Informação em segundo plano

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Alemanha/Germany
www.pilz.com

Proteção para empresas, máquinas e produtos

Safety e Industrial Security: tudo de um só fornecedor

Ostfildern, outubro de 2025 - **Os incidentes de Security não afetam apenas os sistemas de TI, mas, cada vez mais, o ambiente de produção (TO). Na área de Industrial Security, incidentes incluem não apenas ataques direcionados, mas também manipulações não intencionais. O dever da Industrial Security na produção é garantir a disponibilidade das máquinas e das instalações, bem como a integridade e a confiabilidade dos dados e dos processos da máquina. No entanto, a maior meta de proteção é a segurança funcional. Se as empresas não tiverem soberania sobre seus dados, a empresa e a segurança de seus funcionários estarão em risco: sem Security não há Safety e sem Safety não há proteção das pessoas!**

Na União Europeia, a crescente situação de ameaça foi reconhecida e a legislação foi adaptada de acordo: no nível empresarial, a **Diretiva NIS 2** exige medidas para garantir um alto nível comum de segurança cibernética na União Europeia, por exemplo, por meio de um sistema de gerenciamento de segurança da informação.

O **Regulamento de Máquinas da UE 2023/1230** agora fornece proteção contra degradação para máquinas e instalações e exige medidas de Industrial Security para as peças da máquina que influenciam a segurança funcional.

A Lei de Resiliência Cibernética da União Europeia (em inglês, Cyber Resilience Act (CRA)) exige medidas de Security para produtos com elementos digitais. Isso também inclui controladores, sistemas IO e outros componentes usados em máquinas.

Empresas, máquinas e produtos: os fabricantes e operadores de máquinas enfrentam desafios diversos e diferentes enquadramentos legais em todos os níveis.

Segurança de última geração

Independentemente de os legisladores tornarem a Industrial Security obrigatória, há uma série de boas razões para se preocupar com o tema o mais cedo possível e procurar aconselhamento. Os processos e as condições estabelecidos para a operação das máquinas podem favorecer a manipulação se não forem analisados regularmente. Por exemplo, os sistemas de máquinas com uma longa vida útil muitas vezes envelhecem e, em algum momento, já não cumprem os padrões de segurança atuais. Esses sistemas apresentam lacunas de segurança que não podem mais ser eliminadas, porque o provedor não fornece mais atualizações de segurança. Além disso, a proteção contra malwares muitas vezes não pode ser implementada nos dispositivos finais, pois alguns são muito antigos e seu desempenho seria prejudicado, o que pode levar a falhas de produção.

Passo a passo para mais Industrial Security

Em última análise, trata-se de garantir que as operações comerciais permaneçam protegidas, mas, para isso, as empresas têm de superar diferentes desafios: identificação das normas legais aplicáveis, reconhecimento e resolução de vulnerabilidades nos sistemas, sensibilização e treinamento dos colaboradores e posterior implementação de controles. Visto que a Security é um alvo móvel (do inglês, "moving target"), também é necessária uma verificação regular do estado da Industrial Security das máquinas. É importante ter responsabilidades claras dentro da empresa e uma abordagem

sistemática que inclua o desenvolvimento do conhecimento especializado necessário.

A empresa de automação Pilz adaptou-se a essas exigências e desenvolveu um portfólio de serviços personalizados para fabricantes e usuários de máquinas que abrange de forma holística todos os aspectos da proteção de pessoas e máquinas. Os especialistas da Pilz conhecem as exigências legais e normativas atuais e as incorporam em suas recomendações. Para desenvolver ou atualizar o conhecimento sobre Security nas empresas, os cursos de treinamento complementam a oferta. A implementação prática também ocorre com a ajuda das soluções de produtos da Pilz, como a linha de gerenciamento de identificação e acesso I.A.M. (Identification and Access Management), que contribui para maior Safety e Industrial Security.

Estabelecendo a base correta

Para garantir a Industrial Security nas suas máquinas, os especialistas em engenharia mecânica e de instalações precisam de uma base sólida de conhecimentos, principalmente no que diz respeito à legislação e às normas aplicáveis. Os especialistas da Pilz transmitem esse know-how no treinamento "Fundamentos da Industrial Security". Os participantes aprendem a identificar ameaças à Security, aplicar medidas de proteção adequadas e seguir as melhores práticas para a segurança de máquinas e redes. Como resultado, até mesmo novatos no tópico de Security aprenderão quais medidas podem ser tomadas para proteger efetivamente as máquinas contra ataques cibernéticos e manipulação no nível de produção da máquina.

Com a qualificação "CESA - Certified Expert for Security in Automation", a Pilz oferece um curso especializado de dois dias, que

transmite aos participantes um conhecimento aprofundado sobre Security, de acordo com as normas mais recentes, especialmente com relação à série de normas IEC 62443 ("Rede de comunicações industriais - segurança de TI para redes e sistemas"). Além disso, são abordadas medidas práticas de redução de riscos, como controle de acesso, aumento da segurança da rede por meios técnicos e medidas organizacionais para reduzir os riscos de Security. Os participantes aprenderão a aplicar a norma corretamente e a demonstrar que os seus sistemas de automação atendem às exigências de segurança cibernética. Ao passar na prova, os participantes recebem o certificado internacionalmente reconhecido da TÜV NORD para "CESA – Certified Expert for Security in Automation".

Implementar o conhecimento teórico na prática

Com base nos fundamentos teóricos e nos treinamentos, o próximo passo para fortalecer a Industrial Security é aplicar processos estruturados e orientados à prática. A consultoria na área de Tecnologia Operacional (TO) cria a transição da base teórica para estratégias implementáveis. Usando uma abordagem gradual, os Industrial Security Services identificam vulnerabilidades em sistemas complexos e desenvolvem contramedidas para minimizar os riscos. Isso resulta em um conceito de segurança holístico.

Quatro etapas para aumentar a Industrial Security

O processo de Security da TO possui quatro etapas: análise das necessidades de proteção, avaliação dos riscos de Industrial Security, conceito de Industrial Security e verificação do sistema de Industrial Security.

Durante a primeira etapa, a empresa determina as necessidades de proteção dos ativos individuais na máquina ou no sistema e suas metas de proteção. No segundo passo, a avaliação de riscos, são considerados todos os riscos e a probabilidade de ocorrência para cada área ao longo de todo o ciclo de vida do sistema. A próxima etapa é a criação de um conceito detalhado de Industrial Security com estratégias e medidas de defesa e mitigação dos riscos causados por ataques, manipulação e erros operacionais. Além disso, são criadas políticas, regras e diretrizes para a continuidade da operação ou da construção segura do sistema. No último passo, a verificação do sistema de Industrial Security, a eficácia das contramedidas implementadas é avaliada.

Garantir a disponibilidade da máquina

O processo de Industrial Security Services ajuda a mitigar ou evitar ataques cibernéticos. Com ele, diminui-se também o número de incidentes de segurança desencadeados involuntariamente. Isso, por sua vez, aumenta a disponibilidade da máquina e, em última análise, garante economia de custos e manutenção da lucratividade.

Essa abordagem protege principalmente as pessoas na máquina com contramedidas de Security adequadas, porque um incidente de segurança pode se tornar um impeditivo para as medidas de segurança. Uma cortina de luz na frente das máquinas, por exemplo, garante que o operador não entre em uma área de perigo. No entanto, se um invasor puder influenciar o controle e o mecanismo correspondentes, a função protetora da cortina de luz não poderá mais ser garantida. Security protege Safety!

Quando se trata de implementação concreta na máquina, faz sentido considerar Safety e Security em conjunto. Sem Security, não há Safety; e sem Safety, não há proteção de pessoas.

Regulamentação clara: quem pode fazer o que na máquina?

