



## ► Industrial Security

Een whitepaper voor fabrikanten en exploitanten van machines over hoe om te gaan met de huidige EU-wetgeving

Whitepaper  
Versie: April 2025

**PILZ**  
THE SPIRIT OF SAFETY

## Disclaimer

We hebben ons whitepaper zeer zorgvuldig samengesteld. Het bevat informatie over de huidige interpretatie van Pilz van de nieuwe EU-Machineverordening, de NIS-2-richtlijn en de Cyber Resilience Act. Wij hebben alle informatie volgens de huidige stand van kennis en interpretatie en naar eer en geweten verstrekt. Toch zijn wij niet aansprakelijk voor de juistheid en volledigheid van de gegevens, voor zover ons geen grove nalatigheid verweten kan worden, omdat ondanks alle zorgvuldigheid fouten niet volledig vermeden kunnen worden. In het bijzonder hebben de gegevens niet de juridische kwaliteit van toezeggingen of toegezegde eigenschappen. Wij houden ons aanbevolen voor opmerkingen over eventuele onjuistheden.

## Auteursrecht

Alle rechten op deze publicatie zijn voorbehouden aan Pilz GmbH & Co. KG. Technische wijzigingen voorbehouden. Voor bedrijfsintern gebruik mogen kopieën worden gemaakt. De gebruikte product-, handels- en technologieaanduidingen zijn handelsmerken van de betreffende firma's.

Pilz GmbH & Co. KG  
Felix-Wankel-Straße 2  
73760 Ostfildern, Duitsland

© 2025 by Pilz GmbH & Co. KG, Ostfildern  
2. Herziene editie

## In één oogopslag

De term Industrial Security heeft vele facetten en dit whitepaper beschrijft de belangrijkste kernpunten voor machinefabrikanten en -exploitanten. Het doel is om het voor zowel fabrikanten als exploitanten gemakkelijker te maken om met het onderwerp aan de slag te gaan om de nieuwe vereisten te begrijpen en ermee om te gaan.

De whitepaper beschrijft de wettelijke situatie in Europa, geeft een overzicht van de technische basisprincipes, beschrijft de belangrijkste punten voor machinefabrikanten en machine-exploitanten en verwijst naar verdere aanbiedingen voor onze klanten.

In Europa zijn de afgelopen maanden talloze uitgebreide wetteksten verschenen die een directe invloed op de machinebouw hebben:

- ▶ De **Machineverordening** (EU) 2023/1230 stelt nieuwe eisen aan machines, zoals bescherming tegen beschadiging.
- ▶ De **EU-richtlijn over maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau** in de Unie (NIS 2) 2022/2555 vereist voor veel bedrijven een Information Security Management System.
- ▶ De **Cyber Resilience Act** (EU) 2024/2847, definieert vereisten voor producten met digitale elementen, die meestal ook machines omvatten.

Bij de uitvoering van de wetgeving zijn enkele normen en termen van groot belang:

- ▶ Op het gebied van informatiebeveiliging in de industriële omgeving heeft zich de normenfamilie **IEC 62443** ingeburgerd.
- ▶ Het **Security Level** van 0 tot 4 beschrijft de mogelijkheden van de aanvaller.
- ▶ Industrial Security is een continue opgave, daarom zijn naast technische maatregelen ook organisatorische maatregelen onmisbaar. Een **Information Security Management System** (ISMS) helpt hierbij en wordt voor veel bedrijven verplicht.

Machinefabrikanten hebben te maken met verschillende wettelijke vereisten en bewegen zich tussen de specificaties van exploitanten en het aanbod van componentenfabrikanten. Hier zal de machinefabrikant een bemiddelende rol moeten spelen om conforme en kwalitatief hoogwaardige producten te kunnen blijven aanbieden.

Ook de exploitanten van machines zullen in de toekomst moeten nadenken over het beveiligen van hun machines. Om een overzicht te krijgen, is het een goed idee om een systematische risicoanalyse uit te voeren en de kwetsbaarheden efficiënt te sluiten.

Pilz GmbH & Co. KG biedt verdere trainingen en diensten op dit gebied aan.

## De auteur



**Matthias Kuczera** heeft na zijn studie werktuigbouwkunde een uitgebreide kennis opgedaan van machineveiligheid in verschillende industriële sectoren.

Als ontwikkelingsingenieur voor sensoren heeft hij diepgaande kennis opgedaan van de implementatiemogelijkheden van functionele veiligheidseisen.

Tijdens zijn werk als expert op het gebied van transporttechniek was hij verantwoordelijk voor het uitvoeren van typekeuringen van veiligheidscomponenten bij een aangemelde instantie.

In zijn huidige functie als vakkundig expert “Functionele Veiligheid – Normen” bij Pilz is hij actief in normcommissies en houdt hij toezicht op het normbeheer.

Zijn verantwoordelijkheden omvatten:

- ▶ Deelname aan normcommissies voor machineveiligheid
- ▶ De beoordeling van nieuwe wettelijke vereisten
- ▶ De implementatie van interne trainingen

## Pilz – the Spirit of Safety in Digital Automation

Bij alles wat we doen, maken we de wereld veiliger. Als wereldwijde aanbieder van producten, systemen en diensten voor de automatiseringstechniek kan Pilz terugkijken op een succesverhaal van meer dan 75 jaar: De in 1948 opgerichte Pilz-groep heeft tegenwoordig ongeveer 2500 medewerkers in 42 dochterondernemingen en vestigingen. De in Ostfildern gevestigde expert op het gebied van machineveiligheid creëert met zijn complete automatiseringsoplossingen wereldwijd veiligheid voor mens, machine en milieu. Het portfolio van de technologieleider omvat sensor-, regel- en aandrijftechnologie, alsmede systemen voor industriële communicatie, diagnostiek en visualisatie. Een internationaal dienstenaanbod met advies, engineering en trainingen completeert het spectrum. De oplossingen voor Safety en Security worden niet alleen gebruikt in de machine- en installatiebouw, maar ook in tal van andere bedrijfstakken, zoals intralogistiek, spoorwegtechniek en robotica.

# Inhoud

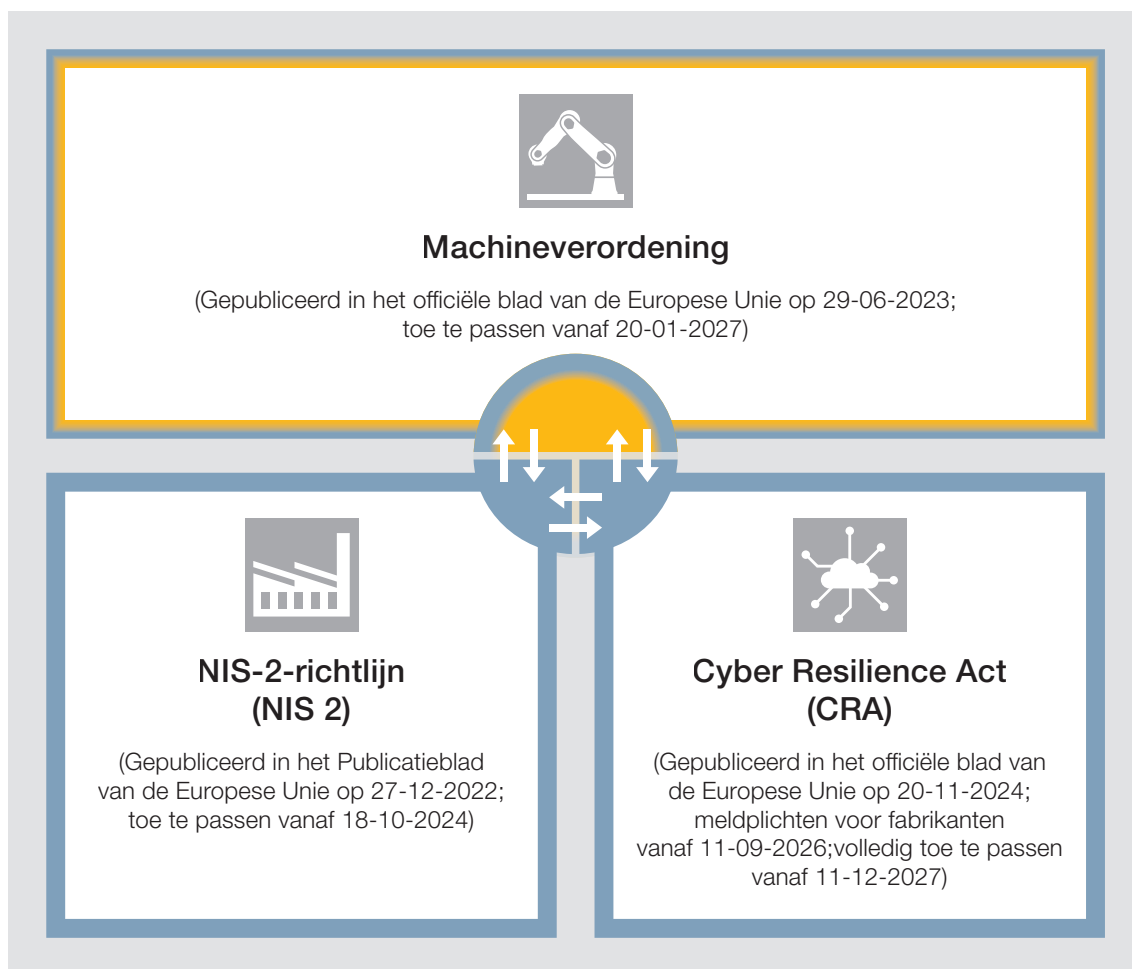
<b>In één oogopslag .....</b>	<b>3</b>
<b>1. De juridische situatie in Europa .....</b>	<b>6</b>
1.1. Machineverordening (EU) 2023/1230 .....	7
1.2. De NIS-2-richtlijn (EU) 2022/2555 .....	8
1.3. Cyber Resilience Act (EU) 2024/2847 .....	9
1.4. Richtlijn 2009/104/EG betreffende de bescherming van de veiligheid en de gezondheid bij het gebruik van arbeidsmiddelen.....	11
<b>2. Security voor machinefabrikanten .....</b>	<b>12</b>
2.1. Security in de Machineverordening .....	12
2.2. Tussen componentenfabrikanten en klanten.....	14
2.3. Cyber Resilience Act voor machinefabrikanten .....	15
<b>3. Security voor machine-exploitanten .....</b>	<b>17</b>
3.1. Omgang met bestaande installaties .....	17
3.2. Van IT-Security naar bedrijfsbrede Security .....	19
<b>4. De weg naar een veilige machine – Safe en Secure.....</b>	<b>20</b>
<b>5. Safety en Security uit één hand.....</b>	<b>22</b>
<b>6. Samenvatting en vooruitzichten .....</b>	<b>24</b>
<b>7. Bijlage .....</b>	<b>26</b>
7.1. Termen op het gebied van Industrial Security .....	26
7.2. IEC 62443 – Basisnorm voor Industrial Security .....	27
7.2.1. Overzicht.....	27
7.2.2. Security Level (SL).....	28
7.2.3. Information Security Management System (ISMS) .....	29
7.3. Andere belangrijke documenten voor machinefabrikanten en -exploitanten.....	30
7.4. Netwerksegmentatie met behulp van het Purdue-model.....	31
<b>8. Literatuur .....</b>	<b>33</b>

