving van het risico voor veiligheid en gezondheid is:

'Risico van afsnijden of verbrijzelen van de vingers en hand door aanraken van het mes van de robotmaaier tijdens het verwijderen van vuil van het mes, wanneer de machine draait of onverwacht aanloopt.

Opmerking: de maaier wordt dagelijks ingezet op een voetbalveld.

Een voorbeeld van een risicobeschrijving

14-punts Risicograaf

Blootstelling		Waarschijnlijkheid					
		1		2		3	
Ernst/effect	(1-2)	1	2	3	4	5	6
	1	3	4	5	6	7	8
	2	5	6	7	8	9	10
	1	7	8	9	10	11	12
	3	9	10	11	12	13	14
	2						
		1	2	1	2	1	2
		Gevaarsofwenning					

Waarderingsaspecten:	
Ernst/effect:	1 Kleine verwonding (meestal geen blijvend letsel) 2 Ernstige verwonding (meestal blijvend letsel) 3 Dood
Blootstelling:	1 Zelden tot soms 2 Vaak tot continu
Waarschijnlijkheid:	1 Laag (zal waarschijnlijk niet plaatsvinden) 2 Gemiddeld (kan plaatsvinden binnen de levensduur van de machine) 3 Hoog (zal meermaals kunnen plaatsvinden)
Gevaarsofwenning:	1 Mogelijk onder speciale omstandigheden 2 Nauwelijks mogelijk

De 14 punts Risicograaf

Totaalscore (prioriteit):

Risico zeer laag	1 - 2	PLr
Risico laag	3 - 4	PLa
Risico middel	5 - 6	PLb
Risico hoog	7 - 9	PLc
Risico zeer hoog	10 - 14	PLd

Toepasselijk voor
restorisico's
gereduceerd dmv.
een
veiligheidsfunctie

De 14 punts Risicograaf in relatie tot het Performance Level required

kan dit leiden tot een kwalitatief goede risicobeoordeling. Een operator zal andere informatie aanleveren dan een monteur of schoonmaker.

Dat werkt ook zo bij het uitvoeren van de risicowaardering. Voor het inschatten van de hoogte van het risico wordt door ISC-S gebruikgemaakt van de 14-punts Risicograaf, gebaseerd op de criteria uit de NEN-EN 1050.

De volgende vier aspecten bepalen de uiteindelijke totaalscore bij een risico:

- Ernst/effect van het letsel: score 1 t/m 3.
- Blootstelling/frequentie: score 1 of 2.
- Waarschijnlijkheid van het optreden van de schade: score 1 t/m 3.
- Gevaarafwending: score 1 of 2.

Dit resulteert in een totaalscore van 1 t/m 14. Van daar de naam 14-punts Risicograaf.

Is het toegestaan om een andere risicograaf te gebruiken? Er is geen wettelijk verplicht gestelde methode. Alle methoden zoals die in diverse normen en vakliteratuur voorkomen hebben hun onderbouwing en het toepassen is een kwestie van voorkeur. Zorg er wel voor dat voor vergelijkbare processen en ook vooral binnen één bedrijf dezelfde methode wordt gebruikt, anders wordt het appels en peren vergelijken. Er is dus geen verplichte methode en mede daarom is bij de invoering van de EN-ISO 13849-1/2 de vertrouwde 14-punts Risicograaf, afgestemd op de 'PLr' (EN-ISO 13849-1: Performance Level required).

De totaalscore (1 t/m 14) bepaalt nu niet alleen de prioriteit van de maatregelen, maar ook de PLr voor de veiligheidsgerelateerde onderdelen van het besturingssysteem als dit als risicoreducerende maatregel

wordt toegepast. In de onderstaande tabel is de relatie tussen de totaalscore en de PLr weergegeven.

Vanuit de stap risicowaardering komt dus belangrijke informatie beschikbaar voor de vervolgstap Risicoreductie.

Risicoreductie via de driestappenmethode

Na de risicowaardering voor alle risico's zal het evalueren van de risico's in veel gevallen leiden tot risicoreductie, waarvoor in de Machinerichtlijn en de Machineverordening dezelfde aanpak is beschreven. De geel gemarkeerde blokken geven deze drie stappen weer, in de verplichte volgorde. Hierbij moet de hiërarchie van de driestappenmethode worden gevolgd:

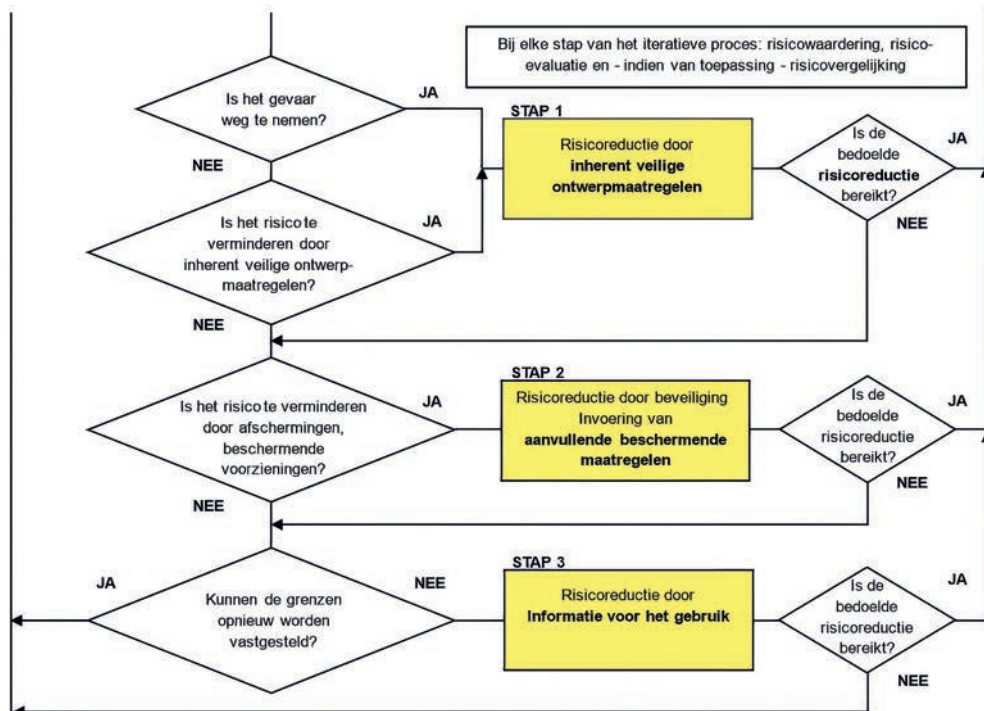
- Stap 1: Inherent veilig ontwerp. Het gevaar wordt weggenomen door ontwerpkeuzes.
- Stap 2: Aanvullende beschermende maatregelen. Als Stap 1 niet slaagt, kunnen afschermingen of veiligheidsfuncties toegepast worden.
- Stap 3: Informatie voor het gebruik. Restriscos beheersen via waarschuwingen, pictogrammen en instructies in de gebruiksaanwijzing.

Risicoreductie blijkt in de praktijk het meest interessante onderwerp te zijn: de engineer wordt weer uitgedaagd! Hierbij is een goede afstemming tussen de mechanisch ontwerper en de besturingsengineer erg belangrijk. Na een goede risicobeoordeling verloopt het komen tot de meest geschikte risicoreductie meestal ook soepel. Zoals in het schema te zien is, wordt na elke risicoreductie maatregel opnieuw geëist het risicobeoordelingstraject te doorlopen, met als doel vast te stellen of te verifiëren of de gemaakte keuze effectief was.

