25.05.2023

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

Mensagem jornalística

Thomas Pilz: Safety e Security para automação digital

Ostfildern, 25.05.2023 - **(A palavra falada prevalecerá)**

Thomas Pilz

Security: O que está por vir na indústria e na engenharia mecânica em termos de legislação

Atualmente, está ocorrendo uma mudança radical nas normas e leis de segurança no ambiente industrial. Isso está sendo capitaneado pela Security e pela inteligência artificial (IA). Para a indústria em geral e para a engenharia mecânica e de instalações, três diretrizes novas ou futuras são relevantes para Security: a Diretriz NIS 2 da UE, o novo Regulamento de Máquinas e a Cyber Resillience Act.

Como na coletiva de imprensa do ano passado, vou me concentrar em Security e gostaria de demonstrar a extensão dos efeitos para toda a indústria.

NIS 2: Mais obrigações e mais sanções para mais empresas

NIS (segurança da rede e da informação) é uma diretriz da União Europeia para fortalecer a segurança cibernética. Esta diretriz está em vigor desde 2016 e, até agora, foi aplicada a provedores de infraestrutura crítica, incluindo energia, transporte, bancos e finanças, saúde, abastecimento e distribuição de água potável e infraestrutura digital. Os provedores desses setores foram obrigados a tomar “medidas de segurança adequadas” e relatar incidentes graves de segurança cibernética. A NIS 2 é a sucessora, tendo entrado em vigor no início de 2023, e deve ser transposta para a legislação nacional pelos estados-membros da União Europeia até o segundo semestre de 2024. A diretriz agora também se aplica aos setores de engenharia mecânica e automotiva, bem com a empresas com mais de 50 funcionários ou faturamento anual superior a 10 milhões de euros. De acordo com a VDMA, isso afeta cerca de 9.000 empresas em toda a Europa. No futuro, essas empresas deverão comprovar que tomaram medidas técnicas, operativas e organizacionais para proteção em caso de incidentes de Security. Em primeiro lugar, isso inclui a análise de riscos dos sistemas existentes, também em ambientes de produção, ou seja, OT (Operations Technology). Em seguida, há o desenvolvimento e a implementação de processos e medidas específicos, como proteção por senha ou criptografia, além de formação contínua e treinamento dos funcionários. Os incidentes de segurança cibernética devem ser relatados às autoridades competentes dentro de 24 horas. A inclusão expressa de cadeias de suprimentos também é nova. Em resumo, a NIS 2 agora afeta mais empresas, amplia as obrigações e prevê sanções mais rigorosas. As empresas que não tomarem nenhuma medida, enfrentarão penalidades severas.

Cyber Resilience Act: Security para todo o ciclo de vida do produto

Em setembro de 2022, a Comissão Europeia apresentou um projeto de regulamentação para aumentar a segurança cibernética dos produtos. Esta Cyber Resilience Act é voltada a fabricantes de produtos com elementos digitais. Isso significa tanto hardware como software (por exemplo, firmware). A regulamentação trata tanto de produtos de consumo como de produtos para aplicação industrial, como sistemas de controle de máquinas. De acordo com a Cyber Resilience Act, somente podem ser comercializados produtos que garantam um nível adequado de segurança cibernética. Além disso, os fabricantes são obrigados a informar os clientes sobre as vulnerabilidades de segurança o mais rápido possível e remediá-las. Sendo assim, a regulamentação afeta todo o ciclo de vida de um produto. Isso significa que agora os fabricantes também devem oferecer atualizações de software além do período normal de garantia para evitar ameaças futuras. Presumimos que o regulamento seja adotado no final de 2024.

O novo Regulamento de Máquinas: segurança cibernética como obrigação

A terceira nova diretrz de Security é o Regulamento de Máquinas da UE. Sua publicação está prestes a ocorrer. Como se trata de um regulamento, ele não precisa ser transposto para a legislação nacional. Os fabricantes de máquinas têm 42 meses para cumprir os novos requisitos. O Regulamento de Máquinas substituirá 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 novo, 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. Até o momento, sabe-se que a conformidade com os requisitos da Cyber Resiliance Act levam a uma presunção de conformidade com o Regulamento de Máquinas.

E agora: Quem deve cuidar do quê?
Qual a importância dos requisitos legais agora? Eu gostaria de usar o setor de geração de energia como exemplo para ilustrar as relações:
Até o momento, somente os fornecedores de energia foram afetados pela Diretriz NIS. Com a NIS 2, os construtores de máquinas, como fabricante 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, precisa de soluções de automação, por exemplo, comandos ou sensores da Pilz. 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.

Desde sempre, os fabricantes de máquinas precisam passar pelo procedimento de avaliação de conformidade para poder importar máquinas para a Europa, ao fim do qual há a marcação CE.Agora, com o novo Regulamento de Máquinas, os fabricantes de máquinas precisam provar que suas máquinas também estão protegidas contra adulteração. E, finalmente, os fabricantes de componentes elétricos estão sujeitos aos requisitos futuros da Cyber Resilience Act planejada.

Em resumo: Não é mais facultativo à empresa lidar ou não com Security e até qual ponto. Trata-se agora de uma obrigação legal! É bom para as empresas lidar com NIS 2 o mais rápido possível e realizar uma avaliação de Security holística para a empresa. Isso inclui, por exemplo, a criação de um sistema de gerenciamento de segurança da informação (ISMS) com certificação de acordo com a norma de segurança da informação ISO 27001.

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 retrospectiva de Security é sempre trabalhosa e, normalmente, significa perdas na facilidade de uso, na funcionalidade e na produtividade. Quando se trata de avaliação de riscos, a Safety agora é acompanhada por Security. Sem Security, sem marcação CE!

E para fabricante de produtos com elementos digitais, a série de normas IEC 62443 oferece uma boa orientação. A norma subordinada IEC 62443-4-1 descreve os requisitos para um processo denominado “Security Development Lifecycle”.

A UE assumiu a liderança na legislação de Security e a Europa aplicará as normas mais rigorosas do mundo. Mas já está ocorrendo a coordenação com outros países, aos quais essas leis também chegarão. A Austrália, por exemplo, está trocando informações com a UE e provavelmente seguirá as normas europeias. Portanto, podemos esperar uma harmonização mundial em Industrial Security.

Thomas Pilz

Padrões de comunicação abertos como tarefa que entrará para a história

Na Pilz, a abertura e a facilidade de uso são características essenciais do portfólio. Queremos oferecer aos clientes produtos que sejam sempre de última geração, fáceis de usar e que se encaixem em qualquer arquitetura de automação.

Com o SafetyBUS p, o primeiro sistema de barramento de campo seguro, e com a Ethernet segura em tempo real SafetyNET p, moldamos o desenvolvimento da comunicação industrial segura. Mas o tempo das soluções proprietárias das empresas ficou para trás. Estamos comprometidos com a criação de padrões industriais. Essa é uma tarefa que entrará para a história!

OPC UA

Para uma conexão segura e de vários fornecedores para instalações industriais, a indústria concordou com a OPC UA (Open Platform Communications Unified Architecture). Este protocolo de comunicação fornece uma interface padronizada (IEC 62541) para a comunicação entre diferentes fontes de dados no setor. Como membro da OPC Foundation, os funcionários da Pilz atuam tanto no comitê diretor como em grupos de trabalho técnicos no grupo de Field Level Communication (FLC). O foco da Pilz está no grupo de trabalho que trata de Safety (Safety over OPC UA).

Nosso know-how no uso da tecnologia publisher/subscriber (Pub/Sub) em conexão com os requisitos de protocolo de barramento de campo funcionalmente seguros é muito valioso. Em comparação com a arquitetura master/slave clássica, os dados podem ser trocados diretamente entre os participantes na Pub/Sub. Assim, o OPC UA pode ser usado para tarefas de automação exigentes e distribuídas. A Pilz dispõe de competência especial, pois o nosso SafetyNET p é o único sistema de barramento de campo seguro baseado em Ethernet e que suporta Pub/Sub desde o início.

Estamos progredindo bem em nosso trabalho em segurança funcional. Em conjunto com as autoridades de auditoria, o grupo está trabalhando na especificação dos testes e nos sistemas de teste, bem como na certificação de stacks de comunicação para OPC UA Safety. A versão 1.05 já foi lançada.

IO-Link Safety

No nível de sensores, a automação já é um grande passo em termos de abertura. O protocolo de comunicação IO-Link Safety está prestes a se tornar comercialmente disponível. A comunicação ponto a ponto oferece muitas vantagens, como instalação simplificada (por exemplo, por meio de fiação padronizada e eliminação da fiação paralela), parametrização automatizada e com suporte de ferramentas, além de mais opções de diagnósitco.

Para poder usar o IO-Link também em tarefas de automação relevantes para a segurança, a Pilz trabalhou intensamente na IO-Link Community na respectiva ampliação com os respectivos testes e certificações. Os especialistas da Pilz estão liderando dois grupos de trabalho de IO-Link Safety (para marketing e tecnologia).

Na SPS em novembro, apresentaremos os primeiros sensores prontos para o mercado. A Pilz oferece um sistema completo, ou seja, sensores, atuadores e módulos master. Isso simplifica a aplicação para o cliente e aumenta o desempenho.

Estamos certos de que, no futuro, as soluções de automação se diferenciarão ainda mais por sua funcionalidade: As interfaces de usuário são mesmo boas, fáceis de operar e com benefícios adicionais? Aqui existe uma grande capacidade de inovação e um amplo potencial para novas aplicações.

Thomas Pilz

O futuro da segurança é dinâmico

O que significa a digitalização para a proteção de pessoas e máquinas? Quais tecnologias atenderão às exigências de segurança? Qual é o papel das pessoas? Hoje, também queremos pensar no futuro. Uma boa notícia: as pessoas estão no centro de tudo. O papel delas está sendo reforçado.

Pessoas como designer ativo

Como, por exemplo, no produto “Fluide Produktion” do Arena 2036. A Pilz está trabalhando com parceiros para desenvolver e implementar um conceito de produção ciberfísico e centrado em pessoas, especialmente para a produção automotiva. A ideia do projeto é dividir as instalações de produção em módulos geograficamente flexíveis, para que seja possível formar e dissolver unidades dinâmicas conforme a necessidade. Os módulos são projetados com foco central na função das pessoas como designers ativos do seu ambiente de produção.

Esses requisitos resultam no desejo de segurança dinâmica, ou seja, uma adaptação mais flexível das funções de segurança às mudanças nos processos de produção e nos requisitos de segurança correspondentes. Isso permite, por exemplo, que os robôs ou as plataformas móveis não precisem ser parados imediatamente quando uma pessoa entrar na área de trabalho, mas possam continuar a trabalhar em velocidade reduzida (ou seja, menos perigoso) ou, melhor ainda, dominar estratégias de evasão segura. Os sensores e atuadores inteligentes nos sistemas distribuídos assumirão cada vez mais as funções de controladores e levarão a uma melhor interação entre os módulos da máquina e entre pessoas e máquinas.

Segurança em tempo real

As situações dinâmicas relacionadas à segurança nos futuros ambientes de produção devem ser verificadas e liberadas em tempo real, de modo que a proteção de pessoas e máquinas sempre seja garantida. O lema é “segurança em tempo real”. É possível que diferentes máquinas, ou ativos em geral, compartilhem equipamentos de segurança no futuro. Essa é a “Shared Safety” que estamos testando na SmartFactory KL. Uma marcação CE clássica como resultado de um procedimento analógico de avaliação de conformidade está fora de questão com esse entendimento de segurança. As informações sobre todos os ativos envolvidos devem estar disponíveis para o período; as palavras-chave aqui são placa de identificação digital e bandejas de gerenciamento.

No projeto “Fluide Produktion” já mencionado, estamos trabalhando em outros temas voltados para o futuro, como identificação (e, com isso, diferenciação) de pessoas e objetos. É nesse ponto que entra a inteligência artificial. Os riscos podem ser reconhecidos e avaliados por algoritmos de IA adaptáveis. A marcação CE “analógica” é a proteção básica. Mas outras medidas podem ser introduzidas para minimizar os riscos, tornar a segurança ainda mais flexível e contribuir para uma maior produtividade.

Legenda:

Você pode encontrar textos e imagens em www.pilz.com também para download. Para ir diretamente às páginas da internet relevantes no centro de imprensa, insira o seguinte código da Web na busca da página inicial.:
237512

Grupo Pilz

O Grupo Pilz é um fornecedor global de produtos, sistemas e serviços para a tecnologia de automação. A empresa familiar com sede em Ostfildern emprega cerca de 2.500 funcionários. Com 42 subsidiárias e filiais, a Pilz fornece segurança para pessoas, máquinas e meio ambiente no mundo inteiro. A líder em tecnologia oferece soluções de automação completas que envolvem sistemas de sensores e tecnologias de controle e de acionamento, inclusive sistemas para comunicação industrial, diagnóstico e visualização. Uma oferta de serviços internacionais com consultoria, engenharia e treinamentos completa o portfólio. As soluções da Pilz vão além das aplicações em máquinas e instalações e se estendem a inúmeros setores como energia eólica, tecnologia ferroviária e a área de robótica.

www.pilz.com

A Pilz nas redes sociais

Em nossos canais nas mídias sociais, fornecemos a você informações gerais sobre a empresa e as pessoas da Pilz e informamos sobre acontecimentos atuais na área da Tecnologia de Automação.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

https://www.linkedin.com/company/pilz

Contato para jornalistas

Martin Kurth
Imprensa corporativa e técnica
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Imprensa técnica
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de