Security

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Isenção de responsabilidade

Elaboramos o nosso Whitepaper com muito cuidado. Ele contém informações sobre a nossa empresa e sobre os nossos produtos. Todas as declarações estão de acordo com as tecnologias mais avançadas e nosso conhecimento e crença. Apesar disso, não aceitamos nenhuma responsabilidade pela precisão e integridade das informações fornecidas, exceto em caso de negligência grave, uma vez que erros não podem ser totalmente evitados, apesar de todos os cuidados. As informações não possuem qualidade jurídica de garantias nem de propriedades asseguradas. Somos gratos por qualquer feedback sobre discrepâncias.

Direitos autorais

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

1ª edição

Visão geral

Com a digitalização da fábrica, os equipamentos estão cada vez mais conectados. Isso também aumenta o risco de manipulação ou exposição de dados importantes. Anteriormente, a automação ocorria principalmente por um *fieldbus*, como CAN e proprietário que se comunicava por um protocolo específico do fabricante. Para causar danos, um invasor tinha que entrar no chão de fábrica ou acessar uma máquina por uma linha telefônica com modem. Enquanto, com o aumento da substituição desse protocolo por protocolos Ethernet e IP, os ataques podem ocorrer também pela internet.

Os motivos podem ser de ataques terroristas a espionagem e sabotagem industrial de dispositivos até extorsões para pagamentos em dinheiro. Isso facilita o trabalho dos invasores, uma vez que a automação frequentemente utiliza software *open source* e componentes de software disponíveis no mercado. Além disso, é possível que existam pontos fracos conhecidos pelos invasores. Esse é um dos motivos pelo o qual Security, ou, a segurança de dados, está se tornando cada vez mais importante.

No entanto, a experiência indica que, por muito tempo, essa mensagem não foi entendida por todos. Portanto, esse Whitepaper foi criado para explicar aspectos de Security e possíveis soluções que foram comprovadas na prática. Com ele, fabricantes de máquinas, engenheiros de projetos, eletricistas e técnicos podem reconhecer qual o papel que seu produto ou prestação de serviços desempenha na estratégia de Security do seu cliente e quais os pontos de atenção. Inclusive os aspectos de segurança (Safety) funcional. Portanto, Security e Safety são dois lados da mesma moeda, que abordam processos de produção mais seguros.

Conteúdo

1. Security & Safety

1.1. Definição

Anteriormente, Security era um tema praticamente exclusivo da tecnologia da informação (TI). Hoje, no entanto, o ambiente de automação e TI crescem cada vez mais juntos. Com isso, o grau de interligação entre as instalações de produção e a utilização de protocolos padrão, como Ethernet para transferência física dos dados, aumenta significativamente. Além disso, são permitidos protocolos padronizados, como OPC UA, que podem assumir o controle do sistema de TI, abrindo ainda mais a comunicação de dados.
Na automação, Security refere-se, acima de tudo, à proteção de máquinas ou sistemas contra acesso externo não autorizado, além da proteção de dados sensíveis contra falsificação, perda ou acesso interno não autorizado. As ameaças são originadas do ambiente virtual, que é composto pela internet e também por todas as tecnologias de comunicação e informação modernas. Começando no controle de acesso no portão da fábrica, até a defesa de ataques por hackers. No entanto, segundo Ralph Langner, um especialista de segurança de TI alemão, os danos não são causados apenas por "criminosos". Muitas violações de Security não acontecem de propósito, mas sim de um erro de operação de colegas e funcionários.
O termo Safety caracteriza a segurança funcional de sistemas e a proteção de pessoas e do meio ambiente contra ameaças previsíveis que podem decorrer das máquinas. Para isso, os riscos residuais, presentes em maior ou menor frequência, não devem exceder os valores razoáveis. Para fins de garantia, são usados componentes, como relés de segurança e disjuntores, que fazem com que, caso ocorra um problema, a máquina seja colocada em uma condição segura, evitando riscos a pessoas, máquinas e meio ambiente.
Depois de estabelecer a segurança funcional de uma máquina de acordo com os padrões da diretriz de máquinas, o operador do sistema não precisará mais se preocupar com Safety, enquanto não forem realizadas modificações importantes. No entanto, esse tempo acaba. Então, com ameaças ao ambiente virtual, Security é um elemento fundamental para Safety.

1.2. Interações

Como o processo de produção pode ser interrompido por funções de Safety, frequentemente, são procuradas formas de contorná-las – ilegalmente, o que era impedido, principalmente, por medidas mecânicas. Um exemplo são os parafusos selados que impedem que um disjuntor seja facilmente removido. No entanto, hoje é possível executar essa manipulação pela rede. Se, por exemplo, uma máquina entra em uma condição segura por causa de uma grade de luz, seu programa pode ser alterado para que os dados correspondentes não sejam mais avaliados. Dessa forma, a função de segurança é desativada e a máquina continua sendo executada em situações de risco.
Por outro lado, os mecanismos de Safety também podem ser usados com o objetivo de paralisar máquinas pela rede. Aqui, a comunicação dos dados deve ser totalmente interrompida. Então, o mecanismo de Safety deverá ser verificado de forma recorrente, se o participante da rede no outro lado da conexão ainda estiver ativo. Assim que não é obtida uma resposta, a máquina para. Uma possibilidade para conseguir fazer isso, é o já mencionado atraque DoS, que cria uma sobrecarga na rede.
Como a rede não afeta apenas os processos de produção, outros riscos podem acontecer. Mecanismos de Safety que controlam ou acionam ou desconectam uma máquina podem ser um ponto de partida para o invasor. Quando esses mecanismos são alterados para uma