Risico nummer	Machinedeel en details		Phase cf. table B.3 EN 12100:2010							Mogelijke gevaar en risico informatie										Initiele risicoschatting 14 pt Risicograaf / PL relatie				
No	Machinedeel	Details	Transport	Installatie	Instellen	Productie	Reinigen	Onderhoud	Storingen	Buiten gebruik	Gevaar- en risico beschrijving	Fotoblad	E	B	W	G	Score	PLr max						
B2	Laadsysteem	Invoer transportband				x					Het risico op letsel aan hand of vingers als gevolg van - bekneeld raken tussen de wals aan de invoerzijde en de band tijdens verwijderen van vuil of oplossen van een blokkade terwijl de machine is ingeschakeld. <u>Opmerking:</u> de band loopt max. 25 m/s.	5	1	2	2	2	4							
B3	Transportsysteem	Doorvoer transportband		x	x	x	x	x	x		Risico op ernstig letsel aan handen of vingers door - ingetrokken worden nadat men vast is komen te zitten tussen de draden van de band van een draaiende machine, bijvoorbeeld bij het verwijderen van vastzittende producten tijdens het zagen <u>Opmerking:</u> Bandsnelheid tussen 2,5 en 25 m/min. (max. 30 m/min) <u>Opmerking:</u> Handmatig laden/lossen is uitgesloten. <u>Opmerking:</u> Dagelijks moet zaagsel worden verwijderd. <u>Opmerking:</u> De openingen in de transportband zijn ca. 20 x 20 mm, vanwege de procesprestaties (grootte van zaagsel en snippers) en mechanische vereisten (sterkte, flexibiliteit).	35	2	2	2	2	8							

Schematische weergave van het risicoreductieproces cf. NEN-EN-ISO 12100:2010 - figuur 1
(incl. de iteratieve 3-stappenmethode)

De risico-reductiestappen volgens figuur 1 – EN-ISO 12100:2010



Documenteren risicobeoordeling en risicoreductie

De norm EN-ISO 12100 speelt een grote rol bij het ontwerpen van een machine. Gedurende het doorlopen van alle stappen van figuur 1 wordt een groot aantal details besproken en worden er keuzes gemaakt voor het definitief ontwerp. Alle stappen van de risicobeoordeling en de keuzes van de risicoreductie moeten vastgelegd worden in het Technisch

Dossier. Voor het documenteren zijn er tegenwoordig een aantal goede mogelijkheden, bijvoorbeeld werken met speciale software-tools of met een zelf-ontwikkelde werkwijze. Ter afsluiting in afbeelding een paar voorbeeldrisico's in een eenvoudige werkwijze met MS-Excel. ●

ISC-S.COM

Risicoreductie aspect					SRS info		Risicoreductie informatie, motivatie, onderbouwingsrapporten, relatie met wetgeving en normen			
Ontwerp	Afscherming	Functionele	Instructies	Diverse	PLr	SF info	Risicoreductie mogelijkheden	Risicoreductie uitvoering	Reden voor gekozen risicoreductie / Onderbouwingsrapport	Referenties (wetgeving / normen)
v	v	v	v	v	?	SRS	OA - Vast rooster cf. EN 13857 / EN 14120 voor de invoerzijde toepassen. Openingen z.d.d. schoonspuiten mogelijk is. OF - Plaats een lichtscherm cf. EN 13855 voor de invoeropening, icm muting. PLr = b. I - Instructions hoe een blokkade of vervuiling te verwijderen in de handleiding zetten.	Vaste afscherming is toegepast. Instructies in de manual.	Vaste afscherming is geen bezwaar voor het werken.	MD Ann. I, 1.3.7 EN 14120 EN 13849 EN 13857 EN 13855
v	v	v	v	v	?	SRS	OAF - Wegneembaar afschermkap cf. EN 13857 / EN 14120 i.c.m. een veiligheidsschakelaar cf. EN 13849 / EN 14119 voor de transport- en zaagomgeving toepassen. Afscherming gesloten geeft vrijgave voor starten van de zaag. PLr = d. Openingen z.d.d. schoonspuiten mogelijk is. OF - Plaats een lichtscherm cf. EN 13855 voor de invoeropening, icm muting. I - Instructies hoe een blokkade of vervuiling te verwijderen in de handleiding zetten.	Verwijderbare afscherming i.c.m. veiligheidsfunctie is toegepast.	Minder complex dan lichtscherm met muting ivm verschillende afmetingen van product.	MD Ann. I, 1.3.7, 1.3.8.2 1.6, 1.7 EN 14120 EN 13849 EN 13857 EN 13855



Axelent Benelux NV
Gestelhoflei 14 C
2820 Bonheiden
België
Website: www.axelent.com/nl

Axelent is een toonaangevende leverancier van innovatieve veiligheidsoplossingen voor industriële omgevingen. Wij beschermen mensen, machines en infrastructuur met duurzame en modulaire systemen zoals aanrijdbeveiliging, machineaafscherming en magazijnbeveiliging. Dankzij onze expertise en eigen montageteam zorgen we voor veilige werkplekken waar efficiëntie en bescherming hand in hand gaan. Veiligheid staat bij ons altijd centraal.



Beckhoff Automation B.V
Oerkapkade 1C
2031 EN Haarlem
Tel: +31 (0)23 518 5140
E-mail: sales@beckhoff.nl
Website: www.beckhoff.com/nl-nl/

Beckhoff Automation ontwikkelt innovatieve oplossingen die machines eenvoudiger, efficiënter en slimmer maken. Met TwinCAT als besturingsplatform, EtherCAT voor snelle en realtime communicatie protocol en TwinSAFE voor geïntegreerde veiligheid, vormt dit één krachtig, overzichtelijk en betrouwbaar geheel.



Bihl+Wiedemann GmbH
Flosswoerthstraße 41
68199 Mannheim
Duitsland
Tel: +49 621 33996-0
Website: www.bihl-wiedemann.com

Bihl+Wiedemann ontwikkelt en produceert complete automatiseringsoplossingen voor functionele veiligheid en datacommunicatie in machines en installaties. Producten en oplossingen van de onderneming zijn wereldwijd in gebruik bij vooraanstaande fabrikanten van consumptie- en investeringsgoederen, met name in industriële automatisering, transporttechniek en machinebouw.

Bihl+Wiedemann loopt technologisch voorop in de automatiserings- en veiligheidstechniek met AS-Interface (ASi) en leverde een belangrijke bijdrage aan de ontwikkeling van alle ASi-generaties



EUCHNER (Benelux) BV
Visschersbuurt 23
NL - 3356 AE PAPENDRECHT
Tel: +31-(0)78-615 4766
Fax: +31-(0)78-615 4311
E-mail: info@euchner.nl
Website: www.euchner.nl

Veiligheid staat bij EUCHNER hoog in het vaandel. Veiligheidstechniek ter bescherming van mensen en machines, maar ook ter verbetering van productieprocessen. EUCHNER ontwikkelt hoogwaardige kwaliteitsproducten die hun weg vinden in uiteenlopende industrieën over de hele wereld. Oplossingen waarin alle veiligheidscomponenten voldoen aan de gestelde normen en de productie optimaal verloopt. EUCHNER heeft voor elke situatie een praktische, duurzame en doeltreffende oplossing.



Festo
Schieweg 62
2627 AN Delft
Tel: 015-2518899
E-mail: info@festo.nl
Website: www.festo.nl

Festo brengt machineveiligheid naar een hoger niveau door te focussen op de plek waar veiligheid écht wordt gemaakt: de output. Met slimme pneumatische en elektrische subfuncties, van energie onderbreking tot gecontroleerde bewegingen, biedt Festo concrete, normconforme oplossingen die direct bijdragen aan een veiligere machine. Praktisch, betrouwbaar en volledig toepasbaar in jouw machine.



fortop
Grote Kranerweerd 53
8064 PE Zwartsluis
Tel: +31 (0)38 - 337 27 00
E-mail: info@fortop.nl
Website: www.fortop.nl

Bij fortop hebben we een natuurlijke drive om dingen beter te maken. Alle onderdelen die van kritisch belang zijn voor bedrijfsprocessen willen wij optimaal zien werken. We kijken mee, denken mee en zorgen met onze partners voor solide oplossingen - ook als die nog niet bestaan.

fortop zorgt niet alleen dat het goedkomt; wij gaan voor optimale techniek!



Kader Group
Dijnselburgerlaan 2
3705 LP Zeist
Tel: 088-9951200
E-mail: info@kader.nl
Website: www.kader.nl

Technische veiligheid vormt de ruggengraat van een veilige werkomgeving waarin je kunt vertrouwen op producten, installaties en machines. Kader helpt organisaties risico's beheersen en medewerkers veilig laten werken. Met expertise in machineveiligheid, procesveiligheid, ATEX en HAZOP bieden we oplossingen die verder gaan dan wetgeving en bijdragen aan compliance, vertrouwen en een toekomstbestendige werkomgeving.



Pilz Nederland
Havenweg 22
4131 NM Vianen
Tel: 0347 32 04 77
E-mail: info@pilz.nl
Website: www.pilz.nl

Pilz is een wereldwijde leverancier van componenten, systemen en diensten voor alles wat met automatisering te maken heeft. Wij sluiten geen compromissen als het gaat om veiligheid voor mens, machine en milieu. Als wereldwijd vertegenwoordigd familiebedrijf met een lange traditie is het ons doel om ter plekke een betrouwbare partner voor u te zijn.



Sick BV
Postbus 186
3720 AD BILTHOVEN
Tel: 030 204 40 00
Fax: (030) 229 39 94
E-mail: info@sick.nl
Website: www.sick.nl

Veiligheid voor alles. De oplossing komt van SICK. In geautomatiseerde productie- en logistieke systemen is effectieve ongeval- en persoonsbeveiliging topprioriteit. SICK loopt voorop in het ontwikkelen en produceren van nieuwe technieken en producten welke het werk veiliger maken. SICK is ook uw partner voor risicoanalyses, het opstellen van veiligheidsconcepten en projectmanagement t.b.v ontwerp, installatie en validatie. Feilloos en betrouwbaar signaleren en reageren, daar draait het om bij SICK. Sensoren die processen sneller en betrouwbaarder maken, sensoren die de continuïteit van productieprocessen bewaken en sensoren die bedrijfsongevallen voorkomen.



