Industrial Security

PILZ
THE SPIRIT OF SAFETY

Um guia para fabricantes e operadores de máquinas sobre como lidar com a corrente legislação da UE

Whitepaper
Versão: Abril 2025

Isenção de responsabilidade

Elaboramos nosso whitepaper com muito cuidado. Contém informações sobre a interpretação atual da Pilz a respeito do novo Regulamento de Máquinas Europeu, da diretriz NIS-2 assim como do Cyber Resilience Act. Todas as informações apresentadas correspondem ao atual estado da interpretação e aos nossos melhores conhecimentos. Portanto, não assumimos nenhuma responsabilidade quanto à exatidão e à completude das informações, a menos que haja acusação de negligência grave, pois falhas não podem ser totalmente evitadas, apesar de todos os cuidados. Sobretudo, as informações não contam com a qualidade legal das garantias ou das propriedades asseguradas. Se você identificar divergências, avise-nos.

Direitos autorais

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

2.ª edição revisada

Resumo

O termo Industrial Security tem muitas facetas. Neste guia, são descritos os pontos mais importantes para fabricantes e operadores de máquinas. É importante facilitar a introdução a este tema tanto para fabricantes como para operadores para que estes possam compreender e gerenciar os novos requisitos.

O guia descreve o estado atual da legislação na Europa, resume os fundamentos técnicos, descreve os pontos mais importantes para fabricantes assim como para operadores de máquinas e indica opções adicionais a nossos clientes.

Na Europa, vários textos legislativos abrangentes, que impactam diretamente a construção de máquinas, foram publicados nos últimos meses:

- O **Regulamento de Máquinas** (UE) 2023/1230 impõe novos requisitos a máquinas, entre eles a proteção contra a corrupção.
- A **Diretriz UE sobre medidas para um elevado nível de segurança cibernético coletivo** na União (NIS 2) 2022/2555 exige a muitas empresas um sistema de Information Security Management System.
- O **Cyber Resilience Act** (EU) 2024/2847 define os requisitos para produtos com elementos digitais, o que geralmente também inclui máquinas.

Ao implementar a legislação, algumas normas e termos têm um significado muito importante:

- A família de normas **IEC 62443** consolidou-se no que respeita ao tema da segurança da informação em ambientes industriais.
- O **Security Level** de 0 a 4 descreve a capacidade do agressor.
- A Industrial Security é uma tarefa contínua. Por isso, as medidas organizacionais são indispensáveis a par das medidas técnicas. Um **Information Security Management System** (ISMS) ajuda e é obrigatório para muitas empresas.

Os fabricantes de máquinas estão sujeitos a vários requisitos legislativos e movimentam-se entre as especificações para operadores e a oferta de produtos de diferentes fabricantes. Os fabricantes de máquinas têm que assumir aqui um papel mediador para poder continuar a oferecer produtos de alta qualidade e de acordo com as normas.

No futuro, os operadores também têm que se preocupar com a segurança das suas máquinas. Para ter uma ideia geral, é recomendada uma avaliação de risco sistemática de modo a detetar com eficiência os pontos vulneráveis.

A Pilz GmbH & Co. KG oferece treinamentos avançados e serviços sobre este tema.

O autor

Matthias Kuczera completou os seus estudos em engenharia mecânica e continuou adquirindo conhecimentos abrangentes em segurança de máquinas nos diferentes ramos industriais.

Como engenheiro de desenvolvimento para sensores, adquiriu conhecimentos aprofundados sobre as possibilidades de implementação de requisitos de segurança funcionais.

Durante a sua atividade como perito na área da tecnologia de transportadores, era responsável pela realização de testes de tipo de componentes de segurança em determinado organismo.

Na sua atividade como especialista em “Segurança Funcional – Normas” na Pilz, está ativo em comitês de normas e supervisiona o gerenciamento das mesmas.

As suas funções incluem:

- Cooperação em comitês de normas para a segurança de máquinas
- Avaliação de novos requisitos legislativos
- Realização de treinamentos internos

Pilz – the Spirit of Safety in Digital Automation

Tudo o que fazemos é para tornar o mundo um lugar mais seguro. Como fornecedora global de produtos, sistemas e serviços de tecnologia de automação, a Pilz relembra sua história de 75 anos de sucesso: fundado em 1948, o grupo Pilz emprega hoje aproximadamente 2 500 funcionários em 42 subsidiárias e filiais. A especialista em segurança de máquinas com sede em Ostfildern produz mundialmente segurança para pessoas, máquinas e meio ambiente com suas soluções de automação completas. O portfólio da líder em tecnologia inclui sensores, tecnologia de controle, tecnologia de acionamento e sistemas para comunicação industrial, diagnóstico e visualização. Uma gama internacional de serviços com consultoria, engenharia e treinamento complementa o leque. As soluções de Safety e Security são utilizadas na engenharia mecânica e industrial e em vários outros setores, como intralogística, tecnologia metroferroviária e robótica.

Índice

Resumo **3**

1. Estado atual da legislação na Europa **6**
1.1. Regulamento de Máquinas (UE) 2023/1230 7
1.2. Diretriz NIS-2 (UE) 2022/2555 8
1.3. Cyber Resilience Act (UE) 2024/2847 9
1.4. Diretriz para Segurança e Saúde no Trabalho para utilização de equipamentos de trabalho 2009/104/EG 11

2. Security para fabricantes de máquinas **12**
2.1. Security no Regulamento de Máquinas 12
2.2. Entre fabricantes de componentes e clientes 14
2.3. Cyber Resilience Act para fabricantes de máquinas 15

3. Security para operadores de máquinas **17**
3.1. Lidar com instalações existentes 17
3.2. Desde a IT Security até à Security na empresa 19

4. O percurso até uma máquina segura – Safe e Secure **20**

5. Safety e Security de um único fornecedor **22**

6. Sumário e perspectivas **24**

7. Apêndice **26**
7.1. Termos da área da Industrial Security 26
7.2. IEC 62443 – norma básica para Industrial Security 27
7.2.1. Resumo 27
7.2.2. Security Level (SL) 28
7.2.3. Information Security Management System (ISMS) 29
7.3. Outros documentos importantes para fabricantes e operadores de máquinas 30
7.4. Segmentação de rede com base no modelo Purdue 31

8. Bibliografia **33**

1. Estado atual da legislação na Europa

Novas tecnologias vêm acompanhadas de chances e riscos. Atualmente, as novidades mais importantes no nosso ramo são a elevada interligação de máquinas através da Internet das Coisas (IoT), inteligência artificial e robótica.

Com a interligação de empresas e máquinas, aumenta o risco de que os pontos vulneráveis nos sistemas de informação possam ser explorados e possam ocorrer perdas econômicas e danos físicos. Por exemplo, nos últimos anos foram registrados cada vez mais casos bem sucedidos de ataques cibernéticos a empresas, causando danos na casa dos bilhões. A Statista.com calcula que no ano de 2023 foram causados aproximadamente 8,15 trilhões de dólares em prejuízo devido a ataques cibernéticos. Só na Alemanha foram quase 206 bilhões de Euros em 2023, o que corresponde a aproximadamente 5 por cento do produto interno bruto.

Para reduzir os riscos, os legisladores europeus introduziram novas regulamentações. Na área da construção de máquinas, estas são basicamente o Regulamento de Máquinas, a Diretriz NIS 2 (NIS 2) e o Cyber Resilience Act (CRA). Através delas, a Industrial Security é obrigatória. Na Diretriz para Segurança e Saúde no Trabalho para utilização de equipamentos de trabalho 2009/104/EG é descrito como lidar com máquinas e instalações já existentes.