A segurança de uma máquina e de seu operador depende da regulação do acesso, seja de pessoas ou de rede. As entradas devem ser protegidas contra acessos não autorizados para que, por exemplo, não haja pessoas na área de perigo durante a operação da máquina, pois mesmo a operação ou a manutenção bem-intencionada de um sistema, seja no local ou através de uma rede, pode ter consequências fatais.

Um componente importante é o gerenciamento de identificação e acesso (I.A.M., Identification and Access Management), que regulamenta claramente as autorizações e os acessos a máquinas e instalações na empresa. Isso inclui medidas e especificações organizacionais, assim como funções de segurança adequadas. Um sistema de autorização de acesso, como a PITreader da Pilz, é o componente de produto adequado nesse caso. Com ele, os usuários atendem aos requisitos de proteção de funcionários, proteção de responsabilidades, produtividade máxima e proteção dos seus dados.

Somente uma abordagem holística de Safety e Security garante uma proteção completa de pessoas e máquinas. Não cabe mais à empresa escolher se quer ou não lidar com Security e até que ponto deve fazê-lo. Atualmente trata-se de uma exigência legal. Na engenharia mecânica, a Security, sob a forma de Industrial Security, não é uma tarefa exclusiva do departamento de TI, mas parte essencial do projeto e da construção. A implementação tardia da Security é trabalhosa e, normalmente, resulta em perdas na facilidade de uso, na funcionalidade e na produtividade.

((Caracteres: 9.784))

((Caixa:))

Uma visão geral da legislação da UE em matéria de Industrial Security

Na Europa, em particular, os legisladores estão respondendo à situação de ameaça com uma série de leis. Com isso, as regulamentações mais rigorosas do mundo se aplicam na Europa. Mas votações já estão sendo realizadas em outros países, nos quais essas leis também chegarão. Portanto, podemos esperar uma harmonização mundial em relação à Industrial Security.

NIS 2: mais obrigações para as empresas

A NIS (Segurança das Redes e da Informação) é uma diretriz da União Europeia que visa fortalecer a segurança cibernética. Esta diretriz está em vigor desde 2016 e, até agora, foi aplicada a fabricantes na área de infraestrutura, incluindo energia, transporte, bancos e finanças, saúde, abastecimento e distribuição de água potável e infraestrutura digital. Os fornecedores desses setores foram obrigados a tomar “medidas de segurança adequadas” e relatar incidentes graves de segurança cibernética. A nova Diretiva NIS 2 ((UE) 2022/2555 ... sobre medidas para um alto nível comum de segurança cibernética em toda a União Europeia) exige que um número significativamente maior de empresas adote medidas de gerenciamento de riscos de segurança cibernética no futuro. A NIS 2 amplia os setores para incluir, por exemplo, a indústria de produção, incluindo engenharia mecânica e fabricantes de equipamentos elétricos.

São exigidas análises de risco e conceitos de segurança para sistemas de informação, proteção da cadeia de abastecimento e segurança da equipe. Também estão incluídos conceitos de controle de acessos e gestão de sistemas, bem como treinamentos obrigatórios para a gestão.

A diretriz foi adotada pelo Parlamento Europeu e pelo Conselho da UE no final de 2022. Como todas as diretrizes da UE, a NIS 2 não é diretamente válida e obrigatória em cada estado-membro da UE, mas deve ser implementada na legislação nacional pelos estados-membros. É bom que as organizações lidem com NIS 2 o mais rápido possível e realizem uma avaliação de Security completa na empresa. Isso inclui, por exemplo, a criação de um sistema de gerenciamento de segurança da informação (ISMS). A certificação de acordo com a norma de segurança da informação ISO 27001 é adequada nesse contexto.

NIS 2 usando instalações eólicas como exemplo: com a NIS 2, os montadores de máquinas, como os fabricantes de usinas de geração de energia (por exemplo, turbinas eólicas), também precisarão atender aos requisitos no futuro. O fabricante de turbinas eólicas, por sua vez, necessita de soluções de automação, controles ou sensores, por exemplo. A partir de um determinado tamanho, os fabricantes de componentes elétricos também se enquadram na NIS 2. E como a NIS 2 estipula que os fornecedores devem ser considerados, uma empresa como a Pilz também precisa cuidar de cadeias de suprimento seguras e impor exigências aos seus fornecedores. Portanto, a NIS 2 cobre toda a cadeia de suprimentos.