Siemens Nederland N.V.
Prinses Beatrixlaan 800
2595 BN Den Haag
Tel: 070-333 3515
E-mail: vip.nl@siemens.com
Website: www.siemens.nl

In Nederland is Siemens actief sinds 1879 en behoort het concern tot de grootste elektrotechnische ondernemingen. Siemens richt zich op automatisering en digitalisering in de proces- en maakindustrie en op intelligente infrastructuur. Met Digital Industries, Smart Infrastructure en Siemens Mobility vormt het bedrijf de industrial core en werken circa 3.000 medewerkers in Nederland aan oplossingen voor maatschappelijke uitdagingen en megatrends.



TCPM Ingenieurs & Adviseurs
Boogschutterstraat 40
7324 BA Apeldoorn
Tel: +31 (0)88 220 1400
E-mail: tcpm@tcpm.nl
Website: www.tcpm.nl

Wij zijn een vooruitstrevend ingenieurs- en adviesbureau, met ruim 200 enthousiaste medewerkers en vijf kantoren verspreid door het land. Met expertises op het gebied van engineering, projectmanagement en industriële veiligheid leveren wij een samenhangend pakket aan diensten. Onze opdrachtgevers in industriële omgevingen helpen we verder met complete en integrale oplossingen. Zo werken we samen aan een technologische en duurzame toekomst.

'Dreamteam' voor Movu Robotics

COMBINATIE DEUR- EN SLEUTELSYSTEEM EUCHNER
BESCHERMT GEVAARLIJKE ZONES

Om het bestaande zelf ontwikkelde systeem voor veilige toegang tot shuttles te upgraden, was Movu Robotics op zoek naar een oplossing die de gevarenczones in automatische magazijnsystemen betrouwbaar beveiligt. Samen met safety engineering specialist Euchner ontstond een op maat gemaakte oplossing bestaande uit het beveiligingsdeursysteem MGB2 *Modular* en het sleutelsysteem CKS2. Het toekomstbestendige systeem voldoet aan alle eisen op het gebied van flexibiliteit, kostenefficiëntie en bedrijfsveiligheid.

TEKST & BEELD: EUCHNER

Movu Robotics presenteert zich sinds het najaar van 2023 onder deze naam op de markt. Sinds die tijd is het aantal medewerkers gestegen van 25 naar meer dan 400 in Europa en de VS. Voorheen

luisterde het bedrijf overigens naar de naam Stow Robotics. De onderneming was ontstaan als *spin-off* van de Stow-groep, al sinds de jaren tachtig actief in de intralogistieke systemen.

Voornamelijk in Europa en de VS

Het hoofdkantoor in het Belgische Lokeren biedt op in totaal 15.000 m² plaats aan kantoren, productie, logistiek en een Experience Center van 2500 m²,



De verouderde zelfontwikkelde beveiligingstechniek uit de beginjaren: een nogal grote aansluitkast met complexe bedrading en mechanische sleutels.



In samenwerking met Euchner ontstond een oplossing op maat op basis van het veiligheidsdeursysteem MGB2 *Modular* en het sleutelsysteem CKS2.





Movu Robotics zocht een betrouwbare beveiliging van de gevarenczones in hun automatische magazijnsystemen.

waar klanten de producten live kunnen ervaren. Voor 2025 stevent Movu af op een omzet van meer dan 200 miljoen euro. Er worden vele benodigdheden voor een modern, geautomatiseerd ma-

MODULAIRE SYSTEMEN NODIG DIE MEEGROEIEN

gazine geproduceerd: pallet-shuttlesystemen, containeroplossingen zoals 'Movu escal', Autonomous Mobile Robots (AMR), pick-robots en de gehele software die gebruik, verkeersregeling en gegevensstromen bijeenhoudt. De klanten zijn divers: logistieke dienstver-

leners, de voedingsmiddelen- en diepvriesindustrie, de farmaceutische industrie, e-commerce, detailhandel en Fast Moving Consumer Goods en traditionele industriële bedrijven – voornamelijk in Europa en de VS, maar ook in de rest van de wereld.

Systemen die meegroeien

Hoe uiteenlopend de gebruikers ook zijn, van de producten van Movu Robotics verwachten ze hetzelfde: "Onze klanten hebben modulaire systemen nodig die meegroeien, ook bij -30 °C betrouwbaar functioneren en tegelijkertijd energie-efficiënt zijn", beschrijft Herman Tesseur, safety director bij Movu Robotics, de taakstelling. "Daarbovenop komt het doel om inbedrijfstellingen zo kort mogelijk en de totale bedrijfskosten zo laag mogelijk te houden." Om zijn klanten ook in de toekomst een optima- ➤

MGB2 MODULAR

Veiligheidsdeursysteem MGB2 Modular beveiligt toegangen in veiligheidsdeuren en hekken waarachter zich gevaarlijke zones van machines en installaties bevinden. Het gehele systeem is modulaair opgebouwd en kan individueel worden aangepast: het bestaat uit een grendelmodule, daarin opgenomen submodules voor bedienings- en indicatorelementen en verder optionele uitbreidingsmodules. De geïntegreerde ethernet-switch vereenvoudigt de verbinding met bestaande ethernet-netwerken. Naast Profinet/Profisafe en EtherCAT (P)/FSOE is de busmodule nu ook verkrijgbaar voor EtherNet/IP/CIP Safety. De MGB2 biedt de gebruiker maximale veiligheid van categorie 4/PLe/SIL3 en is compatibel met alle gangbare besturingen. Het robuuste systeem bezit wereldwijde toelatingen (UL, CCC, FCC en IC) en werkt betrouwbaar bij temperaturen tot -30 °C.



Herman Tesseur (Movu Robotics): "Nu kunnen de installatie en instelling bij de klant aanzienlijk eenvoudiger en ongeveer 60 procent sneller verlopen."



le oplossing te kunnen bieden, werkt Movu Robotics continu aan het verbeteren van zijn installaties. Eind 2024 werd de focus gelegd op de beveiligingstechniek bij de toegang tot gangen in het magazijn. Mensen lopen achter het hek namelijk acuut gevaar door geautomatiseerde installaties, bewegende machineonderdelen en transportsystemen zonder bestuurder.

Belangrijkste eisen

De zelfontwikkelde beveiligingstechniek

uit de beginjaren, een nogal grote aansluitkast met complexe bedrading en mechanische sleutels, was verouderd. Veel installatiewerk, zeer weinig flexibiliteit. "Wij zochten een flexibel aanpasbare en toekomstbestendige oplossing die voldoet aan alle veiligheidseisen van EN 528, eenvoudig te installeren en in bedrijf te stellen is", vertelt Renaat Mondelaers, Safety Robotics engineer bij Movu Robotics. Hij somt de belangrijkste eisen op: "De oplossing moest internationaal schaalbaar zijn, ervoor

zorgen dat niemand onopgemerkt de gangen kan betreden en tegelijk verhinderen dat de installatie in de automatische modus start terwijl er personen in de gevarenszone aanwezig zijn. Bovendien moest het mogelijk zijn om bij onderhouds- en reparatiewerkzaamheden gericht afzonderlijke zones uit te schakelen, in plaats van de gehele installatie te moeten stoppen."

EtherCAT- en Profinet-ready

Ronny Slenders, manager Sales & Safety Services bij Euchner Benelux, voegt daaraan toe: "Movu Robotics vond het bovendien belangrijk dat het deursluitstelsel EtherCAT- en Profinet-ready is, in alle intralogistieke installaties van Movu kan worden gebruikt en een functioneel design biedt – tegen dezelfde kosten als de oude oplossing. Daarom stelde ik ons **dreamteam** MGB2 en CKS2 aan Movu Robotics voor. Bij de MGB2 **Modular** zegt de naam het al: dit stelsel is modulair opgebouwd en kan individueel worden vormgegeven." Voor de vereiste flexibiliteit op het gebied van communicatie zorgt de busmodule, die Profinet, EtherCAT (P) en EtherNET/IP ondersteunt. "Ons veel-

CKS2

Het sleutelsysteem CKS2 is geschikt voor het blokkeren en starten van machines en installaties, voor het verstrekken van autorisaties voor het selecteren van een bedrijfsmodus of als sleuteltransfersysteem. Dankzij hooggecodeerde RFID-sleutels biedt het systeem maximale veiligheid. Het kan ofwel afzonderlijk in een installatie als compact systeem met evaluatie-elektronica ofwel apart als submodule in het deursluitstelsel MGB2 *Modular* worden geïntegreerd, waardoor de gebruikers een groot aantal combinatiemogelijkheden hebben. Het CKS2-systeem kan gemakkelijk worden aangepast aan individuele vereisten. Bij het gebruik als blokkeerinzetstuk kan de installatie bijvoorbeeld niet worden gestart zonder sleutel. Dat betekent: de sleutel zit tijdens het bedrijf in het sleutelopnamestation. Voor het stoppen wordt deze eruit gehaald. Pas dan kan een gevaarlijke zone worden betreden.