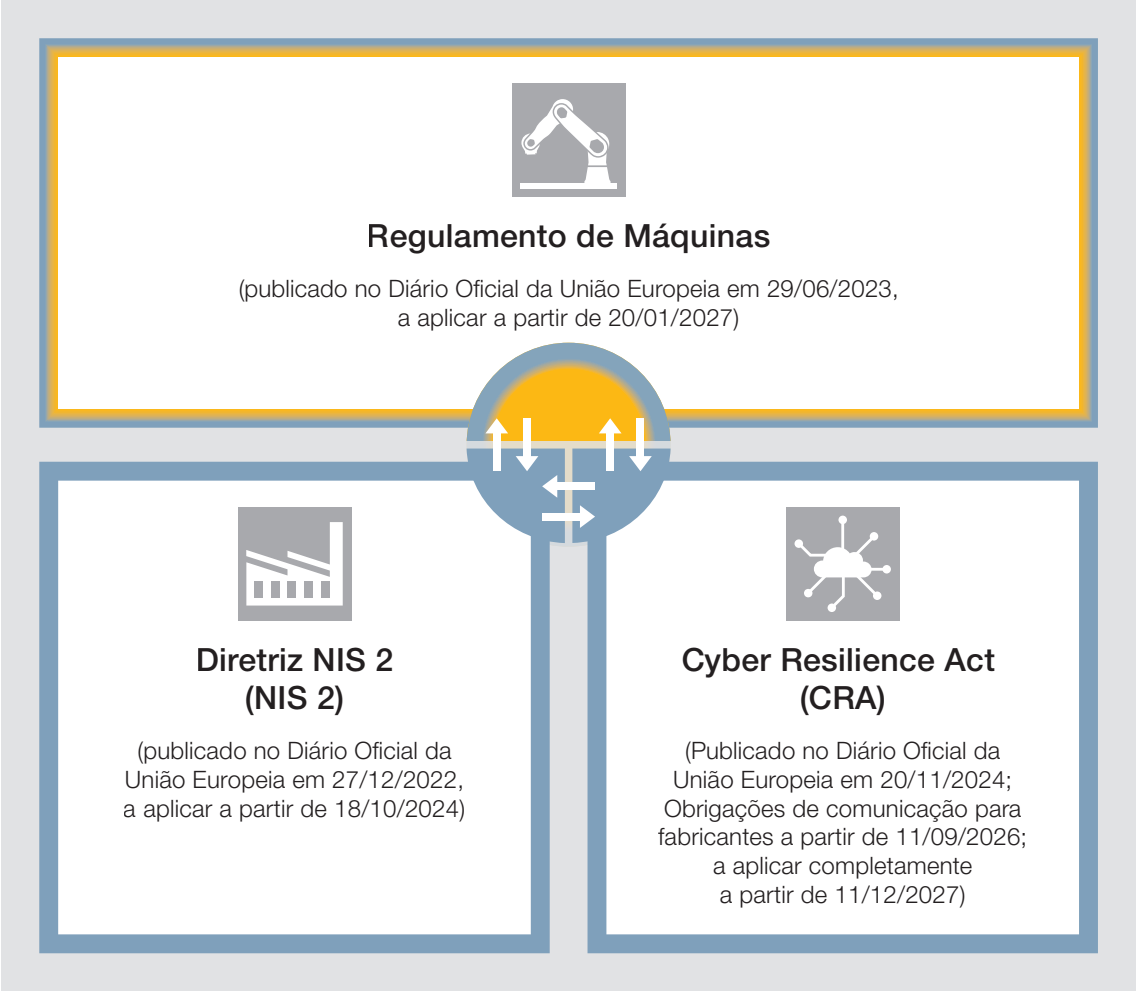

Figura 1: Representação de um excerto de nova legislação básica que descreve os requisitos para Industrial Security

	Regulamento de Máquinas (UE) 2023/1230	Diretriz NIS 2 (UE) 2022/2555	Cyber Resilience Act (UE) 2024/2847
Dirigido a	Máquinas	Empresas	Componentes
Emitido em	29/06/2023	27/12/2022	20/11/2024
Vinculativo a partir de	20/01/2027	18/10/2024	11/12/2027
Obrigações	▸ Proteção contra corrupção (com foco em funções de segurança funcional) ▸ Atenção a tentativas mal intencionadas por terceiros	▸ Medidas de gerenciamento de riscos de segurança cibernética ▸ Cumprimento de medidas técnicas e organizacionais ▸ Notificação de incidentes de segurança significativos	▸ Obrigações de comunicação do fabricante a partir de 11/09/2026 ▸ Secure Development Lifecycle Process ▸ Teste de tipo UE para produtos críticos ▸ Notificação de pontos vulneráveis ▸ Disponibilização de atualizações de segurança

Tabela 1: Resumo comparativo: Regulamento de Máquinas, Diretriz NIS 2 e Cyber Resilience Act

1.1. Regulamento de Máquinas (UE) 2023/1230

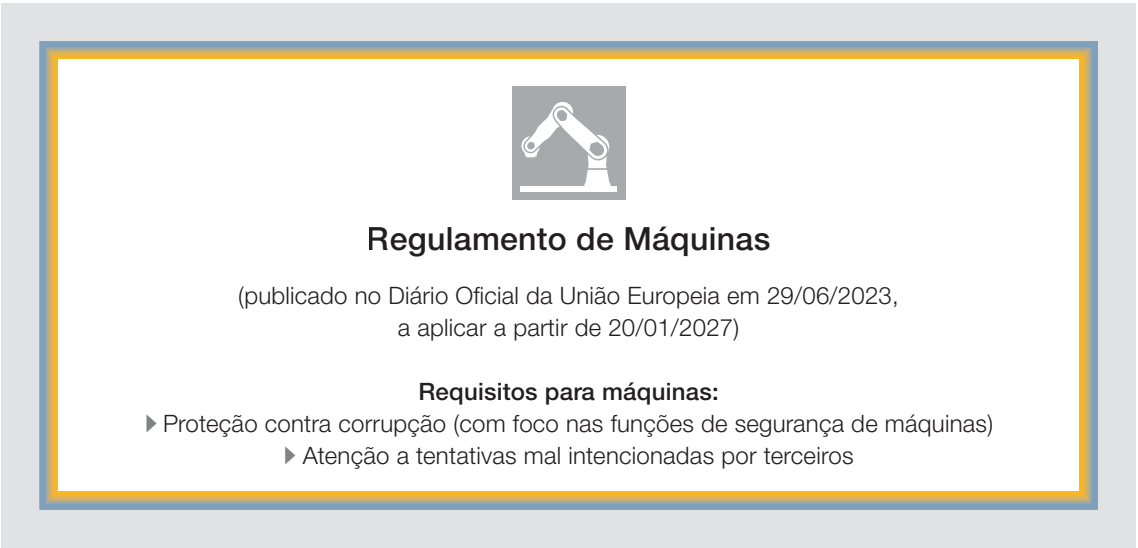

Figura 2: Resumo do Regulamento de Máquinas

O Regulamento de Máquinas (UE) 2023/1230 foi emitido em Junho de 2023, é vinculativo após um período de transição de 42 meses para todos os países membros da UE e substitui a Diretriz de Máquinas 2006/42/EG a partir de 20 de janeiro de 2027.

O Regulamento de Máquinas afeta os fabricantes, importadores, distribuidores e representantes de máquinas e produtos associados. No futuro, estes têm que confirmar que as máquinas respeitam o Regulamento de Máquinas, incluindo os requisitos de Security. Isto também inclui a proteção de funções de comando relacionadas à segurança contra corrupção. Os fabricantes de máquinas têm que tomar precauções contra riscos que possam vir de ações mal intencionadas de terceiros e que afetem a segurança da máquina. O cumprimento do Regulamento de Máquinas é confirmado formalmente na Declaração de Conformidade e indicado com a marcação CE na máquina. Máquinas que não cumpram com as exigências do novo Regulamento de Máquinas não podem circular mais na UE.

Sugestão prática:
Em comparação com a Diretriz de Máquinas, o tema Security não é a única novidade no Regulamento de Máquinas. Foram adicionados outros requisitos, nomeadamente os relacionados com a inteligência artificial. A Pilz oferece uma guia sobre o Regulamento de Máquinas para baixar em: **www.pilz.com/mr**

1.2. Diretriz NIS 2 (UE) 2022/2555

Diretriz NIS 2 (NIS 2)

(publicado no Diário Oficial da União Europeia em 27/12/2022,
a aplicar a partir de 18/10/2024)

Obrigações para entidades essenciais e importantes:
- Medidas de gerenciamento de riscos de segurança cibernética
- Cumprimento de medidas organizacionais e técnicas
- Obrigações de comunicação em caso de incidentes de segurança cibernética

Figura 3: Resumo da Diretriz NIS 2

Você pode encontrar a Diretriz NIS 2 no Diário Oficial da União Europeia em “Diretriz (UE) 2022/2555 … sobre medidas para um elevado nível de segurança cibernético coletivo na União ... (Diretriz NIS 2)”. A abreviatura “NIS” é histórica e significa “Segurança das Redes e da Informação”. A Diretriz NIS 1 aplicava-se sobretudo a infraestruturas críticas e aos prestadores de serviços digitais relevantes. A Diretriz NIS 2 amplia os sectores para incluir indústrias de produção, entre outros: construção de máquinas, fabricantes de equipamentos de processamento de dados, produtos eletrônicos e óticos, equipamentos elétricos, veículos com motor e componentes de veículos assim como qualquer outro tipo de construção de veículos. **Entre estas indústrias, são afetadas companhias com mais de 50 funcionários ou com um lucro anual ou semestral acima de 10 milhões de Euros.**

Estas empresas serão no futuro obrigadas a implementar medidas de gerenciamento de riscos para a segurança cibernética. Ela inclui:

- **Análises de risco e conceitos de segurança** para sistemas de informação, proteção da cadeia de abastecimento e segurança da equipe
- Conceitos para o **controle de acesso** e o gerenciamento de instalações
- **Treinamentos obrigatórios** para o gerenciamento
- Em caso de incidentes graves de segurança, um **alerta prévio** dentro de 24 horas e dentro de 72 horas uma **notificação às entidades responsáveis**

A NIS 2 foi adotada pelo Parlamento Europeu e pelo Conselho da UE no final de 2022.
Os estados-membros da UE devem transpor a diretriz para a legislação nacional até 18 de outubro de 2024.

Sugestão prática:
A Agência da União Europeia para a Cibersegurança (ENISA) oferece muitas informações úteis sobre o tema da cibersegurança, incluindo uma ferramenta para a autoavaliação com a qual as empresas podem controlar a sua estratégia de segurança cibernética: **www.enisa.europa.eu**

Sugestão prática:
Ferramenta de software, como por exemplo OpenVAS, podem ajudar as empresas a encontrar os pontos vulneráveis e verificar as contramedidas.

1.3. Cyber Resilience Act (UE) 2024/2847

Cyber Resilience Act (CRA)

(Publicado no Diário Oficial da União Europeia em 20/11/2024; Obrigações de comunicação para fabricantes a partir de 11/09/2026; a aplicar completamente a partir de 11/12/2027)

Obrigações do fabricante para produtos com elementos digitais:
- Secure Development Lifecycle Process
(Ciclo de vida para um desenvolvimento seguro de produtos)
- Notificação de pontos vulneráveis
- Disponibilização de atualizações de segurança

Figura 4: Resumo do Cyber Resilience Act

A Comissão Europeia considera os ataques cibernéticos uma matéria de interesse público, uma vez que estes não só têm consequências críticas para a economia da União mas também para a democracia, segurança dos consumidores e saúde.

Como tal, em setembro de 2022, a Comissão Europeia apresentou um projeto de regulamentação para aumentar a segurança cibernética dos produtos.

O Cyber Resilience Act (CRA) é voltado a **fabricantes de produtos com elementos digitais (hardware e software)** capazes de se comunicar com outros produtos.

Ele envolve produtos do setor B2C, como smartphones ou robôs aspiradores, produtos do setor B2B, como **comandos e sensores, e** também produtos de software puros, como sistemas operacionais.

De acordo com o CRA, somente podem ser colocados no mercado produtos que garantam um nível adequado de segurança cibernética durante todo seu ciclo de vida. O Regulamento foi publicado no Diário Oficial da União Europeia a 20/11/2024. As obrigações de comunicação de pontos vulneráveis para os fabricantes são válidas a partir de 11/09/2026. Produtos com elementos digitais terão que cumprir os requisitos do CRA a partir de 11/12/2027 para poderem estar disponíveis no mercado europeu. O CRA é um regulamento UE e, como tal, será imediatamente válido nos países membros da UE.

O CRA deve ser aplicado paralelemente ao Regulamento de Máquinas. Isto significa que uma máquina também é considerada um produto com elementos digitais. Por sua vez, isto faz com que aos requisitos do Regulamento de Máquinas se juntem os requisitos do CRA.

Isto é necessário uma vez que o Regulamento de Máquinas tem como objetivo a proteção de pessoas nas imediações da máquinas, enquanto que o CRA protege adicionalmente a pessoa física e jurídica de danos econômicos.

Na prática, poderá dar-se um efeito sinergético, como por exemplo quando uma medida de segurança cibernética preenche requisitos do CRA e do Regulamento de Máquinas. Estes efeitos sinergéticos têm por exemplo que ser demonstrados pelo fabricante através da aplicação de normas harmonizadas.

Sugestão prática:
Subscreva a newsletter e RSS feeds em **https://eur-lex.europa.eu** para ficar sempre informado sobre alterações na lei ao nível da UE.

1.4. Diretriz para Segurança e Saúde no Trabalho para utilização de equipamentos de trabalho 2009/104/EG

Também os operadores de máquinas e instalações se devem colocar a questão quais as obrigações que devem cumprir. A Diretriz sobre os requisitos mínimos para segurança e proteção da saúde na utilização de equipamentos por funcionários durante o trabalho apresenta especificações a este respeito. A Diretriz foi publicada a 3 de outubro de 2009 no Diário Oficial da União Europeia, sendo em seguida implementada por todos os estados membro pela legislação nacional. Esta define “equipamentos de trabalho” como qualquer máquina, aparelho, ferramenta ou instalação utilizados no trabalho.

De acordo com esta Diretriz, uma das obrigações da entidade empregadora é disponibilizar aos funcionários equipamentos de trabalho adequados de modo a que durante a sua utilização seja garantida a sua segurança e proteção da saúde.

Durante todo o período de utilização, os equipamentos têm que ser mantidos de acordo com os requisitos de todas as diretrizes comunitárias válidas na UE. Isto deve ser garantido, por exemplo, através de manutenção adequada.

Mesmo que o Regulamento de Máquinas seja formalmente um regulamento e não uma Diretriz, devemos assumir que é reconhecido como uma diretriz comunitária importante do ponto de vista jurídico. Como tal, os novos requisitos do Regulamento de Máquinas também são válidos para máquinas já existentes a partir do momento em que este regulamento entra em vigor.

Figura 5: É obrigatório respeitar e cumprir os requisitos legislativos para a segurança de máquinas

2. Security para fabricantes de máquinas

Os requisitos de segurança para máquinas têm aumentado por duas razões: por um lado, clientes mais exigentes já colocam questões relacionadas às características de segurança das máquinas. Por outro lado, a partir de 2027, as entidades legisladoras exigem determinados requisitos para que as máquinas possam ser colocadas no mercado europeu.

E não podemos esquecer que a maioria dos fabricantes de máquinas são considerados como organizações importantes pelas entidades legisladoras e, como tal, são abrangidos pela Diretriz NIS 2. Isto significa que é aconselhável pensarem na introdução de um **Information Security Management System (ISMS)**.

Resumindo:
Máquinas que não cumpram com as exigências de segurança do novo Regulamento de Máquinas não podem circular mais na UE a partir de 20/01/2027. Uma avaliação de riscos poderá determinar se há necessidade de tomar medidas e quais poderão ser essas medidas.

O Cyber Resilience Act (CRA) irá também exigir mais obrigações de informação e documentação. As obrigações de comunicação para fabricantes são válidas a partir de 11/09/2026, o CRA deve ser aplicado completamente a partir de 11/12/2027.

2.1. Security no Regulamento de Máquinas

O Regulamento de Máquinas exige a proteção contra corrupção nos requisitos de segurança e saúde básicos no parágrafo 1.1.9. Descrição:

> "[…] A máquina ou o produto associado deve ser construído e montado **de maneira a que a sua conexão a outro componente através de qualquer função do próprio equipamento** ou **qualquer dispositivo em comunicação remota** com a máquina ou produto associado se processe **sem levar a uma situação perigosa.**
>
> **Um componente de hardware que transmita sinais ou dados** relevantes para a conexão ou acesso a software de importância decisiva para a conformidade de uma máquina ou produto associado com os requisitos de segurança e de saúde relevantes, **deve estar construída de maneira a que esteja protegida de forma adequada contra corrupção involuntária ou calculada. As máquinas** ou produtos associados **devem recolher provas de uma intervenção legítima ou ilegítima ao componente de hardware mencionado** quando é relevante para a conexão ou acesso ao software **de importância decisiva** para a conformidade das máquinas ou produtos associados.
>
> **Software e dados** de importância decisiva para a conformidade da máquina ou do produto associado com os requisitos de segurança e de saúde relevantes **devem ser identificados como tal e protegidos adequadamente contra corrupção involuntária ou calculada.**

> A máquina ou produto associado deve identificar o software instalado necessário para a operação segura e deve estar em condições de disponibilizar essa informação de forma acessível em qualquer altura.
>
> As máquinas ou produtos associados devem recolher provas de uma intervenção legítima ou ilegítima no software ou de alterações no software instalado ou sua configuração na máquina ou produtos associados. […]“

O parágrafo 1.2.1. sobre a segurança e fiabilidade de comandos inclui também o seguinte requisito:

> “[…] Os comandos têm que ser concebidos e fabricados de maneira que
>
> a) possam resistir se, de acordo com as circunstâncias e riscos, as exigências de operação previstas e também as influências exteriores previstas e não previstas, **incluindo tentativas razoavelmente mal intencionadas de terceiros previstas possam levar a uma situação de perigo;** […]”

A nova norma EN 50742 terá uma definição mais específica do objetivo de “proteção contra corrupção” e sua implementação técnica. Esta está atualmente em desenvolvimento. Uma vez que ainda não se pode prever se esta norma será publicada e harmonizada a tempo do final do período de transição do Regulamento de Máquinas, recomendamos que se informe já sobre o estado da tecnologia. Uma fonte útil é, por exemplo, a IEC TS 63074. Esta especificação descreve os aspetos de segurança em relação à segurança funcional de sistemas de comando relacionados com a segurança. A IEC 62443-3-3 esclarece também os requisitos de segurança para sistemas de automação industriais. O anexo deste guia contém algumas informações básicas sobre a família de normas.

É possível satisfazer algumas exigências do Regulamento de Máquinas selecionando componentes adequados, enquanto que outras requerem documentação adicional. Para encontrar um caminho pragmático, recomendamos o planejamento de uma avaliação de riscos sistemática logo durante a fase de concepção do desenvolvimento da máquina. Isto também pode ser feito mais tarde, mas a prática mostrou que quanto mais avançado o desenvolvimento, maior o trabalho.

Figura 6: O Regulamento de Máquinas da UE torna a Industrial Security obrigatória no processo de conformidade

2.2. Entre fabricantes de componentes e clientes

A operação segura e conforme com as leis é o objetivo dos fabricantes de máquinas. Durante a implementação, os fabricantes de máquinas e integradores movimentam-se entre os requisitos dos clientes e a oferta dos fabricantes de componentes.

As normas do tipo C podem auxiliar. Estas descrevem o estado da tecnologia para certas áreas de aplicação e especificam o nível mínimo de segurança que uma máquina necessita. Uma vez que atualmente não existe nenhuma norma C harmonizada que contemple o aspecto da Security, o único procedimento possível é uma avaliação de riscos aplicando normas internacionais comprovadas e concluir assim medidas para redução dos riscos.

Para poder realizar a avaliação de riscos corretamente, é importante conhecer as condições do ambiente e os requisitos de Security para a máquina. Aqui há dois fatores importantes: por um lado, a possível extensão dos danos, ou seja, a motivação do agressor para causar danos, e por outro lado a probabilidade de um ataque. Podemos partir do princípio que uma máquina de livre acesso está mais susceptível a agressões do que uma máquina à qual só um grupo restrito de pessoas tem acesso.

Todos conhecemos as atualizações de segurança de produtos do cotidiano como telefones móveis ou computadores. Os comandos de máquinas ou outros componentes da máquina também necessitam de atualizações caso tenha sido detetada uma falha na segurança. Atualmente, a maior parte dos componentes não realizam atualizações automáticas e os fabricantes dos componentes não estão normalmente em contato direto com os operadores. Isto levanta a questão de como pode o operador garantir que a sua máquina recebe a tempo todas as atualizações necessárias.

O integrador, ou seja, o fabricante da máquina ou o integrador no sistema, tem aqui um papel decisivo servindo de ponte entre operador e o fabricantes de componentes. Ele pode por um lado abordar o fabricante de componentes com os requisitos de Security do operador selecionando os componentes certos. Por outro lado, pode partilhar com o operador as informações relativas aos componentes, por exemplo, atualizações de segurança.

Sugestão prática:
Para promover um procedimento uniforme, a Associação Alemã de Fabricação de Máquinas e Instalações Industriais (VMDA) criou a documentação “Supply Chain Security” no grupo de trabalho de Industrial Security para facilitar a comunicação entre operadores, integradores e fabricantes de componentes: **www.vdma.org**

A imagem seguinte mostra as interligações entre operadores, integradores e fabricantes de componentes.

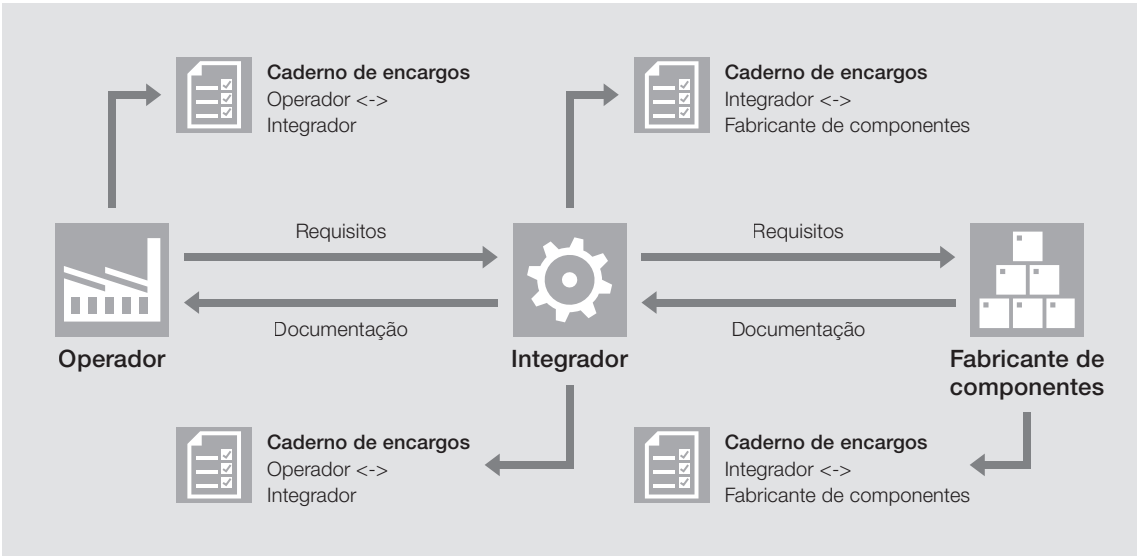

Figura 7: Recomendação de cadeia de abastecimento da VMDA (fonte: https://www.vdma.org/cybersecurity)

2.3. Cyber Resilience Act para fabricantes de máquinas

O Cyber Resilience Act (CRA) é um regulamento publicado a 20/11/2024 no Diário Oficial da União Europeia. Aplica-se a produtos com elementos digitais. Todos os produtos com elementos digitais têm que cumprir os requisitos do CRA a partir de 11/12/2027. Fabricantes de produtos com elementos digitais têm que cumprir com as obrigações de comunicação já a partir de 11/09/2026. Podemos prever que, a partir do momento em que uma máquina é abrangida pelo CRA, o fabricante também deverá ter que certificar a conformidade com o CRA. Isto significa que devem ser cumpridos vários requisitos.

Neste ponto, vale a pena mencionar os seguintes requisitos, entre outros:

- **Obrigação de comunicação** de pontos vulneráveis explorados por parte dos fabricantes às entidades responsáveis dentro de 24 horas
- Produtos com elementos digitais serão concebidos, desenvolvidos e produzidos de maneira a garantir **um determinado grau de segurança cibernética** que corresponda ao risco determinado
- Com base na avaliação de riscos, os produtos **só poderão ser colocados no mercado sem que existam pontos vulneráveis** explorados conhecidos
- Garantia de que os pontos vulneráveis podem ser eliminados através de **atualizações de segurança**
- **Proteção da disponibilidade de funções fundamentais e básicas,** mesmo após um incidente, incluindo através de segurança contra falhas e recursos de ajuda contra ataques de negação de serviço
- Identificação e documentação de **pontos vulneráveis e componentes de fabricantes com elementos digitais,** incluindo através da criação de uma lista de materiais de software em um formato legível por máquina que abranja pelo menos as dependências mais importantes dos produtos
- **Documentação adicional sobre como lidar com brechas de segurança,** como por exemplo o período de tempo em que o fabricante disponibiliza atualizações de segurança para o seu produto
- Criação de uma Declaração de Conformidade UE

Esta lista (incompleta) dos requisitos do CRA mostra claramente que será necessário um grande esforço por parte de todos os operadores econômicos envolvidos. Ainda está por determinar como estas exigências se irão repercutir na variedade de produtos e se o período de transição de três anos será suficiente.

A Pilz recomenda a todos os fabricantes de máquinas que se familiarize o mais rápido possível com este tema e que trabalhe em conjunto com os fabricantes de componentes e operadores com o objetivo de criar conceitos que respondam às exigências do CRA.

Sugestão prática:
O Common Security Advisory Framework (CSAF) é uma estrutura padronizada e de código aberto para a comunicação e a distribuição automatizada de informações sobre vulnerabilidades e mitigações processáveis por máquina, as chamadas Security Advisories:
https://oasis-open.github.io/csaf-documentation

Sugestão prática:
Devido à introdução de lista de materiais de software (SBOM), é possível manter o controle sobre todas as versões de software utilizadas.

3. Security para operadores de máquinas

Os operadores das máquinas também estão abrangidos pela nova legislação: quer seja ao adquirir máquinas novas, ao fazer alterações nas máquinas já existentes, ou inspeções recorrentes para continuar a manter o estado da tecnologia.

Uma vez que as máquinas são normalmente utilizadas na indústria transformadora, os operadores de máquinas também têm que respeitar a Diretriz NIS 2.

Resumindo:
Os operadores de instalações já existentes também são abrangidos pelo Regulamento de Máquinas. Através da segmentação de rede e da restrição de possibilidades de acesso, a proteção pretendida pode muitas vezes ser alcançada em retrospetiva. Com uma avaliação de riscos realizada previamente, é possível determinar a necessidade de intervenção.

A Diretriz NIS 2 exige conceitos de segurança abrangentes de um grande grupo de empresas de produção. As máquinas interligadas têm que ser incluídas nesta planificação.

3.1. Lidar com instalações já existentes

Operadores de máquinas tipicamente utilizadas como equipamento de trabalho têm garantir que seus funcionários desfrutem de suficiente proteção de trabalho e que não acorrem acidentes. Isto é descrito na **Diretriz UE acima apresentada para segurança e proteção da saúde na utilização de equipamentos** de 2009 e que foi implementada em todos os estados membros pela legislação nacional.

Esta diretriz exige que o operador garanta através de testes periódicos que os seus equipamentos se mantenham a um nível em que cumpram as disposições de todas as diretrizes comunitárias vigentes durante todo o tempo de utilização e recorrendo a uma manutenção adequada.

Em conclusão inversa, isto significa que: a partir do dia em que o Regulamento de Máquinas entre em vigor, ou seja, a partir do dia 20 de janeiro de 2027, é necessário controlar se todas as restantes máquinas ativas correspondem ao nível do Regulamento de Máquinas. Em alguns casos, a entidade empregadora não poderá corresponder na totalidade aos requisitos. Mesmo nestes casos, ele é obrigado a adotar medidas adequadas para reduzir os riscos ao máximo.

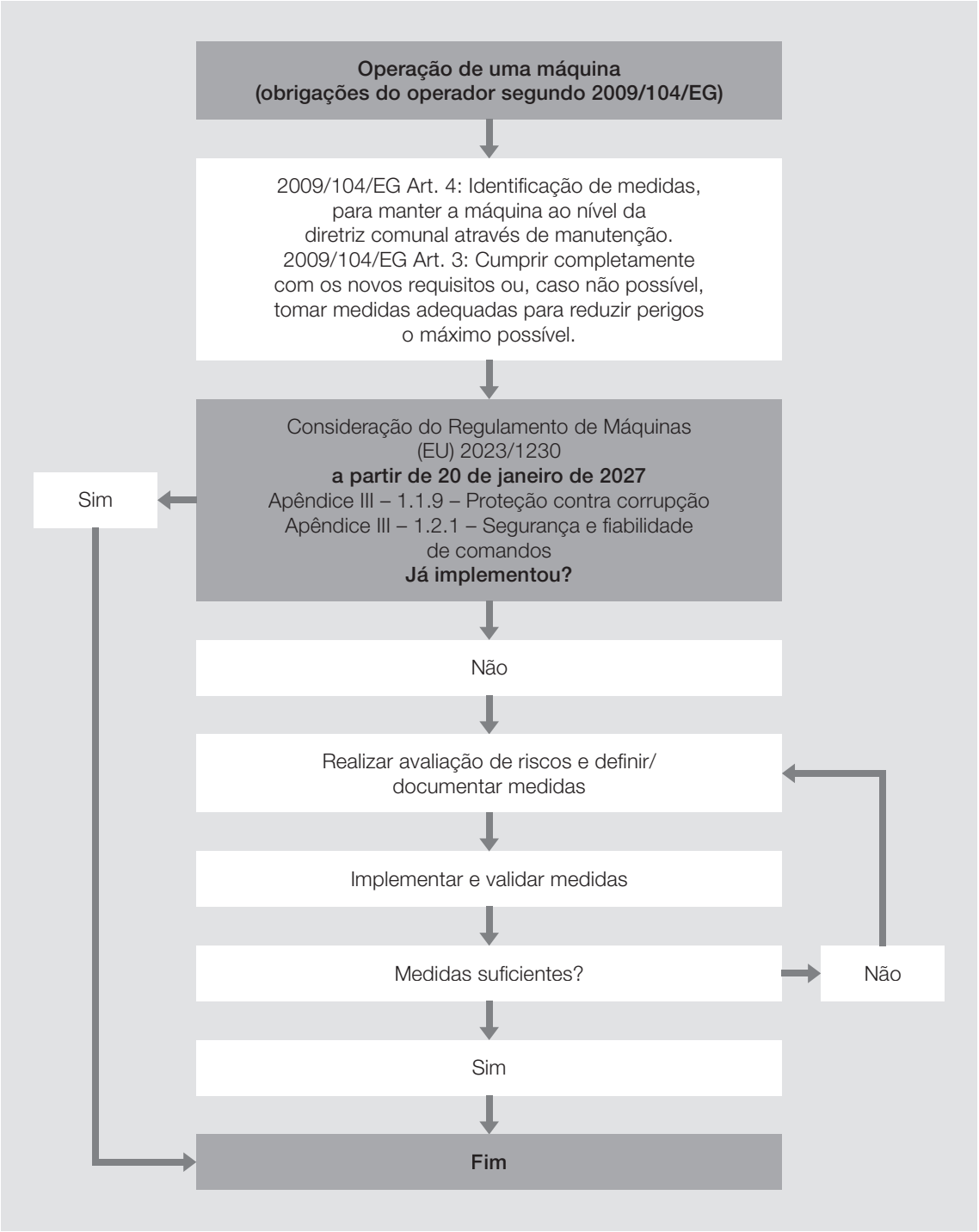

Figura 8: Desenvolvimento do processo – Lidar com instalações já existentes

Operadores que ainda não se ocuparam com o tema, têm que adotar medidas para cumprir com os novos requisitos relativos à segurança cibernética.

O primeiro passo é uma avaliação de riscos. A partir desta análise, são determinadas as medidas a aplicar. Na maior parte dos casos, isto inclui uma segmentação da rede e a restrição de possibilidades de acesso.

3.2. Desde a IT Security até à Security na empresa

De maneira geral, o departamento de IT (Information Technology) é responsável pela tecnologia de informação e comunicação em empresas, incluindo a segurança informática.

Nas empresas, o tema Security é entregue a uma equipa própria. Estes especialistas ou responsáveis pela Security, por exemplo no papel de Chief Information Security Officer (CISO), devem estar familiarizados com os requisitos da Diretriz NIS 2 e ter um conceito para a aplicar em toda a empresa.

A experiência mostra que a área de produção de uma empresa deixa as questões relacionadas com a segurança informática para o departamento de IT tendo uma relação apenas superficial com este tema.

É essencial uma nova abordagem, uma vez que as máquinas que se encontram na área de produção são uma parte integrante do conceito de Security da empresa. Para pode implementar o conceito de forma holística e correta, a empresa tem que estar subdividida em zonas de segurança e é importante definir e implementar as interligações e requisitos desde as zonas IT até ao nível das máquinas.

Figura 9: A Industrial Security também inclui a relação entre segurança informática (IT) e segurança de tecnologia operacional (OT)

Sugestão prática:
Através do motor de busca **https://www.shodan.io/**, é possível encontrar dispositivos interligados, frenquentemente também dispositivos que já não se deveriam poder encontrar devido à segmentação de rede. Seus dispositivos também se encontram nesta lista?

Sugestão prática:
Um dos tipos de ataques mais frequentes é através dos funcionários(as) de uma empresa, por exemplo via e-mails de phishing. O treinamento regular da equipa reduz esse risco.

4. O percurso até uma máquina segura – Safe e Secure

Resumindo:
Através de uma avaliação de riscos, é possível reduzir de forma drástica os custos para as contramedidas e também para a própria análise. Assim se reduz a consideração do número de possíveis ataques aos que realmente representam uma ameaça aos objetivos de proteção definidos. A avaliação do nível potencial de danos e da probabilidade de ocorrência dá também informações adicionais de como reduzir os riscos da maneira mais razoável.

Os perigos para a segurança das máquinas podem surgir de variadas formas, quer seja através de redes de dados ou fisicamente através do acesso direto à máquina. Para proteger uma máquina da maneira mais eficiente e econômica possível, recomendamos o procedimento estruturado que descrevemos em seguida.

- **Identificar os bens**
  O primeiro passo é definir quais os bens que se devem proteger e os distinguir entre si. O resultado mostrará uma imagem consistente e completa das instalações e partes das instalações que se devem proteger. Esta medida garante que não são esquecidas partes mas também que não se consideram vetores de ataque desnecessariamente mais do que uma vez.
- **Analisar ameaças**
  No passo seguinte, é avaliado o nível potencial de danos em caso de comprometimento. Esta questão é mais fácil de responder se considerarmos as três finalidades da proteção da segurança de informação. São elas: Confidencialidade, Integridade e Disponibilidade – em inglês, Confidentiality, Integrity e Availability, frequentemente abreviado como CIA.
  - **Confidentiality (Confidencialidade)**
    Esta máquina contém informações cuja divulgação possa prejudicar a empresa? Este pode ser o caso de, por exemplo, informações sobre o processo de fabrico, receitas ou outros segredos do negócio que garantam a uma empresa a vantagem frente à concorrência. Qual o nível potencial do dano?
  - **Integrity (Integridade)**
    Que efeitos pode ter a alteração não desejada de dados? A alteração de dados pode causar danos econômicos, por exemplo através de danos na máquina, ou colocar pessoas em perigo, por exemplo, afetando funções de segurança? Qual o nível potencial do dano?
  - **Availability (Disponibilidade)**
    Que danos econômicos são causados pela falha de uma máquina, por exemplo, por interrupções na produção?
- **Definir objetivos de produção**
  Após este trabalho preliminar, é possível formular os objetivos de produção. Quanto mais concretamente se definem os objetivos, mais especificamente se podem determinar os vetores de ataque. Isto evita medidas desnecessárias que possam aumentar a segurança das máquinas, mas não contribuem para atingir os objetivos de proteção definidos.
- **Avaliar riscos**
  Depois de definidos os objetivos de proteção, é calculada a probabilidade de ocorrência dos riscos definidos. O resultado dá informações sobre o âmbito razoável de medidas a tomar.

- **Analisar vetores de ataque**
  Neste passo, é definido de forma sistemática quais as fontes possíveis de um ataque e que medidas de proteção já existem, por exemplo, através de medidas de proteção intrínsecas em componentes de máquinas utilizados. O resultado é uma lista das fontes de perigo restantes.
- **Criar e implementar um conceito de segurança**
  O conceito de segurança (Security) descreve de forma concreta todas as medidas necessárias para atingir os objetivos de proteção definidos para a máquina em questão. Estas tanto podem ser medidas construtivas na máquina como também adaptações organizacionais nos processos.
- **Controlar a implementação**
  A eficácia real das medidas implementadas só pode ser testada através de testes de penetração complicados nos quais os ataques de hackers são simulados por serviços especializados. Como alternativa, a implementação correta do conceito de segurança deve ser testada.
- **Realizar novas avaliações com frequência**
  Ao contrário da Safety, as medidas de proteção para a Security não são casos únicos. Uma vez que em sistemas complexos surgem sempre novos pontos vulneráveis, a avaliação deve ser feita em intervalos regulares ou sempre que há conhecimento de novas ameaças. Os novos pontos vulneráveis podem surgir em todos os níveis da pirâmide de aquisições, por exemplo, componentes de hardware, open source code em dispositivos ou firmware de dispositivos específicos. Assim que é detetado um ponto vulnerável, os fabricantes responsáveis publicam as respectivas Security Advisories com informações sobre a ameaça e sobre contramedidas adequadas. Recomendamos que se informe frequentemente sobre novas Security Advisories dos fornecedores.

Figura 10: Apenas uma inspeção de segurança pode proteger mesmo de forma segura as máquinas, componentes e instalações contra corrupção

Sugestão prática:
Pode consultar os Pilz Security Advisories em **www.pilz.com/advisories**

5. Safety e Security de um único fornecedor

Com as novas legislações sobre o tema da segurança, surgem novos desafios para os fabricantes e operadores de máquinas. Os processos para redução de riscos de ataques a máquinas (Security) são muito semelhantes aos processos para redução dos riscos que podem advir de máquinas (Safety). Como especialista em segurança de máquinas, a Pilz o ajuda passo-a-passo a chegar a soluções precisas e máquinas seguras – Safe e Secure.

Figura 11: Safety e Security fazem ambas parte da segurança de máquinas como conceito holístico

- Conhecimento técnico e know-how através da participação em comitês de normas
- Pesquisa e acompanhamento do estado atual das leis e normas
- Treinamentos básicos e especializados para a Industrial Security de máquinas
- Serviços no âmbito da Industrial Security de máquinas
  - Análise das necessidades de proteção
  - Avaliações de riscos
  - Conceitos de segurança holísticos
  - Validações/Certificações
  - Otimizações de processos
- Produtos e soluções para controle físico de acesso e segurança cibernética na máquina

Figura 12: Passo-a-passo para uma máquina segura com soluções de Industrial Security

Sugestão prática:
Mais sobre soluções de Industrial Security na Pilz em **www.pilz.com/security**

6. Sumário e perspectivas

O aumento das ameaças através de ataques cibernéticos e corrupção teve um impacto direto na situação legislativa na Europa resultando numa clara tendência por parte dos legisladores na direção da Industrial Security: no futuro, as entidades legisladoras colocarão novas exigências à Industrial Security, em particular através do Regulamento de Máquinas, da Diretriz NIS 2 e o CRA. Para os fabricantes e operadores de máquinas, isto implica um envolvimento ativo de desenvolvimento e implementação de medidas organizacionais e técnicas para cumprir com os novos requisitos para empresas, máquinas e componentes. O presente guia explicou essas tarefas e como lidar com elas.

A Diretriz NIS 2 já é obrigatória para a maior parte dos fabricantes e operadores de máquinas, em 2027 seguirá o novo Regulamento de Máquinas e também o CRA. Agindo preventivamente, poderá planejar e implementar todos os projetos necessários a tempo.

Os comitês de normas orientam os fabricantes para que possam implementar os novos requisitos. É importante uma abordagem estruturada como descrito na série de normas IEC 62443.

Serviços experientes e qualificados ajudam a analisar passo-a-passo as medidas necessárias para cumprir com os novos objetivos com um esforço fácil de gerenciar.

Segurança de máquinas irá significar no futuro Safety e Security – para a proteção de pessoas e de máquinas. Com um conceito holístico e coordenado, é possível segmentar problemas complicados de segurança de máquinas de forma eficiente e limpa. Uma avaliação de riscos representa também o primeiro passo para a Industrial Security e oferece uma orientação estruturada e método para compreender as exigências para a própria empresa.

Esta abordagem dá às empresas as ferramentas necessárias para fazer frente aos desafios crescentes na área da Industrial Security.


Mais informações sobre Industrial Security da Pilz – descubra agora
PILZ
Saiba mais em:
www.pilz.com/security

7. Apêndice

7.1. Termos da área da Industrial Security

Cibersegurança ou segurança cibernética designa todas as atividades necessárias proteger sistemas de rede e de informação, os usuários desses sistemas e outras pessoas afetadas por ameaças cibernéticas.

Ameaça cibernética designa uma possível circunstância, um possível evento ou uma possível ação que possa danificar, interferir ou afetar negativamente os sistemas de rede/informação, os usuários desses sistemas e outras pessoas.

Industrial Security tem como objetivo garantir a disponibilidade das máquinas e das instalações, bem como a integridade e a confidencialidade dos dados e dos processos da máquina.

IT Security (Information Technology) é a proteção dos dados fora dos processos físicos.

OT Security (Operational Technology) é a proteção de máquinas e instalações que fazem parte dos processos físicos.

IACS é uma abreviatura da IEC 62443 e significa Industrial Automation and Control System(s) – em português, sistemas de automação e controle industrial.

Security Level da série de normas IEC 62443 é o nível que corresponde às medidas necessárias e às propriedades de segurança inerentes de dispositivos e sistemas para uma zona ou conduta com base na avaliação dos riscos para os mesmos.

Zona é o resumo de unidades que representam a divisão de um sistema inspecionado com base em suas relações funcionais, lógicas ou físicas (incluindo o local).

Conduta é o agrupamento lógico de canais de comunicação que liga duas ou mais zonas para as quais se aplicam requisitos informáticos em comuns.

7.2. IEC 62443 – norma básica para Industrial Security

IEC 62443 é uma série de normas internacionais para “Redes de comunicação industriais – Segurança IT para Redes e Sistemas”:

7.2.1. Resumo

A família de normas IEC 62443 é composta por diferentes partes; dessas partes, as seguintes normas já foram ao presente publicadas.

A parte 1 trata os seguintes princípios:
- IEC TS 62443-1-1: Parte 1: Termos e Modelos
- IEC TS 62443-1-5: Parte 1-5: Esquema para perfis de segurança informática IEC 62443

A parte 2 refere-se às exigências de segurança para operadores e prestadores de serviços:
- IEC 62443-2-1: Criação de um programa para a segurança informática para sistemas de automação industriais
- IEC 62443-2-2: IACS Classificações de programa de segurança
- IEC TR 62443-2-3: Gerenciamento de patches para sistemas de automação industrial
- IEC 62443-2-4: Requisitos ao programa de segurança informático de prestadores de serviços para sistemas de automação industriais

A parte 3 refere-se às exigências de segurança para sistemas de automação
- IEC TR 62443-3-1: Técnicas para sistemas de automação industriais
- IEC TR 62443-3-2: Avaliação de riscos de segurança e configuração do sistema
- IEC 62443-3-3: Requisitos de sistema para segurança informática e nível de segurança

A parte 4 descreve os requisitos de segurança para componentes do sistema
- IEC 62443-4-1: Requisitos para o ciclo de vida para um desenvolvimento de produto seguro
- IEC 62443-4-2: Requisitos para componentes de sistemas de automação industrial

A parte 5 define os perfis da IEC 62443
- IEC TS 62443-1-5: Esquema para perfis de segurança informática IEC 62443

A parte 6 descreve a metologia de avaliação
- IEC 62443-6-1: Metodologia da avaliação de segurança para IEC 62443-2-4

7.2.2. Security Level (SL)

Os requisitos para sistemas e componentes são descritos em níveis de segurança, ou seja, Security Levels. Estes definem-se da forma seguinte:

- Security Level 0: Nenhum requisito ou proteção em especial
- Security Level 1: Proteção contra utilização indevida involuntária ou acidental
- Security Level 2: Proteção contra utilização indevida intencional utilizando meios simples com poucos recursos, competências gerais e baixa motivação
- Security Level 3: Proteção contra utilização indevida intencional com meios sofisticados com recursos moderados, conhecimentos específicos de IACS e motivação moderada
- Security Level 4: Proteção contra utilização indevida intencional utilizando meios sofisticados com recursos extensivos, conhecimentos específicos de IACS e motivação elevada

Isto significa que, quando mais elevado o Security Level, mais eficazes são as medidas implementadas.

Existem sete requisitos básicos (em inglês: Foundational Requirements, FR):

- FR 1 – Identificação e Autenticação
- FR 2 – Controlo de utilização
- FR 3 – Integridade do sistema
- FR 4 – Confidencialidade dos dados
- FR 5 – Fluxo limitado de dados
- FR 6 – Reação atempada a eventos
- FR 7 – Disponibilidade de recursos

Por trás de cada um destes requisitos básicos encontram-se medidas com qualidades variadas que podem ser aplicadas para atingir o nível requerido. Medidas típicas são a autenticação multi-fator ou mecanismos de encriptamento.

O Security Level que deve ser atingido depende do risco cibernético. Os legisladores europeus distinguem entre entidades importantes e entidades essenciais. O risco cibernético a assumir depende do tipo de empresa, do tamanho da empresa e do potencial impacto. Muitas associações de organização de normas se ocupam neste momento com esta temática definindo requisitos universais para indústrias e tipos de máquinas.

7.2.3. Information Security Management System (ISMS)

A par dos requisitos técnicos para componentes e sistemas, existem também medidas organizacionais que têm que ser implementadas para reduzir o risco de um ataque realizado com sucesso. Cada companhia tem que decidir por si como gostaria de criar o seu Information Security Management System (ISMS). A série de normas ISO/IEC 27000 está estabelecida e é geralmente conhecida. A IEC 62443-2-1 pode ser vista como um guia para a implementação de ISO/IEC 27001 a sistemas de automação industrial. A par disso, existem também, entre outros, o programa de certificação TISAX que também provou ser adequado.

No ISMS, são nomeados, classificados e avaliados os riscos e também a forma de lidar com eles. Normalmente é necessário definir primeiro a área de aplicação e as interligações a outras áreas. Também é essencial:
- Assunção da responsabilidade pela Segurança por parte da direção
- Clarificação das responsabilidades
- Definição de medidas de treinamento avançado
- Criação de diretrizes de segurança em empresas

O ISMS ajuda a considerar sistematicamente os riscos e a adotar medidas adequadas.

Os riscos podem incluir:
- Danos econômicos causados pela interrupção na produção
- Ferimento de funcionários
- Violação da proteção de dados
- Danos ambientais
- Perda da confiança do cliente

Medidas típicas podem incluir, entre outras:
- Desenvolvimento de planos de emergência a aplicar
- Definição de usuários autorizados
- Controles de acesso físicos e virtuais
- Segmentação de rede

A implementação de medidas também é descrita no ISMS. Esta inclui:
- Desenvolvimento do sistema
- Manutenção do sistema
- Proteção de dados
- Planejamento e forma de lidar com incidentes

7.3. Outros documentos importantes para fabricantes e operadores de máquinas

Para além da família de normas IEC 62443, já existem outras normas de segurança que afetam a construção de máquinas e definem requisitos.

A IEC TS 63074 descreve os aspetos de segurança em relação à segurança funcional de sistemas de comando relacionados com a segurança. Nesta especificação técnica são definidos os aspetos relevantes da família de normas IEC 62443 que têm que ser considerados para garantir a operação segura da máquina.

Para o requisito “Proteção contra corrupção” do Regulamento de Máquinas, encontra-se neste momento em desenvolvimento um nova norma europeia: EN 50742. A Pilz é um membro ativo do comitê de normas.

A partir da Diretriz relativa aos equipamentos de rádio 2014/53/EU e do seu regulamento respetivo (EU) 2022/30 também resultam requisitos de segurança. Para estes requisitos, foi desenvolvida e série de normas EN 18031.

7.4. Segmentação de rede com base no modelo Purdue

Para uma melhor compreensão do tema segmentação de rede, é útil o modelo Purdue desenvolvido por Theodore Joseph Williams (professor de Engenharia na Universidade americana de Purdue) e publicado em 1990. Na imagem seguinte, o modelo Purdue foi ampliado para incluir exemplos de medidas para os nossos fins.

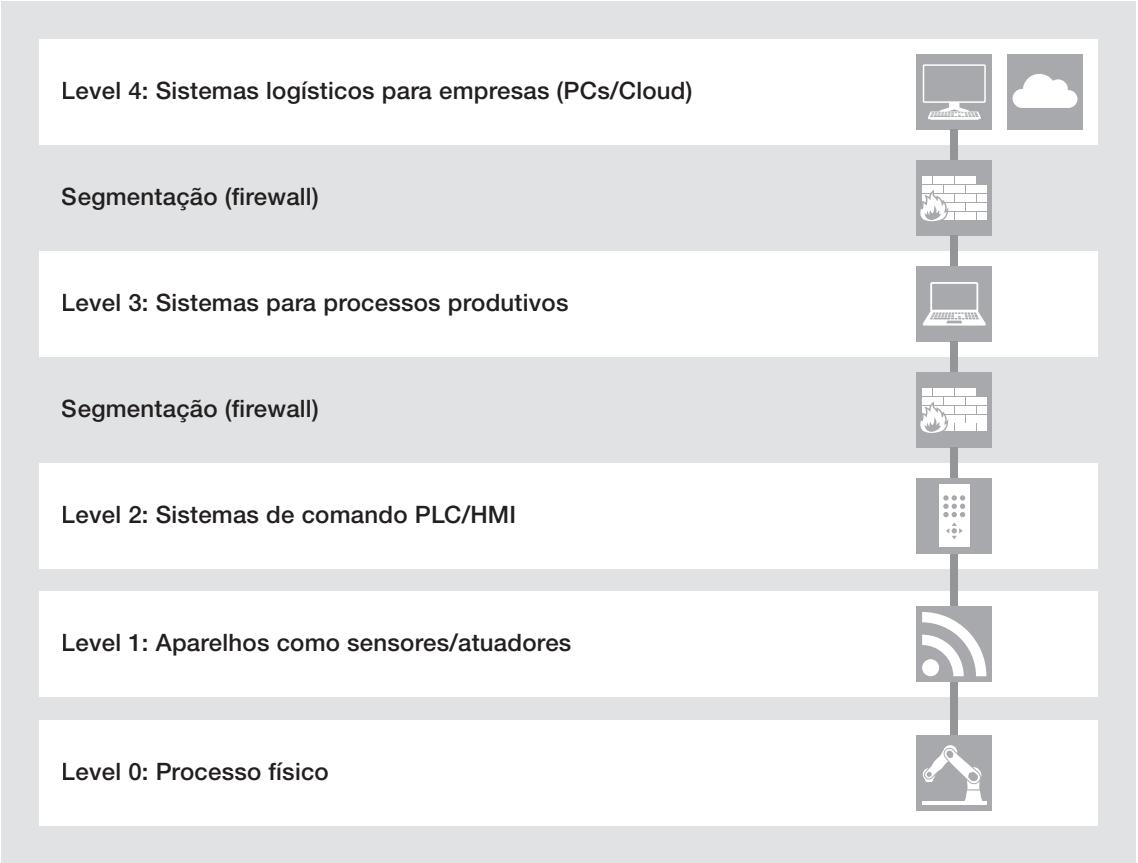

Figura 13: Segmentação de rede com base no modelo Purdue

O Level 0 é o processo físico real normalmente executado na indústria transformadora. Este é normalmente monitorado e operado com sensores e atuadores. Estes dispositivos pertencem ao Level 1. O processo é normalmente controlado por um comando de memória programável (PLC) que pertence ao Level 2. A programação do PLC é feita via sistemas para processos de produção no Level 3. As encomendas efetivas vêm do sistema logístico no Level 4.

Level 0 até 3 estão incluídos na designação Operational Technology (OT), Level 4 e tudo para além disso está incluído na designação Information Technology (IT).

A imagem mostra já uma forma de segmentação que, neste caso, funciona via firewalls que limitam a transferência de dados entre Level 4 e 3 ou 3 e 2 de modo a reduzir a superfície de perigo potencial.

O objetivo é implementar uma segmentação bem sucedida, ou seja, tanto foram reduzidas com eficácia as possibilidades de ataque como se manteve um sistema que não tem o seu desempenho limitado. Para tal, é importante que as interligações estejam definidas de forma clara; o resultado sendo que, por exemplo, todas as portas e tipos de protocolo tenham sido considerados na configuração da firewall.

A seleção correta dos componentes adequados é fundamental para uma operação segura. Na verdade, a melhor firewall não produz efeito se existirem pontos vulneráveis nos níveis inferiores devido aos componentes. Dependendo do nível de segurança exigido, poderá ser necessário que os componentes dentro de um sistema se autentifiquem uns aos outros, monitorando assim alterações no sistema. Isto também deve ser considerado na seleção dos componentes e sua configuração.

Neste exemplo, todos os componentes a partir do Level 3 estão interligados permanentemente e o fluxo de informação é protegido por duas firewalls. No campo industrial é perfeitamente normal que os sistemas possuam interligações sem cabos (por exemplo, no caso dos sistemas de transporte autônomos). Aqui é necessário testar como se podem implementar medidas de seguranças com eficácia.

Sugestão prática:
Consulte a **www.pilz.com** para obter exemplos práticos de configuração de seus dispositivos. Para tal, insira na função de busca: “application notes”.

8. Bibliografia

- 1.a Reference model for computer integrated manufacturing (CIM): a description from the viewpoint of industrial automation. Edited by 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. Regulamento de Máquinas da UE 2023/1230 (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023R1230)
- 5. Diretriz (UE) 2022/2555 sobre medidas para um elevado nível de segurança cibernético na União (https://eur-lex.europa.eu/legal-content/DE/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)
- 7. Diretriz 2009/104/EG (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32009L0104)
- 8. Agência da União Europeia para a Cibersegurança (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)
- 13. Guia sobre o Regulamento de Máquinas whitepaper (Pilz 2023) (www.pilz.com/mr)
- 14. https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview (visto 20/01/2025)
- 15. Cybersecurity Act EU 2019/881, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1728407971719

Suporte

O suporte técnico da Pilz está à sua disposição 24 horas por dia.

América
Brasil
+55 11 97569-2804
Canadá
+1 888 315 7459
México
+52 55 5572 1300
EUA (grátis)
+1 877-PILZUSA (745-9872)

Ásia
China
+86 400-088-3566
Coréia do Sul
+82 31 778 3390
Japão
+81 45 471-2281

Austrália e Oceania
Austrália
+61 3 95600621
Nova Zelândia
+64 9 6345350

Europa
Alemanha
+49 711 3409-444
Áustria
+43 1 7986263-444
Bélgica, Luxemburgo
+32 9 3217570
Escandinávia
+45 74436332
Espanha
+34 938497433
França
+33 3 88104003
Grã-Bretanha
+44 1536 460866
Holanda
+31 347 320477
Irlanda
+353 21 4804983
Itália, Malta
+39 0362 1826711
Suíça
+41 62 88979-32
Türkiye
+90 216 5775552

Para contatar nossa linha de assistência internacional, marque:
+49 711 3409-222
support@pilz.com

A Pilz desenvolve produtos inofensivos ao meio ambiente, com o uso de materiais ecológicos e tecnologias que economizam energia. Em edificações ecológicas, trabalha-se e produz-se com economia de energia e respeito ao meio ambiente. Deste modo, a Pilz lhe oferece sustentabilidade aliada à segurança de estar comprando produtos eficientes em termos energéticos e ecológicos.

BLUeCOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards
BRAND OF THE CENTURY 2022

Quality Management ISO 9001:2015 REG. NO. 2462
Environmental Management ISO 14001 REG. NO. 2462
Energy Management ISO 50001 REG. NO. 2462

Entregue por:

Nós somos representados internacionalmente. Para maiores informações consulte o nosso sítio na Internet www.pilz.com ou contate a nossa matriz.

Matriz: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Alemanha
Telefone: +49 711 3409-0, E-mail: info@pilz.com, Internet: www.pilz.com

Impresso em papel 100% reciclado para o bem do meio ambiente.

PILZ
THE SPIRIT OF SAFETY

8-4-pt-3-023, 2025-05 Printed in Germany