# 1. De wettelijke situatie in Europa

Nieuwe technologieën brengen kansen en risico's met zich mee. Waarschijnlijk de belangrijkste innovaties in onze branche op dit moment zijn de hoge mate van netwerkvorming van machines via het Internet of Things, kunstmatige intelligentie en robotica.

Met de netwerkvorming van bedrijven en machines neemt het risico toe dat kwetsbaarheden in informatiesystemen worden uitgebuit en economische en fysieke schade optreedt. In de afgelopen jaren is er bijvoorbeeld een toename geweest van gevallen van succesvolle cyberaanvallen op bedrijven, die miljarden dollars aan schade veroorzaken. Statista.com schat dat in 2023 wereldwijd ongeveer 8,15 biljoen dollar aan schade is veroorzaakt door cyberaanvallen. Alleen al in Duitsland bedroeg het in 2023 iets minder dan 206 miljard euro, wat overeenkomt met ongeveer 5 procent van het bruto binnenlands product.

Om de risico's te beperken, heeft de Europese wetgever nieuwe regelgeving in het leven geroepen. Voor de machinebouw is dit in wezen de machineverordening, de NIS-2-richtlijn (NIS 2) en de Cyber Resilience Act (CRA). Ze maken Industrial Security verplicht. De omgang met bestaande machines en installaties wordt beschreven in Richtlijn 2009/104/EG betreffende de bescherming van de veiligheid en de gezondheid bij het gebruik van arbeidsmiddelen.



Afbeelding 1: Weergave van een uittreksel van nieuwe wetsvoorstellen waarin de eisen voor Industrial Security worden beschreven

	<b>Machineverordening (EU) 2023/1230</b>	<b>NIS-2-richtlijn (EU) 2022/2555</b>	<b>Cyber Resilience Act (EU) 2024/2847</b>
<b>Gericht op</b>	Machines	Ondernemingen	Componenten
<b>Aangenomen op</b>	29-06-2023	27-12-2022	20-11-2024
<b>Verplicht vanaf</b>	20-01-2027	18-10-2024	11-12-2027
<b>Plichten</b>	<ul style="list-style-type: none"> <li>▶ Bescherming tegen corrumperen (met de nadruk op functionele veiligheidsfuncties)</li> <li>▶ Inachtneming van kwaadwillige pogingen van derden</li> </ul>	<ul style="list-style-type: none"> <li>▶ Maatregelen voor risicobeheer op het gebied van cyberbeveiliging</li> <li>▶ Naleving van technische en organisatorische maatregelen</li> <li>▶ Melden van significante beveiligingsincidenten</li> </ul>	<ul style="list-style-type: none"> <li>▶ Meldplichten voor de fabrikanten vanaf 11-09-2026</li> <li>▶ Secure Development Lifecycle Process</li> <li>▶ EU-typeonderzoek voor kritieke producten</li> <li>▶ Meldingen van kwetsbaarheden</li> <li>▶ Beschikbaarstelling van veiligheidsupdates</li> </ul>

Tabel 1: Overzicht Machineverordening, NIS-2-richtlijn en Cyber Resilience Act in vergelijking

### 1.1. Machineverordening (EU) 2023/1230



Afbeelding 2: De Machineverordening in één oogopslag

De Machineverordening (EU) 2023/1230 is in juni 2023 aangenomen, is na een overgangperiode van 42 maanden bindend voor alle EU-staten en vervangt de Machinerichtlijn 2006/42/EG op de afsluitingsdatum van 20 januari 2027.

De Machineverordening is van toepassing op fabrikanten, importeurs, handelaren en gemachtigden van machines of aanverwante producten. In de toekomst zullen zij moeten bevestigen dat de machines voldoen aan de Machineverordening, waarin ook veiligheidseisen zijn opgenomen. Dit omvat onder andere de bescherming van veiligheidsrelevante controlefuncties tegen corrumperen. Fabrikanten van machines moeten voorzorgsmaatregelen nemen tegen risico's die kunnen voortvloeien uit kwaadwillige acties van derden en die de machineveiligheid in gevaar kunnen brengen. De naleving van de Machineverordening wordt formeel bevestigd in de conformiteitsverklaring en gemarkeerd met de CE-markering op de machine. Machines die niet voldoen aan de eisen van de nieuwe Machineverordening mogen in de EU niet meer op de markt worden gebracht.



#### Praktische tip:

In vergelijking met de Machinerichtlijn is het thema Security niet de enige vernieuwing in de Machineverordening. Andere eisen, zoals hoe om te gaan met kunstmatige intelligentie, zijn toegevoegd. Pilz biedt een leidraad voor de Machineverordening ter beschikking om te downloaden: [www.pilz.com/mr](http://www.pilz.com/mr)



## 1.2. De NIS-2-richtlijn (EU) 2022/2555



### NIS-2-richtlijn (NIS 2)

(Gepubliceerd in het officiële blad van de Europese Unie op 27-12-2022;  
toe te passen vanaf 18-10-2024)

**Verplichtingen voor essentiële en belangrijke inrichtingen:**

- ▶ Maatregelen om cybersecurityrisico's te beheersen
- ▶ Naleving van organisatorische en technische maatregelen
- ▶ Verplichtingen inzake het melden van cyberbeveiligingsincidenten

Afbeelding 3: De NIS-2-richtlijn in één oogopslag

De NIS-2-richtlijn is te vinden in het officiële blad van de EU onder de naam “Richtlijn (EU) 2022/2555 ... over maatregelen voor een hoog niveau van gemeenschappelijke cyberbeveiliging in de Unie ... (NIS-2-richtlijn)”. De afkorting “NIS” is historisch en staat in taalgebruik voor “Netwerk en informatiebeveiliging”. De NIS-1-richtlijn was vooral van toepassing op kritieke infrastructuren en aanbieders van relevante digitale diensten. De NIS-2-richtlijn breidt de sectoren uit met onder meer de producerende industrie: Machinebouw, fabrikanten van computers, elektronische en optische producten, elektrische apparatuur, motorvoertuigen en opleggers en ander transportmaterieel. **Binnen deze sectoren worden bedrijven met meer dan 50 werknemers of een jaarmzet of -balans van meer dan 10 miljoen euro getroffen.**

Deze bedrijven zullen in de toekomst verplicht zijn om risicobeheersmaatregelen te nemen voor cyberbeveiliging. Daartoe behoren:

- ▶ **Risicoanalyses en beveiligingsconcepten** voor informatiesystemen, bescherming van de toeleveringsketen en veiligheid van personeel
- ▶ Concepten voor de **toegangscontrole** en het beheer van installaties
- ▶ **Verplichte trainingen** voor het management
- ▶ In het geval van significante Security-incidenten, een **vroegtijdige waarschuwing** binnen 24 uur en een **melding aan de bevoegde autoriteit binnen 72 uur**

De NIS 2 werd eind 2022 door het Europees Parlement en de Raad van de EU aangenomen. De EU-lidstaten moeten de richtlijn voor 18 oktober 2024 omzetten in nationaal recht.



**Praktische tip:**

Het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) biedt veel nuttige informatie over cyberbeveiliging, waaronder een zelfbeoordelingsinstrument om bedrijven te helpen hun cyberbeveiligingsstrategie te kunnen controleren: [www.enisa.europa.eu](http://www.enisa.europa.eu)



**Praktische tip:**

Softwaretools zoals OpenVAS kunnen bedrijven helpen kwetsbaarheden te vinden en tegenmaatregelen te controleren.

### 1.3. Cyber Resilience Act (EU) 2024/2847



## Cyber Resilience Act (CRA)

(Gepubliceerd in het officiële blad van de Europese Unie op 20-11-2024;  
meldplichten voor fabrikanten vanaf 11-09-2026; volledig toe te passen vanaf 11-12-2027)

**Verplichtingen van de fabrikant voor producten met digitale elementen:**

- ▶ Secure Development Lifecycle Process (levenscyclus voor een veilige productontwikkeling)
  - ▶ Melding van kwetsbaarheden
  - ▶ Levering van beveiligingsupdates

Afbeelding 4: De Cyber Resilience Act in één oogopslag

De Europese Commissie beschouwt cyberaanvallen als een zaak van algemeen belang, aangezien zij niet alleen een kritieke impact kunnen hebben op de economie van de Unie, maar ook op de democratie, de veiligheid van de consument en de gezondheid.