Het sleutelsysteem CKS2 voor het blokkeren en starten van machines en installaties, verstrekken van autorisaties en het selecteren van een bedrijfsmodus of als sleuteltransfersysteem. Dankzij hooggecodeerde RFID-sleutels biedt het systeem maximale veiligheid.

INSTALLATIE EN INSTELLING BIJ DE KLANT VERLOPEN NU ONGEVEER 60 PROCENT SNELLER

zijdige, codeerbare sleutelsysteem CKS2 completeert het pakket en vervangt de tot nu toe gebruikte mechanische sleutels."

Nieuw beveiligingssysteem

Het basisidee overtuigde, en Movu Robotics koos voor samenwerking met Euchner. "Wij hadden vroeger al goede ervaringen opgedaan met Euchner en de producten", vertelt Tesseur. "Daarom waren wij ervan overtuigd dat we ook hier samen een passende oplossing zouden vinden." Deze inschatting was volkomen juist: in slechts enkele, maar zeer vruchtbare workshops paste een team van experts uit beide bedrijven het nieuwe beveiligingssysteem samen aan de speciale eisen van de magazijnsystemen aan.

De oplossing bestaat uit deurvergrendeling, individueel codeerbare sloten en software in een compacte eenheid. Deze

vervangt de oude aansluitkast. Het systeem kon ook meteen tonen wat het kan: het eerste klantproject was complex en omvatte veiligheidso oplossingen bij in totaal twintig deuren, waarvan veertien voor shuttle-niveaus en zes bij liftsystemen. Binnen enkele maanden was de implementatie geslaagd, ondanks hoge technische eisen en de integratie van talrijke subsystemen.

60 procent sneller

Tesseur is positief: "Nu kunnen de installatie en instelling bij de klant aanzienlijk eenvoudiger en ongeveer 60 procent sneller verlopen." Circa 200 van

deze beveiligingssysteem heeft Movu Robotics inmiddels ingebouwd in installaties in heel Europa. Het project kon alleen worden gerealiseerd omdat van beide kanten oplossingsgericht en als partners is samengewerkt. "Dat was op alle vlakken heel goed. We hebben met volledige inzet samengewerkt om de beste oplossing te creëren", concludeert Tesseur. ●

WWW.EUCHNER.NL

WWW.MOVU-ROBOTICS.COM

Ronny Slenders (Euchner Benelux): "Movu Robotics vond het bovendien belangrijk dat het deursluitsysteem [...] in alle intralogistieke installaties [...] kan worden gebruikt."



Safety en Industrial Security

BESCHERMING VOOR BEDRIJVEN, MACHINES EN PRODUCTEN

Security-incidenten komen niet meer alleen bij IT-systemen, maar steeds vaker ook in de productieomgeving (OT) voor. Gerichte aanvallen en ook onbewuste manipulatie worden beschouwd als incidenten op het gebied van Industrial Security. De taak van Industrial Security bij de productie is om de beschikbaarheid van machines en installaties alsmede de integriteit en vertrouwelijkheid van machinale gegevens en processen te garanderen.

TEKST & BEELD: PILZ

Het belangrijkste beschermingsdoel is echter functionele veiligheid. Als bedrijven immers geen controle meer hebben over hun gegevens, staat niet alleen het bedrijf zelf maar ook de veiligheid van hun medewerkers op het spel: zonder Security geen Safety en zonder Safety geen bescherming van mensen! Binnen de EU is er aandacht voor de toenemende dreiging en is de wet- en regelgeving dienovereenkomstig aangepast: Op bedrijfsniveau zijn in het kader de NIS2-richtlijn maatregelen vereist om een hoog gemeenschappelijk niveau van cyberveiligheid in de EU te waarborgen, bijvoorbeeld door middel van een informatiebeveiligingsmanagementsysteem. De EU-Machineverordening 2023/1230 beschrijft nu voor machines en installaties de bescherming tegen corruptie voor en verlangt Industrial Security-maatregelen voor die onderdelen van de machine die invloed op de functionele veiligheid hebben. De Cyber Resilience Act (CRA) brengt nieuwe security-eisen met zich mee voor producten met digitale elementen. Daartoe behoren ook besturingen, IO-systemen en andere componenten die in machines worden gebruikt. Bedrijven, machines en producten – op elk niveau hebben machinefabrikanten en -exploitanten te maken met verschillende uitdagingen en verschillende wettelijke kaders.

State-of-the-art veiligheid

Ongeacht of de wet- en regelgeving Industrial Security verplicht stelt, zijn er goede redenen om in een vroeg stadium met dit onderwerp aan slag te gaan

Alleen een integrale benadering van Safety en Security waarborgt een uitgebreide bescherming van mens en machine.



en advies in te winnen. Gangbare processen en omstandigheden voor de werking van machines kunnen namelijk manipulatie in de hand werken wanneer ze niet regelmatig onder de loep worden genomen. Een lange levensduur van machines betekent bijvoorbeeld vaak dat de bijbehorende systemen verouderd raken en op een gegeven moment niet meer aan de huidige security-normen voldoen. Deze systemen hebben beveiligingslekken die niet meer kunnen worden gedicht, omdat de aanbieder geen security-updates meer levert. Ook kan de beveiliging tegen schadelijke software vaak niet op de



MEER Plichten VOOR BEDRIJVEN

NIS (Network and Information Security) is een richtlijn van de Europese Unie voor het versterken van de cyberveiligheid. De nieuwe NIS2-richtlijn ((EU) 2022/2555 ... betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie) verplicht aanzienlijk meer bedrijven dan voorheen om in de toekomst risicobeheermaatregelen op het gebied van cyberveiligheid te nemen. NIS2 breidt de sectoren uit met bijvoorbeeld de producerende industrie, waaronder ook machinebouw en fabrikanten van elektrische apparatuur.

Risicoanalyses en veiligheidsconcepten voor informatiesystemen, de bescherming van de toeleveringsketen en de veiligheid van het personeel worden vereist. Ook concepten voor de toegangscontrole en het beheer van installaties horen erbij, evenals verplichte trainingen voor het management. De richtlijn werd eind 2022 aangenomen door het Europees Parlement en de Raad van de EU. Zoals alle EU-richtlijnen is ook NIS2 niet onmiddellijk van kracht en bindend in de afzonderlijke EU-lidstaten, maar moet deze richtlijn door de lidstaten worden omgezet in nationaal recht.

eindapparaten worden geïmplementeerd, omdat deze soms te oud zijn en hun performance daardoor zou verslechteren met als gevolg dat er productieonderbrekingen kunnen optreden.

Stap voor stap naar meer Industrial Security

Uiteindelijk gaat het erom dat de bedrijfsvoering beschermd blijft, maar daarvoor moeten bedrijven verschillende uitdagingen overwinnen: van het identificeren van de geldende wettelijke voorschriften, het detecteren en elimineren van zwakke plekken in systemen en het bewust maken en trainen

van de medewerkers tot de aansluitende implementatie van controles. Aangezien security een zogenaamd “moving target” is, moet bovendien de status van de Industrial Security van de machines regelmatig worden gecontroleerd. Het is belangrijk dat er sprake is van duidelijke verantwoordelijkheden binnen het bedrijf, evenals een systematische aanpak, waaronder het ontwikkelen van de benodigde expertise.

Het automatiseringsbedrijf Pilz heeft zich ingesteld op deze eisen en voor machinefabrikanten en gebruikers een dienstenportfolio op maat samenge- ➤

steld die alle aspecten voor de bescherming van mens en machine omvat. De experts van Pilz kennen de huidige wettelijke en normatieve vereisten en nemen deze mee in hun advies. Om security-kennis in bedrijven te ontwikkelen of te actualiseren, wordt het aanbod aangevuld met trainingen. De praktische uitvoering vindt ook plaats met behulp van Pilz-productoplossingen, zoals het aanbod op het gebied van Identification and Access Management (I.A.M.) voor meer Safety en Industrial Security.

De juiste basis

Om Industrial Security op de eigen machines te garanderen, hebben vakmensen in de machine- en installatiebouw gedegen basiskennis nodig, vooral van wetgeving en geldende normen. De experts van Pilz geven deze knowhow door in de training "Fundamentals of Industrial Security". Deelnemers leren Security-bedreigingen, passende beveiligingsmaatregelen en best practices in de context van machine- en netwerkveiligheid te begrijpen. Hierdoor leren ook beginners op het gebied van security met welke maatregelen ze machines effectief kunnen beveiligen tegen cyberaanvallen en manipulatie bij de machinale productie.