operação contínua, no pior dos casos, a máquina pode quebrar. Como os bens de equipamento têm muitos custos, como turbinas eólicas, a segurança frequentemente é duplicada ou triplicada.

2. Significado de Security na automação

2.1. Objetivos

Com a chegada da Indústria 4.0, em que a conexão é fundamental, as ameaças do ambiente cibernético são um problema muito grave para empresas de manufatura. De fato, são protegidos principalmente todos os processos baseados em TI, mas isso é difícil e caro. Por isso, em um primeiro momento, é preciso examinar quais riscos existem de fato. Por fim, uma estratégia de Security deve ponderar os custos e a utilização em comparação com a produtividade da empresa.
Security tem o objetivo de disponibilizar a rede e garantir os dispositivos, assim como a integridade e a confiabilidade dos dados. Para esse propósito, por exemplo, os sistemas de controle distribuído devem ser protegidos contra ataques (como ataques DoS) e erros de software, de dispositivos e de operação. Uma outra possibilidade de interromper o processo de produção, consiste na transferência ou armazenamento de dados para manipulação, já que a sua integridade é muito importante. E uma violação na confidencialidade dos dados pode ter consequências sérias, por exemplo, o programa de aplicação de uma máquina pode ser espionado e, portanto, recriado.

2.2. Mais sobre a segurança de TI

Para lidar com diferentes cenários de ameaças de forma flexível, as estratégias de Security são implementadas atualmente e possuem diferentes camadas de proteção: No núcleo em que estão os componentes de automação. Depois, na rede em que esses componentes se comunicam entre si ou com um sistema ERP (Enterprise Resource Planning). A camada principal representa a fábrica, que é protegida de fora com um conceito de Firewall.
Contudo, esse conceito não é suficiente para proteger todos os sistemas. As ameaças também podem ser internas. Portanto, a proteção física contra o acesso não autorizado a dispositivos de rede, como firewalls e switches, é a base de qualquer estratégia de Security. Apenas quando esses dispositivos não são acessíveis para todos, é que se pode evitar que eles sejam manipulados no local. Uma medida simples, mas eficaz, que pode ser implementada é trancar dispositivos de rede em armários de distribuição ou instalar caixas de distribuição. Isso também reduz o risco de erros de operação de profissionais não autorizados.

2.3. Impacto do ciclo de vida do sistema

Os sistemas podem ter um ciclo de vida de 20 anos ou mais. Até o momento, todas as regras utilizam o princípio "Never change a running system". Isso significa que, quando um mecanismo de Safety deve ser atualizado, normalmente, o controle deve ser substituído por um novo modelo do mesmo tipo. Já que a segurança funcional é garantida, desde que não sejam feitas alterações importantes na máquina. Ele se baseia em modelos de erro estatísticos que indicam a probabilidade de ocorrer um dano. E isso praticamente não muda com o tempo.

Por outro lado, Security é um "Moving Target". Em Safety, isso não acontece, pois, a probabilidade de acontecer um erro pode ser de 1:100.000, mas, uma vez que o invasor entra na rede, pode ser de 1:1. Além disso, são desenvolvidos métodos mais sofisticados, para corrigir as medidas de defesa e para provar que algoritmos que antes eram considerados seguros não o são. Há alguns anos atrás, o Data Encryption Standard (DES) era um procedimento comum. Hoje, o BSI (Escritório Federal de Segurança em Tecnologia da Informação, na Alemanha) recomenda que ele não seja mais utilizado. O mesmo acontece com o algoritmo de *hashing* MD5. Com computadores quânticos, em breve será possível calcular chaves criptográficas em apenas alguns minutos ou segundos, o que leva muito tempo com os computadores atuais.
Como Security não é físico, mas sim um "Moving Target", as medidas devem ser atualizadas constantemente para ameaças cibernéticas. A responsabilidade recai para a linha de frente, os operadores do sistema, que veem a segurança de dados como uma proteção ao investimento. Visto que uma estratégia de Security efetiva permite que eles utilizem seus sistemas por muito tempo. Por outro lado, os fabricantes de máquinas e componentes têm a obrigação de informar o operador sobre problemas de segurança e fornecer atualizações para o software disponibilizado em seus dispositivos para corrigir essas vulnerabilidades. Isso exige que os dois lados trabalhem juntos, durante todo o ciclo de vida do produto.