Daarom presenteerde de Europese Commissie in september 2022 een ontwerpverordening om de cyberbeveiliging van producten te 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 dus 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.

Volgens de CRA mogen in de toekomst – en wel gedurende de gehele levenscyclus van een product – alleen producten op de markt worden gebracht die een adequaat niveau van cyberbeveiliging waarborgen. De verordening is op 20-11-2024 in het officiële blad van de Europese Unie gepubliceerd. Meldplichten van misbruik maken van zwakke punten voor fabrikanten zijn van toepassing vanaf 11-09-2026. Producten met digitale elementen moeten vanaf 11-12-2027 voldoen aan de vereisten van de CRA, om in de EU op de markt te kunnen worden aangeboden. De CRA is een EU-verordening en zal dus rechtstreeks van toepassing zijn in de EU-lidstaten.

De CRA moet parallel worden toegepast met de Machineverordening. Dit betekent dat een machine ook wordt gezien als een product met digitale elementen. Dit betekent weer dat er naast de eisen uit de Machineverordening aanvullende eisen vanuit de CRA komen.

Dit is nodig omdat de Machineverordening tot doel heeft mensen in de directe omgeving van de machine te beschermen, terwijl de CRA ook natuurlijke of rechtspersonen beschermt tegen economische schade.

In de praktische implementatie kunnen er synergie-effecten zijn, dat bijvoorbeeld een cyberbeveiligingsmaatregel aan vereisten uit de CRA en uit de Machineverordening voldoet. Deze synergie-effecten moeten bijvoorbeeld door het gebruik van geharmoniseerde normen door de fabrikant worden aangetoond.



**Praktische tip:**

Abonneer u op nieuwsbrieven en RSS-feeds op <https://eur-lex.europa.eu>, om op de hoogte te blijven van wetswijzigingen op EU-niveau.



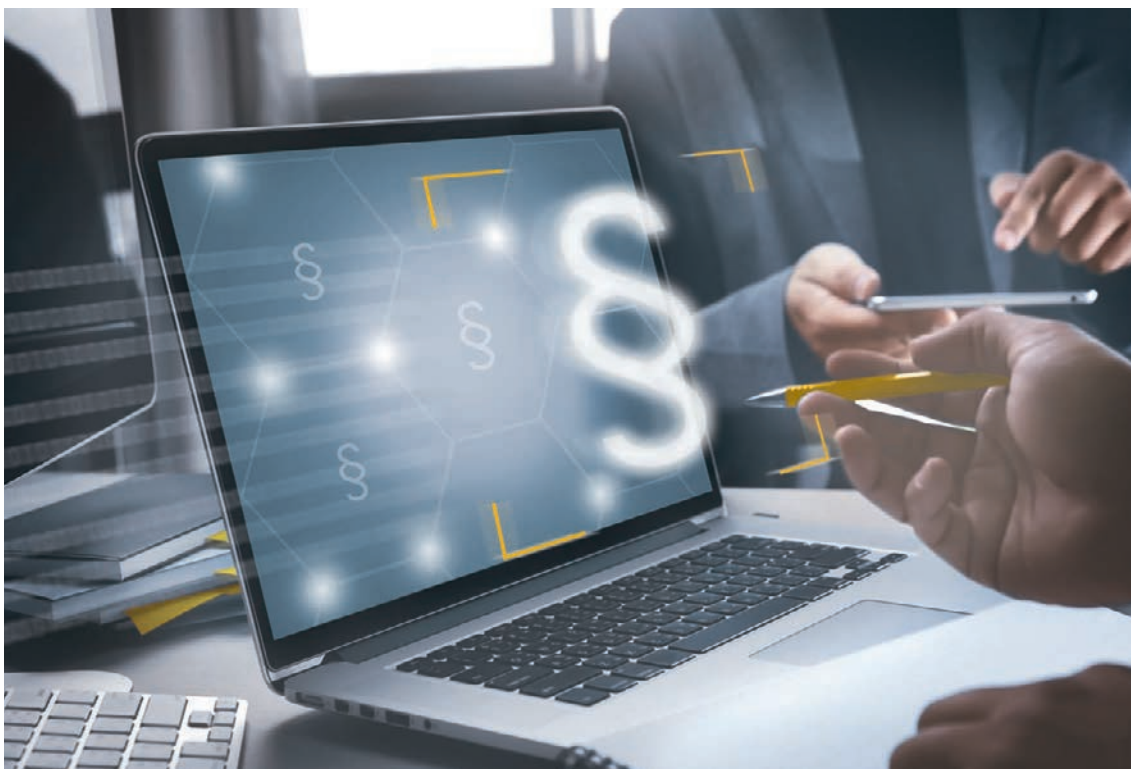
#### 1.4. Richtlijn 2009/104/EG betreffende de bescherming van de veiligheid en de gezondheid bij het gebruik van arbeidsmiddelen

Voor de exploitanten van machines en installaties rijst ook de vraag aan welke verplichtingen zij moeten voldoen. De richtlijn betreffende minimumvoorschriften inzake veiligheid en gezondheid bij het gebruik van arbeidsmiddelen door werknemers op de arbeidsplaats bevat in dit verband regels. De richtlijn is op 3 oktober 2009 bekendgemaakt in het Publicatieblad van de Europese Unie en vervolgens door alle lidstaten in nationaal recht omgezet. Het definieert “arbeidsmiddelen” als machines, apparaten, gereedschappen of installaties die tijdens het werk worden gebruikt.

Volgens deze richtlijn is het onder meer de algemene verplichting van de werkgever om de werknemers te voorzien van geschikte arbeidsmiddelen, zodat de veiligheid en de gezondheid van de werknemers bij het gebruik ervan gewaarborgd zijn.

Arbeidsmiddelen moeten gedurende de gehele gebruiksperiode in een staat worden gehouden, bijvoorbeeld door middel van passend onderhoud, om ervoor te zorgen dat ze voldoen aan de bepalingen van alle toepasselijke relevante communautaire EU-richtlijnen.

Hoewel de Machineverordening formeel een verordening is – en geen richtlijn – kan worden aangenomen dat deze vanuit juridisch oogpunt als een toepasselijke relevante communautaire richtlijn zal worden erkend. De nieuwe eisen uit de Machineverordening gelden dus ook voor bestaande machines vanaf het tijdstip dat de Machineverordening van kracht is.



Afbeelding 5: Er moet rekening worden gehouden met de wettelijke eisen voor machineveiligheid en deze moeten worden nageleefd

## 2. Security voor machinefabrikanten

De Security-eisen voor machines nemen toe om twee redenen: Enerzijds stellen veeleisende klanten nu al vragen over de Security-eigenschappen van de machines, en anderzijds zal de wetgever vanaf 2027 basiskenmerken eisen om machines in Europa op de markt te kunnen brengen of beschikbaar te maken.

Hierbij mag niet worden vergeten dat de meeste machinefabrikanten door de wetgever worden gezien als een belangrijke instelling en dus onder de NIS-2-richtlijn vallen. Dit betekent dat zij er goed aan doen om na te denken over de invoering van een **Information Security Management System (ISMS)**.



### In het kort:

Machines die niet voldoen aan de Security-eisen van de Machineverordening mogen vanaf 20-01-2027 niet meer in de EU op de markt worden gebracht. Of en welke maatregelen genomen moeten worden, kan worden bepaald door middel van een gestructureerde risicoanalyse.

Daarnaast zal de Cyber Resilience Act (CRA) verdere informatie- en documentatieverplichtingen vereisen. De meldplichten voor fabrikanten gelden vanaf 11-09-2026; volledig toe te passen is de CRA vanaf 11-12-2027.

### 2.1. Security in de Machineverordening

De Machineverordening vereist bescherming tegen corrumperen als een van de essentiële veiligheids- en gezondheidseisen in paragraaf 1.1.9. Dit wordt als volgt omschreven:

“[...] De machine of het bijbehorende product moet zo zijn ontworpen en gebouwd **dat de verbinding van een ander apparaat met de machine of het bijbehorende product geen gevaarlijke situatie oplevert via enige functie van het aangesloten apparaat** zelf of via een apparaat voor externe toegang dat met de machine of het product communiceert.

**Een hardwarecomponent dat signalen of gegevens verzendt**, die relevant zijn voor de verbinding met of toegang tot de software en die essentieel zijn **voor de conformiteit van een machine of bijbehorend product met de relevante gezondheids- en veiligheidseisen**, moet zodanig zijn ontworpen dat het **adequaat wordt beschermd tegen onbedoeld of opzettelijk corrumperen**. Machines of gerelateerde producten moeten bewijs verzamelen van een **rechtmatige of onrechtmatige interventie in het genoemde hardware-onderdeel**, voor zover dit relevant is voor de verbinding of toegang tot de software die **essentieel is** voor de conformiteit van de machines of gerelateerde producten.

**Software en gegevens**, die van cruciaal belang zijn voor de conformiteit van de machine of het bijbehorende product met de relevante gezondheids- en veiligheidseisen, **moeten als zodanig worden geïdentificeerd en adequaat worden beschermd tegen onbedoeld of opzettelijk corrumperen**.

De machine of het gerelateerde product moet de geïnstalleerde software identificeren die nodig is voor een veilige werking en deze informatie te allen tijde in een gemakkelijk toegankelijke vorm kunnen verstrekken.

Machines of gerelateerde producten moeten bewijs verzamelen van rechtmatige of onrechtmatige interventie in de software of wijziging van de software die is geïnstalleerd in machines of gerelateerde producten of de configuratie ervan. [...]"