Met de kwalificatie "CESA - Certified Expert for Security in Automation" biedt Pilz een tweedaagse expert cursus aan, die deelnemers diepgaande Security-kennis geeft op basis van de nieuwste normen, met name met betrekking tot de normen IEC 62443 ("Industriële communicatienetwerken - IT-beveiliging voor netwerken en systemen"). Bovendien worden er praktische risicobeperkende maatregelen, zoals toegangscontrole en het verbeteren van de netwerkbeveiliging met technische mid-

delen, alsmede organisatorische maatregelen voor het verminderen van security-risico's behandeld. Deelnemers leren hoe ze de norm correct kunnen toepassen en hoe ze kunnen aantonen dat hun automatiseringssystemen voldoen aan de vereisten voor cyberveiligheid. Als de deelnemers slagen voor het examen, ontvangen ze het wereldwijd erkende TÜV NORD-certificaat "CESA – Certified Expert for Security in Automation".

Theoretische kennis in de praktijk brengen

Voortbouwend op de theoretische basis en de trainingen is de volgende stap in het versterken van Industrial Security het toepassen van gestructureerde, praktijkgerichte processen. Advies ten aanzien van Operational Technology (OT) slaat een brug tussen de theoretische basis en praktijkstrategieën. Met behulp van een gefaseerde aanpak worden in het kader van Industrial Security Services de kwetsbaarheden in complexe systemen geïdentificeerd en maatregelen ontwikkeld om de risico's te minimaliseren, wat uiteindelijk resulteert in een integraal veiligheidsconcept.

Vier stappen voor meer Industrial Security

Het OT-Security-proces omvat vier stappen; analyse van de beschermingsbehoeften, Industrial Security-risicobeoordeling, Industrial Security-concept en Industrial Security-systeemverificatie.

Bij de analyse van de beschermingsbehoeften worden in het bedrijf de beschermingsbehoefte van de afzonderlijke "assets" in de machine of installatie alsmede hun beschermingsdoelen vastgesteld. In de tweede stap, de risicobeoordeling, worden alle risico's en de waarschijnlijkheid van optreden beoor-

ZONDER SECURITY GEEN CE-MARKERING

De Machinerichtlijn 2006/42/EG speelt een belangrijke rol in het kader van de functionele veiligheid. Machinefabrikanten moeten van oudsher een passende conformiteitsbeoordelingsprocedure, eindigend met de CE-markering, doorlopen om machines in Europa te kunnen invoeren.

De in juni 2023 opnieuw als Machineverordening gepubliceerde voorschriften zijn op de huidige stand van de techniek gebracht. De Machineverordening vervangt de huidige Machinerichtlijn en stelt, in tegenstelling tot haar voorganger, cybersecurity verplicht. Waar de Machinerichtlijn uitsluitend

betrekking had op de Safety, is in de Machineverordening ook het beschermingsdoel security opgenomen onder "Protection against corruption" in de "Essential Health and Safety Requirements (EHSR)": de veiligheidsfuncties van een machine mogen niet worden beïnvloed door onopzettelijke of opzettelijke vervalsing.

Deze nieuwe weg naar de CE-markering werpt een aantal nieuwe vragen voor machinefabrikanten en -operators op, omdat ze hun bestaande veiligheidsconcepten voor Safety en Security zullen moeten herzien.

deeld en wel voor elk deel gedurende de complete levenscyclus van het systeem. In de volgende stap wordt een gedetailleerd Industrial Security-concept ontwikkeld, met strategieën en maatregelen voor het afwenden en verminderen van risico's als gevolg van aanvallen, manipulatie en verkeerde bediening. Ook worden er policies, regels en richtlijnen voor de verdere veilige werking of opbouw van het systeem opgesteld. In de laatste stap, de Industrial Security-systeemverificatie, wordt de effectiviteit van de geïmplementeerde tegenmaatregelen gecontroleerd.

Machinebeschikbaarheid waarborgen

Het Industrial Security Services-proces helpt cyberaanvallen te beperken of te voorkomen. Ook het aantal onbedoeld veroorzaakte security-incidenten neemt af. Dit verhoogt de machinebeschikbaarheid en zorgt uiteindelijk voor kostenbesparing en het behoud van de rentabiliteit.

Deze aanpak zorgt er vooral voor dat mensen bij de machine door middel van passende security-maatregelen zijn beschermd. Een security-incident kan namelijk een belemmering voor Safety-maatregelen vormen. Zo zorgt een lichtschermblokkade voor machines er bijvoorbeeld voor dat de operator niet een gevaarzone instapt. Als een hacker echter de bijbehorende besturing en het mechanisme kan beïnvloeden, kan de beschermende functie van het lichtschermblokkade niet meer worden gegarandeerd. Security beveiligd Safety! Bij de concrete uitvoering bij de machine is een gemeenschappelijke benadering van Safety en Security dus zinvol. Want zonder Security geen Safety en zonder Safety geen bescherming van mensen.

Duidelijk geregeld: Wie mag wat bij de machine?

De veiligheid van een machine en haar operators staat of valt met het reguleren van de toegang – voor mensen of netwerken. Ingangen moeten worden beveiligd tegen ongevoegde toegang, zodat er bijvoorbeeld tijdens het bedrijf van de machine geen personen in de gevaarzone aanwezig zijn. Want zelfs het goedbedoeld bedienen of onderhouden van een machine – ter plekke of via een netwerk – zou fatale gevolgen kunnen hebben.

Een belangrijke bouwsteen is het Identification and Access Management (I.A.M.), dat rechten en de toegang op machines en installaties in bedrijven duidelijk regelt. Daartoe behoren organisatorische maatregelen en voorschriften alsmede geschikte veiligheidsfuncties. Een toegangsautorisatiesysteem

SECURITY GEDURENDE DE GEHELE PRODUCTLEVENSCYCLUS

Naast het beoordelen van het bedrijf en de machines is ook het direct implementeren van security-maatregelen in de apparaten (zoals besturingen) absoluut noodzakelijk. In september 2022 presenteerde de Europese Commissie een ontwerp van een verordening die de cyberveiligheid van producten moet vergroten. Deze Cyber Resilience Act (CRA) is gericht op fabrikanten van producten met digitale elementen (hard- en software) die met andere producten kunnen communiceren. Het gaat om producten uit zowel de B2C-sector, zoals smartphones of robotstofzuigers, als de B2B-sector, zoals besturingen en sensoren, maar ook op om pure softwareproducten zoals besturingssystemen of de machine zelf.

De verplichting voor fabrikanten om misbruikte kwetsbaarheden te melden, geldt vanaf 11 september 2026. Producten met digitale elementen moeten vanaf 11 december 2027 voldoen aan de vereisten van de CRA, om in de EU op de markt te kunnen worden gebracht. De CRA is een EU-verordening en wordt daarom onmiddellijk van kracht in de EU-lidstaten.

Hoe groot de impact van de CRA daadwerkelijk zal zijn, hangt af van welke criteria er uiteindelijk worden toegepast voor het classificeren van de producten. Volgens de CRA mogen er alleen nog maar producten op de markt worden gebracht die een passend cyberveiligheidsniveau garanderen – en wel gedurende de gehele levenscyclus van een product. Security begint dus bij de productontwikkeling.

zoals dat PITreader van Pilz is daarbij de juiste productbouwsteen. Hiermee kunnen gebruikers voldoen aan de eisen op het gebied van werknemersbescherming, aansprakelijkheidsbescherming, maximale productiviteit en de bescherming van uw gegevens. Alleen een integrale benadering van Safety en Security waarborgt een uitgebreide bescherming van mens en machine. Of en in welke mate een bedrijf zich met security wil bezighouden, is niet langer iets dat het bedrijf naar eigen inzicht kan bepalen. Het is inmiddels wettelijk voorgeschreven. In de machinebouw is security in de vorm van Industrial Security niet alleen de taak van de IT, maar een integraal onderdeel van het ontwerp en de constructie. Het achteraf implementeren van security is omslachtig en betekent meestal een verlies aan gebruiksvriendelijkheid, functionaliteit en productiviteit. ●

WWW.PILZ.NL

Geen CE-markering, geen markt

WAAROM DE CYBER RESILIENCE ACT DE EUROPESE PRODUCTMARKT VERANDERT

Blokkeert de Cyber Resilience Act de toegang tot de Europese markt? Ja — voor elk product dat niet voldoet. De Cyber Resilience Act (EU 2024/2847) is sinds december 2024 van kracht en stelt voor het eerst uniforme cybersecurityeisen aan elk product met digitale elementen dat op de Europese markt wordt gebracht. Geen richtlijn die lidstaten naar eigen inzicht invullen, maar een verordening: rechtstreeks bindend, zonder omzetting. (Deel I van III).

