Industrie 4.0: segura e inteligente

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Exclusión de responsabilidad

En la elaboración de nuestro libro blanco (Whitepaper) hemos cuidado el más mínimo detalle. Contiene información sobre nuestra empresa y nuestros productos. Todos los datos se basan en el estado actual de la técnica y en nuestro mejor saber y entender. Sin embargo, puesto que no es posible evitar completamente los errores y salvo negligencia grave por nuestra parte, declinamos toda responsabilidad en relación con la exactitud e integridad de la información. Hacemos hincapié en que los datos no tienen la calidad legal de garantías o propiedades garantizadas. Agradeceremos nos comuniquen cualquier discrepancia.

Propiedad intelectual

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

2.ª edición

Contenido

1. Acerca de Industrie 4.0 4
1.1. Historia y antecedentes: desde la máquina de vapor a la fábrica inteligente 4
1.2. La fábrica inteligente: Smart Factory 5
1.2.1. Smart Factory^{KL} 5
1.2.2. Módulo de demostración Smart-Factory de Pilz 6
1.3. Seguridad: Safety & Security 7
1.4. Máquina modular y descentralización 8

2. Industrie 4.0 y Pilz 9
2.1. La aportación de Pilz 9
2.2. Industrie 4.0 en la producción de Pilz 9
2.2.1. TI en la producción conectada en red 10
2.2.2. "Pilz Denkfabrik 4.0" 10
2.3. Campos de actuación de Industrie 4.0 10

3. Campo de actuación Seguridad: Safety y Security 11
3.1. Safety 11
3.1.1. Safety: de seguridad estática a seguridad dinámica 12
3.1.2. Safety 4.0: de estructuras monolíticas a soluciones modulares 12
3.1.3. Certificación modular 13
3.2. Security 14
3.2.1. Enfoques de solución en el ámbito de la Security 14
3.2.2. Soluciones de automatización 15
3.3. Interacción entre Safety y Security 15

4. Campo de actuación del enfoque modular 16
4.1. Sistemas inteligentes distribuidos: el sistema de automatización PSS 4000 16
4.2. Herramienta de ingeniería PAS4000 17
4.3. Visualización PASvisu 18

Glosario 19

1. Acerca de Industrie 4.0

Industrie 4.0 no es tan solo una visión de futuro. La fusión inteligente es una oportunidad única para la industria. Con una producción flexible es posible optimizar el grado de utilización de las instalaciones. A pesar de la posibilidad de fabricar productos a medida al coste de la fabricación en masa, con el consiguiente aumento de la productividad de la instalación, sigue habiendo muchas empresas reacias a implantar Industrie 4.0 en su propio sistema de producción. Según el estudio "Industry 4.0 – How to navigate digitization of the manufacturing sector, 2015"[1] del instituto McKinsey, solo seis de cada diez empresas de Alemania consideran estar preparadas para Industrie 4.0 a pesar de que el 91% percibe las oportunidades que brinda la digitalización de la producción industrial. Para contrarrestar esta situación, nuestro propósito es ofrecer soluciones y productos para Industrie 4.0 a las empresas de todo el mundo. La razón es la importancia que el tema Industrie 4.0 está adquiriendo también a nivel internacional: la creciente globalización obliga a crear las condiciones que hagan posible la conexión en red mediante la digitalización de los procesos de producción en la cadena de creación de valor.

1.1. Historia y antecedentes: desde la máquina de vapor a la fábrica inteligente

La primera revolución industrial consistió en la mecanización basada en la fuerza hidráulica y de vapor y abrió las puertas a la segunda revolución industrial: la fabricación en serie a destajo utilizando líneas de fabricación y energía eléctrica. Después siguió la revolución digital, conocida también como "Industrie 3.0". El trabajo con el PC se convirtió en una tarea usual y entró en escena el primer control programable PLC.
El término "Industrie 4.0" simboliza la cuarta revolución industrial, que hace posible los sistemas ciberfísicos (CPS), el "Internet de las cosas" y Smart Factory. Para Pilz, sin embargo, Industrie 4.0 representa más bien una evolución, pues la implementación de Industrie 4.0 no sería posible sin la voluntad de cambio de todos los actores implicados.

El término "Industrie 4.0" se dio a conocer al gran público por primera vez en la Hannover Messe de 2011. En octubre de 2012, el grupo de trabajo Industrie 4.0 transmitió recomendaciones de implementación al grupo de promotores de comunicación de la unión de investigación del Gobierno Federal alemán. En abril de 2013 el grupo de trabajo Industrie 4.0 entregó su informe final a renombrados representantes del Gobierno Federal en la Hannover Messe. En estas fechas inició también sus actividades la plataforma Industrie 4.0, creada por las asociaciones sectoriales Bitkom[2], VDMA[3]y ZVEI[4]. Su misión es coordinar las actividades en este ámbito vanguardista. Pilz ha participado en estas actividades desde el principio y canaliza su dilatada experiencia con la ingeniería de automatización en el apoyo de proyectos.