Daarnaast bevat punt 1.2.1 Veiligheid en betrouwbaarheid van besturingen de eis:

"[...] Besturingen moeten zodanig zijn ontworpen en gebouwd dat

- a) indien de omstandigheden en risico's dit passend maken, zij bestand zijn tegen de verwachte bedrijfsbelastingen en opzettelijke en onopzettelijke invloeden van buitenaf, **met inbegrip van redelijkerwijs te voorziene kwaadwillige pogingen van derden, die tot een gevaarlijke situatie kunnen leiden; [...]"**

Een preciezere specificatie van het beschermingsdoel "bescherming tegen corrumperen" en de technische uitvoering ervan moet worden geboden door een nieuwe Europese norm, EN 50742. Deze wordt momenteel ontwikkeld. Aangezien het nog niet te voorzien is of deze norm op tijd voor het einde van de overgangperiode van de Machineverordening zal worden gepubliceerd en geharmoniseerd, is het raadzaam om de stand van de techniek vandaag te informeren. IEC TS 63074 helpt hier bijvoorbeeld. Deze specificatie beschrijft de veiligheidsaspecten met betrekking tot de functionele veiligheid van veiligheidsgerelateerde besturingssystemen. Bovendien legt IEC 62443-3-3 de Security-eisen voor industriële automatiseringssystemen uit. De bijlage bij deze leidraad bevat basisinformatie over de familie van normen.

Aan sommige eisen uit de Machineverordening kan worden voldaan door geschikte componenten te selecteren, voor andere is aanvullende documentatie vereist. Om een pragmatische weg te vinden, is het raadzaam om al in de conceptuele fase van de machineontwikkeling te voorzien van een systematische risicoanalyse. Dit kan ook op een later tijdstip worden uitgevoerd, maar de ervaring heeft geleerd dat de inspanning toeneemt naarmate de ontwikkeling verder gevorderd is.



Afbeelding 6: De EU-Machineverordening stelt Industrial Security verplicht in het conformiteitsbeoordelingsproces

## 2.2. Tussen fabrikanten van componenten en klanten

Een veilig en conform wettelijk bedrijf van de machine is de eis van machine-exploitanten. Als het op implementatie aankomt, bewegen machinefabrikanten of integratoren zich tussen de eisen van de klanten en het assortiment van de componentenfabrikanten.

De Type-C-normen bieden ondersteuning. Ze beschrijven de stand van de techniek voor specifieke toepassingen en specificeren het minimale veiligheidsniveau dat een machine moet hebben. Aangezien er nog geen geharmoniseerde C-normen zijn die rekening houden met het Security-aspect, zit er niets anders op dan naar eer en geweten een risicoanalyse uit te voeren aan de hand van gevestigde internationale normen en daaruit risicobeperkende maatregelen af te leiden.

Om de risicoanalyse correct uit te kunnen voeren, is het belangrijk om de omgevingscondities en Security-eisen aan de machine toe te kennen. Twee dingen spelen hierbij een rol: enerzijds de mogelijke omvang van de schade, d.w.z. hoe hoog de motivatie van de aanvaller is om schade aan te richten, en anderzijds de kans op een aanval. Aangenomen kan worden dat een vrij toegankelijke machine meer kans heeft om aangevallen te worden dan een machine waar slechts een beperkte groep mensen toegang toe heeft.

Iedereen is bekend met beveiligingsupdates van alledaagse producten zoals smartphones en computers. Machinebesturingen of andere machinecomponenten hebben ook een update nodig nadat een beveiligingslek bekend is geworden. Op dit moment voeren de meeste componenten geen automatische updates uit en staan fabrikanten van componenten meestal niet in direct contact met de exploitanten. Dit leidt tot de vraag hoe de exploitant ervoor kan zorgen dat zijn machine op tijd de nodige updates krijgt.

Hier speelt de integrator, d.w.z. de machinefabrikant of de systeemintegrator, een sleutelrol en kan hij via zijn functie bemiddelen tussen de exploitant en de componentenfabrikant. Aan de ene kant kan hij de fabrikanten van componenten benaderen met de Security-eisen van de exploitant en de juiste componenten selecteren. Aan de andere kant kan hij informatie over de componenten, bijvoorbeeld nieuwe beveiligingsupdates, delen met de exploitant.



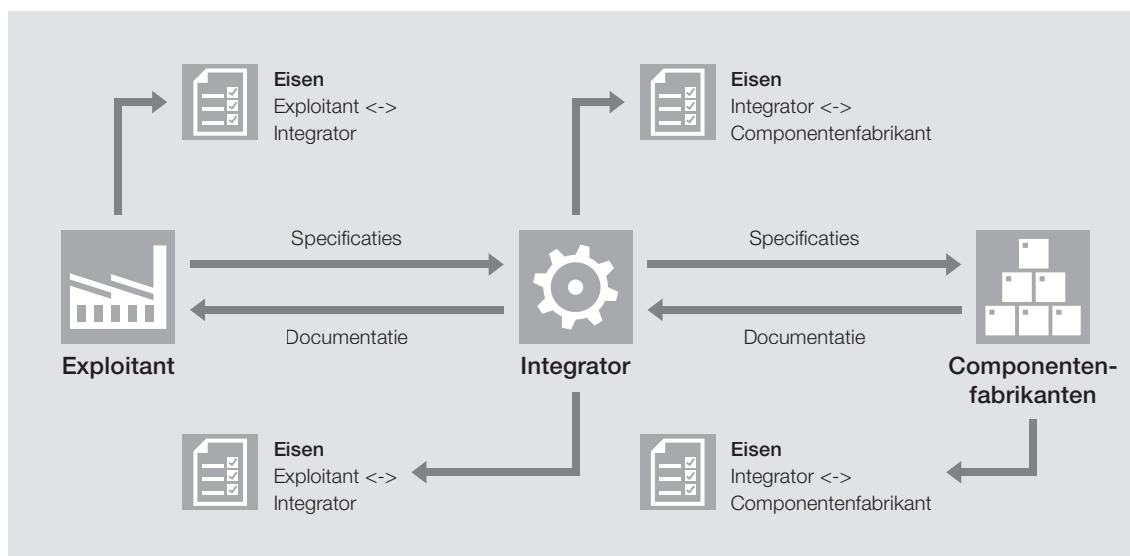
#### Praktische tip:

Om een uniforme aanpak te bevorderen, heeft de Duitse Ingenieursfederatie (Verband Deutscher Maschinen- und Anlagenbau e. V.) (VDMA) in het kader van de werkgroep Industrial Security de documentenreeks "Supply Chain Security" in het leven geroepen, die bedoeld is om de communicatie tussen exploitanten, integratoren en fabrikanten van componenten te vergemakkelijken:

[www.vdma.org](http://www.vdma.org)



De volgende afbeelding illustreert de interfaces tussen exploitanten, integrators en fabrikanten van componenten.



Afbeelding 7: Aanbeveling van de toeleveringsketen van VDMA (Quelle: <https://www.vdma.org/cybersecurity>)

### 2.3. Cyber Resilience Act voor machinefabrikanten

De Cyber Resilience Act (CRA) is een verordening, die op 20-11-2024 in het officiële blad van de Europese Unie werd gepubliceerd. Het verwijst naar producten met digitale elementen. Alle producten met digitale elementen moeten voldoen aan de vereisten van de CRA vanaf 11-12-2027. Fabrikanten van producten met digitale elementen moeten al vanaf 11-09-2026 voldoen aan de meldplichten. Aangenomen kan worden dat zodra een machine onder de CRA valt, de fabrikant ook de conformiteit met de CRA moet certificeren. Dit betekent dat er aan verschillende eisen moet worden voldaan.

Vermeldenswaardig zijn op dit punt onder meer de volgende vereisten:

- ▶ **Verplichting** voor fabrikanten van misbruikte kwetsbaarheden om zich binnen 24 uur te melden bij de autoriteit
- ▶ Producten met digitale elementen worden zo ontworpen, ontwikkeld en vervaardigd dat ze een **passend niveau van cyberbeveiliging waarborgen** dat overeenkomt met het geïdentificeerde risico
- ▶ Op basis van de risicoanalyse mogen de producten alleen op de markt worden aangeboden **zonder bekende kwetsbaarheden die kunnen worden misbruikt**
- ▶ Ervoor zorgen dat kwetsbaarheden kunnen worden verholpen door middel van **beveiligings-updates**
- ▶ **Bescherm de beschikbaarheid van wezenlijke en essentiële functies**, ook na een incident, o.a. door uitvalveiligheid en herstelmaatregelen tegen Denial-of-Service-aanvallen
- ▶ Identificatie en documentatie van **kwetsbaarheden en componenten door fabrikanten van producten met digitale elementen**, met inbegrip van het opstellen van een softwarestuklijst in een machinaal leesbaar formaat die ten minste de belangrijkste afhankelijkheden van de producten dekt
- ▶ Aanvullende **documentatie over hoe om te gaan met zwakke plekken in de beveiliging**, zoals de periode waarin de fabrikant beveiligingsupdates voor zijn product ter beschikking stelt
- ▶ Opstellen van een EU-conformiteitsverklaring

Deze (onvolledige) lijst van eisen uit de CRA maakt duidelijk dat er een aanzienlijke inspanning zal moeten worden geleverd voor alle betrokken economische acteurs. Het valt nog te bezien hoe deze vereisten de productdiversiteit zullen beïnvloeden en of de geschatte overgangperiode van drie jaar voldoende zal zijn.

Pilz raadt alle machinefabrikanten aan om dit probleem zo snel mogelijk aan te pakken en samen met fabrikanten en exploitanten van componenten concepten te ontwikkelen om aan de eisen van de CRA te voldoen.



**Praktische tip:**

Het Common Security Advisory Framework (CSAF) is een gestandaardiseerd opensource framework voor de communicatie en automatiseerbare verspreiding van machinaal verwerkbare informatie over kwetsbaarheden en mitigatie, zogenaamde security advisories:

<https://oasis-open.github.io/csaf-documentation>



**Praktische tip:**

Door het invoeren van een Software Bill of Materials (SBOM) is het mogelijk om alle gebruikte softwareversies te behouden.

## 3. Security voor machine-exploitanten

Ook exploitanten van machines zijn van de nieuwe rechtshandelingen betroffen: of het nu gaat om de aanschaf van nieuwe machines, wijzigingen aan bestaande machines of de periodieke controle of dat de stand der techniek nog steeds wordt nageleefd.

Aangezien machines doorgaans in de producerende industrie worden gebruikt, moeten machine-exploitanten ook voldoen aan de NIS-2-richtlijn.



### In het kort:

Ook exploitanten van bestaande installaties worden door de nieuwe Machineverordening getroffen. Door netwerksegmentatie en de beperking van toegangsmogelijkheden kan de vereiste beveiliging meestal ook achteraf worden bereikt. Aan de hand van een vooraf uitgevoerde gestructureerde risicoanalyse wordt de noodzaak van actie bepaald.

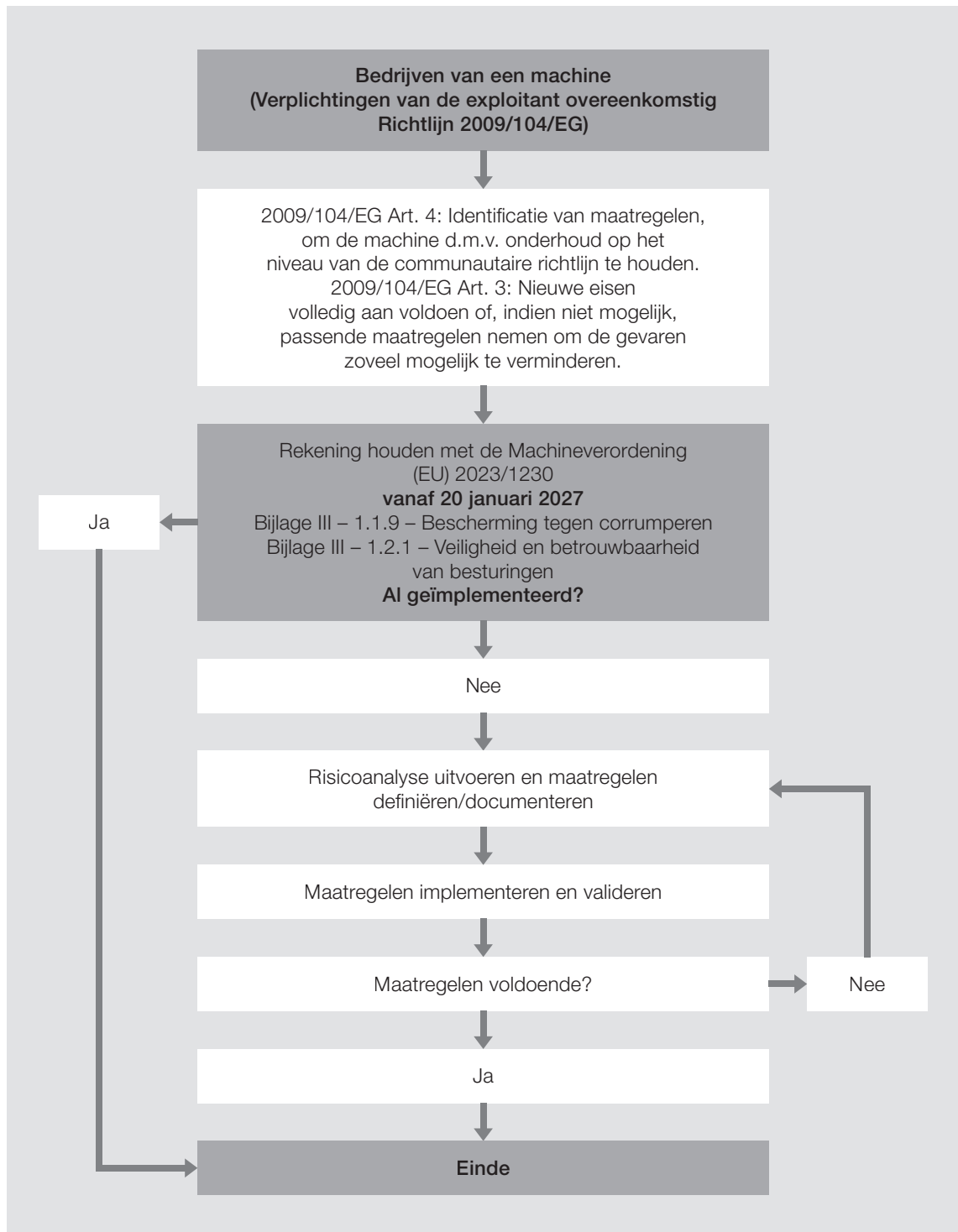
De NIS-2-richtlijn vereist van een grote groep productiebedrijven uitgebreide Security-concepten. Netwerkmachines moeten in deze overwegingen worden opgenomen.

### 3.1. Omgaan met bestaande installaties

Exploitanten van machines, die doorgaans als arbeidsmiddel worden gebruikt, moeten ervoor zorgen dat werknemers voldoende arbeidsveiligheid genieten en dat niemand gewond raakt. Dit wordt beschreven in de hierboven gepresenteerde **EU-richtlijn betreffende de bescherming van de veiligheid en de gezondheid bij het gebruik van arbeidsmiddelen** uit 2009, die door alle lidstaten in nationale wetgeving is omgezet.

Deze richtlijn bepaalt dat de exploitant er door middel van periodieke inspecties voor moet zorgen dat zijn arbeidsmiddelen op een zodanig niveau worden gehouden dat het gedurende de gehele gebruiksperiode voldoet aan de bepalingen van alle relevante communautaire richtlijnen die van kracht zijn.

Omgekeerd betekent dit: Vanaf de dag waarop de Machineverordening van toepassing is, d.w.z. 20 januari 2027, moeten alle actieve machines worden gekeurd om er zeker van te zijn dat ze voldoen aan het niveau van de Machineverordening. Er zullen gevallen zijn waarin de werkgever niet volledig aan de eisen kan voldoen. Ook in deze gevallen is hij echter verplicht passende maatregelen te nemen om de gevaren zoveel mogelijk te beperken.



Afbeelding 8: Procesafloop – omgang met bestaande installaties

Exploitanten die het probleem nog niet hebben aangepakt, zullen actie moeten ondernemen om te voldoen aan de nieuwe cybeveiligheidseisen.

De eerste stap is een analyse van de Security-risico's. Deze risicoanalyse resulteert in de uit te voeren maatregelen. In de meeste gevallen gaat het om het segmenteren van het netwerk en het beperken van de toegangsmogelijkheden.

### 3.2. Van IT-Security naar bedrijfsbrede Security

In de regel is de IT-afdeling (informatietechnologie) verantwoordelijk voor de informatie- en communicatietechnologie in bedrijven, inclusief IT-Security.

In bedrijven is het onderwerp Security bijv. in de vorm van een personeelseenheid ondergebracht. Deze Security-experts of -functionarissen, bijvoorbeeld in de rol van Chief Information Security Officer (CISO), moeten bekend zijn met de vereisten van de NIS-2-richtlijn en een concept hebben over hoe deze in de hele organisatie kunnen worden geïmplementeerd.

De ervaring heeft geleerd dat de productieafdeling van het bedrijf bij vragen over IT-Security afhankelijk is van de IT-afdeling en het onderwerp nogal marginaal behandelt.

Hier is dringend een heroverweging nodig, aangezien de machines in de productieruimte deel uitmaken van het Security-concept van het bedrijf. Om het totaalconcept correct te kunnen implementeren, moet het bedrijf worden onderverdeeld in veiligheidszones en moeten de interfaces en vereisten van de afzonderlijke zones tot aan het machineniveau in het bedrijf worden gedefinieerd en geïmplementeerd.



Afbeelding 9: Industrial Security gaat ook in op de relatie tussen IT-beveiliging en OT-beveiliging



**Praktische tip:**

De <https://www.shodan.io/> zoekmachine kan worden gebruikt om netwerkapparaten te vinden, vaak inclusief apparaten die niet langer gevonden zouden moeten worden via netwerksegmentatie. Zitten uw apparaten er ook bij?



**Praktische tip:**

Een van de meest voorkomende soorten aanvallen loopt via de medewerksters en medewerkers van een bedrijf, bijvoorbeeld via phishing-e-mails. Regelmatige training van het personeel vermindert dit risico.

## 4. De weg naar een veilige machine – Safe en Secure



### In het kort:

Met een gestructureerde risicoanalyse kunnen de kosten voor tegenmaatregelen en ook voor de analyse zelf drastisch worden verlaagd. Daarbij wordt de beschouwing van de veelheid aan mogelijke aanvalspaden beperkt tot die welke bepaalde beschermingsdoelen daadwerkelijk in gevaar brengen. De beoordeling van de mogelijke omvang van de schade en de waarschijnlijkheid van het optreden geeft ook aanwijzingen op de zinvolle inspanning om het risico tot een minimum te beperken.

Bedreigingen voor de Security van machines kunnen op vele manieren ontstaan, zowel via datanetwerken als fysiek door directe toegang tot de machine. Om een machine zo kosten-effectief mogelijk te beschermen, is een gestructureerde aanpak aan te bevelen, die hieronder wordt beschreven.

### ► Activa identificeren

In de eerste stap worden de te beschermen activa gedefinieerd en van elkaar onderscheiden. Het resultaat geeft een compleet en consistent beeld van de te beschermen installaties en installatiedelen. Deze maatregel zorgt ervoor, dat er geen delen worden vergeten, maar ook dat aanvalsvectoren niet onnodig meerdere keren worden overwogen.

### ► Bedreigingen analyseren

De volgende stap is het bepalen van de hoogte van de mogelijke schade in het geval van een compromis. Deze vraag kan eenvoudiger worden beantwoord door de drie beschermingsdoelen van de informatiebeveiliging afzonderlijk te bekijken. Deze zijn: Vertrouwelijkheid, integriteit en beschikbaarheid – de Engelse termen zijn Confidentiality, Integrity en Availability, vaak afgekort als CIA.

#### - Confidentiality (vertrouwelijkheid)

Bevat de machine informatie waarvan de openbaarmaking het bedrijf schaadt? Dit kan bijvoorbeeld informatie zijn over productieprocessen, recepten of andere handelsgeheimen die een concurrentievoordeel voor bedrijven opleveren. Hoe groot is de potentiële schade?

#### - Integrity (integriteit)

Welke effecten kan de ongewenste wijziging van gegevens hebben? Kan de wijziging van gegevens leiden tot economische schade, bijvoorbeeld door beschadiging van de machine, of mensen in gevaar brengen, bijvoorbeeld door het beïnvloeden van veiligheidsfuncties? Hoe groot is de potentiële schade?

#### - Availability (beschikbaarheid)

Wat is de economische schade die wordt veroorzaakt door het falen van een machine, bijvoorbeeld door productieonderbrekingen?

### ► Bepalen van beschermingsdoelen

Na dit voorbereidende werk kunnen de beschermingsdoelen worden geformuleerd. Hoe specifiek de doelen zijn gedefinieerd, hoe specifiek aanvalsvectoren kunnen worden bepaald. Dit voorkomt onnodige maatregelen die misschien de Security van de machines verhogen, maar niet dienen om de gedefinieerde beveiligingsdoelen te bereiken.

### ► Risico's beoordelen

Nadat de beschermingsdoelen zijn bepaald, wordt een inschatting gemaakt van de kans dat de geïdentificeerde risico's zich daadwerkelijk voordoen. Het resultaat geeft een indicatie van de zinvolle omvang van verdere maatregelen.

► **Analyse van aanvalsvectoren**

In deze stap wordt systematisch bepaald hoe een aanval daadwerkelijk kan plaatsvinden en welke beschermingsmaatregelen er al zijn, bijvoorbeeld door intrinsieke beschermingsmaatregelen in de gebruikte machinecomponenten. Dit resulteert in een lijst van de overige oorzaken van gevaar.

► **Security-concept opstellen en implementeren**

Het Security-concept beschrijft specifiek alle maatregelen die nodig zijn om de gedefinieerde beschermingsdoelen voor de betreffende machine te bereiken. Dit kunnen zowel constructieve maatregelen aan de machine zijn als organisatorische aanpassingen aan de processen.

► **Implementatie controleren**

De daadwerkelijke effectiviteit van de uitgevoerde maatregelen kan alleen worden geverifieerd door middel van zeer uitgebreide penetratietests, waarbij hackeraanvallen door gespecialiseerde serviceproviders worden gesimuleerd. Als alternatief moet de correcte implementatie van het Security-concept worden gecontroleerd.

► **Regelmatig herbeoordelingen uitvoeren**

In tegenstelling tot Safety zijn beschermende maatregelen voor Security niet eenmalig. Aangezien er voortdurend nieuwe kwetsbaarheden opduiken in complexe systemen, moet de analyse met regelmatige tussenpozen worden herhaald of wanneer bedreigingen bekend worden. Nieuwe kwetsbaarheden kunnen zich voordoen op alle niveaus van de inkooppiramide, zoals hardware-componenten, opensourcecode in apparaten of specifieke apparaat-firmware. Zodra een kwetsbaarheid wordt gedetecteerd, publiceren de verantwoordelijke fabrikanten overeenkomstige Security-adviezen met informatie over het risico en advies over passende tegenmaatregelen. Het is raadzaam om u regelmatig te informeren over nieuwe Security-adviezen van leveranciers.



Afbeelding 10: Alleen door Security-overwegingen zijn machines, componenten en installaties echt veilig en beschermd tegen corrumperen



**Praktische tip:**

De Security-adviezen van Pilz zijn beschikbaar op [www.pilz.com/advisories](http://www.pilz.com/advisories)



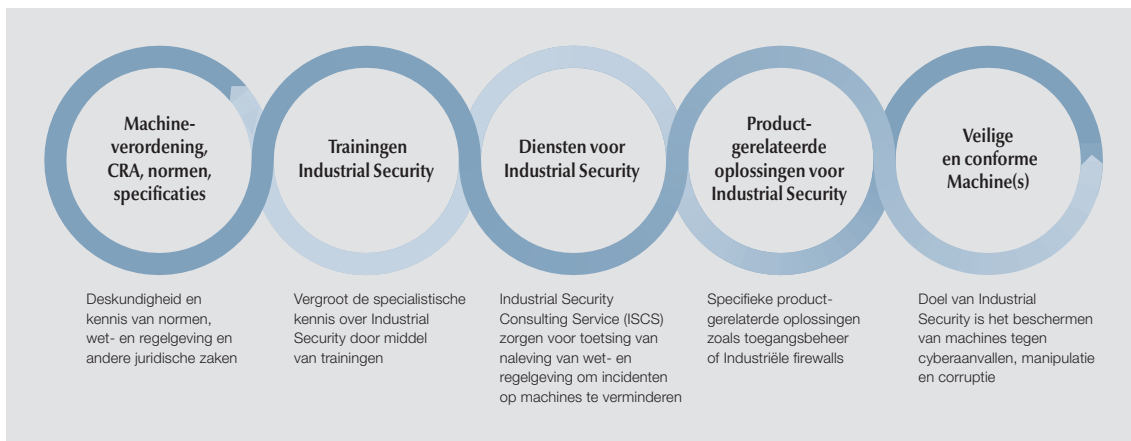
## 5. Safety en Security uit één hand

Met de nieuwe wettelijke eisen voor Security staan machinefabrikanten en -exploitanten voor nieuwe uitdagingen. De processen voor het verminderen van risico's van aanvallen op machines (Security) lijken sterk op de processen voor het verminderen van risico's, die van machines kunnen uitgaan (Safety). Pilz als expert voor machineveiligheid helpt stap voor stap bij het vinden van op maat gemaakte oplossingen en veilige machines – Safe en Secure.



Afbeelding 11: Safety en Security horen bij elkaar als een holistisch concept in machineveiligheid

- ▶ Expertise en knowhow door deelname aan normcommissies
- ▶ Onderzoek en opvolging van de huidige wet- en normsituatie
- ▶ Basis- en expertopleidingen voor machinegerichte Industrial Security
- ▶ Diensten in het kader van machinegerichte Industrial Security
  - Beoordeling van de beschermingsbehoeften
  - Risicoanalyses
  - Holistische beveiligingsconcepten
  - Validaties/verificaties
  - Procesoptimalisaties
- ▶ Producten en oplossingen voor fysieke toegangscontrole en cybersecurity aan de machine



Afbeelding 12: Stap voor stap naar een veilige machine met Industrial Security-oplossingen



**Praktische tip:**

Meer informatie over Industrial Security-oplossingen vindt u bij Pilz onder [www.pilz.com/security](http://www.pilz.com/security)



## 6. Samenvatting en vooruitzichten

De toename van de dreiging van cyberaanvallen en corrumperen heeft een directe impact op de wettelijke situatie in Europa en leidt tot een duidelijke koers van de wetgever in de richting van Industrial Security: In de toekomst zullen door de wetgever nieuwe eisen worden gesteld aan Industrial Security, met name via de Machineverordening, de NIS-2-richtlijn en de CRA. Voor machinefabrikanten en -exploitanten betekent dit actieve actie door de ontwikkeling en implementatie van organisatorische en technische maatregelen om te voldoen aan de nieuwe eisen voor bedrijven, machines en componenten. In deze leidraad zijn deze taken uitgelegd en hoe u ermee om kunt gaan.

De NIS-2-richtlijn is al bindend voor het merendeel van de machinefabrikanten en -exploitanten, en in 2027 volgen de nieuwe Machineverordening en de CRA. Door met een vooruitziende blik te handelen, kunnen de noodzakelijke projecten tijdig worden gepland en uitgevoerd.

Normcommissies geven machinefabrikanten advies over de implementatie van de nieuwe eisen. Een gestructureerde aanpak is belangrijk, zoals beschreven in de IEC 62443-normenreeks.

Ervaren en gekwalificeerde dienstverleners helpen stap voor stap de noodzakelijke maatregelen te analyseren om de nieuwe doelstellingen met meestal beheersbare inspanningen te bereiken.

Machineveiligheid betekent in de toekomst Safety en Security – ter bescherming van mens en machine. Met een holistisch en gecoördineerd concept kunnen complexe problemen op het gebied van machineveiligheid efficiënt en duidelijk worden gesegmenteerd. Een risicoanalyse is ook de eerste stap voor Industrial Security en biedt een gestructureerde oriëntatie en methodologie om de vereisten voor uw eigen bedrijf op te splitsen.

Met deze aanpak zijn bedrijven goed voorbereid, om de groeiende uitdagingen op het gebied van Industrial Security aan te gaan.

► Meer informatie van Pilz over Industrial Security – nu ontdekken



Lees meer op:  
[www.pilz.com/security](http://www.pilz.com/security)



## 7. Bijlage

### 7.1. Termen op het gebied van Industrial Security

**Cyberbeveiliging**, in de zin van de EU-commissie, beschrijft alle activiteiten die nodig zijn, om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen die door cyberdreigingen worden getroffen, te beschermen.

**Cyberdreiging** betekent een mogelijke omstandigheid, gebeurtenis of actie die de netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen beschadigen, verstoren of anderszins kan aantasten.

**Industrial Security** streeft ernaar de beschikbaarheid van machines en installaties te waarborgen, evenals de integriteit en vertrouwelijkheid van machinegegevens en -processen.

**IT-Security** (informatietechnologie) is de beveiliging van gegevens, los van fysieke processen.

**OT-Security** (Operational Technology) is de beveiliging van machines en installaties die betrokken zijn bij fysieke processen.

**IACS** is een afkorting van IEC 62443 en staat voor Industrial Automation and Control System(s) – in het Nederlands industrieel automatiseringssysteem.

**Security Level** uit de IEC 62443-normenreeks is het level, dat overeenkomt met de vereiste maatregelen en de inherente beveiligingskenmerken van apparatuur en systemen voor een zone of Conduit, op basis van de beoordeling van het risico voor de zone of Conduit.

**Zone** is de verzameling eenheden die een indeling van een bekeken systeem op basis van zijn functionele, logische of fysieke relaties (inclusief locatie) weergeven.

**Conduit** is de logische groepering van communicatiekanalen die twee of meer zones met gemeenschappelijke IT-beveiligingsvereisten met elkaar verbindt.

## 7.2. IEC 62443 – Basisnorm voor Industrial Security

IEC 62443 is een internationale normenreeks voor “Industriële communicatienetwerken – IT-beveiliging voor netwerken en systemen”.

### 7.2.1. Overzicht

De IEC 62443-normenfamilie bestaat uit verschillende onderdelen, waarvan de volgende normen op dit moment al zijn gepubliceerd.

Deel 1 gaat over de algemene grondbeginselen:

- ▶ IEC TS 62443-1-1: Deel 1: Termen en modellen
- ▶ IEC TS 62443-1-5: Deel 1–5: Schema voor IT-beveiligingsprofielen uit IEC 62443

Deel 2 heeft betrekking op de beveiligingseisen voor exploitanten en dienstverleners:

- ▶ IEC 62443-2-1: Opzetten van een IT-beveiligingsprogramma voor industriële automatiseringssystemen
- ▶ IEC 62443-2-2: Classificaties van het IACS-veiligheidsprogramma
- ▶ IEC TR 62443-2-3: Patchbeheer voor industriële automatiseringssystemen
- ▶ IEC 62443-2-4: Vereisten voor het IT-beveiligingsprogramma van dienstverleners voor industriële automatiseringssystemen

Deel 3 heeft betrekking op de veiligheidseisen voor automatiseringssystemen

- ▶ IEC TR 62443-3-1: Technieken voor industriële automatiseringssystemen
- ▶ IEC TR 62443-3-2: Beoordeling van beveiligingsrisico's en systeemontwerp
- ▶ IEC 62443-3-3: Systeemvereisten voor IT-beveiliging en Security Level

Deel 4 beschrijft de beveiligingseisen voor automatiseringscomponenten

- ▶ IEC 62443-4-1: Levenscyclusvereisten voor veilige productontwikkeling
- ▶ IEC 62443-4-2: Eisen aan componenten van industriële automatiseringssystemen

Deel 5 specificeert de profielen van IEC 62443

- ▶ IEC TS 62443-1-5: Schema voor IT-beveiligingsprofielen uit IEC 62443

Deel 6 beschrijft de evaluatiemethodologie

- ▶ IEC 62443-6-1: Methodologie van beveiligingsevaluatie voor IEC 62443-2-4

### 7.2.2. Security Level (SL)

De eisen aan systemen en componenten worden beschreven met Security Levels.

Deze zijn als volgt gedefinieerd:

- ▶ Security Level 0: Geen speciale vereisten of bescherming vereist
- ▶ Security Level 1: Bescherming tegen onbedoeld of toevallig misbruik
- ▶ Security Level 2: Bescherming tegen opzettelijk misbruik met eenvoudige middelen met weinig middelen, algemene vaardigheden en een lage motivatie
- ▶ Security Level 3: Bescherming tegen opzettelijk misbruik met geavanceerde middelen met matige resources, IACS-specifieke kennis en matige motivatie
- ▶ Security Level 4: Bescherming tegen opzettelijk misbruik met behulp van geavanceerde middelen met uitgebreide resources, IACS-specifieke kennis en hoge motivatie

Dit betekent dat hoe hoger het vereiste Security Level, hoe effectiever de maatregelen moeten worden geïmplementeerd.

Er zijn zeven basisvereisten (Engels: Foundational Requirements, FR):

- ▶ FR 1 – Identificatie en authenticatie
- ▶ FR 2 – Controle van het gebruik
- ▶ FR 3 – Integriteit van het systeem
- ▶ FR 4 – Vertrouwelijkheid van de gegevens
- ▶ FR 5 – Beperkte gegevensstroom
- ▶ FR 6 – Tijdig reageren op gebeurtenissen
- ▶ FR 7 – Beschikbaarheid van resources

Achter elk van deze basisvereisten gaan maatregelen van verschillende kwaliteit schuil die kunnen worden toegepast om het vereiste level te bereiken. Typische maatregelen zijn multifactor-authenticatie of versleutelingsmechanismen.

Welk beschermingsniveau moet worden bereikt, hangt af van het cyberrisico. Zo maakt de Europese wetgever een onderscheid tussen belangrijke en essentiële instellingen. Het aan te nemen cyberrisico hangt dus af van het type bedrijf, de grootte van het bedrijf en de potentiële impact. Verschillende normalisatie-instellingen houden zich momenteel met het onderwerp bezig en zijn bezig met het definiëren van algemeen geldende eisen voor industrieën en machinetypen.

### 7.2.3. Information Security Management System (ISMS)

Naast de technische vereisten voor componenten en systemen zijn er ook organisatorische maatregelen die moeten worden geïmplementeerd om het risico op een succesvolle aanval te verkleinen. Elk bedrijf moet zelf bepalen hoe zij het Information Security Management System (ISMS) willen inrichten. De ISO/IEC 27000-normenreeks is algemeen bekend en ingeburgerd. IEC 62443-2-1 kan worden gezien als een leidraad voor de implementatie van ISO/IEC 27001 in industriële automatiseringssystemen. Daarnaast is er ook het certificeringsprogramma van de automobielenindustrie TISAX, dat ook geschikt blijkt te zijn.

Het ISMS identificeert, classificeert, evalueert de risico's en beschrijft hoe ermee om te gaan. Doorgaans moeten eerst het toepassingsgebied en de interfaces met andere gebieden worden gedefinieerd. Ook essentieel is:

- ▶ het opnemen van de verantwoordelijkheid voor Security door de directie
- ▶ De verduidelijking van de verantwoordelijkheden
- ▶ De definitie van opleidingsmaatregelen
- ▶ Het opstellen van beveiligingsbeleid in het bedrijf

Het ISMS helpt om systematisch de risico's af te wegen en passende maatregelen af te leiden.

Bedrijfsrisico's kunnen zijn:

- ▶ Economische schade door productieverlies
- ▶ Letsel aan werknemers
- ▶ Overtredingen van privacybescherming
- ▶ Milieuschade
- ▶ Het verlies van het vertrouwen van de klant

Typische maatregelen zijn onder meer:

- ▶ De ontwikkeling van noodplannen die moeten worden toegepast
- ▶ De definitie van geautoriseerde gebruikers
- ▶ Fysieke en virtuele toegangscontroles
- ▶ Netwerksegmentatie

De implementatie van maatregelen wordt ook beschreven door het ISMS. Deze omvatten:

- ▶ Systeemontwikkeling
- ▶ Onderhoud van het systeem
- ▶ Gegevensbescherming
- ▶ Planning en omgang met incidenten

### **7.3. Verdere baanbrekende documenten voor machinefabrikanten en -exploitanten**

Naast de IEC 62443-normenfamilie zijn er al andere Security-normen die van invloed zijn op de machinebouw en eisen definiëren.

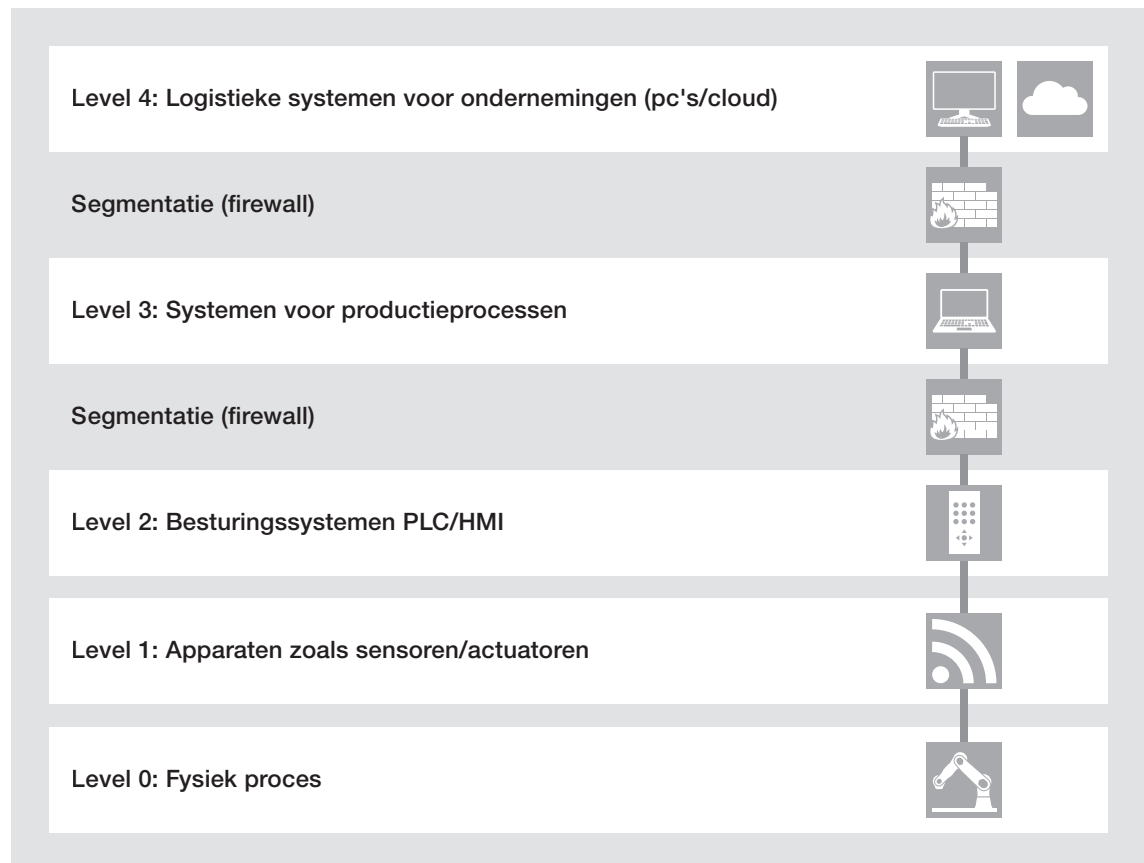
IEC TS 63074 beschrijft de veiligheidsaspecten met betrekking tot de functionele veiligheid van veiligheidsgerelateerde besturingssystemen. Deze technische specificatie specificeert de relevante aspecten van de IEC 62443-normenfamilie waarmee rekening moet worden gehouden om de veilige werking van een machine te garanderen.

Een nieuwe Europese norm, EN 50742, wordt momenteel ontwikkeld voor de eis “bescherming tegen corrumperen” uit de Machineverordening. Pilz is actief betrokken bij de normcommissie.

Beveiligingseisen vloeien ook voort uit de Richtlijn radioapparatuur 2014/53/EU en de Gedelegeerde Verordening (EU) 2022/30 daarvan. Voor deze eisen is de normenreeks EN 18031 ontwikkeld.

#### 7.4. Netwerksegmentatie met behulp van het Purdue-model

Om het onderwerp netwerksegmentatie te illustreren, helpt het Purdue-model, dat Theodore Joseph Williams (hoogleraar engineering aan de Purdue University in de VS) al in 1990 publiceerde. In de volgende afbeelding werd het Purdue-model voor ons doel uitgebreid met maatregelen als voorbeeld.



Afbeelding 13: Netwerksegmentatie met behulp van het Purdue-model

Level 0 is het daadwerkelijke fysieke proces dat doorgaans wordt uitgevoerd in de producerende industrie. Dit wordt meestal bewaakt en aangedreven door sensoren en actuatoren. Deze apparaten behoren tot level 1. Het proces wordt doorgaans bestuurd door een PLC, die tot level 2 behoort. De PLC wordt via de systemen geprogrammeerd voor productieprocessen in level 3. De daadwerkelijke opdrachten komen uit het logistieke systeem in level 4.

Levels 0 t/m 3 vallen onder de benaming Operationele Technologie (OT), level 4 en alles daarboven valt onder de benaming Informatietechnologie (IT).

De afbeelding toont al een type segmentatie dat in dit voorbeeld werkt via firewalls die de gegevensoverdracht tussen level 4 en 3 of 3 en 2 beperken, om het potentiële aanvalsoppervlak te minimaliseren.

Het doel is om succesvolle segmentatie te realiseren, d.w.z. om zowel een effectieve vermindering van aanvalsmogelijkheden te hebben als een systeem dat niet beperkt is in prestaties. Daarvoor is het noodzakelijk dat de interfaces duidelijk zijn gedefinieerd, met als gevolg dat bijvoorbeeld bij het configureren van de firewalls rekening wordt gehouden met alle benodigde poorten en protocoltypes.

De correcte selectie van de juiste componenten is essentieel voor een veilig bedrijf. Aan de beste firewall heb je immers niets als de componenten in de lagere levels voor nog meer kwetsbaarheden zorgen. Afhankelijk van het vereiste Security Level kan het nodig zijn dat de componenten in het systeem elkaar authenticeren en daarmee wijzigingen in het systeem monitoren. Hiermee moet ook rekening worden gehouden bij het selecteren van componenten en het configureren ervan.

In dit voorbeeld zijn alle componenten vanaf level 3 met elkaar verbonden en wordt de informatiestroom beveiligd door twee firewalls. In de industriële omgeving is het vrij gebruikelijk dat de systemen ook draadloze interfaces hebben (bijvoorbeeld in AGV's). Hier moet worden onderzocht, hoe beveiligingsmaatregelen effectief kunnen worden geïmplementeerd.

**Praktische tip:**

Praktische voorbeelden van hoe u uw apparaten kunt configureren, vindt u op [www.pilz.com](http://www.pilz.com), gebruik gewoon de zoekfunctie met het trefwoord "application notes".



## 8. Literatuur

- ▶ 1. Reference model for computer integrated manufacturing (CIM): a description from the viewpoint of industrial automation. Uitgegeven door Theodore J. Williams, 1989
- ▶ 2. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels IEC 62443-3-3:2013
- ▶ 3. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components IEC 62443-4-2:2019
- ▶ 4. EU-Machineverordening 2023/1230  
(<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023R1230>)
- ▶ 5. Richtlijn (EU) 2022/2555 over maatregelen voor een hoog niveau van cyberbeveiliging in de unie  
(<https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022L2555>)
- ▶ 6. Cyber Resilience Act P9\_TA(2024)0130  
([https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf))
- ▶ 7. Richtlijn 2009/104/EG  
(<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32009L0104>)
- ▶ 8. Agentschap van de Europese Unie voor cyberbeveiliging  
(<https://www.enisa.europa.eu/>)
- ▶ 9. Pilz GmbH & Co. KG  
(<https://www.pilz.com/en-INT/products/industrial-security/security-incident-management>)
- ▶ 10. VDMA e. V. (<https://www.vdma.org/cybersecurity>)
- ▶ 11. Information security, cybersecurity and privacy protection – Information security management systems – Requirements ISO/IEC 27001
- ▶ 12. Whitepaper Industrial Security (Pilz 2018) ([www.pilz.com/security](http://www.pilz.com/security))
- ▶ 13. Whitepaper leidraad voor de Machineverordening (Pilz 2023) ([www.pilz.com/mr](http://www.pilz.com/mr))
- ▶ 14. <https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview> (gezien 20-01-2025)
- ▶ 15. Cybersecurity Act EU 2019/881, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1728407971719>





# Support

U ontvangt van Pilz dag en nacht technische ondersteuning.

## Amerika

### Brazilië

+55 11 97569-2804

### Canada

+1 888 315 7459

### Mexico

+52 55 5572 1300

### USA (toll-free)

+1 877-PILZUSA (745-9872)

## Azië

### China

+86 400-088-3566

### Japan

+81 45 471-2281

### Zuid-Korea

+82 31 778 3390

## Australië en Oceanië

### Australië

+61 3 95600621

### Nieuw Zeeland

+64 9 6345350

## Europa

### België, Luxemburg

+32 9 3217570

### Duitsland

+49 711 3409-444

### Frankrijk

+33 3 88104003

### Groot-Brittannië

+44 1536 460866

### Ierland

+353 21 4804983

### Italië, Malta

+39 0362 1826711

## Nederland

+31 347 320477

## Oostenrijk

+43 1 7986263-444

## Scandinavië

+45 74436332

## Spanje

+34 938497433

## Türkiye

+90 216 5775552

## Zwitserland

+41 62 88979-32

**Onze internationale  
hotline is bereikbaar via:**

+49 711 3409-222

support@pilz.com

Pilz ontwikkelt milieuvriendelijke producten met ecologische materialen en energiebesparende technologieën. We maken en bewerken onze producten milieubewust en energiezuinig, in ecologisch ontworpen gebouwen. Zo biedt Pilz u duurzaamheid bij de zekerheid dat u energie-efficiënte producten en milieuvriendelijke oplossingen krijgt.



Partner of the Engineering Industry  
Sustainability Initiative



Aangeboden door:



Wij zijn internationaal vertegenwoordigd. Voor meer informatie kunt u onze homepage [www.pilz.com](http://www.pilz.com) raadplegen of contact opnemen met ons hoofdkantoor.

Hoofdkantoor: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Duitsland  
Telefoon: +49 711 3409-0, E-mail: [info@pilz.com](mailto:info@pilz.com), Internet: [www.pilz.com](http://www.pilz.com)

Gedrukt op 100% gerecycleerd papier voor het welzijn van het milieu.

8-4-nl-3-023, 2025-05 Printed in Germany  
© Pilz GmbH & Co. KG, 2025

CECE, CHRE, CMSE®, INDUSTRIAL Pi®, Leansafe®, Myzel®, PAS4000®, PASca®, PASconfig®, Pilz®, PIZ®, PMCPrimo®, PMCProtego®, PMCiendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVS®, SafetyBUS p®, SafetyNET p®, THE SPIRIT OF SAFETY® zijn in sommige landen geregistreerde en beschermde merken van Pilz GmbH & Co. KG. Wij wijzen u erop dat de producteigenschappen kunnen afwijken van de gegevens in dit document, afhankelijk van de stand van de techniek bij het ter perse gaan en de uitvoering van de installatie. Wij zijn niet aansprakelijk voor de actualiteit, juistheid en volledigheid van de in de tekst en afbeeldingen vermelde informatie. Als u vragen hebt, kunt u contact opnemen met onze technische ondersteuning.

**PILZ**  
THE SPIRIT OF SAFETY