3. Formas de ameaças

3.1. Ataques externos

Redes de automação baseadas em Ethernet são expostas a cenários de ameaças complexos que podem ser categorizados com a ajuda de pontos de partida. Os motivos variam desde ataques internos e externos a violações de Security involuntárias.
Quando as redes sofrem um ataque externo, geralmente, isso acontece com intenções maliciosas. Isso inclui a sabotagem de equipamentos. As consequências podem ser ilustradas por um exemplo que foi publicado abertamente, mas sem identificações: Na Alemanha, após um ataque a um alto-forno ele teve que ser demolido, pois o derretimento endureceu.
Um outro cenário de ameaças que pode ter um impacto negativo é a espionagem industrial. Quando as informações sobre os produtos ou know-how de produção são espionadas, é possível que a competitividade ameace os negócios. Isso também é válido para o roubo de dados financeiros ou informações sobre clientes, propostas e pedidos.
Para obter acesso a senhas e dados, os invasores, às vezes, usam sites e e-mails falsos muito realistas, chamados de *phishing*. Se o destinatário não for cuidadoso, o invasor terá um jogo fácil. Por isso, é importante que as empresas orientem seus funcionários sobre o tema Security e estabeleçam diretrizes obrigatórias para todos.
Por fim, em um curto período aconteceram ataques frequentes, que simplesmente tinham um propósito criminal. Atualmente, uma das opções é o chamado Ransomware, que pode ser inserido em arquivos Word, PowerPoint ou Excel que são enviados por e-mail. Quando o destinatário o abre, todos os arquivos em seu computador são codificados. Além disso, esse malware pode se espalhar para outros dispositivos na rede. A única possibilidade de recuperar os dados é o pagamento de um resgate.

3.2. Ataques internos

Embora os ataques externos recebam mais destaque, os ataques internos são igualmente perigosos. Já que estratégias de Security podem ser ignoradas. As intenções dos invasores são similares àquelas dos ataques externos, mas os procedimentos são diferentes.
Uma possibilidade é que invasores entrem na empresa e procurem uma conexão Ethernet livre para inserir o malware na rede. Pode ser por meio de um pequeno pen drive que pode passar despercebido pelo controle de entrada.
No entanto, é muito mais provável que os invasores aproveitem o fato de que, mesmo em Security, as pessoas são o elo mais fraco. Um método eficiente de manipular as pessoas é, por exemplo, a chamada engenharia social.
Nesse método, eles se aproveitam da confiança dos funcionários e os utilizam como uma ferramenta. Os invasores realizam uma pesquisa completa em locais, como o site da empresa, em que podem encontrar os nomes e cargos dos funcionários. Às vezes, é suficiente que um invasor mencione para um funcionário que ele conversou com uma determinada pessoa que disse para ele ir até a empresa.

3.3. Violações de Security não intencionais

No entanto, a maior parte dos incidentes cibernéticos, não resulta de ataques externos ou internos, mas sim de uma forma não intencional. As consequências podem ser tão graves quanto àquelas dos outros dois cenários de ameaça, como a falha de redes ou a divulgação de informações sensíveis. As causas podem ser um dispositivo configurado incorretamente ou erros de operação.
Apesar de os funcionários da produção normalmente não serem especialistas em TI, eles devem ser treinados adequadamente. Além disso, as redes podem ser implementadas de forma que o impacto de um dispositivo configurado ou operado incorretamente seja limitado por uma segmentação, uma segmentação em sub-rede e o uso de mecanismos de Security diferentes.

4. Classificação de Security

4.1. Princípios regulamentares

Por muito tempo, Security desempenha um papel central na TI, por isso, existem diversas normas, como "ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2016); German version EN ISO/IEC 27000:2017". No entanto, esses requisitos não devem ser transmitidos para a automação imediatamente. Como a disponibilização dos dados é prioridade, pois é uma condição essencial para processos de produção sem problemas, na TI a confidencialidade das informações possui a maior prioridade.
Para possibilitar soluções de Security eficazes para automação, várias organizações começaram a elaborar normas apropriadas. No entanto, são descritos apenas aspectos parciais, como a delimitação de Security e Safety. Além disso, não são planos ou normas oficiais, mas sim uma referência técnica.

Já a IEC 62443 "Rede de comunicação industrial – Segurança de TI para redes e sistemas" possui uma série de normas internacionais aprovados parcialmente e que abrangem a segurança de TI em automação. O tema abrange a análise de riscos das *Best Practices*