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

[2] Bitkom (Digitalverband Deutschlands/Asociación digital de Alemania/Germany's digital association), https://www.bitkom.org/EN/index-EN.html

[3] VDMA (Verband Deutscher Maschinen- und Anlagenbau/Asociación Alemana de Maquinaria e Industria Manufacturera/Mechanical Engineering Industry Association), http://www.vdma.org/ueber-uns

[4] ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e. V./Asociación Alemana de la Industria Electrotécnica y Electrónica), http://www.zvei.org/en/Pages/default.aspx

1.2. La fábrica inteligente: Smart Factory

Smart Factory es la fábrica inteligente del mañana. Este término es producto de la investigación en la ingeniería de fabricación. Smart Factory es el objetivo de la estrategia de tecnología avanzada del Gobierno Federal alemán como parte del proyecto pionero Industrie 4.0.[5] La Smart Factory ha de favorecer un entorno de producción en el que las instalaciones de fabricación y los sistemas logísticos se organicen y optimicen principalmente de forma automática. En la Smart Factory se sabe en todo momento en qué parte se encuentran los productos que se fabrican allí, se conoce su historial, su estado actual y los pasos de producción que les falta hasta ser productos acabados. Pero, ¿cómo puede conseguirse?
La base tecnológica son sistemas ciberfísicos[6] que se comunican a través del Internet de las cosas[7]. La comunicación entre el producto o portapiezas y la instalación de fabricación forma parte de este escenario vanguardista: el producto transporta su información de fabricación en formato legible por la máquina, p. ej. en un chip RFID. Con estos datos se controla el recorrido del producto por la instalación y los distintos pasos de fabricación. La Smart Factory se desarrolla sobre la base de fábricas modelo en diferentes escuelas superiores y centros de investigación.

1.2.1. Smart Factory^{KL}

Como principal centro de competencias y plataforma de demostración e investigación independiente, SmartFactory^{KL} es la precursora de la fábrica inteligente del mañana. En ella se desarrollan sistemas de fabricación innovadores en los que la visión de Industrie 4.0 ya es una realidad.[8] La meta es trabajar sobre nuevos conceptos, estándares y soluciones en una red con colaboradores de renombre de la industria y la investigación que formen la base de una ingeniería de automatización de alta flexibilidad.
Como miembro respetado, Pilz contribuye a diseñar el objetivo de la iniciativa en todos los apartados. Pilz evalúa y aplica a su propia oferta los conocimientos derivados del trabajo conjunto sobre la plataforma de desarrollo.
SmartFactory^{KL} dispone hoy día de la primera instalación Industrie 4.0 no propietaria del mundo.[9] La seguridad y la modularización son temas fundamentales. Aprovechando su experiencia en el terreno de la seguridad de las máquinas, Pilz aboga por una estandarización y un procedimiento común en el tema de la seguridad en los apartados Safety (seguridad de la maquinaria) y Security (seguridad TI). Por otra parte, se implica en el tema de la modularización. La configuración de las instalaciones según el enfoque mecatrónico hace posible la modularización completa en forma de elementos mecánicos. Las funciones pueden estandarizarse y utilizarse repetidamente en todos los módulos. La base serán sistemas de automatización capaces de distribuir funciones de control, como el PSS 4000 de Pilz. La Smart Factory es un escenario perfecto para ensayar estos conceptos de automatización. Hace ya varios años que la SmartFactory^{KL} exhibe una instalación de producción modular no propietaria en la que interactúan perfectamente módulos individuales de diferentes fabricantes con distintas arquitecturas de control. Pilz amplía esta instalación de demostración de la Smart Factory^{KL} con un módulo de almacenamiento automático inteligente.

[5] http://www.hightech-strategie.de/de/Industrie-4-0-59.php
[6] Definición en el glosario, página 20 y sig.
[7] Definición en el glosario, página 20 y sig.
[8] http://www.smartfactory.de/
[9] http://www.smartfactory.de/

Figura 1: SmartFactory^{KL} en la Hannover Messe 2015

1.2.2. Módulo de demostración Smart-Factory de Pilz

Con el módulo de demostración Smart-Factory queremos demostrar que es posible fabricar productos personalizados de forma rápida, flexible y económica. La línea de producción modular ilustra la comunicación de sistemas de automatización distribuidos en conjunción con accionadores y sensores. El sistema de automatización PSS 4000 preparado para Industrie 4.0 coordina los procesos de todos los componentes conectados en red para seguridad y automatización, desde la ingeniería hasta la visualización.
Nuestra línea de producción inteligente fabrica estuches para tarjetas de visita y bolígrafos personalizados. La transparencia de los procesos de producción es uno de los principales requisitos. Nuestras soluciones permiten representar de manera sencilla máquinas e instalaciones complejas con funciones sofisticadas, típicas, por ejemplo, de los sistemas digitales conectados en red de Industrie 4.0.

El módulo de demostración se compone de tres módulos de función diferentes:
- Un almacén para portapiezas
- Un robot con cargador de piezas/una estación de salida del producto
- Una estación láser

Los datos del cliente (contacto, dirección, etc.) se introducen en un terminal cliente a través de un PC. Aquí, el cliente elige además si quiere un estuche para tarjetas de visita o un bolígrafo, personalizados con su nombre (bolígrafo) o una tarjeta de visita digital rotulada con su nombre (estuche de tarjetas).
Los datos introducidos se almacenan en un chip RFID digital integrado en el portapiezas. De este modo se asegura la disponibilidad de la información en todos los módulos. La información necesaria para los distintos módulos se lee del chip y se ejecutan los pasos requeridos. Los datos del chip RFID se borran a la salida del producto después de completarse correctamente el proceso de fabricación. El chip queda disponible para la grabación del siguiente registro de datos. Después del proceso de borrado, el portapiezas con el chip RFID se almacena

nuevamente si no hay más registros de datos que grabar o se reincorpora al circuito de producción.

Figura 2: Módulo de demostración Smart-Factory en la Hannover Messe 2016

1.3. Seguridad: Safety & Security

Con la evolución del entorno de automatización hacia Industrie 4.0, las empresas se enfrentan a nuevos requisitos de seguridad. El mundo de la automatización se funde con el mundo TI. Las perspectivas de la seguridad de estos dos mundos se diferencian claramente: los conceptos internacionales "Safety" para la seguridad de las máquinas y "Security" para la seguridad informática y de datos facilitan una diferenciación básica.