MARCEL DEPRÉ, TECHNOLOGIECONSULTANT | EU-CYBER-LAWS.COM

De reikwijdte is breder dan veel fabrikanten denken. Niet alleen routers en laptops: ook industriële controllers, embedded systemen, slimme sensoren en elk apparaat met ook maar één digitale interface vallen onder de wet. Wat de CRA onderscheidt van eerdere productregels is de sanctie: geen CE-markering betekent geen toegang tot de Europese markt. De details — en de valkuilen — leest u hierna.

Geen CE-markering, geen markt

Je maakt een product met digitale componenten. Een sensor, een controller, een machine, een softwarepakket dat draait op hardware van een ander. Misschien denk je: “Mijn product hangt niet aan een netwerk, dus dit geldt niet voor mij.” Fout.

Elke fysieke poort is een digitale voordeur. Of er nu een kabel in zit of niet: de aanwezigheid van de interface bepaalt de wetgevingsplicht.

- *Vanaf december 2027 is de regel simpel: geen geldige CE-markering onder de CRA, geen plek op de Europese markt. Geen genadeperiode. Geen boete en doorgaan. Uw product is geblokkeerd.*

Dat is een fundamenteel ander risico dan fabrikanten gewend zijn. Bij eerdere productregels eindigde een overtreding vaak met een boete of een correctieperiode. Bij de CRA is het eindspel marktblokkering. De route naar CE-markering is geen administratieve horde, maar een technisch mijnenveld waar veel transitieplannen op vastlopen.

OVER DE AUTEUR

Marcel Depré is specialist op het snijvlak van industriële software en Europese cybersecuritywetgeving. Hij helpt organisaties de kloof te overbruggen tussen technische ontwikkeling en EU-compliance, met specifieke expertise in IEC 62443 en de Cyber Resilience Act. Als oprichter van eu-cyber-laws.com ondersteunt hij bedrijven bij het toepassen van actuele cyberwetgeving binnen industriële omgevingen. Wilt u verder de diepte in? Vanaf 12 mei 2026 verzorgt Marcel modulaire CRA-trainingen bij Mikrocentrum, afgestemd op uw rol.

eu-cyber-laws.com

Wat valt er precies onder de CRA?

De CRA is van toepassing op ‘producten met digitale elementen’. Dat is een bewust brede categorie. Het omvat hardware met ingebbede software, standalone software, softwarecomponenten die als onderdeel van een groter systeem worden geleverd, en digitale diensten die direct verbonden zijn met een product.

Er zijn vrijstellingen, maar die zijn smaller dan velen denken. Open-source software die commercieel wordt gedistribueerd valt gewoon onder de CRA. Software-as-a-Service valt er grotendeels buiten, maar een *on-premise* software-product met dezelfde functionaliteit valt er volledig onder. Producten die uitsluitend voor defensie of nationale veiligheid



De Cyber Resilience Act is geen papierwerk, het is engineering.

worden ontwikkeld zijn uitgezonderd — een commercieel product dat ook door overheden wordt gebruikt is dat niet automatisch.

Daarbij geldt: de conformiteitsverplichting stopt niet bij de eigen code. Fabrikanten zijn verantwoordelijk voor de cybersecurity van het volledige product — inclusief de software van hun leveranciers die daarin is opgenomen.

De praktische vraag voor fabrikanten is niet “valt ons product er wel onder?” maar “welke categorie?” De CRA maakt onderscheid tussen standaardproducten, Klasse I- en Klasse II-producten. Die indeling bepaalt uitsluitend wie de conformiteit mag beoordelen — niet welke eisen gelden. De essentiële cybersecurityvereisten uit Annex I zijn identiek voor elk product, ongeacht de klasse.

Voor fabrikanten van industrieel automatiseringsmateriaal, netwerkapparatuur of beveiligingsgerelateerde componenten is de kans groot dat het product in Klasse I of II valt. Wat verschilt is de beoordelingsroute: een aangemelde instantie (NoBo, van het Engelse *Notified Body*) moet de

DE BOETES ONDER DE CRA

Overtreding	Maximale boete
Non-conform product op de EU-markt brengen	€ 15 mln / 2,5% omzet
Tekortkomingen in vulnerability handling & rapportage	€ 10 mln / 2,0% omzet
Onjuiste of misleidende informatie aan toezichthouders	€ 5 mln / 1,0% omzet

Een boete doet pijn. Maar de echte sanctie is marktblokkering: een product zonder geldige CE-markering mag na december 2027 simpelweg niet meer worden verkocht in de EU.

conformiteit verifiëren, en dat traject begint niet in 2027.

CYBER RESILIENCE ACT

Regelgeving: EU Verordening 2024/2847	Meldplicht actief: 11 september 2026	Volledige conformiteit: 11 december 2027
Van toepassing op: Alle producten met digitale elementen op de EU-markt	Boete bij overtreding: Tot € 15 mln of 2,5% wereldwijde omzet	Toezichthouder NL: RDI (Rijksinspectie Digitale Infrastructuur)

De wachtlijsten bij NoBo's: begin nu

De capaciteit van NoBo's is eindig. CRA-specifieke accreditatie staat in veel EU-lidstaten nog in de kinderschoenen. Wanneer de deadline van december 2027 nadert, kloppen duizenden fabrikanten tegelijkertijd aan bij een kleine groep instanties. Dit is geen speculatie: de medische sector worstelt nog steeds met achterstanden van meerdere jaren na de invoering van de Verordening Medische Hulpmiddelen (MDR) — NoBo's sloten hun wachtlijsten, fabrikanten konden geen beoordeling meer inplanen. De CRA genereert een grotere golf — in een kortere tijdspanne.

Safety Integrated Machine safety is a must

SIEMENS



NET DAT BEETJE EXTRA - VOOR EEN DUURZAME EN VEILIGE TOEKOMST

WE HELPEN JE GRAAG MET:

- ATEX
- CE-markering
- Drukvasen en drukapparatuur
- Risico-inventarisatie & -evaluatie

Bezoek onze stand op het
Engineering Safety Event.

CONTACT? 088 220 1400

tcpm.nl

**WE LOVE
ENGINEERING**

TCPM INGENIEURS
& ADVISEURS

KLASSE-INDELING ONDER DE CRA

De CRA verdeelt producten in drie categorieën. De indeling bepaalt uitsluitend de conformiteitsroute — niet de inhoudelijke eisen. Annex I geldt voor alle producten gelijk.

Standaardproducten vormen de grootste categorie. Self-assessment is toegestaan, mits onderbouwd met een volledig technisch dossier en, zodra beschikbaar, geharmoniseerde normen.

Klasse I omvat producten waarbij een kwetsbaarheid een aanzienlijk risico vormt: identiteits- en toegangsbeheersystemen, browsers, wachtwoordbeheerders, beveiligingssoftware, netwerk-scanners. Self-assessment is mogelijk op basis van geharmoni-

seerde normen of door een NoBo goedgekeurde specificaties. Zijn die normen nog niet beschikbaar, dan is een NoBo verplicht.

Klasse II omvat producten met het hoogste risicoprofiel: besturingssystemen voor servers, industriële besturingssystemen, firewalls, routers, switches en geavanceerde beveiligingsproducten. Zelfbeoordeling is uitgesloten — NoBo-beoordeling is altijd verplicht.

Een veelgemaakte misvatting: “Wij zijn Klasse I, dus onze eisen zijn zwaarder.” Onjuist. De essentiële cybersecurityvereisten uit Annex I zijn identiek voor elk product. Alleen de route naar CE-markering verschilt.

- *Fabrikanten van Klasse I- en Klasse II-producten die in 2026 nog geen NoBo hebben gecontracteerd, lopen een reëel risico hun product niet op tijd beoordeeld te krijgen.*

De voorbereiding vergt bovendien tijd die los staat van de wachtrij. Een hiënanalyse, het samenstellen van het technisch dossier, de interne beoordeling en het oplossen van tekortkomingen: voor een gemiddeld complex product duurt dat drie tot zes maanden. Het startpunt is nu, niet begin 2027.

DIRECT AAN DE SLAG: GRATIS TOOLS OP EU-CYBER-LAWS.COM

Tool	Omschrijving
Gap Analysis	Ontdek waar uw organisatie staat ten opzichte van de CRA-vereisten.
Product Checker	Controleer of uw product onder de CRA valt en in welke klasse het valt.
Risico-classificatie	Bepaal de risicoklasse van uw product en de bijbehorende verplichtingen.
Compliance Checklist	Stapsgewijze checklist om uw CRA-implementatie te volgen en te delen.
CRA Overzicht	Uitgebreid overzicht van de Cyber Resilience Act in begrijpelijk Nederlands.
Compliance Scan	Brede scan over CRA, NIS2, GDPR en andere EU-cyberwetten.