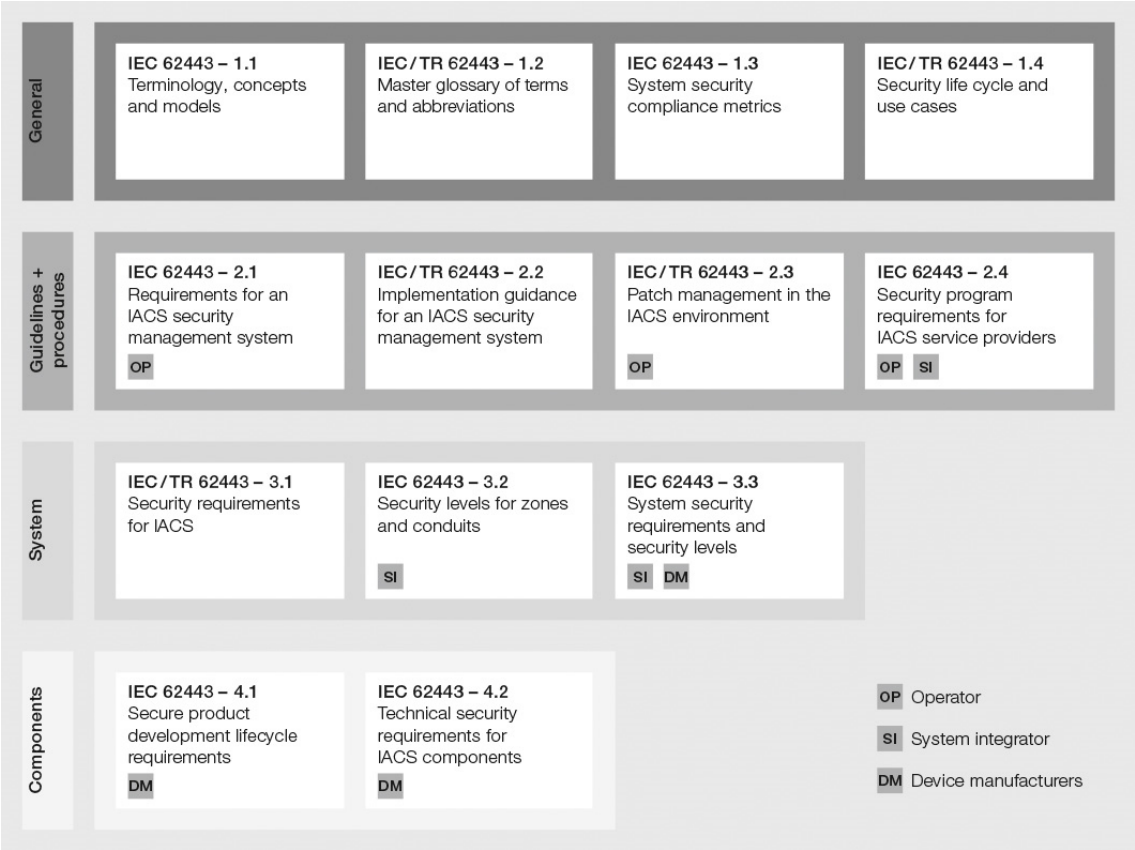


Ilustração 1: Norma IEC 62443

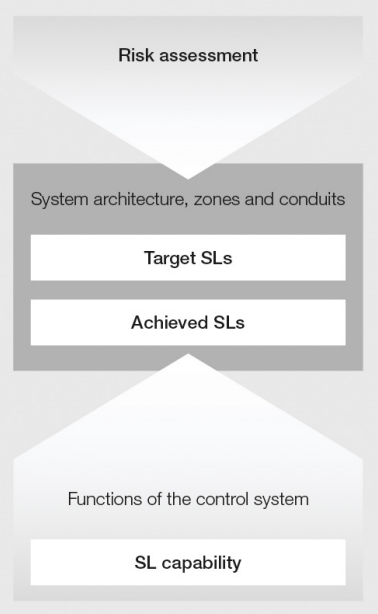
(procedimentos aprovados) até o desenvolvimento seguro de produtos (Security by Design). Como resultado, a IEC 62443 é, atualmente, a melhor orientação para os operadores de sistemas e fabricantes de dispositivos no que se refere à implementação efetiva de Security.
O documento "ICS Security Kompendium" elaborado pelo Escritório Federal de Segurança da Informação (BSI) é voltado especialmente para operadores de sistemas de controle industriais. Ele exemplifica os princípios gerais e também outros requisitos e normas relevantes. Além disso, são visualizadas medidas adequadas e são demonstradas as formas como elas podem ser executadas.
Enquanto a IEC 62443 e o "ICS Security Kompendium" são voltados para especialistas, a Diretriz VDI VDI/VDE 2182 é uma introdução mais fácil para essa temática. Além disso, também existem diferentes empresas do ramo de automação que publicam textos tão completos quanto livros. Devido à complexidade da Security industrial, é aconselhável contatar especialistas externos, pelo menos durante a implementação.

4.2. Análise de riscos

Uma estratégia de Security começa da mesma forma que outra estratégia, com um levantamento, em outras palavras: Os operadores do sistema devem, primeiramente, construir

Ilustração 2: Etapas do projeto de análise de riscos

um cenário em que são expostas todas as ameaças e os valores da empresa estejam protegidos. Na segunda etapa, devem ser definidos cinco Security Level de acordo com a IEC 62443, de 0 (não representa perigo) a 5 (extremamente perigoso) e as especificações da aplicação de todas as variáveis. Não é preciso estabelecer como elas serão cumpridas na prática.



Security Level	Protection
SL 0	No protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

Ilustração 3: Risk Assessment

Como regra geral, todos os dispositivos que possuem uma conexão Ethernet estão em risco. Pois, eles podem ser uma entrada para ataques externos e internos ou ser o ponto de partida para violações de Security não intencionais. Além disso, quando esses dispositivos são instalados em um sistema operacional atual, o risco aumenta. Especialmente quando não existem atualizações de segurança disponíveis. É possível pesquisar em um mecanismo de busca como esses sistemas podem ser atacados e quais malwares existem.
Uma análise de risco sempre é apenas um retrato do momento. A qualquer momento podem surgir novas ameaças que devem ser incluídas. Os processadores não eram considerados críticos, mas, recentemente, foram descobertas vulnerabilidades de segurança chamadas "Meltdown" e "Spectre" e muitos PCs ficaram vulneráveis. Portanto, dispositivos como o Soft-SPSen (software baseado em controlador lógico programável) estão na mira dos invasores.
Resumo: Security é um processo contínuo que precisa de paciência.

4.3. Contramedidas

Após identificar e priorizar os valores corporativos que devem ser protegidos (um ataque bem-sucedido a um controlador, normalmente têm consequências mais graves do que em uma ferramenta de visualização), é preciso decidir como lidar com as ameaças.
A estratégia consiste em, primeiramente, impedir ataques e violações de Security não intencionais. No entanto, devido à complexidade e à dinâmica desse assunto, isso nem sempre pode ser feito. Mesmo que os especialistas procurem de forma constante por possíveis vulnerabilidades na rede, hoje, praticamente não existe uma segurança completa contra qualquer eventualidade.
Portanto, é necessário reconhecer e lidar imediatamente com os problemas de Security. É possível, por exemplo, protocolar todos os eventos na rede (Event Logging) e, então, avaliá-los. Com isso, é possível determinar quando um dispositivo específico foi acessado. Quando, por exemplo, uma manutenção aconteceu em um período diferente do estabelecido, um alarme é acionado.

Se um ataque for bem-sucedido ou se a segurança de dados tiver sido violada involuntariamente, o problema deverá ser resolvido o mais rápido possível e a causa completamente analisada, para que no futuro, isso não ocorra novamente.

5. Implementação de estratégias de Security

5.1. Firewalls

Uma medida para implementar a estratégia de Security é a proteção da rede por dispositivos especiais. Embora mecanismos de segurança, como roteadores e switches possam ajudar, o firewall tem uma função central. Ele lida com soluções de software ou aplicações (combinações de software e hardware), que, com a ajuda de regras definidas individualmente e funções como Deep Packet Inspection ou Intrusion Detection, monitora todas as transferências de dados. Como, normalmente, o firewall é difícil de ser configurado, é preciso um grande conhecimento de TI para evitar erros no chão de fábrica. Por isso, a Pilz desenvolveu o firewall SecurityBridge que é ideal para a indústria. Com configurações de fábrica específicas para aplicações e o princípio Plug-and-play ele pode ser facilmente colocado em funcionamento. Ele não apenas protege os sistemas de controle da Pilz contra ataques e acesso não autorizado, mas também processa dados com baixa latência.
No entanto, os dispositivos de Security mais eficazes não serão tão eficientes se não tiverem sido completamente desenvolvidos. Esse aspecto também é observado durante todo o ciclo de vida, a palavra de ordem é Secure by Design. Como mencionado no exemplo de Meltdown e Spectre os processadores já não podem mais ser considerados seguros. Além disso, é possível que um malware seja introduzido em um processo de produção e, em seguida, instalado nos produtos para funcionar como uma porta de entrada para ataques. Para evitar esses cenários, os fabricantes devem procurar constantemente no mundo cibernético novas ameaças e, se necessário, integrar mecanismos de segurança adicionais em seus dispositivos, fornecendo patches (atualizações de segurança) o mais rápido possível.

5.2. Segmentação da rede

Normalmente, os firewalls são colocados na transição entre uma rede segura e uma rede não segura, por exemplo, entre uma intranet e a internet. No entanto, a proteção de perímetro atinge rapidamente seus limites ao impedir que o malware se espalhe por toda a rede, como uma epidemia, chegando até mesmo a paralisar os sistemas conectados.

Por isso, a norma IEC 62443 segmenta as redes de acordo com o modelo "Zones and Conduits".

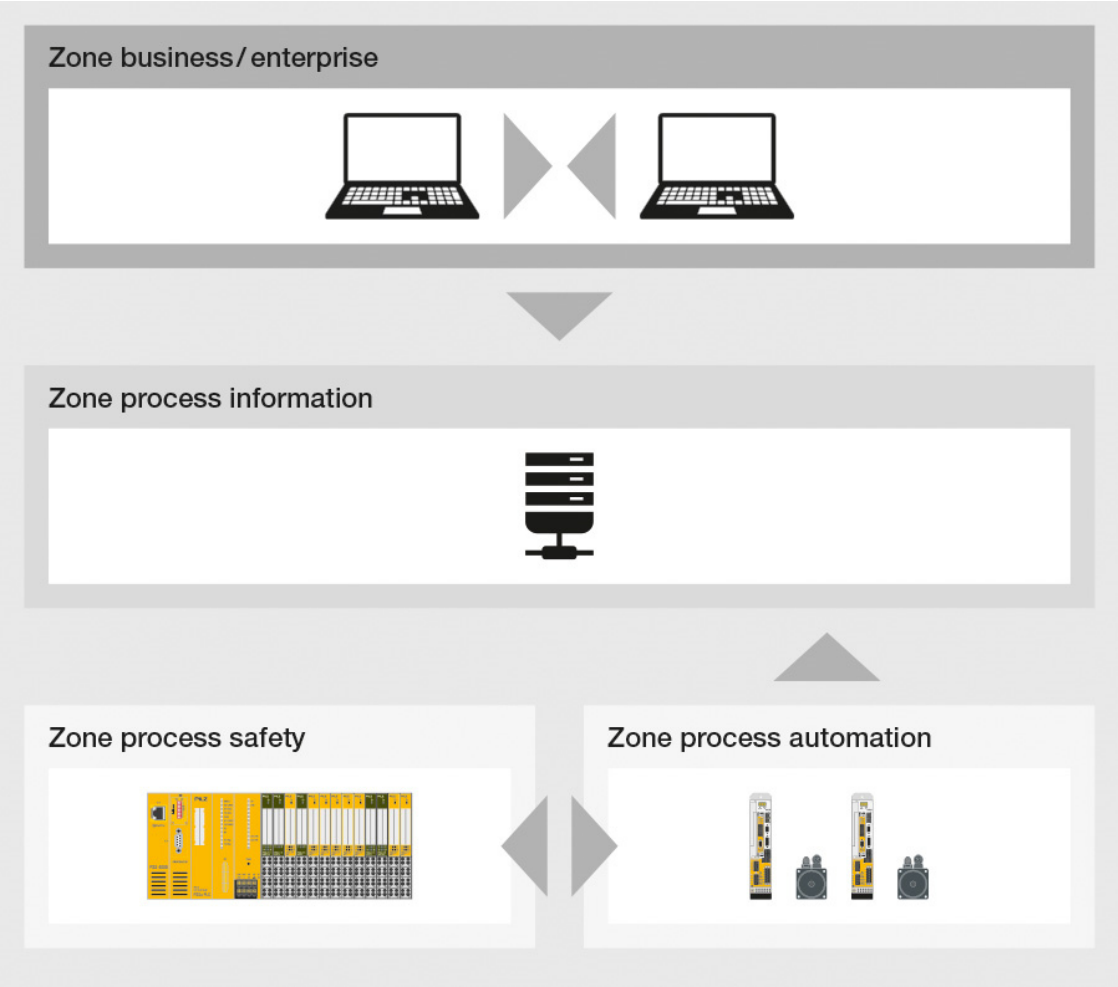


Ilustração 4: Modelo "Zones and Conduits"

É possível usar esse método para separar as redes administrativas e de produção, por exemplo. Se necessário, a rede também pode ser segmentada em células de fabricação individuais. Para isso, primeiro são identificadas as zonas que possuem dispositivos com requisitos de Security semelhantes e, em seguida, elas são protegidas por firewalls ou roteadores seguros. Isso garante que apenas os dispositivos autorizados possam enviar e receber por meio das linhas (canais) entre as zonas.
O exemplo a seguir mostra o que isso significa na prática: Geralmente, as violações de Security não intencionais são causadas por dispositivos configurados incorretamente. As consequências podem ser uma transmissão de dados ou um ataque broadcast que pode afetar outros dispositivos. Quando as redes são segmentadas em sub-redes protegidas, apenas os dispositivos localizados na zona em que o problema ocorreu são afetados. Isso também é válido para o impacto de acesso interno acidental ou mal-intencionado.

5.3. Defense-in-Depth

Para dificultar ao máximo o trabalho dos invasores, o modelo "Zones and Conduits" pode ser um elemento central para a defesa em profundidade (Defense-in-Depth) da rede. Este princípio, que é utilizado na construção de fortalezas é baseado na colocação constante de novos obstáculos para os invasores. Na Idade Média, por exemplo, os castelos eram protegidos por fossos, armadilhas, pontes levadiças, torres e muitos muros.
As zonas e linhas de uma rede são os portões do castelo. Os muros e outros obstáculos são os firewalls e roteadores seguros que oferecem suporte a diferentes mecanismos de Security. Como o controle de acesso IEEE 802.1x e Access Control Lists que bloqueiam dispositivos e protocolos desconhecidos. Além disso, também existem mecanismos que disparam ou detectam alertas quando ocorre uma atividade suspeita na rede, como o envio de pacotes IP com endereços de remetentes falsos (*spoofing* de IP).
Com isso, garante-se que um ataque que utiliza apenas um método não seja bem-sucedido.

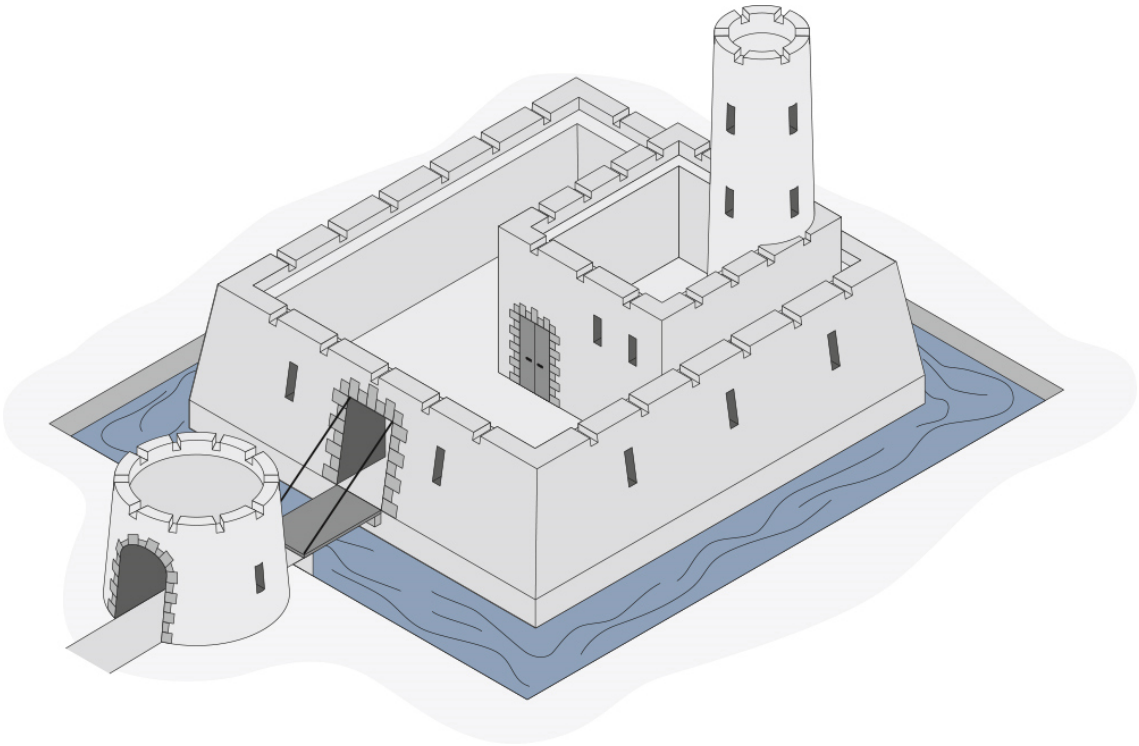


Ilustração 5: Níveis de proteção como um castelo

Para entrar na rede, o invasor deve superar novas camadas de proteção que se sobrepõem. E, mesmo que ele consiga entrar em uma sub-rede de uma célula de fabricação, dificilmente conseguirá atacar outras sub-redes a partir dela.

5.4. Medidas organizacionais

Mesmo que as empresas de produção se protejam das ameaças do mundo cibernético, como já mencionado, sempre deve ser avaliado os custos e a utilização. Na Alemanha, por exemplo, de acordo com a Lei de Segurança de TI, apenas os operadores de infraestruturas que têm um impacto na sociedade, como energia, tráfego e saúde, são obrigados a se proteger. Em outros

países, também existem exigências legais semelhantes, por exemplo, a proteção de redes elétricas nos EUA.
Em face de inúmeras ameaças, os sistemas devem ser protegidos contra violações de Security intencionais e não intencionais. No entanto, apenas um conceito de firewall sofisticado não é suficiente. É necessário que toda a empresa internalize Security. Além disso, é preciso elaborar diretrizes que se apliquem não apenas aos funcionários, mas também a parceiros, como fabricantes de equipamentos e prestadores de serviços.
Além disso, é importante que os especialistas de TI e automação trabalhem juntos, familiarizando-se com seus diferentes métodos e necessidades. Por fim, uma organização deve se basear no princípio de que todos os membros são responsáveis pela segurança dos dados na fabricação e pela melhoria contínua. Idealmente, deve haver um agente de Security que pertence, ou pelo menos reporta diretamente, à alta direção.

5.5. Treinamentos

"Quando você para de melhorar, você deixa de ser bom", essa é a receita para o sucesso que as empresas também devem aplicar a Security. Uma maneira de fazer isso é fornecer regularmente treinamentos que aumentem a conscientização dos funcionários. Outros conteúdos podem incluir informações sobre ameaças atuais ou instruções sobre como corrigir vulnerabilidades de segurança específicas. Somente quando a competência Security é um objetivo de todos, é possível evitar que funcionários que não são qualificados tomem decisões erradas.
Existem inúmeras ofertas de treinamentos de Security. Os seminários da Pilz, tanto na sede em Ostfildern (perto de Stuttgart) quanto nos locais do cliente (ou por um webinar com conteúdo resumido), são voltados especialmente para construtores de máquinas e engenheiros de projetos. Eles fornecem uma visão geral básica e explicam como detectar e minimizar os riscos. Os tópicos variam desde a arquitetura de rede até a autenticação dos participantes da rede e a criptografia de dados para manutenção remota segura.

6. Resumo e visão geral

Para obter maior Security, é importante conhecer muito bem a arquitetura da rede, os protocolos de comunicação e o tipo de tráfego de dados. Dessa forma, é possível evitar ameaças externas e internas, intencionais ou não.
No passado, Security era apenas um tópico da tecnologia da informação (TI). No entanto, com chegada da Indústria 4.0, estão sendo implementados sistemas de fabricação produzidos em massa e sistemas operacionais complexos, portanto, a automação também deve se preocupar com esse tópico. Como as normas de TI não se aplicam totalmente, novos foram elaboradas novas normas, dentre elas, a IEC 62443 é a mais importante. Ela define que uma estratégia Security abrangente para o setor industrial pode ser desenvolvida e implementada passo a passo.
Ao mesmo tempo, essas estratégias também devem incluir Safety, pois suas funções somente poderão ser garantidas se os dados adequados forem transmitidos de forma confiável. Como as ameaças de Security podem mudar constantemente, as contramedidas devem agir da mesma forma. Ou seja, embora esses dois aspectos da automação continuem sendo independentes, eles devem estar muito alinhados. A boa notícia é que: qualquer pessoa

familiarizada com Safety terá facilidade com Security, uma vez que os procedimentos são semelhantes.

Glossário

Access Control List	Uma Access Control List (ACL, em português: lista de controle de acesso) determina a extensão do acesso de cada pessoa, computador ou rede para cada serviço no roteador ou switch. O acesso pode ser determinado para cada computador ou rede e para cada método de acesso individual.
Ataques broadcast	Um ataque broadcast é um acúmulo de tráfego em uma rede de computadores, que impossibilita a criação de conexões de rede e pode interromper as conexões existentes. Um ataque broadcast pode acontecer em configurações incorretas ou projetos de rede inadequados.
Deep Packet Inspection	Deep Packet Inspection é um procedimento para filtrar e monitorar tecnologias de rede e pacotes de dados. O Deep Packet Inspection evita spams e o pode ser usado para o controle de sobrecarga e a redução de tráfego de dados.
DES (Data Encryption Standard)	O Data Encryption Standard, abreviado como DES, é um procedimento de codificação simétrico padronizado.
Intrusion Detection System	Com a ajuda do Intrusion-Detection, é possível direcionar um ataque em um sistema de computador ou rede de computadores e reconhecer de forma precoce, para que todas as medidas possam ser introduzidas rapidamente.
Spoofing de IP	O Spoofing de IP identifica endereços de IP de remetente falsos em pacotes de IP na rede de computadores e audita as identidades falsas dos sistemas de TI atacados. Cada pacote de IP armazena em seu cabeçalho os endereços de remetente. Um invasor pode falsificar o endereço de remetente no cabeçalho para que pareça que o pacote foi enviado de outro computador. Muitos protocolos do tipo TCP/IP podem ser autenticados apenas por um endereço de IP. Essas falsificações podem enganar medidas de segurança, como a autenticação baseada em endereço IP na rede. Portanto, o Spoofing de IP é apenas um tipo de Spoofing. Atualmente, qualquer método que contorne técnicas de autenticação e identificação com endereços confiáveis ou nomes de host em protocolos de rede é considerado um "Spoofing".
Algoritmo hashing MD5	O MD5 (Message Digest Algorithm 5) pertence a um grupo de funções matemáticas unilaterais. Isso significa que não existe uma maneira simples de deduzir o resultado de um parâmetro de entrada. Com o MD5, é representado uma quantidade de dados de entrada com um valor de 128 bits. Um algoritmo hash

	presume que é extremamente difícil encontrar dois documentos de entrada que produzem um mesmo resultado (colisão). No caso do MD5, as falhas são conhecidas há algum tempo, o que possibilita ao invasor criar uma colisão.
Meltdown e Spectre	Meltdown e Spectre são falhas de segurança detectadas em microprocessadores, que possibilitam o acesso não autorizado à memória de processos externos.
Norma de rede IEEE 802.1x	A IEEE 802.1X é uma norma de rede para autenticação de usuários em redes IEEE-802. Essa norma funciona como uma instância de controle, que verifica usuários antes de eles acessarem a rede LAN ou WLAN.
Objetivo de Security: Integridade	A integridade, no contexto de dados, garante que os dados e as funcionalidades de um sistema estejam corretos. A garantia da integridade pode reconhecer e impedir alterações não autorizadas ou não notificadas.
Segmentação de redes	Segmentação significa que uma rede foi dividida em unidades menores. Essas unidades podem ser conectadas a firewalls ou outros dispositivos que restringem a comunicação. Com isso, minimiza-se o impacto de ataques broadcast ou outros incidentes "não intencionais".

Índice de figuras

Nós possuímos presença internacional. Para obter mais informações, acesse nosso site www.pilz.com ou entre em contato com a nossa matriz.

Matriz: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Alemanha
Telefone: +49 711 3409-0, Telefax: +49 711 3409-133, E-mail: info@pilz.de, Site: www.pilz.com

PILZ
THE SPIRIT OF SAFETY