Safety exige que los riesgos residuales de una máquina o instalación no superen valores aceptables. Esto incluye tanto los peligros del entorno de la instalación (p. ej., daños ambientales) como los peligros en la propia instalación (p. ej., las personas que se encuentran en la instalación).
Security se refiere a la protección de una máquina o instalación contra accesos no autorizados desde el exterior y a la protección de datos sensibles contra falsificación, pérdida y acceso no autorizado a nivel interno. Esto incluye tanto ataques explícitos como sucesos Security involuntarios.

La protección global de datos de control relevantes en términos de producción y de Safety en la transmisión, el procesamiento y el almacenamiento debe estar enfocada a los siguientes ámbitos de Security:

- Seguridad física y disponibilidad de los sistemas TI
- Seguridad de redes
- Seguridad de aplicación de software
- Seguridad de los datos

- Seguridad de funcionamiento

1.4. Máquina modular y descentralización

La fabricación de máquinas e instalaciones modulares está considerada desde hace años como una de las claves para aumentar la flexibilidad de la producción. Una instalación se compone de varios módulos de maquinaria autónomos. Cada módulo representa uno o más pasos de producción estandarizados y puede combinarse con otros módulos para formar un proceso completo. Para ello, todo los módulos se conectan a una red troncal (Backbone) que les suministra energía (corriente trifásica 400 V AC, aire comprimido, etc.) y datos de proceso y control. Es posible sustituir uno o más módulos o agregar módulos idénticos en caso de tener que modificar el proceso de producción o aumentar la productividad.

En consecuencia, la modularización y la descentralización son dos de los principales factores de éxito hacia el futuro de la automatización. El requisito son sistemas de automatización capaces de controlar de forma intuitiva la inteligencia distribuida en los módulos de la maquinaria. Todas las máquinas e instalaciones pueden descomponerse en unidades perfectamente delimitadas que trabajan independientemente.

La estructura modular de máquinas e instalaciones se basa en el enfoque mecatrónico, cuya filosofía es la de hacer confluir a todos los niveles todas las disciplinas que intervienen en el proceso de fabricación de una máquina: mecánica, electricidad y tecnología de automatización. La interacción de diferentes componentes de automatización individuales y de las herramientas de software correspondientes confluye en una solución de automatización y está definida de manera sistemática. Esta transversalidad abarca los cuatro niveles de la pirámide de automatización (nivel de dirección, nivel de gestión de la empresa, nivel de control y nivel de campo). El enfoque mecatrónico requiere que las funciones de control puedan "migrarse" también a las unidades mecatrónicas modulares.
Este es el punto crítico de los sistemas actuales. Aunque es posible crear módulos de función, si han de ser ejecutados por potentes sistemas de control centralizados, la complejidad asociada convierte la puesta en marcha de módulos individuales en una tarea excesivamente laboriosa. Esta dificultad se extiende también a las eventuales modificaciones de la configuración y programación de módulos de función individuales que puedan resultar necesarias.
La utilización de sistemas descentralizados simplifica la puesta en marcha de los módulos. Como también se simplifica la creación de la configuración gracias a la posibilidad de utilizar programas y subfunciones de control idénticas para módulos diferentes.

Por consiguiente, las tareas de automatización del futuro requieren soluciones que permitan distribuir la inteligencia de control y a la vez garanticen que la necesaria interconexión de varios controles siga siendo sencilla de manejar para los usuarios. El sistema de automatización PSS 4000 de Pilz satisface estos requisitos.

2. Industrie 4.0 y Pilz

2.1. La aportación de Pilz

Susanne Kunschert, socia administrativa de Pilz, fue invitada en 2010 por el Gobierno Federal alemán a representar en persona a la mediana empresa en la unión de investigación. Este era el organismo asesor central en materia de política de investigación del Gobierno Federal para la implementación y el desarrollo de la estrategia de tecnología avanzada. La misión de Susanne Kunschert era aportar las perspectivas de la mediana empresa innovadora a este organismo.

Como miembro del grupo promotor de la seguridad, la socia gerente de Pilz se ocupa de la protección eficaz de redes de comunicación y del desarrollo de Alemania como mercado líder en tecnología de seguridad. La unión científica elaboró en grupos de trabajo proyectos de futuro para los sectores de demanda identificados. Industrie 4.0 es uno de los principales.

Pilz respaldó activamente en diferentes proyectos el trabajo de la recién creada comisión "Industrie 4.0" bajo el paraguas de las asociaciones profesionales Bitkom, ZVEI y VDMA, y participó en la elaboración de las recomendaciones de actuación. Estas recomendaciones se entregaron al Gobierno Federal con ocasión de la Hannover Messe 2013.