Bestaande producten: geen automatische vrijstelling

Een veelgehoorde misvatting: de CRA geldt alleen voor nieuwe producten die na december 2027 op de markt komen. Dat is onjuist. De CRA kent geen automatische vrijstelling voor bestaande producten — er is geen overgangsregeling die producten die vóór de deadline zijn ontworpen of gelanceerd buiten schot houdt. De CRA geldt voor elk product dat ná die datum op de EU-markt beschikbaar wordt gesteld, ongeacht wanneer het ontworpen of eerder gelanceerd werd. Een product dat al jaren wordt verkocht en na december 2027 gewoon in de webshop staat, moet CRA-conform zijn.

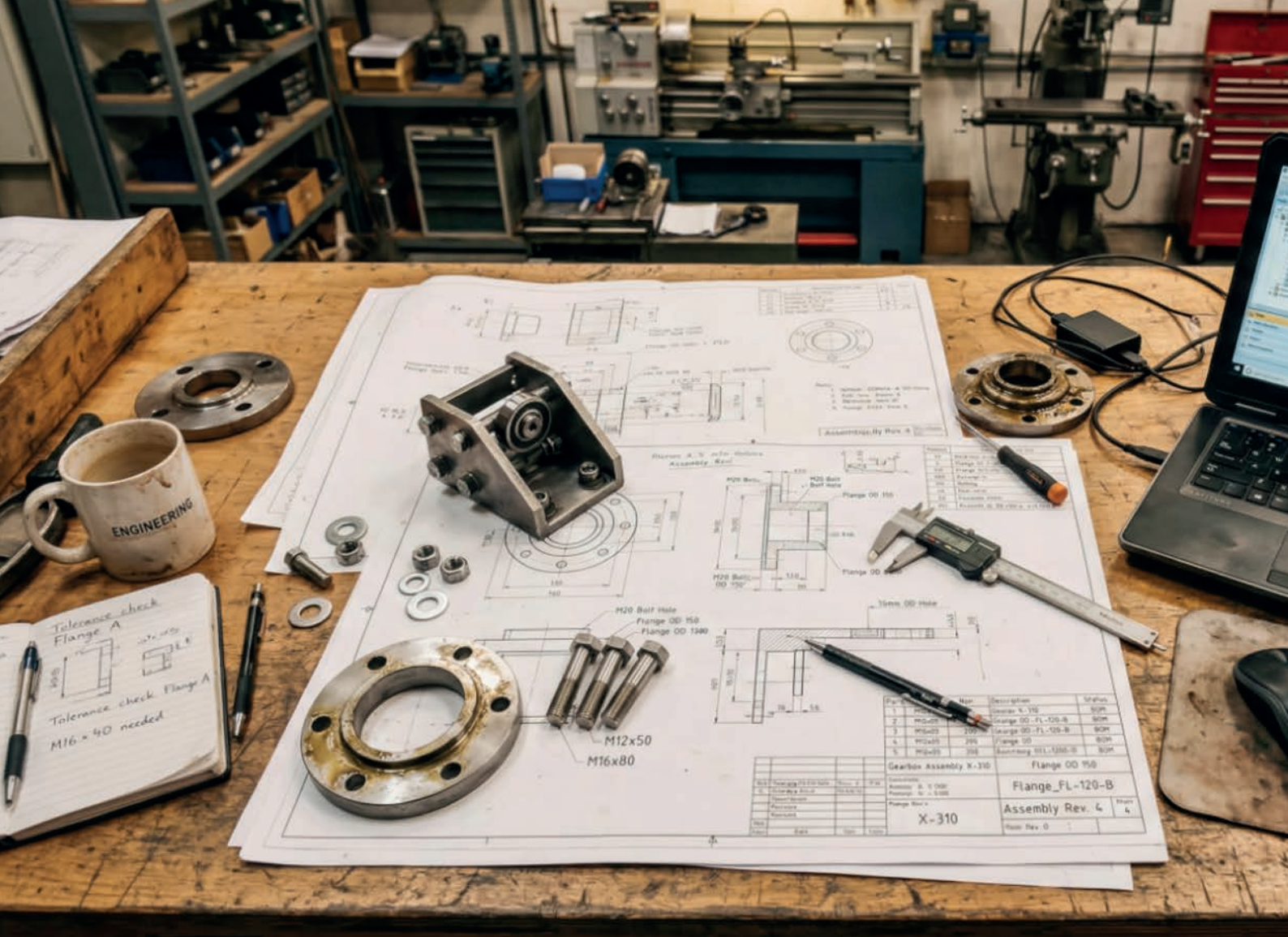
- *Fabrikanten die hun bestaande productcatalogus niet hebben geëvalueerd lopen het risico hun eigen producten na december 2027 niet meer legaal te kunnen verkopen.*

CRA is geen papierwerk, het is engineering

De CRA vraagt om werkende systemen, niet om beschreven systemen. Documentatie is noodzakelijk, maar documentatie die op de werkelijkheid vooruitloopt is een aansprakelijkheid, geen bescherming.

De tijdlijn is strakker dan de meeste organisaties beseffen. De meld- en responsvereisten gelden al vanaf 11 september 2026. De wachtrijen bij NoBo's beginnen nu al te vormen. En de producten die in 2027 worden geblokkeerd zijn niet van bedrijven die de CRA niet kenden, ze zijn van bedrijven die haar reduceerden tot een documentatieproject. ●

Vanaf 11 september 2026 gelden de eerste operationele verplichtingen van de CRA. In het volgende artikel in dit drieluik (Constructeur 3, 2026) kijken we naar de processen die organisaties vóór die datum operationeel moeten hebben — en wat het kost als ze dat niet zijn.



SAFETYWIJZER 2026

Digitaal Product Paspoort en ESPR

OOK DE MACHINE IS EEN DATASET

Stel je voor: je levert een machine op bij een klant. De installatie draait, de CE-verklaring is getekend, de documentatie overhandigd. En dan komt de vraag: "Welke materialen zitten er precies in deze machine? Waar komen de grondstoffen vandaan? En wat moet er gebeuren als we hem over vijftien jaar willen ontmantelen?"

TEKST EN BEELD: ANNE RADEMAKER EN MARTIN DE JONG (EMPACT)



Elke machine is tegenwoordig ook een dataset. Welke materialen zitten erin? Welke componenten zijn toegepast? Is die informatie later nog terug te vinden?

ONDERWERP	MACHINEVERORDENING	ESPR
Hoofddoel	Veiligheid en CE-conformiteit	Duurzaamheid en circulariteit
Type informatie	Technische documentatie, gebruiksinstructies	Productinformatie over volledige levenscyclus
Vorm	Digitaal beschikbaar (o.a. online, QR)	Digital Product Passport (gestructureerde dataset)
Inhoud	Veiligheid, gebruik, conformiteit	Materialen, substances of concern, gebruik, end-of-life
Beschikbaarheid	Minimaal 10 jaar toegankelijk	Beschikbaar voor meerdere partijen (keten, gebruiker, autoriteiten)
Traceerbaarheid	Identificatie (type, serie, fabrikant)	Traceability over hele waardeketen

Machineverordening en ESPR: de verschillen en de overlap.

Dit soort vragen is niet nieuw, maar de frequentie en de diepgang ervan wel. Ze komen allang niet meer alleen van auditors. Klanten stellen ze, inkopers stellen ze, en steeds vaker staan ze gewoon in de aanbesteding. Wat opvalt: die vragen stoppen niet bij oplevering. Ze blijven terugkomen. Tijdens gebruik, bij onderhoud, bij een retrofit. Je levert een machine misschien één keer op, maar de informatie erover moet jarenlang beschikbaar blijven.

Dat heeft gevolgen voor het vak. Je bent niet meer alleen verantwoordelijk voor wat je maakt, maar ook voor de informatie die daarbij hoort. Twee Europese kaders versterken die verschuiving: de Machineverordening (Verordening (EU) 2023/1230) en de Ecodesign for Sustainable Products Regulation (ESPR).

Machine een dataset

Elke machine is tegenwoordig ook een dataset. En die dataset moet kloppen. Waar documentatie vroeger bestond uit handleidingen, technische dossiers en losse pdf-bestanden, verschuift dit naar

gestructureerde, voor een machine leesbare informatie die gekoppeld is aan het product en beschikbaar blijft over de volledige levensduur. De map op de gedeelde schijf maakt plaats voor informatie die vindbaar, actueel en uitwisselbaar moet zijn.

Dat klinkt als een IT-verhaal, maar het begint gewoon bij engineering. Welke materialen zitten erin? Welke componenten zijn toegepast? Is die informatie later nog terug te vinden? Het wordt vooral zichtbaar op momenten dat je die informatie nodig hebt. Bij een retrofit, een storing of een audit. Dan blijkt hoe lastig het kan zijn om de juiste gegevens boven tafel te krijgen. Verschillende versies, verouderde documenten, ontbrekende specificaties: het zorgt voor vertraging, fouten en frustratie. Niet alleen de machine moet kloppen, maar ook de informatie erachter.

Machineverordening en ESPR

In de praktijk komen twee ontwikkelingen samen die voorheen gescheiden werelden waren. Aan de ene kant veiligheid

en CE-conformiteit. Aan de andere kant duurzaamheid en productinformatie over de hele levenscyclus. Voor constructeurs en engineers betekent dit dat ontwerp, documentatie en regelgeving steeds meer één geheel worden. Dat gebeurt onder invloed van de Machineverordening en de ESPR; de verschillen en overlap zie je in de tabel.

De ESPR maakt duurzaamheid iets wat je moet kunnen aantonen op productniveau. Denk aan materiaalgebruik, herkomst, reparatiebaarheid en wat er aan het einde van de levensduur gebeurt. Daarvoor introduceert de ESPR het Digital Product Passport (DPP): een digitale set productinformatie die gekoppeld is aan het product. In de praktijk lijkt dit op een uitgebreid technisch dossier, maar dan gestructureerd, toegankelijk en bedoeld om gedurende de hele levenscyclus actueel te blijven.

Tegelijkertijd vraagt de Machineverordening al dat documentatie digitaal beschikbaar is en jarenlang toegankelijk blijft. De overlap is duidelijk: beide kaders draaien om betrouwba-

re, vindbare productinformatie. Dat klinkt als extra administratie, maar in de praktijk valt dat mee. Veel van de benodigde informatie is er al, maar zit verspreid over systemen, documenten en afdelingen. Door die informatie beter te structureren en aan je product te koppelen, ontstaat inzicht in je eigen ontwerp en keten. Denk aan beter zicht op leveranciers, sneller kunnen inspelen op service en onderhoud, of het koppelen van reserve-onderdelen en garantie-informatie aan één centrale plek.

Ontwerp moet ook uitlegbaar zijn

De verschuiving wordt als eerste zichtbaar in de ontwerpfase. Traditioneel draait het daar om functionaliteit, veiligheid, kosten en maakbaarheid. Dat blijft zo. Maar er komt iets bij: de informatiewaarde van het ontwerp.

Ontwerpkeuzes bepalen hoe een machine werkt, maar ze bepalen óók welke informatie later beschikbaar is en hoe bruikbaar die is. Welke materialen gebruik je, en kun je die herleiden tot de leverancier? Kies je voor een gesloten constructie of een modulair ontwerp? Hoe eenvoudig zijn onderdelen te vervangen? Wat is de impact van geïntegreerde software en updates op de levensduur?

Dat zijn geen theoretische vragen. Ze raken aan keuzes die je nu al maakt. Een gelijmde verbinding kan constructief optimaal zijn, maar maakt demontage en recycling lastig. Een geschroefde verbinding is minder elegant, maar wel beter te demonteren. Een modulair ontwerp maakt onderhoud eenvoudiger, maar kan extra kosten en complexiteit met zich meebrengen. De consequentie: engineering bepaalt met het ontwerp ook welke informatie er later over het product beschikbaar is.

Stuklijst niet meer genoeg

In de realisatiefase wordt pas echt duidelijk hoe groot de verandering is. Een stuklijst in je ERP alleen is niet meer voldoende. Naast componenten moet ook informatie worden vastgelegd over materiaalsamenstelling, leveranciers en herkomst, gebruiks- en onderhoudsinstructies, en eigenschappen zoals reparerbaarheid en verwachte levensduur. Die informatie komt uit verschillende hoeken van de organisatie. De construc-



Een veelgehoorde zorg is dat het DPP leidt tot ongewenste openbaarmaking van leveranciersdata of constructieve details. Alleen markttoezichtautoriteiten hebben toegang tot de volledige dataset.

teur bepaalt het ontwerp, inkoop kent de leveranciers, productie weet wat er daadwerkelijk is toegepast en service bouwt kennis op tijdens gebruik. Het samenbrengen van die informatie blijkt in de praktijk vaak lastiger dan gedacht. Ook de vorm verandert. Waar voorheen werd gewerkt met statische documenten en pdf's, verschuift dit naar gestructureerde data. Informatie moet beschikbaar zijn, maar tegelijk leesbaar voor systemen en uitwisselbaar met ketenpartners. Data moet gestructureerd, actueel en te koppelen zijn. Precies wat nodig is voor het Digital Product Passport.

Niet elk product vraagt overigens om dezelfde mate van detail. Voor standaardcomponenten kan één dataset gelden voor een hele productiebatch. Voor machines ligt dat anders. Variaties in configuratie, gebruik en onderhoud zorgen ervoor dat elke machine een eigen geschiedenis opbouwt. In die gevallen is een individueel paspoort nodig dat

meegroeit met het product. In de praktijk ontstaat vaak een combinatie: basisinformatie op batchniveau, aanvullende informatie per individuele machine.

Vertrouwelijkheid

Een veelgehoorde zorg is dat het DPP leidt tot ongewenste openbaarmaking van leveranciersdata of constructieve details. De ESPR houdt hier rekening mee via verschillende toegangsniveaus. De exacte invulling wordt nog nader bepaald, maar de richting is helder. Consumenten zien basisinformatie. Professionele partijen krijgen toegang tot gedetailleerde materiaaldata. Recyclers ontvangen demontage-instructies. Alleen markttoezichtautoriteiten hebben toegang tot de volledige dataset. Concurrentiegevoelige informatie hoeft dus niet publiekelijk gedeeld te worden.

Impact raakt de hele organisatie

Het DPP is geen los IT-project, maar iets dat dwars door de hele organisatie



"HET DIGITAL PRODUCT PASSPORT DWINGT JE OM NAAR JE HELE KETEN TE KIJKEN. EN DAAR ZIT METEEN DE GROOTSTE UITDAGING, MAAR OOK DE **MEESTE WINST**"

BART KROESBERGEN, JOOP VAN ZANTEN STAALSERVICE BV

loopt. Een groot deel van de benodigde informatie zit bovendien buiten de eigen organisatie: materiaalherkomst, componentdata, informatie over stoffen. Dat betekent dat leveranciers naast producten ook data moeten leveren. En dat die data betrouwbaar en bruikbaar moet zijn. Dit wordt structureel onderdeel van inkoopafspraken en samenwerkingsovereenkomsten.

'We hebben nog niets'

Voor veel machinebouwers voelt het DPP als een grote opgave. Begrijpe-

lijk, maar in de praktijk klopt dat beeld niet. Een aanzienlijk deel van de benodigde informatie is al aanwezig. Denk aan technische dossiers, CE-documentatie, REACH-informatie, leverancierscontracten en materiaalspecificaties.

Het probleem is meestal niet dat data ontbreekt, maar dat die verspreid zit: in het ERP-systeem, in e-mails naar leveranciers, in bestanden op een gedeelde schijf, in de hoofden van collega's. De eerste stap is daarom eenvoudig: welke data is er al? Waar staat die?

In welke vorm? En wat ontbreekt er nog? Pas daarna komt de vraag hoe je die informatie structureert en aanvult.

Tijdslijn

Voor machinebouwers lopen twee tijdslijnen naast elkaar. De Machineverordening ligt vast. De hoofdregels gelden vanaf 14 januari 2027. De richting is duidelijk: documentatie moet digitaal, beter toegankelijk en langdurig beschikbaar zijn.

De ESPR werkt anders. Daar worden eisen per productgroep verder ingevuld via zogenaamde gedelegeerde handelingen. Het eerste werkplan laat zien welke productgroepen de komende jaren prioriteit krijgen.

Het Digital Product Passport speelt in beide trajecten een centrale rol. Wachten tot alle details bekend zijn is geen verstandige strategie. Niet omdat alles al vastligt, maar omdat het op orde brengen van productdata, documentatie en keteninformatie in de praktijk veel tijd kost. Wie nu begint met inventariseren, heeft straks een voorsprong.

DPP-tool: eenvoudig inventariseren

Om machinebouwers op weg te helpen heeft Empact een gratis AI-tool ontwikkeld. De DPP-tool analyseert bestaande technische productdocumentatie en vertaalt deze naar een gestructureerde DPP-opzet. Tegelijkertijd wordt automatisch een GAP-analyse opgesteld: welke informatie is er al en wat ontbreekt er nog? Zo krijg je direct inzicht in je huidige dataniveau en kun je gericht aan de slag.

Wat betekent dit voor jouw werk?

Het vak verbreedt. Naast functionaliteit en veiligheid worden ook transparantie en levenscyclusinformatie onderdeel van ontwerp en realisatie. Het product dat je vandaag ontwerpt, moet over tien of twintig jaar nog uitlegbaar zijn.

Dat vraagt om andere keuzes, andere samenwerking met leveranciers en soms ook andere prioriteiten in het ontwerpproces. Wie daar nu al rekening mee houdt, merkt dat het Digitaal Product Paspoort geen extra last wordt. Het is dan gewoon een bijproduct van goede engineering. ●

EMPACT.NU