O novo Regulamento de Máquinas: sem Security, sem marcação CE

No âmbito da segurança funcional de máquinas, a Diretriz de Máquinas 2006/42/CE sempre teve importância essencial.

Desde sempre, os fabricantes de máquinas precisam passar por um procedimento de avaliação de conformidade para poder importar máquinas para a Europa, ao fim do qual há a marcação CE.

Em junho de 2023, com a nova publicação do Regulamento de Máquinas, as especificações foram atualizadas. Como se trata de um regulamento, ele não precisa ser transposto para a legislação nacional. Os fabricantes de máquinas têm até 20 de janeiro de 2027 para se adaptarem aos novos requisitos e cumpri-los dentro do prazo.

O Regulamento de Máquinas substitui a Diretriz de Máquinas anterior e, ao contrário da antecessora, tornará a segurança cibernética obrigatória. Enquanto a Diretriz de Máquinas se preocupava puramente com Safety, no Regulamento o objetivo de proteção Safety em "Protection against corruption" foi incluído em "Essential health and safety requirements EHSR": as funções de segurança da máquina não devem ser prejudicadas por adulteração acidental ou intencional.

Este novo caminho para a marcação CE levanta uma série de novas questões para os fabricantes e operadores de máquinas, pois terão que rever os seus conceitos de segurança anteriores para Safety e Security.

Cyber Resilience Act: segurança durante todo o ciclo de vida do produto

Além de olhar para a empresa e as máquinas, é absolutamente essencial implementar medidas de Security diretamente em

dispositivos, como controladores. 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 tanto produtos do setor B2C, como smartphones ou robôs aspiradores, como do setor B2B, como controladores e sensores, mas também produtos de software puros, como sistemas operacionais ou a própria máquina.

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 estados-membros da UE.

A dimensão real do impacto do CRA dependerá dos critérios que serão usados para categorizar os produtos. De acordo com o CRA, somente podem ser comercializados produtos que garantam um nível adequado de segurança cibernética durante todo seu ciclo de vida. Security, então, começa na fase de desenvolvimento do produto. Há alguns anos, a Pilz vem alinhando seus processos de desenvolvimento à IEC 62443-4-1 "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements" e desenvolvendo, por exemplo, o SecurityBridge de forma comprovadamente segura.

((Caracteres: 6.062))

A Pilz é uma fornecedora global de produtos, sistemas e serviços de tecnologia de automação. Pioneira na área de automação segura, a Pilz cria segurança para pessoas, máquinas e meio ambiente. Fundada em 1948, a empresa familiar com sede em Ostfildern hoje está presente no mundo todo com 2.500 colaboradores em 42 filiais e subsidiárias.

Líder em tecnologia, a empresa oferece soluções completas de automação para Safety e Industrial Security de máquinas. Entre essas soluções há sensores, bem como tecnologia de comando e acionamento, incluindo sistemas para comunicação industrial, diagnóstico e visualização. Uma gama internacional de serviços com consultoria, engenharia e treinamento complementa o portfólio. As soluções da Pilz são utilizadas não somente na engenharia mecânica e industrial, mas também em numerosos setores, como intralogística, embalagem, tecnologia metroferroviária e robótica.

www.pilz.com

A Pilz nas redes sociais:

Em nossos canais de mídia social, oferecemos informações básicas sobre a empresa e a equipe da Pilz, além de comunicação sobre as últimas novidades da tecnologia de automação.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contato para a imprensa:

Martin Kurth

Imprensa corporativa e especializada
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Imprensa especializada e corporativa
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Imprensa especializada

Tel: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle

Imprensa especializada

Tel.: +49 711 3409-7147
e.roessle@pilz.de