En la actualidad, Pilz participa activamente en los siguientes organismos e iniciativas:
- Colaboración en la plataforma Industrie 4.0
- Colaboración en el círculo dirigente de Industrie 4.0 de la asociación ZVEI
- Colaboración en la Landesnetzwerk Mechatronik BW (red estatal de mecatrónica de Baden-Württemberg)
- Miembro del comité directivo de Allianz Industrie 4.0 Baden-Württemberg
- Miembro de la plataforma de demostración e investigación independiente Smart Factory^{KL}
- Miembro de ARENA2036, el futuro de la construcción del automóvil

2.2. Industrie 4.0 en la producción de Pilz

Más allá de la participación en la unión de investigación y la plataforma de investigación SmartFactory^{KL}, en Pilz, Industrie 4.0 ha pasado de ser un proyecto pionero a estar plenamente integrado en el proceso de producción**.**
La progresiva conexión en red de maquinaria e infraestructuras de la fabricación mediante el uso de tecnologías TI permite a Pilz trasladar su condición de líder tecnológico también a su propia producción. Con la mirada puesta en Industrie 4.0, se creó la infraestructura necesaria para la producción inteligente y se avanzó en la implementación de elementos de Industrie 4.0. Actualmente ya está en servicio un sistema de transporte de piezas inteligente, desarrollado por la propia empresa, que acelera y simplifica, por ejemplo, el equipamiento de placas de circuitos y el proceso de soldado. Los portapiezas llevan un chip RFID que los dirige automáticamente de la estación de soldadura a la unidad de montaje.
Pilz seguirá implementando paso a paso la producción inteligente: los datos de la maquinaria se recopilan y procesan selectivamente para el control de la fabricación. Su evaluación proporciona información importante sobre cambios de estado y el desgaste de las máquinas y hace posible un mantenimiento preventivo. El **"**Predictive Maintenance**"** evita fallos y tiempos

de parada. Se implementará asimismo el almacenamiento de los documentos de trabajo más recientes en la nube "Pilz Cloud". Todos los datos y documentos estarán disponibles en tiempo real y actualizados y podrán consultarse en cualquiera de los terminales móviles de la producción.

2.2.1. TI en la producción conectada en red

Pilz conoce perfectamente los retos que una producción completamente conectada en red supone en términos de TI-Security. Por esta razón, Pilz está invirtiendo en una extensa infraestructura de Security para controlar el tráfico de datos completo. Esto incluye también un centro de cálculo propio diseñado conforme a los últimos estándares. El análisis permanente y el registro en log de todos los parámetros de fabricación relevantes aseguran la detección anticipada de anomalías. Para las distintas áreas de fabricación se instalaron además diferentes cortafuegos que permiten definir un nivel de Security específico para cada zona. La meta es minimizar fallos y riesgos para la seguridad y proteger el "know-how".

2.2.2. "Pilz Denkfabrik 4.0"

Otro de los puntos de máxima prioridad para Pilz y fundamental para Industrie 4.0 es la colaboración entre los departamentos de Tecnologías de la información e Ingeniería de producción. En la "Pilz Denkfabrik 4.0" (fábrica de ideas) creada especialmente al efecto, el personal de Producción y TI trabaja con los recursos necesarios para planificar e implementar proyectos conjuntos relativos a Industrie 4.0.

2.3. Campos de actuación de Industrie 4.0

Uno de los requisitos para la aceptación a largo plazo de los mercados es la creación de mecanismos estandarizados en la comunicación entre las máquinas y dentro de cada máquina. La obtención de soluciones viables y merecedoras de la aceptación de los usuarios depende de que se tengan en cuenta los requisitos de ambos mundos (automatización y TI).
En resumen: Pilz apuesta por arquitecturas de control modernas en el contexto de Industrie 4.0.

Los dos temas siguientes centran nuestra atención:

- Safety y Security:
  - Ambos guardan claros paralelismos en lo que a la estandarización y al procedimiento del proceso de ingeniería se refiere. Queremos utilizar nuestra experiencia en seguridad de las máquinas y automatización para impulsar este proyecto tan importante.
  - Todos los dispositivos y componentes de automatización que requieren la función de automatización tienen acceso directo a Internet para el intercambio de datos de proceso y datos de parametrización para diagnóstico y mantenimiento (remoto). Como consecuencia, aumentan los requisitos relativos a Security y a una conexión y representación de diagnóstico unificada para todos los dispositivos de automatización participantes.
- Enfoque modular:
  - Nuestras modernas funciones de control están diseñadas para la distribución y orientación en los objetos; los sensores y actuadores adquieren inteligencia. De este modo, trasladamos la tendencia hacia objetos de control mecatrónicos (componentes de automatización) a nuestros productos y las herramientas de ingeniería asociadas.

3. Campo de actuación Seguridad: Safety y Security

Safety y Security son requisitos importantes para el funcionamiento de las instalaciones conformes a Industrie-4.0 que, a diferencia de las instalaciones de producción tradicionales, disponen de puntos de conexión con su entorno.

En el futuro, las instalaciones Industrie 4.0 podrán reconfigurarse y optimizarse de forma autónoma y esto exige una nueva evaluación de la seguridad (Safety y Security) en tiempo de ejecución, es decir, durante el funcionamiento por la propia instalación. Asimismo, deberá garantizarse que las lagunas de Security restantes no generarán riesgos inaceptablemente altos en términos de Safety.

Finalmente, otro de los objetivos es fomentar la confianza en la pequeña y mediana empresa, la base decisiva para la producción en redes concebidas para este fin. La transparencia, la participación y una comunicación abierta son requisitos fundamentales en este sentido.

Figura 3: Interacción entre Safety y Security

3.1. Safety

Hoy día, el ámbito "Safety" ya se caracteriza por una elevada seguridad de inversión y seguridad jurídica. Esto se debe en gran medida a la regulación mediante normas y estándares. Todos los procesos de análisis y evaluación de riesgos y la ejecución del análisis

están claramente definidos mediante niveles de integridad de la seguridad (SIL) en las clasificaciones estandarizadas internacionales y es posible comparar con validez jurídica las soluciones.

3.1.1. Safety: de seguridad estática a seguridad dinámica

El término Safety describe la seguridad funcional de máquinas o, dicho de otro modo: la protección de personas y del medio ambiente contra amenazas provenientes de las máquinas. Safety exige que los riesgos residuales de una máquina o instalación no superen valores aceptables. Esto incluye tanto los peligros del entorno de la instalación (p. ej., daños ambientales) como los peligros en la propia máquina o instalación (p. ej., las personas que circulan por la instalación).
Una de las posibilidades es interrumpir inmediatamente la alimentación en caso de fallo y parar la máquina en caliente. La manera clásica de realizarlo es mediante un cableado de seguridad especial y componentes como, p. ej., relés de seguridad. Sin embargo, al tratarse de un enfoque basado principalmente en el hardware y por tanto estático, es poco adecuado para procesos de fabricación inteligentes que requieren modificaciones continuas de la configuración de la instalación. La desconexión brusca tiene asociados generalmente inconvenientes adicionales, como una pérdida de productividad, tiempos de parada prolongados debido a procedimientos de nueva puesta en marcha más laboriosos o una limitación del concepto de manejo y mantenimiento de la máquina.

Una de las alternativas válidas son los conceptos de seguridad dinámica basados en un enfoque global de los procesos de automatización modificables y de los requisitos de seguridad funcional. Como consecuencia, cambia también la forma de interpretar la seguridad como tal, que se entiende no tanto como una característica del hardware sino como una función universal que abarca todos los dispositivos. Con este enfoque, desarrollado ya antes de los tiempos de Industrie 4.0, es posible la gestión segura de los procesos sin que deban interrumpirse inmediatamente cada vez que se produzca un error. No obstante, la implementación eficiente del enfoque dinámico requiere tener en cuenta desde el principio la seguridad funcional en la planificación de los proyectos de automatización. De lo contrario, puede ser necesario modificar la secuencia de pasos de fabricación determinados o de todo un proceso, cosa que dificulta el establecimiento de soluciones óptimas y significa además un incremento considerable de los costes.
Mientras que en la seguridad estática a menudo se transmiten solo señales binarias para desconectar, por ejemplo, el movimiento de una máquina después de abrir una puerta protectora, se requiere información más completa para la Safety dinámica. Esto se debe a que en este procedimiento existen varios modos de funcionamiento que permiten el "funcionamiento con puerta protectora abierta". Sin embargo, la información sobre los modos de funcionamiento seguros ha de figurar en todos los componentes implicados. En el ejemplo de la puerta protectora, y según del nivel de autorización del usuario, la apertura de la puerta ya no provoca automáticamente la desconexión inmediata de la máquina, sino que existen mecanismos de seguridad que supervisan el ajuste de una velocidad límite reducida o que generan y supervisan de forma segura la especificación de consigna del eje de giro.

3.1.2. Safety 4.0: de estructuras monolíticas a soluciones modulares

En la Smart Factory ha de ser posible reconfigurar de forma rápida y sencilla o modificar conjuntamente instalaciones con estructura modular. La validación de la solución de seguridad

deberá poder gestionar esta (posterior) flexibilización. Las disposiciones que no se tuvieron en consideración en el proceso del Marcado CE tampoco son sencillas de incorporar para la empresa usuaria. La razón es que la operación $CE_{módulo1} + CE_{módulo2} = CE_{máquina\ completa}$ no se puede aplicar directamente.
La ventaja funcional de los sistemas de máquinas modulares salta a la vista. Se gana flexibilidad en el proceso de producción a la vez que aumenta la capacidad de estandarización a nivel funcional. El grado máximo de estandarización se alcanzable cuando es posible configurar de forma idéntica los límites de las divisiones de los distintos módulos, ya sean módulos con funciones mecánicas, eléctricas, de seguridad o de visualización. El enfoque mecatrónico tiene como meta este tipo de creación estandarizada de objetos de automatización.
Las ventajas de la modularización quedan anuladas muchas veces por conceptos de seguridad rígidos y basados en un extenso cableado físico. También los sistemas programables (autómatas) de seguridad electrónicos tienen casi siempre una réplica de la seguridad basada en hardware (en forma de circuitos de seguridad fijos), a pesar de que puedan implementarse en forma de un sistema de conexionado lógico libremente programable.
El elemento básico de las arquitecturas de control modernas es la ausencia general de reglas basadas en los sistemas. El usuario ha de tener libertad para optimizar según sus grados de modularización. Si a esto se añade la desaparición de la barrera que suponen los distintos enfoques de las funciones de la automatización y la seguridad de la maquinaria, el usuario habrá ganado muchos grados de libertad.
El PSS 4000 es un sistema de automatización que integra la modularización y la flexibilización como dos de sus funciones básicas. Por primera vez ha sido posible gestionar todas las variables del proceso (incluidas las de las funciones de seguridad) de forma completamente simbólica y sin ninguna referencia al hardware del sistema. Este logro se refleja en la disponibilidad a nivel de sistema de todas las variables del proceso y la disponibilidad automática de todos los controles en el sistema de automatización distribuido gracias a la arquitectura Multi-Master.

3.1.3. Certificación modular

Cuanto mayor es el grado de modularización de la maquinaria, mayor es el número de componentes que deben conectarse a nivel descentralizado. La modularidad de las máquinas y partes de máquinas tiene varias ventajas significativas: los módulos de las máquinas pueden recombinarse y sustituirse, es posible ampliar las máquinas o realizar cambios de herramienta, p. ej., en pleno proceso de producción. Las máquinas son más flexibles. La empresa puede fabricar más productos con el mismo número de máquinas. Desde el convencimiento de que esto representa beneficios para la empresa usuaria, crece la descentralización de los sistemas de control. El tema Safety y Security ocupa un lugar destacado en este contexto. La palabra clave se llama certificación de los módulos de instalación individuales. Hoy día, las máquinas son homologadas como unidad por los organismos de certificación. Una modificación pequeña, como la sustitución de dos módulos, requiere un nuevo proceso de aceptación. Aunque se están debatiendo posibles soluciones, no existe todavía un procedimiento unificado. Uno de los enfoques es que la máquina es segura cuando cada uno de sus módulos es seguro. El objetivo es sensibilizar a las empresas y los responsables políticos a través de las asociaciones, pues no cabe pensar en avances en este ámbito sin el oportuno marco legal.

3.2. Security

El reto para la Security es que, a diferencia de la seguridad funcional, los mecanismos de Security han de adaptarse continuamente a la situación de amenaza. Esto se consigue, por ejemplo, mediante actualizaciones coordinadas caso por caso, ya que los virus, gusanos, troyanos, etc. evolucionan continuamente y las lagunas en la Security pueden menoscabar la producción junto con todos sus elementos funcionales.
Para poder reaccionar de manera flexible a los distintos escenarios de amenaza, es preciso implantar también la protección de aplicaciones Safety mediante una estrategia de Security global compuesta por varias capas: en el centro están los componentes de automatización. Después sigue la red en la que estos componentes se comunican con otros o con un sistema ERP (Enterprise Resource Planning). La fábrica constituye la capa superior, protegida del exterior por un concepto de cortafuegos especial, la "zona desmilitarizada".

Los requisitos que el mundo de las TI y el de la automatización plantean a la Security se diferencian claramente. Mientras en la oficina tiene máxima prioridad la confidencialidad de la información, a nivel de producción es la disponibilidad de los datos, pues es un requisito crucial para procesos de fabricación que funcionan correctamente. Actualmente se está elaborando una norma internacional (IEC 62443) que consiga unificar los dos mundos de Security. Dado el carácter dinámico de las amenazas del mundo cibernético, Safety y Security seguirán siendo dos ámbitos separados que, no obstante, estarán estrechamente vinculados.

Es importante desarrollar métodos y herramientas que permitan analizar los efectos de lagunas de Security sobre riesgos residuales adicionales en el sentido de Safety. Estos métodos y herramientas deben integrarse preferiblemente en el desarrollo como producto de sistemas ciberfísicos (CPS): Security by Design.

Aspectos que deben tenerse en cuenta:
- Protección de interfaces (PLC) con el exterior (Internet, red corporativa, etc.)
- Protección de sistemas de comunicación en la máquina o instalación según los tipos de utilización (funcionamiento constante, mantenimiento remoto, diagnóstico remoto, conexiones específicas (ad-hoc))
- Security como "Moving Target"; no existe una sola solución de seguridad invariable

3.2.1. Enfoques de solución en el ámbito de la Security

¿Cómo pueden protegerse las aplicaciones de Safety contra las amenazas del mundo cibernético? La respuesta es clara: solo mediante la combinación de diferentes medidas y directrices de Security aplicadas de manera consecuente por todos los implicados.
Por lo que se refiere a la conexión en red, la receta más eficaz se llama "Defense in Depth" o defensa diferenciada en función de la capa. Uno de los elementos centrales, aplicado dicho sea de paso a la construcción de castillos durante la Edad Media, es el modelo de Security "Zones and Conduits" (Zonas y transiciones), que está definido ya en la norma IEC 62443. Prevé la división de una red de automatización en varias zonas en las que los dispositivos pueden comunicarse entre sí. El intercambio de datos con dispositivos de otras zonas tiene lugar solo a través de una única transición, supervisada por un router seguro o un cortafuegos, que filtra el flujo de datos mediante reglas definidas y bloquea accesos no autorizados. Por consiguiente, aun en el supuesto de que un agresor consiguiera entrar en una zona, comprometería solo la seguridad de los dispositivos locales mientras que los restantes seguirían estando seguros.

3.2.2. Soluciones de automatización

En la IEC 62443 de la serie de normas relativas a la seguridad de la TI en sistemas de automatización industrial se han definido siete "Foundational Requirements" como mecanismo de seguridad de las soluciones de automatización:

- 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 básico puede dividirse en los siguientes 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 uno de estos elementos tiene cuatro niveles de Security en función del esfuerzo invertido en el desarrollo de soluciones de automatización. Aquí entran en escena los integradores de sistemas y explotadores de instalaciones, que deben definir los niveles de protección correspondientes a la aplicación y al modelo zonal derivado. El nivel de protección más alto "Level 4" seguramente no será aplicable en todos los casos, pues puede suponer un gasto enorme.

Sin embargo, incluso la mejor medida de Security técnica puede no servir para nada si no se implementa o, peor aún, se elude deliberadamente para ahorrar tiempo o por incomprensión y desconocimiento. Las medidas técnicas deben ir acompañadas de directrices y medidas organizativas. ¿De qué sirven los ajustes de cortafuegos más eficaces si no se modifica la contraseña predeterminada del manual o es muy fácil establecer una relación entre contraseña y dispositivo? Es la interacción entre medidas técnicas y organizativas lo que establece realmente un "Protection-Level" (nivel de protección) para una parte de una instalación.

3.3. Interacción entre Safety y Security

Los conceptos de seguridad integrales no solo requieren la interacción de Safety y Security. Se requieren sobre todo arquitecturas de sistema orientadas específicamente a estos aspectos, que apliquen estándares abiertos y que incluyan, además, consideraciones no propietarias. Con la vista puesta en el aspecto Safety, deberá comprobarse en qué medida los temas de Security influyen en la seguridad funcional.
Los temas centrales son certificados identitarios unívocos y seguros de productos, procesos y máquinas, incluido el intercambio de información seguro en todas las fases del proceso de producción.

Se requieren además soluciones fáciles de usar: Safety y Security deben ser manejables y orientarse a las necesidades de los usuarios. Desde una perspectiva económica, la seguridad es también un motor para la innovación que engloba la inclusión de estructuras de costes referidos a la productividad. La posibilidad de asegurar el daño y los métodos de cálculo correspondientes son requisitos irrenunciables.
Por lo que respecta al factor humano, prevalece la "Usable Security and Privacy". La meta es reducir en lo posible el esfuerzo en tiempo y comprensión de las medidas de Security requeridas.

Existen analogías con la seguridad funcional en este punto: la disponibilidad no debe verse perjudicada por medidas de Safety. Los principios del mundo de Safety pueden trasladarse directamente al mundo de Security. La seguridad exige un enfoque integral.

4. Campo de actuación del enfoque modular

En vista de los retos, la receta para el éxito a medio y largo plazo pasa por un "pensamiento modular" interdisciplinario coherente. Los sistemas de control que implementen este enfoque desempeñan una función central.

4.1. Sistemas inteligentes distribuidos: el sistema de automatización PSS 4000

Pilz utiliza el sistema de automatización PSS 4000 para implementar el enfoque mecatrónico. La noción principal de PSS 4000 es la fusión de automatización y seguridad. A través del sistema de comunicación Multi-Master SafetyNET p se intercambian y sincronizan datos de proceso o control, datos Fail-safe e información de diagnóstico. La función de control no depende de la ubicación en que se ejecuta la sección de programa correspondiente. En lugar de un control centralizado, el usuario dispone de un programa de aplicación distribuido en tiempo de ejecución en el marco de una vista de proyecto centralizada. A través de esta configuración de proyectos centralizada se configuran, programan y diagnostican todos los participantes de la red. Después de completar la configuración, las distintas secciones del programa se asignan a los diferentes dispositivos de control sobre la base de especificaciones de aplicación unívocas para la agrupación de unidades funcionales. El resultado es un manejo sencillo y unificado dentro del proyecto global. Además de la creación de módulos y la capacidad de estandarización, se obtienen ventajas adicionales, como una reacción flexible a los errores, más disponibilidad y una mayor productividad como consecuencia de los tiempos de reacción más cortos del sistema.

Mientras en la automatización clásica hay un solo control PLC centralizado para supervisar la máquina o instalación y procesar todas las señales, el sistema de automatización PSS 4000 permite la distribución coherente de funciones de control. El sistema de automatización PSS 4000 se compone de elementos de hardware y software, de Ethernet en tiempo real SafetyNET p y de varios editores de programas para diferentes ámbitos, junto con los correspondientes módulos de función para aplicaciones. El hardware incluye controles de diferentes clases de potencia. A través de Ethernet se intercambian y sincronizan datos de proceso o control, datos Fail-safe e información de diagnóstico. La confluencia consecuente de funciones de seguridad

y automatización reduce la complejidad de la comunicación y contribuye además a optimizar los costes.

4.2. Herramienta de ingeniería PAS4000

El objetivo del sistema de automatización PSS 4000 es el de simplificar la descentralización de las funciones de control sin incrementar la complejidad de manejo. La plataforma de software PAS4000 desempeña una función central en este sentido. Abarca módulos de software y diferentes editores de programación de PLC y configuración. Las herramientas de configuración de proyectos, programación, puesta en marcha y servicio están estrechamente ligadas en PAS4000.

PAS4000 simplifica la descomposición de la función de una máquina/instalación en módulos de función cada vez más pequeños conforme a los límites de división de las unidades mecatrónicas. La modularización es un aspecto fundamental: con las funciones básicas se forman elementos, con los elementos módulos y con los módulos se forman máquinas e instalaciones, todo mediante un sencillo anidado jerárquico de los bloques. Las funciones básicas, los elementos y los módulos vertebran la creación del software y pueden reutilizarse óptimamente como componentes de software mediante encapsulado y orientación en los objetos.

PAS4000 proporciona bibliotecas de software que contienen las funciones básicas, los elementos y los módulos. La selección de componentes definidos en bibliotecas no es nada nuevo. En el caso de PAS4000, la particularidad es que estos componentes están dotados de propiedades ("Properties") que permiten parametrizar cómodamente las funciones elegidas. Esto es especialmente ventajoso para la estandarización de funciones.

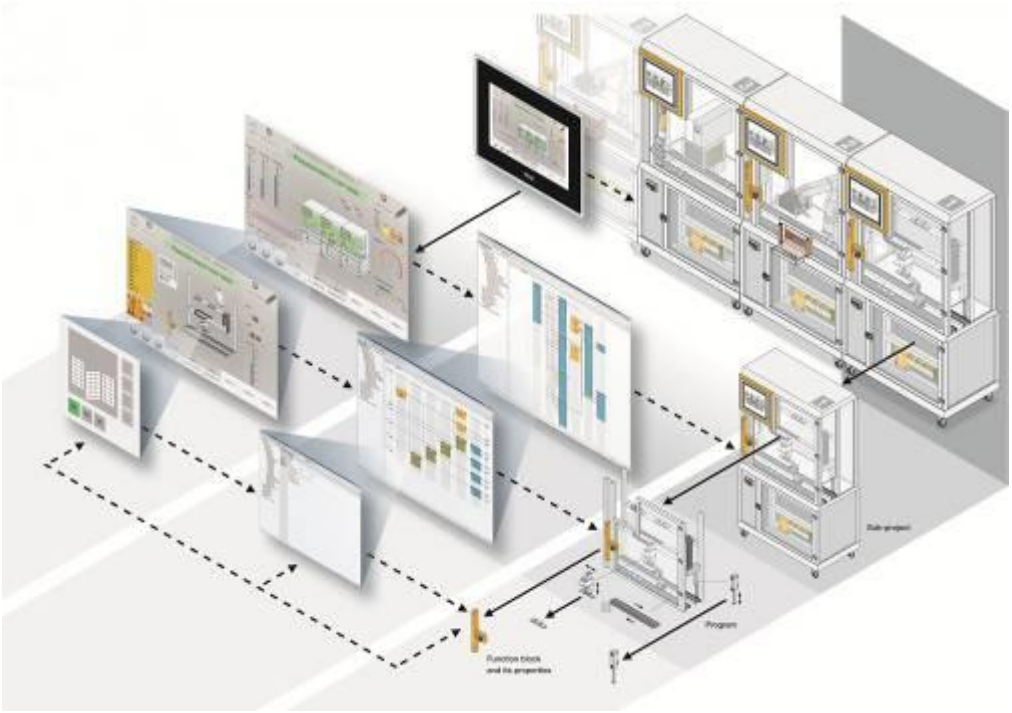

Figura 4: Las instalaciones pueden descomponerse en unidades perfectamente delimitadas que trabajan independientemente.

4.3. Visualización PASvisu

La visualización y el programa de control pueden descomponerse en las unidades más pequeñas siguiendo el mismo principio. Una base de datos común para los distintos módulos asegura la comunicación entre ellos. Esta estructura unificada facilita la reutilización de los datos de configuración.

El software de visualización permite crear y configurar fácilmente proyectos de visualización mediante el PASvisu Builder.
El acceso a todos los datos de un proyecto de automatización, incluidas las variables del proceso y los espacios de nombres OPC, elimina la introducción manual, susceptible de errores, y la asignación de variables. De este modo es posible consultar, por ejemplo, información como la checksum del proyecto o la versión de firmware del módulo de control en cabecera.

En Industrie 4.0 se considera el "valor de los datos", en este caso, de los datos de configuración. Una base de datos común favorece la reducción de posibles fuentes de error mediante la aplicación automática de los datos "adecuados" y el control de coherencia automático se encarga de reducir los tiempos de ingeniería: la creación de módulos uniformes para el control y la visualización simplifica la reutilización de los elementos y módulos de maquinaria.

Glosario

Smart Product
El producto inteligente incorpora información esencial sobre su fabricación en forma de ID o integrada directamente que le permite controlar su proceso de producción. Como objeto inteligente, forma la base del "Internet de las cosas".

Internet de las cosas
En el Internet de las cosas (Internet of Things, IoT), elementos, objetos o "cosas" inteligentes se comunican entre sí a través de una red digital universal. Los ordenadores desaparecen paulatinamente como dispositivos individuales en favor de las "cosas inteligentes". Están conectadas a Internet para poder comunicarse independientemente y ejecutar diferentes tareas y quitar trabajo al propietario.
Así, por ejemplo, el hecho de que hoy día los objetos puedan identificarse ya de forma autónoma y tengan un cierto grado de autocontrol es fruto sobre todo de la tecnología de localización inteligente Radio Frequency Identification (RFID). Los objetos tienen grabada información específica sobre el proceso que han de seguir. De este modo, los propios productos informan a la instalación de flujo de material y de producción sobre los siguientes pasos. La intervención humana ya no es necesaria.

Sistemas ciberfísicos (CPS, por sus iniciales del inglés)
Los componentes fundamentales son instalaciones, dispositivos y máquinas móviles y fijas (incluidos robots), sistemas integrados y objetos conectados en red (Internet de las cosas). La transmisión y el intercambio de datos y el control se producen en tiempo real a través de una estructura del tipo Internet.
Pueden controlarse y leerse sin contacto directo y tomar sus propias decisiones basándose en la inteligencia asignada. Los sistemas ciberfísicos se caracterizan por un alto grado de complejidad y son fruto de la conexión de sistemas integrados en redes de comunicación por cable o inalámbricas.

Modelo de arquitectura de referencia (RAMI)
Antiguamente, la automatización se caracterizaba por una estructura orientada en el hardware (pirámide de automatización). Hoy día se considera una estructura anticuada porque la automatización no es solo el cableado de dispositivos físicos sino también la conexión entre nubes y datos. Además, durante el proceso es posible acceder no solo a datos de producción, sino también a datos del control desde el exterior. Por esta razón se creó el modelo de arquitectura de referencia (RAMI) como pirámide de automatización modernizada. ZVEI ha desarrollado las ideas y los conceptos del sector de la automatización en colaboración con los organismos VDI/VDE-GMA, DKE y los partners Bitkom y VDMA de la plataforma de asociaciones de Industrie 4.0.[10] El modelo conjuga por primera vez los elementos esenciales de Industrie 4.0 en un modelo de capas tridimensional.[11] Sobre la base de esta estructura es posible clasificar y desarrollar sistemáticamente Industrie 4.0. El modelo define asimismo

[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

estándares para Industrie 4.0. La estandarización es necesaria para garantizar la comunicación entre componentes de diferentes empresas en el entorno de Industrie 4.0.

Estamos representados internacionalmente. Para más información,
visite nuestra Homepage www.pilz.com o póngase en contacto con nuestra sede central.

Casa matriz: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Alemania
Teléfono: +49 711 3409-0, Fax: +49 711 3409-133, Correo-e: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY