



Indústria 4.0 – segura e inteligente

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Exclusão de responsabilidade

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

Direitos autorais

Todos os direitos sobre esta publicação são propriedade da Pilz GmbH & Co. KG. Reservamos o direito de realizar alterações técnicas. Podem ser feitas cópias para as necessidades internas dos usuários. Os nomes dos produtos, mercadorias e tecnologias utilizados são marcas comerciais de suas respectivas empresas.

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

© 2016 by Pilz GmbH & Co. KG, Ostfildern
2. Edição

Conteúdo

1. Sobre a indústria 4.0	4
1.1. História e contexto	4
1.2. A fábrica inteligente.....	4
1.2.1. Smart Factory ^{KL}	5
1.2.2. Demonstrador Smart Factory da Pilz	6
1.3. Segurança – Safety & Security	7
1.4. Máquina modular e descentralização	8
2. Indústria 4.0 e a Pilz	9
2.1. A contribuição da Pilz.....	9
2.2. Indústria 4.0 na produção da Pilz	9
2.2.1. TI na produção conectada	10
2.2.2. „Think Thank 4.0 da Pilz“	10
2.3. Áreas de atuação da indústria 4.0	10
3. Área de atuação de segurança – Safety & Security	11
3.1. Safety	12
3.1.1. Safety – da segurança estática para dinâmica	12
3.1.2. Safety 4.0 – de estrutura monolítica para soluções modulares.....	13
3.1.3. Certificação modular	13
3.2. Security	14
3.2.1. Soluções na área de Security	14
3.2.2. Soluções de automação.....	15
3.3. Cooperação entre Safety & Security.....	15
4. Área de atuação da abordagem modular	16
4.1. Sistemas inteligentes distribuídos.....	16
4.2. Ferramenta de engenharia PAS4000	17
4.3. Visualização no PASvisu	17
Glossário	19

1. Sobre a Indústria 4.0

Indústria 4.0 é mais do que uma visão do futuro. Redes inteligentes são uma grande oportunidade para a indústria. Através de uma produção flexível é possível atingir uma utilização ideal dos sistemas. Produtos individualizados podem ser adaptados às condições da produção em massa, e ainda com aumento da produtividade da unidade de produção. Apesar disso, muitas empresas ainda estão hesitantes com a implementação da Indústria 4.0 nas suas próprias produções. Segundo o estudo “Industry 4.0 – How to navigate digitization of the manufacturing sector, 2015”¹ do instituto McKinsey, somente seis de cada dez empresas na Alemanha se sentem prontas para a Indústria 4.0, apesar de 91 por cento perceber a digitalização da produção industrial como uma oportunidade. Por isso, queremos agir e oferecer para empresas em todo mundo as soluções e produtos para a Indústria 4.0. No mundo todo o assunto Indústria 4.0 está cada vez mais em foco: Exatamente por causa da globalização contínua que é necessário criar condições para garantir a interconexão pela digitalização dos processos de produção ao longo de toda cadeia de valor.

1.1. História e contexto - da máquina a vapor até a fábrica inteligente

A primeira revolução industrial foi a mecanização com energia da água e do vapor, depois veio a segunda revolução industrial: Produção em massa com ajuda de linhas de montagem e de energia elétrica. Ela foi seguida pela revolução digital, também conhecida como “Indústria 3.0”. O trabalho em computadores se tornou normal e foi implementado o primeiro CLP. A designação “Indústria 4.0” é a quarta revolução industrial, que possibilita sistemas ciberfísicos (CPS), a “Internet das coisas” e Smart Factory. Para a Pilz, a Indústria 4.0 é uma evolução, sem a participação de todos os atores participantes não é possível implementar a Indústria 4.0.

O termo Indústria 4.0 foi levado a público pela primeira vez em 2011 na Feira de Hannover. Em outubro de 2012, o governo alemão recebeu recomendações sobre a implementação da Indústria 4.0 do grupo de trabalho de promoção de comunicação da união de pesquisa. O grupo de trabalho da Indústria 4.0 entregou em abril de 2013 na Feira de Hannover o seu relatório final para representantes de renome do governo federal alemão. Ao mesmo tempo, as três associações Bitkom², VDMA³ e ZVEI⁴ assumiram em seus trabalhos a plataforma Indústria 4.0. O grupo de trabalho deve coordenar futuramente as atividades neste campo de futuro. Desde o início, a Pilz acompanha estas atividades e apoia projetos com sua longa experiência em tecnologia de automação.

1.2. A fábrica inteligente – Smart Factory

Smart Factory é a fábrica inteligente de amanhã. O termo foi criado através da pesquisa em engenharia de produção. Smart Factory é o objetivo da estratégia Hightech do governo alemão

¹ https://www.mckinsey.de/sites/mck_files/files/mck_industry_40_report.pdf

² Bitkom (Associação Digital da Alemanha / Germany's digital association), <https://www.bitkom.org/EN/index-EN.html>

³ VDMA (Associação Alemã de Mecânica e Engenharia, Mechanical Engineering Industry Association), <http://www.vdma.org/ueber-uns>

⁴ ZVEI (Associação Central da Indústria de Engenharia Elétrica e Eletrônica e. V.), <http://www.zvei.org/en/Pages/default.aspx>

como parte do projeto de futuro Indústria 4.0.⁵ Na Smart Factory, deve haver um ambiente de produção, onde os sistemas de produção e de logística organizam e se otimizam de forma ampla e autônoma. Para os produtos fabricados na Smart Factory, sabe-se a qualquer momento, sua localização, seu histórico, sua condição atualizada e as etapas de produção que ainda faltam para o produto final. Mas como isso é possível?

A base técnica são sistemas ciberfísicos⁶ que se comunicam entre si através da Internet das coisas⁷. Parte deste cenário do futuro é a comunicação entre produto ou o seu suporte da peça de trabalho e o sistema de produção: O produto traz consigo as suas informações de produção em um formato legível por máquina, como por exemplo, em um chip RFID. Com estes dados, é controlado o caminho do produto no sistema de produção e as etapas individuais de produção. Em universidades e institutos de pesquisa, trabalha-se no Smart Factory no âmbito das assim denominadas fábricas-modelo.

1.2.1. Smart Factory^{KL}

SmartFactory^{KL} é o centro de competência principal e plataforma de demonstração e pesquisa independente de fabricantes para preparar o caminho das fábricas inteligentes do amanhã. Ali são desenvolvidos sistemas de fábrica inovadores, em que a visão da Indústria 4.0 já se torna realidade.⁸ O objetivo é trabalhar em uma rede com parceiros renomados da indústria e da pesquisa em novos conceitos, padrões e soluções que formam a base para uma tecnologia de automação altamente flexível.

Como membro pleno, a Pilz colabora em todos os aspectos no objetivo da iniciativa. A Pilz acompanha os resultados do trabalho conjunto na plataforma de desenvolvimento e utiliza-os em seus próprios produtos.

SmartFactory^{KL} já possui hoje o primeiro sistema do mundo da Indústria 4.0 entre os fabricantes.⁹ Segurança e modularização são neste caso temas importantes. Primeiro, a Pilz disponibiliza a sua experiência na área de segurança de máquinas para uma padronização e procedimento comum em relação ao tema segurança com suas concretizações Safety (segurança de máquinas) e Security (segurança de TI). Por outro lado, a Pilz envolve-se no tema modularização. A estrutura dos sistemas com abordagem mecatrônica possibilita a completa modularização na forma de elementos da máquina. Funções podem ser padronizadas e reutilizadas por módulos. Base para isso são sistemas de automação, como o PSS 4000 da Pilz, que são capazes de distribuir funções de controle. No Smart Factory, estes conceitos de automação podem ser testados. Há diversos anos a SmartFactory^{KL} demonstra um sistema de produção modular para qualquer fabricante que possibilita o trabalho em conjunto de módulos individuais de diferentes fabricantes com diferentes arquiteturas de controle. A Pilz ampliou este sistema de demonstração da SmartFactory^{KL} em um módulo inteligente e automatizado de armazenagem.

⁵ <http://www.hightech-strategie.de/de/Industrie-4-0-59.php>

⁶ Definição no glossário, página 20 f.

⁷ Definição no glossário, página 20 f.

⁸ <http://www.smartfactory.de/>

⁹ <http://www.smartfactory.de/>



Ilustração 1: SmartFactory^{KL} na Feira de Hannover de 2015

1.2.2. Demonstrador Smart Factory da Pilz

Com o demonstrador Smart Factory mostramos como é possível produzir produtos individualizados de forma rápida, flexível e eficiente. A linha de produção montada de forma modular exemplifica a comunicação dos sistemas de automação distribuídos em interação com atuadores e sensores. O sistema de automação PSS 4000 com capacidade de Indústria 4.0 coordena a execução de todos os componentes interconectados - segurança e automação desde a engenharia até a visualização.

A nossa linha de produção inteligente produz porta-cartões personalizados e canetas esferográficas. Sendo assim, é importante que processos de produção sejam transparentes. Com nossas soluções, é possível representar de forma simples máquinas e sistemas com funções complexas, como os sistemas interconectados digitalmente na Indústria 4.0.

O demonstrador é composto de três módulos de função:

- ▶ um armazém para o suporte da peça de trabalho
- ▶ um robô com magazine de peças de trabalho / uma estação de entrega para o produto
- ▶ uma estação de laser

Em um terminal para o cliente, são inseridos em um computador os dados do cliente (contato, endereço, ...). Além disso, o cliente escolhe no terminal se ele quer um porta-cartões de visita ou uma caneta esferográfica, que será fornecida individualmente para ele com o seu nome (caneta), ou um cartão de visita digital com seu nome escrito (porta-cartões de visita).

Os dados inseridos são salvos digitalmente em um chip RFID que se encontra no suporte da peça de trabalho. Assim assegura-se que todas as informações estejam disponíveis em todos os módulos. Nos módulos individuais as informações necessárias são lidas no chip e as etapas de trabalho necessárias executadas. Após produção bem-sucedida, o chip RFID é apagado na saída do produto. Ele volta a ficar disponível para registrar o próximo conjunto de dados. O suporte da peça de trabalho com o chip RFID será novamente armazenado após este procedimento de apagamento, se não houver nenhum outro conjunto de dados para salvar, ou será enviado novamente para o ciclo de produção.



Ilustração 2: Demonstrador Smart Factory da Pilz na Feira de Hannover de 2016

1.3. Segurança – Safety & Security

Com o desenvolvimento do ambiente de automação para a Indústria 4.0, surgem para as empresas novas exigências de segurança. O mundo da automação funde-se com o mundo do TI. Os diferentes pontos de vista sobre o tema segurança diferem claramente: Os termos internacionalmente utilizados “Safety” para segurança de máquinas e “Security” para segurança de TI e segurança de dados auxiliam primeiramente na diferenciação fundamental.

Safety exige que os riscos remanescentes provenientes de uma máquina ou sistema não ultrapassem valores aceitáveis. Isso inclui tanto riscos do ambiente do sistema (por exemplo danos ambientais) como também riscos dentro do sistema (por exemplo pessoas que estejam no sistema).

Security refere-se à proteção de uma máquina ou sistema contra acesso não autorizado, além da proteção de dados sensíveis contra falsificação, perda ou acesso não autorizado internamente. Isso inclui tanto ataques explícitos como também incidentes não intencionais de segurança.

A ampla proteção na transmissão, processamento e armazenamento de dados de controle relevantes a segurança da produção, precisa ser endereçado aos seguintes setores de Security:

- ▶ Segurança física e disponibilidade dos sistemas de TI
- ▶ Segurança da rede
- ▶ Segurança na utilização de software
- ▶ Segurança de dados
- ▶ Segurança operacional

1.4. Máquina modular e descentralização

Há muitos anos, a construção modular de máquinas e sistemas é a chave para maior flexibilidade na produção. Um sistema completo é composto por diversos módulos de máquinas autônomos. Assim um módulo forma uma ou várias etapas de produção padronizadas e pode ser combinado com outros módulos para formar um processo completo. Para isso, todos os módulos são conectados a um Backbone, que fornece aos módulos tanto energia (400 VAC trifásico, ar comprimido, ...) como também dados de processo e controle. Se o processo de produção precisa ser alterado ou se a produtividade precisa aumentar, é possível trocar um ou mais módulos ou adicionar módulos iguais.

No caminho para o futuro da automação, os dois principais fatores de sucesso são, portanto, a modularização e a descentralização. Pré-requisito para isso são sistemas de automação que são capazes de controlar, com interface amigável ao usuário, a inteligência distribuída nos módulos da máquina. Todas as máquinas e sistemas podem ser divididos em unidades claras que operam de forma independente.

A estrutura modular das máquinas e sistemas segue a abordagem mecatrônica. Esta segue a filosofia de reunir universalmente todas as disciplinas envolvidas no processo de concepção de uma máquina: Mecânica, elétrica e tecnologia de automação. Sendo assim é definido universalmente a interação de diversos componentes individuais de automação e das respectivas ferramentas de software para uma solução de automação. Esta universalidade estende-se sobre os quatro níveis da pirâmide de automação (nível de gerenciamento, nível de direção operacional, nível de controle e nível de campo). A abordagem mecatrônica exige também que as funcionalidades de controle nos módulos mecatrônicos individuais possam "interagir".

É aqui que sistemas até então atingiam seus limites. Apesar de ser possível criar módulos de função, quando estes precisavam ser realizados através de poderosos sistemas de controle centralizados, o comissionamento de módulos individuais rapidamente se tornava dispendioso devido à complexidade. Da mesma forma surge um aumento de custos nas mudanças posteriores necessárias na configuração e na programação dos módulos de função individuais. Com auxílio de sistemas projetados de forma descentralizada, os módulos podem ser colocados em funcionamento com facilidade. A elaboração da configuração também é muito simples, porque podem ser utilizados os programas de controle e funções parciais idênticas para diferentes módulos.

Para a automação do futuro, também são solicitadas soluções que sejam por um lado capazes de distribuir a inteligência de controle, e por outro lado assegurem que a interconexão necessária de diversos controles permaneça simples de ser manuseada pelo usuário. A Pilz oferece uma solução assim com o sistema de automação PSS 4000.

2. Indústria 4.0 e a Pilz

2.1. A contribuição da Pilz

Susanne Kunschert, diretora geral da Pilz, foi nomeada em 2010 pelo governo alemão e convocada pessoalmente como representante das empresas de médio porte na união de pesquisa. Este era o grêmio consultivo central da política de inovação do governo federal para a implementação e desenvolvimento da estratégia Hightech. Susanne Kunschert foi solicitada a apresentar a este grêmio as perspectivas de inovação das empresas de médio porte.

Como membro do grupo de promoção de segurança, a diretora geral da Pilz se envolveu na segurança efetiva de redes de comunicação e no desenvolvimento da Alemanha como mercado líder em tecnologia de segurança. Para as áreas de demanda identificadas, a união de pesquisa trabalhou em grupos em projetos para o futuro. Um dos mais importantes é a Indústria 4.0.

A Pilz apoiou ativamente o trabalho em diversos projetos do novo escritório da Indústria 4.0, sob a égide de associações comerciais como Bitkom, ZVEI e VDMA e contribuiu para a elaboração das recomendações de conduta. Estas foram entregues ao governo federal na Feira de Hannover de 2013.

A Pilz é atualmente ativa nos seguintes grêmios e iniciativas:

- ▶ Cooperação na plataforma Indústria 4.0
- ▶ Cooperação no círculo de liderança Indústria 4.0 na ZVEI
- ▶ Cooperação na rede de mecatrônica do estado de Baden-Württemberg
- ▶ Membro no círculo de controle da aliança Indústria 4.0 em Baden-Württemberg
- ▶ Membro da plataforma de demonstração e de pesquisa independente de fabricantes Smart Factory^{KL}
- ▶ Membro do ARENA2036 – O futuro da indústria automobilística

2.2. Indústria 4.0 na produção da Pilz

Através da participação na união de pesquisa e na plataforma de pesquisa SmartFactory^{KL} a Indústria 4.0 é para a Pilz mais que um projeto de futuro, já está presente em seu processo de produção.

Com a crescente conexão de máquinas e infraestrutura com abordagem de tecnologias de TI na produção, a Pilz também é considerada líder em tecnologia, também em sua própria produção. No âmbito da Indústria 4.0, foi desenvolvida a infraestrutura necessária para a produção inteligente e os elementos da Indústria 4.0 foram antecipadamente implementados. Já é utilizado um transporte inteligente da peça de trabalho, que foi desenvolvido internamente. Ele acelera e facilita, por exemplo, a montagem de placas de circuito impresso e o processo de soldagem. O suporte da peça de trabalho encontra sozinho, através de um chip RFID instalado, o caminho do processo de solda por onda para a unidade de montagem.

A Pilz continuará a implementação da produção inteligente passo a passo: Para o controle da fabricação, são coletados e processados dados de máquinas. Através da avaliação, são obtidas informações importantes sobre alterações de estado e o desgaste das máquinas. Com isso, é possível realizar a manutenção preventiva. “Predictive Maintenance” evita avarias e períodos de parada. O armazenamento de documentos de trabalho atuais na Pilz Cloud

também está sendo implementado. Todos os dados e documentos estão disponíveis em tempo real e constantemente atualizados podendo ser acessados na produção de qualquer lugar através de aparelhos móveis.

2.2.1. TI na produção conectada

A Pilz está ciente dos desafios para Security de TI decorrentes da produção completamente conectada. Por este motivo, a Pilz está investindo em uma ampla infraestrutura de segurança para o monitoramento de todo o tráfego de dados. Isso inclui também um centro de dados independente que satisfaz os padrões mais recentes. Uma análise e protocolização permanente de todos os parâmetros relevantes da produção possibilita uma detecção antecipada de anomalias. Adicionalmente, foram instalados diferentes sistemas de Firewall para cada área de produção, de forma que o nível de segurança necessário para cada zona possa ser determinado individualmente. Falhas e riscos de segurança são minimizados e o know-how é protegido.

2.2.2. “Think Thank 4.0 da Pilz”

Assim como a Indústria 4.0, a Pilz também dá prioridade máxima para a importante colaboração entre os departamentos de tecnologia da informação e tecnologia de produção. Nos “Think Thank 4.0 da Pilz”, os funcionários dos departamentos de produção e de TI se reúnem e recebem os recursos necessários para planejar e implementar projetos em conjunto para a Indústria 4.0.

2.3. Áreas de atuação da Indústria 4.0

Uma das bases para uma aceitação sustentável de mercado, é a criação de mecanismos padronizados na comunicação entre as máquinas e dentro da máquina. Apenas quando as exigências de ambos os mundos (automação e TI) são consideradas, surgem soluções viáveis e aceitas pelos usuários.

Resumindo, isso significa que a Pilz está engajada em arquiteturas de controle modernas no contexto da Indústria 4.0.

Assim os seguintes temas formam as nossas prioridades:

► Safety & Security:

- Ambas possuem paralelos nítidos na padronização e no procedimento do processo de engenharia. Com nossa experiência em segurança de máquinas e automação queremos levar este importante trabalho adiante.
- Todos os aparelhos e componentes de automação necessários para a função de controle possuem um acesso direto à internet para a troca de dados do processo e dos dados de parametrização para o diagnóstico e a manutenção (remota). Com isso aumentam as exigências em relação à segurança para todos os aparelhos de automação participantes e um acesso e representação uniforme do diagnóstico.

► Abordagem modular:

- Nossas modernas funções de controle são projetadas para uma distribuição e orientação do objeto - sensores e atuadores tornam-se inteligentes. Com isso, formamos a tendência de objetos de controle mecatrônicos (componentes de automação) nos nossos produtos e nas nossas respectivas ferramentas de engenharia.

3. Área de atuação de segurança – Safety & Security

Safety & Security são condições importantes para o funcionamento dos sistemas da Indústria 4.0 que diferem dos sistemas de produção tradicionais que dispõem de interfaces em seu ambiente.

Os sistemas da Indústria 4.0 poderão, no futuro, ser reconfigurados e otimizados de forma autônoma durante a operação, isto é, pelo próprio sistema em operação, o que exigirá uma nova avaliação de segurança (Safety & Security). Além disso, deve ser assegurado que as lacunas de segurança remanescentes não constituam riscos inaceitavelmente altos no âmbito de segurança.

Por fim, deve-se formar, nesta área de atuação, confiança nas pequenas e médias empresas, cuja base é decisiva para a produção em redes Ad-hoc. Para isso, a transparência, a participação e a comunicação aberta são pré-requisitos importantes.



Ilustração 3: Colaboração entre Safety e Security

3.1. Safety

A área Safety já é caracterizada pela grande segurança de investimento e segurança jurídica. Isso também ocorre devido as normas e padrões. Todos os processos para análise e avaliação de risco e execução da análise estão claramente definidos conforme os níveis internacionais padronizados em Safety Integrity Levels (SIL) e o mesmo é possível em comparação com o efeito jurídico das soluções.

3.1.1. Safety – da segurança estática para dinâmica

O termo Safety caracteriza a segurança funcional de máquinas, ou formulado de outra maneira: a proteção de pessoas e do meio ambiente contra ameaças que podem decorrer das máquinas. Safety exige que os riscos remanescentes provenientes de uma máquina ou sistema não ultrapassem valores aceitáveis. Isso inclui tanto riscos do ambiente do sistema (por exemplo, danos ambientais) assim como riscos dentro da máquina ou do sistema (por exemplo, para pessoas que permanecem no sistema).

Uma possibilidade é, no caso de uma ocorrência, interromper imediatamente o fornecimento de energia e para a máquina bruscamente. Isso normalmente é realizado por cabeamento especial de segurança e componentes como um relé de segurança. Como esta abordagem é baseada em Hardware e, portanto, é estática, ela é pouco apropriada para processos inteligentes de produção, nos quais o Layout do sistema precisa constantemente ser alterado. Um desligamento forçado está normalmente associado a outras desvantagens, seja uma perda de produtividade, paradas prolongadas devido aos procedimentos complexos para o reinício do sistema ou uma limitação no conceito de operação e de manutenção da máquina.

Uma alternativa oferece o conceito de segurança dinâmica, que se baseia em uma visão integral que toca nos processos de automação em constante mudança e nas exigências da segurança funcional. Isso também muda como a segurança em si é vista; ela é vista menos como uma característica de Hardware, e muito mais como uma função que abrange mais aparelhos. Com esta abordagem que já foi desenvolvida antes dos tempos da Indústria 4.0, podem ser executados processos com segurança, sem que seja preciso realizar uma interrupção imediata sempre que ocorrer um erro. A abordagem dinâmica só poderá ser implementada com eficiência se a segurança funcional for considerada desde o início no planejamento dos projetos de automação. Caso contrário, sob determinadas circunstâncias, a sequência das etapas individuais de produção ou todo o processo deve ser alterado posteriormente, o que impede soluções otimizadas e ainda causam custos elevados. Enquanto na segurança estática frequentemente apenas sinais binários podem ser transmitidos, como quando depois de abrir uma porta de proteção o movimento da máquina é desligado, já para a segurança dinâmica são necessárias informações mais abrangentes. Porque, neste processo, existem diferentes tipos de operação segura que permitem a “Operação com a porta de segurança aberta”. As informações sobre os tipos de operação segura devem estar disponíveis em todos os componentes participantes. Em relação ao exemplo da porta de segurança, a abertura da mesma não causa mais o desligamento automático e imediato da máquina, dependendo do nível de autorização do usuário, mas faz com que os mecanismos de segurança monitorem e operem com uma velocidade reduzida ou que monitorem o ponto de ajuste nominal do eixo de rotação.

3.1.2. Safety 4.0 – de estrutura monolíticas para soluções modulares

Na Smart Factory, os sistemas modulares instalados devem ser reconfigurados com rapidez e flexibilidade ou podem ter suas combinações alteradas. A validação de uma solução de segurança deve ser capaz de lidar com esta maior flexibilização (tardia). Por que todas as compilações que não foram consideradas na identificação CE, também não poderão ser facilmente reconstituídas pelo operador. Não se aplica uma simples portabilidade: $CE_{Módulo1} + CE_{Módulo2} = CE_{Máquina completa}$!

A vantagem funcional dos conceitos de máquinas modulares é óbvia. Você se beneficia com flexibilidade no processo de produção e ao mesmo tempo uma maior possibilidade de padronização a nível funcional. O maior grau de padronização pode ser atingido quando os limites de divisão dos diferentes módulos podem ser projetados identicamente - não importando se se trata de um módulo mecânico, elétrico, de tecnologia de controle ou de função de visualização. A abordagem mecatrônica tem como objetivo um formato padronizado dos objetos de automação.

As vantagens da modularização são frequentemente anuladas devido a um conceito de segurança rígido, possivelmente ainda com cabeamento. Até os controles eletrônicos de segurança possuem quase sempre uma segurança baseada em Hardware, na forma de circuitos fixos de segurança, mesmo quando oferecidos na lógica de comutação programável livre.

O elemento básico das arquiteturas de controle modernas é, em contrapartida, a ampla desistência de regulamentos sistêmicos. O usuário deve ser capaz de otimizar completamente livre para os seus graus de modularização. Ao omitir a barreira das diferentes perspectivas das funções de automação e de segurança de máquinas, o usuário ganha significativos níveis de liberdade.

O PSS 4000 é um sistema de automação que contém os aspectos da modularização e flexibilização como suas duas funções básicas. Pela primeira vez, é possível gerenciar todas as variáveis do processo no sistema, até as funções de segurança, de forma completamente simbólica e sem nenhuma relação com o Hardware. Isto é demonstrado, de forma que todas as variáveis do processo ficam disponíveis em todo o sistema e, graças à arquitetura Multi-Master, todos os controles ficam disponíveis automaticamente no sistema de automação.

3.1.3. Certificação modular

Quanto mais a máquina for construída em módulos, mais componentes precisam ser conectados de forma descentralizada. A modularidade de máquinas ou das peças de máquinas possui diversas grandes vantagens: Módulos de máquinas podem ser recombinações e substituídos, pode-se ampliar a máquina ou, por exemplo, executar uma troca de ferramenta com a produção em andamento. As máquinas são mais flexíveis. Com a mesma quantidade de máquinas, o operador pode produzir uma quantidade maior de produtos. Sob a premissa de que isto representa um benefício ao operador, conceitos de controle tornam-se descentralizados. O tema Safety & Security assume assim uma maior ênfase. A palavra-chave é certificação modular dos módulos individuais do sistema. Hoje, as máquinas são certificadas como um todo pelas certificadoras. Uma pequena alteração, como por exemplo, a troca de dois módulos, exige uma nova certificação. Soluções estão sendo discutidas, mas não existe hoje um procedimento uniforme. Uma solução é: A máquina será segura se os seus módulos individuais forem seguros. Trata-se neste momento de sensibilizar empresas e decisores na política através de associações, já que progressos são inconcebíveis sem o enquadramento jurídico correspondente.

3.2. Security

O desafio para Security é que, ao contrário da segurança funcional, os mecanismos de Security devem ser constantemente adaptados para as ameaças. Por exemplo, por uma atualização ocasional planejada, porque vírus, worms, cavalos de troia etc. sempre evoluem para encontrar as lacunas na Security e podem afetar a produção e todos os seus elementos funcionais. Para poder reagir de forma flexível ao respectivo cenário de ameaça, a proteção das aplicações de Safety deve ser auxiliada por uma estratégia ampla de Security, que é composta de diversas camadas: No núcleo estão os componentes de automação. Depois a rede, através da qual estes componentes conseguem se comunicar entre si ou com um sistema ERP (Enterprise Resource Planning). A camada externa forma a fábrica, que é protegida de fora através de um conceito especial de Firewall, a chamada zona desmilitarizada.

As exigências impostas à Security pelo mundo de TI e pelo mundo da automação diferem claramente. Enquanto no ambiente de escritórios a confidencialidade das informações possui a maior prioridade, na área de produção a prioridade é a disponibilização dos dados, porque os dados são pré-requisito essencial para processos de produção sem problemas. Atualmente trabalha-se em uma norma internacional (IEC 62443) na qual os dois mundos de Security devem ser unificados. Como as ameaças do mundo cibernético são dinâmicas, a Safety e a Security permanecem como dois temas separados, mas que estão intimamente ligados.

Para isso, é importante desenvolver métodos e ferramentas, com as quais é possível analisar o impacto das lacunas de Security nos riscos remanescentes adicionais para o Safety. Estes métodos e ferramentas devem ser introduzidos, se possível logo no desenvolvimento do produto por sistemas ciberfísicos (CPS), com: Security by Design.

Os aspectos a serem considerados são:

- ▶ Proteção das interfaces (CLP) para fora (Internet, rede da empresa, ...)
- ▶ Proteção dos sistemas de comunicação na máquina e no sistema, com base nos tipos de uso (operação constante, manutenção remota, diagnóstico remoto, conexões Ad-hoc)
- ▶ Security como "Moving Target", não existe uma solução constante de segurança

3.2.1. Soluções na área de Security

Como é possível proteger as aplicações de Safety contra as ameaças do mundo cibernético? A resposta é simples, somente com a combinação de diferentes medidas e diretivas de Security e que estas sejam mantidas consequentemente por todos os participantes envolvidos. Em relação à conexão, a receita para o sucesso é "Defense in Depth", ou seja, uma defesa com diferentes profundidades. Um elemento central que foi utilizado na construção de castelos desde a Idade Média é a base do modelo de Security "Zones and Conduits" (zonas e transições), definido na norma IEC 62443. Este modelo estipula uma rede de automação a ser dividida em diferentes zonas, em que os aparelhos podem comunicar-se entre si. A troca de dados com aparelhos em outras zonas somente é possível através de uma única transição, que é monitorada por um roteador seguro ou um Firewall, que filtra o fluxo de dados com regras definidas e, assim, bloqueia acessos não autorizados. Mesmo se fosse possível para um hacker acessar uma zona, somente as unidades locais seriam comprometidas, todas as outras unidades permaneceriam em segurança.

3.2.2. Soluções de automação

Para a proteção das soluções de automação, na IEC 62443 estão definidos os chamados sete “Foundational Requirements” para a segurança deste tipo de soluções de automação na série de normas de segurança de TI dos sistemas de automação industrial:

- ▶ Identification and authentication control (IAC)
- ▶ Use control (UC)
- ▶ Data integrity (DI)
- ▶ Data confidentiality (DC)
- ▶ Restricted data flow (RDF)
- ▶ Timely response to events (TRE)
- ▶ Resource availability (RA)

Cada requisito fundamental pode ser dividido nos seguintes elementos:

- ▶ Identification & authentication
- ▶ Human user identification
- ▶ Multifactor authentication for untrusted networks
- ▶ Software process and device identification
- ▶ Unique identification and authentication
- ▶ Strength of password-based authentication
- ▶ Password generation and lifetime restrictions for human users

Cada um dos elementos possui quatro níveis de segurança, que pode ser obtido dependendo da complexidade de desenvolvimento das soluções de automação. O integrador de sistemas e o operador do sistema devem definir os níveis de proteção correspondentes para a utilização e para o modelo de zonas derivado. O maior nível de proteção “Level 4” será com certeza pouco utilizado, já que este pode significar um enorme trabalho.

A melhor medida técnica de Security será inútil se não for praticada ou, pior, se for debilitada por causa da exigência de tempo ou por causa da incompreensão ou ignorância. As medidas técnicas devem seguir diretivas e medidas organizacionais. Do que adianta utilizar a melhor configuração de Firewall se a senha padrão do manual não for alterada ou se for possível estabelecer com facilidade uma conexão entre senha e aparelho. Somente com a interação de medidas técnicas e organizacionais é obtido o nível de proteção desejado para uma parte do sistema.

3.3. Cooperação entre Safety & Security

Conceitos amplos de segurança exigem mais do que a cooperação de Safety & Security. Eles precisam de arquiteturas de sistema com orientação especial, que seguem normas publicadas e incluem as considerações de diversos fabricantes. Com visão ao aspecto Safety deve-se verificar até que ponto temas de Security influenciam a segurança funcional.

Temas centrais são comprovantes de identidade claros e seguros dos produtos, processos e máquinas, incluindo a troca segura de informação ao longo de todo processo de produção.

Além disso, são solicitadas soluções fáceis ao usuário: Safety & Security devem ser gerenciáveis e devem ser orientadas para as necessidades do usuário. De uma perspectiva comercial, a segurança também impulsiona inovações: Isto engloba a inclusão de estruturas de

custos em relação a produtividade. Indispensáveis são neste caso a segurabilidade de danos e os métodos de cálculo necessários.

Quando o fator humano está envolvido, trata-se de “Usable Security and Privacy”. O objetivo é manter o custo em relação ao tempo e compreensão das medidas necessárias de Security o mais baixo possível.

Existem analogias com a segurança funcional: A disponibilidade não deve ser influenciada pelas medidas de Safety. Os princípios do mundo de Safety podem ser transmitidos diretamente para o mundo de Security. Segurança exige uma abordagem holística.

4. Área de atuação da abordagem modular

Somente será possível lidar com os desafios desta área com o “pensamento modular” interdisciplinar a médio e longo prazo. Os sistemas de controle possuem uma função central que precisam apoiar esta abordagem.

4.1. Sistemas inteligentes distribuídos - Sistema de automação PSS 4000

Com o sistema de automação PSS 4000, a Pilz segue consequente a abordagem mecatrônica. A ideia central do PSS 4000 é a união da automação e da segurança. Dados do processo ou de controle, dados de segurança e informações de diagnóstico são trocados e sincronizados através do sistema de comunicação Multi-Master SafetyNET p. Portanto, para a função de controle não é importante onde a respectiva parte do programa é processada. Ao invés de um controle central, está disponível para o usuário um programa de usuário dividido por todo tempo de execução para um projeto central. Através deste projeto central, são configurados, programados e diagnosticados todos os participantes da rede. Se a fase de projeto foi concluída, as peças individuais do programa são atribuídas aos aparelhos individuais de controle. Isso é realizado com especificações claras de usuário para o Clustering das unidades funcionais. Assim é possível uma abordagem simples e unificada em todo projeto. Além da formação de módulos e da padronização, sugerem outras vantagens na forma de uma resposta flexível a erros, uma maior disponibilidade assim como uma maior produtividade, por causa dos tempos mais curtos de reação de todo o sistema.

Enquanto na automação clássica um único controle central controla a máquina ou o sistema e processa todos os sinais, o PSS 4000 possibilita uma distribuição das funções de controle. No detalhe, o sistema de automação PSS 4000 é composto de componentes de Hardware e de Software, além da Ethernet SafetyNET p em tempo real e diversos editores de programação com seus blocos de funções voltados para a abordagem que podem ser usados em diferentes áreas. Ao hardware pertencem controles de diferentes classes de desempenho. Dados de processo ou de controle, dados de segurança e informações de diagnóstico são trocados e sincronizados através da Ethernet. Esta fusão consequente de funções de segurança e de automação reduz a complexidade na área de comunicação e leva a uma otimização dos custos.

4.2. Ferramenta de engenharia PAS4000

O objetivo do sistema de automação PSS 4000 é facilitar a descentralização das funções de controle e manter o manuseio com visão clara. A plataforma de Software PAS4000 desempenha neste caso uma função crucial. Ela inclui diversos editores para a programação e configuração do CLP assim como blocos de software. No PAS4000, as ferramentas para a elaboração do projeto, programação, comissionamento e operação são compatíveis entre si.

O PAS4000 auxilia a desmontagem de uma função de máquina/sistema em módulos de função cada vez menores, que seguem os mesmos limites de divisão das unidades de mecatrônica. A modularização é um aspecto central: Das funções básicas surgem elementos, de elementos surgem módulos, de módulos surgem máquinas e sistemas - muito simples através do agrupamento hierárquico dos blocos. Funções básicas, elementos e módulos formam a base da criação de software e podem ser reutilizados como componentes de Software, por causa do encapsulamento e da orientação para os objetos.

O PAS4000 disponibiliza bibliotecas de software, que contém as funções básicas, elementos e módulos mais comuns. A seleção de componentes acabados da biblioteca não é novidade. O que é novo no PAS4000 é que estes componentes podem receber propriedades, as chamadas "Properties". Com estas, é possível fazer uma parametrização simples das funções desejadas. Isso traz inúmeras vantagens para uma padronização das funções.

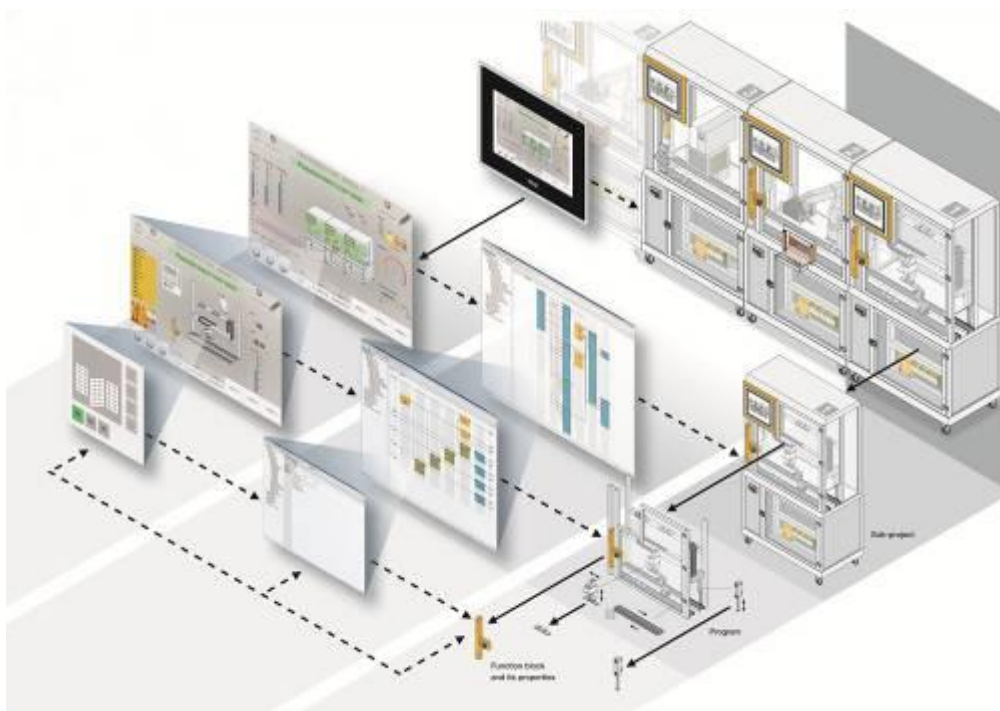


Ilustração 4: Todos os sistemas podem ser divididos em unidades claras que operam de forma independente.

4.3. Visualização no PASvisu

Visualização e programa de controle podem ser divididos até a menor unidade seguindo o mesmo princípio. A base de dados comum dos módulos individuais garante que os módulos

possam se comunicar uns com os outros. Graças à estrutura uniforme, os dados dos projetos podem ser reutilizados com facilidade.

O Software de visualização possibilita elaborar e configurar de forma simples, através do PASvisu Builder, projetos de visualização.

Graças ao acesso a todos os dados de um projeto de automação, incluindo todas as variáveis do processo e espaços de nomes OPC, é eliminado o erro da inserção e atribuição manual de variáveis. Com isso, é por exemplo possível também acessar informações, como a soma de controle do projeto ou versão do Firmware do controle.

A Indústria 4.0 considera o “Valor dos dados”, neste caso, dos dados da fase de projeto. Uma base comum de dados garante a redução de possíveis erros pela transferência automática dos dados “correspondentes”, pela verificação automática de consistência e garante uma redução do tempo de engenharia: A formação modular uniforme no controle e na visualização facilita a reutilização de módulos e elementos da máquina.

Glossário

Smart Product

O produto inteligente possui uma identificação ou está conectado diretamente com informações importantes da sua fabricação e consegue controlar o seu processo de produção automaticamente com estas informações. O objeto inteligente é a base para a Internet das coisas.

Internet das coisas

Na Internet das coisas (Internet of Things, IoT), “coisas” respectivamente elementos ou objetos inteligentes comunicam-se entre si através de uma rede digital universal. Computadores estão desaparecendo como aparelho único e são substituídos por “coisas inteligentes”. Estas estão conectadas com a Internet, se comunicam independentemente com a Internet e, com isso, podem realizar diversas tarefas para os seus proprietários.

Assim podemos agradecer principalmente o Radio Frequency Identification (RFID) como tecnologia de localização inteligente, porque os objetos já conseguem identificar-se sozinhos e podem controlar-se parcialmente. Nos objetos, são salvas determinadas informações sobre o que deve acontecer com eles. Os produtos informam ao sistema de fluxo de material ou ao sistema de produção quais são as suas próximas etapas de trabalho. A ajuda de pessoas não é mais necessária.

Sistemas ciberfísicos (CPS)

Componentes essenciais são dispositivos, aparelhos e máquinas (incluindo robôs) móveis e portáteis, sistemas incorporados e objetos conectados (Internet das coisas). A transferência e transmissão de dados, além do controle ou comando são realizados por uma infraestrutura, como Internet em tempo real.

Sem contato direto, é possível comandar e acessar informações, usando a inteligência própria, os equipamentos podem até tomar decisões sozinhos. Um sistema ciberfísico é caracterizado pelo alto grau de complexidade. Os sistemas ciberfísicos são compostos pela conexão de sistemas integrados pela rede de comunicação com fios ou sem fios.

Modelo de arquitetura de referência (RAMI)

No passado, a automação estava marcada por uma estrutura baseada em Hardware (pirâmide de automação). Hoje a estrutura está ultrapassada, porque a automação não se trata mais apenas do cabeamento de aparelhos de hardware, mas também da conexão entre nuvens e dados. Além disso, não estão disponíveis apenas dados de produção no processo, também é possível acessar de fora dados do controle. Foi por este motivo que o modelo de arquitetura de referência (RAMI) foi desenvolvido como pirâmide modernizada de automação. A ZVEI desenvolveu as ideias e os conceitos da indústria de automação em conjunto com a VDI/VDE-GMA, DKE e os parceiros na plataforma de associações da Indústria 4.0, Bitkom e VDMA.¹⁰ O modelo apresenta pela primeira vez os elementos essenciais da Indústria 4.0 em um modelo de camadas tridimensional.¹¹ Com esta estrutura, é possível classificar e desenvolver sistematicamente a Indústria 4.0. O modelo também definiu as normas para a Indústria 4.0. Tal

¹⁰ <http://www.zvei.org/Themen/Industrie40/Seiten/Das-Referenzarchitekturmodell-RAMI-40-und-die-Industrie-40-Komponente.aspx>

¹¹ http://www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf

padronização é necessária, porque os componentes da Indústria 4.0 de diferentes empresas devem ser capazes de comunicar-se entre si.

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, Telefax: +49 711 3409-133, E-mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY