



Industrie 4.0 – sécurité et intelligence

PILZ
THE SPIRIT OF SAFETY

Livre blanc

Exclusion de la garantie

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 se reserva todos los derechos sobre esta publicación. Nos reservamos el derecho de modificaciones técnicas. Pueden realizarse copias para uso interno del usuario. Las denominaciones de productos, mercancías y tecnologías son marcas registradas de las empresas correspondientes.

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

© 2016 by Pilz GmbH & Co. KG, Ostfildern
2.^a edición

Sommaire

1. À propos de l'Industrie 4.0	4
1.1. Histoire et arrière-plan – de la machine à vapeur à l'usine intelligente	4
1.2. L'usine intelligente – Smart Factory.....	5
1.2.1. Smart Factory ^{KL}	5
1.2.2. L'installation de démonstration Smart Factory de Pilz.....	6
1.3. Sécurité et sûreté	7
1.4. Machine modulaire et décentralisation	8
2. L'Industrie 4.0 et Pilz.....	9
2.1. La contribution de Pilz.....	9
2.2. L'Industrie 4.0 au niveau de la production chez Pilz.....	9
2.2.1. La technologie de l'information dans la production en réseau	10
2.2.2. « Groupe de réflexion Pilz 4.0 ».....	10
2.3. Champs d'action de l'Industrie 4.0.....	10
3. Champ d'action – sécurité & sûreté.....	11
3.1. Sécurité	12
3.1.1. Sécurité – de la sécurité statique à la sécurité dynamique.....	12
3.1.2. Safety 4.0 – des structures monolithiques aux solutions modulaires	13
3.1.3. Certification modulaire	13
3.2. Sûreté.....	14
3.2.1. Approches proposées dans le domaine de la sûreté.....	14
3.2.2. Solutions d'automatismes	15
3.3. Interaction entre la sécurité et la sûreté.....	16
4. Champ d'action de l'approche modulaire	16
4.1. Systèmes avec intelligence répartie – système d'automatismes PSS 4000	16
4.2. Logiciel d'ingénierie PAS4000	17
4.3. Visualisation PASvisu	18
Glossaire	19

1. À propos de l'Industrie 4.0

L'Industrie 4.0 est plus qu'une vision du futur. La mise en réseau intelligente est une grande opportunité pour l'industrie. Grâce à une production flexible, vous obtenez une utilisation optimale de vos installations. Des produits personnalisés peuvent être fabriqués dans les conditions de la production de masse, ce qui augmente la productivité de l'installation. Toutefois, de nombreuses entreprises hésitent encore à recourir à l'Industrie 4.0 dans leur propre production. Selon l'étude « Industry 4.0 – How to navigate digitization of the manufacturing sector, 2015 »¹ (Comment gérer la numérisation du secteur manufacturier) de l'institut McKinsey, seules six entreprises en Allemagne sur dix se sentent préparées pour l'Industrie 4.0, bien que 91 % d'entre elles considèrent la numérisation de la production industrielle comme une opportunité. Nous souhaitons aller à contre-courant de cette tendance et offrir aux entreprises dans le monde entier des solutions et des produits pour l'Industrie 4.0. En effet, la question de l'Industrie 4.0 attire de plus en plus l'attention au niveau international : il est particulièrement nécessaire, en raison des progrès de la mondialisation, de mettre en place les conditions permettant la mise en réseau par la numérisation des procédés de fabrication tout au long de la chaîne de création de valeur.

1.1. Histoire et arrière-plan – de la machine à vapeur à l'usine intelligente

La première révolution industrielle était constituée de la mécanisation des processus avec la force de l'eau et de la vapeur et elle a été suivie de la deuxième révolution industrielle : la fabrication de masse utilisant des lignes de montage et l'énergie électrique. La révolution numérique, également connue sous le nom « Industrie 3.0 » a alors suivi. Le travail sur ordinateur s'est répandu et le premier API programmable a vu le jour. La désignation « Industrie 4.0 » correspond à la quatrième révolution industrielle qui permet les systèmes cyberphysiques (SCP), l'« Internet des objets » et l'usine intelligente. Pour Pilz, l'Industrie 4.0 s'apparente cependant plus à une évolution, car sans la disposition de tous les acteurs concernés au changement, l'Industrie 4.0 ne pourra pas être mise en œuvre.

Le terme Industrie 4.0 a été évoqué pour la première fois dans la sphère publique en 2011 lors du Salon de Hanovre. En octobre 2012, le groupe d'études Industrie 4.0 du groupe de promoteurs de la communication de l'Organisme allemand pour la Recherche a transmis au gouvernement allemand des recommandations pour la mise en œuvre. Le groupe d'études Industrie 4.0 a remis en avril 2013 son rapport final à des représentants du gouvernement fédéral à l'occasion du Salon de Hanovre. Simultanément, la plate-forme Industrie 4.0, créée par les trois associations industrielles Bitkom², VDMA³ et ZVEI⁴, a commencé son travail. Elle aura pour objectif de coordonner à l'avenir les activités dans ce domaine. Depuis le début, Pilz accompagne ces activités et soutient des projets avec sa longue expérience dans les techniques d'automatismes.

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

² Bitkom (Digitalverband Deutschlands / association allemande pour les technologies de l'information, les télécommunications et les nouveaux médias), <https://www.bitkom.org/EN/index-EN.html>

³ VDMA (Verband Deutscher Maschinen- und Anlagenbau, fédération allemande de la construction mécanique et de l'ingénierie), <http://www.vdma.org/ueber-uns>

⁴ ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e. V. – Fédération de l'industrie électrotechnique et électronique), <http://www.zvei.org/en/Pages/default.aspx>

1.2. L'usine intelligente – Smart Factory

Smart Factory est l'usine intelligente du futur. Le terme a été empreint par la recherche dans la technique de fabrication. L'usine intelligente est l'objectif de la stratégie haute technologie du gouvernement fédéral allemand, dans le cadre du projet Industrie 4.0.⁵ L'usine intelligente doit comprendre un environnement de production dans lequel les installations de fabrication et les systèmes logistiques s'organisent et s'optimisent de plus en plus par eux-mêmes. Les produits créés dans l'usine intelligente savent à tout moment où ils sont, connaissent leur histoire, leur état actuel et les étapes de production encore nécessaires pour devenir des produits finis. Mais comment y parvenir ?

Des systèmes cyberphysiques⁶ qui communiquent ensemble via l'Internet des objets⁷ en sont la base technique. Une partie de ce scénario d'avenir est la communication entre le produit et l'usine de fabrication : le produit apporte ses informations de fabrication sous une forme lisible, par exemple sur une puce RFID. À l'aide de ces données, le trajet du produit est guidé à travers l'usine de fabrication et les différentes étapes de fabrication. Des travaux sont effectués dans les établissements d'enseignement supérieur et dans les instituts de recherche sur le thème de l'usine intelligente dans le cadre d'usines modèles.

1.2.1. Smart Factory^{KL}

En tant que centre de compétence leader et plate-forme de recherche et de démonstration indépendante de tout fabricant, SmartFactory^{KL} représente le pionnier de l'usine intelligente du futur. On y développe des systèmes de fabrication innovants dans lesquels la vision d'Industrie 4.0 devient dès aujourd'hui une réalité.⁸ L'objectif est de travailler dans un réseau, aux côtés de partenaires renommés de l'industrie et de la recherche, sur de nouveaux concepts et de nouvelles normes et solutions qui constituent la base pour des techniques d'automatismes très flexibles.

En tant que membre à part entière, Pilz contribue entièrement à cet objectif de l'initiative. Pilz poursuit les résultats du travail commun sur la plate-forme de développement et les utilise pour ses propres produits.

SmartFactory^{KL} dispose dès aujourd'hui de la première installation Industrie 4.0 au monde indépendante de tout fabricant.⁹ La sécurité et la modularisation y constituent des thèmes importants. D'une part, grâce à son expérience dans le domaine de la sécurité des machines, Pilz s'engage en faveur d'une standardisation et d'une procédure commune sur le thème de la sécurité, avec ses deux facettes, la sécurité (sécurité des machines) et la sûreté (sécurité informatique). D'autre part, Pilz s'investit dans le thème de la modularisation. L'architecture des installations selon l'approche mécatronique permet la modularisation complète sous forme d'éléments de machines. Les fonctions peuvent être standardisées et réutilisées dans différents modules. Ce thème a pour principe fondamental les systèmes d'automatismes tels que le PSS 4000 de Pilz qui est en mesure de répartir les fonctions de commande. Dans l'usine intelligente, il est possible de mettre à l'épreuve de tels concepts d'automatismes. Depuis plusieurs années, SmartFactory^{KL} expose une installation de production modulaire, indépendante de tout fabricant, dans laquelle plusieurs modules de différentes marques, avec

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

⁶ Définition dans le glossaire à partir de la page 20.

⁷ Définition dans le glossaire à partir de la page 20.

⁸ <http://www.smartfactory.de/>

⁹ <http://www.smartfactory.de/>

des architectures de commande différentes, fonctionnent parfaitement ensemble. Pilz complète cette installation de démonstration de Smart Factory^{KL} avec un module de stockage intelligent et automatisé.



Illustration 1 : SmartFactory^{KL} sur le Salon de Hanovre 2015

1.2.2. L'installation de démonstration Smart Factory de Pilz

L'installation de démonstration Smart Factory nous permet de montrer comment des produits personnalisés peuvent être fabriqués rapidement, en toute flexibilité et à moindres coûts. La ligne de fabrication modulaire concrétise la communication des systèmes d'automatismes répartis en interaction avec les actionneurs et les capteurs. Le système d'automatismes PSS 4000, compatible avec l'Industrie 4.0, coordonne le fonctionnement de tous les composants mis en réseau – pour la sécurité et le standard, de l'ingénierie à la visualisation. Notre ligne de fabrication intelligente produit des porte-cartes de visite et des stylos à bille personnalisés. Dans ce cadre, il est important que les déroulements de la production soient transparents. Avec nos solutions, il est possible de représenter de manière simple les machines et installations complexes avec des fonctions compliquées, telles qu'elles apparaissent dans l'Industrie 4.0 dans des systèmes numériques mis en réseau.

L'installation de démonstration est composée de trois modules de fonction différents :

- ▶ un stockage pour les porte-pièces
- ▶ un robot avec magasin de pièces / une station de transfert pour le produit
- ▶ une station laser

Sur un terminal client, les données du client (contact, adresse, ...) sont saisies via un PC. Par ailleurs, le client choisit à ce moment-là s'il souhaite obtenir un stylo à bille personnalisé avec son nom ou un porte-cartes de visite personnalisé avec son nom et un code QR contenant ses coordonnées.

Les données saisies sont enregistrées de manière numérique sur une puce RFID qui se trouve sur le porte-pièce. Cela garantit la disponibilité des informations dans chaque module. Les informations nécessaires sont lues sur les différents modules depuis la puce et les opérations de travail nécessaires sont exécutées. Après la fabrication, le contenu de la puce RFID est effacé lors de la sortie du produit. La puce est alors disponible pour la prochaine inscription avec le paquet de données suivant. Après ce processus de suppression, le porte-pièce avec la puce RFID est soit rangé si aucun autre paquet de données n'est prévu, soit renvoyé dans le circuit de production.



Illustration 2 : L'installation de démonstration Smart Factory de Pilz au Salon de Hanovre 2016

1.3. Sécurité et sûreté

Avec l'évolution des systèmes d'automatismes liés à l'Industrie 4.0, les entreprises doivent désormais relever de nouveaux défis sur la sécurité. Le monde des automatismes fusionne avec l'univers informatique. Les conceptions de la sécurité sont très différentes : les termes internationaux « safety » – qui désigne la sécurité des machines – et « security » – qui caractérise la sûreté informatique et la protection des données – permettent tout d'abord d'opérer une première différenciation fondamentale.

La sécurité exige que des risques résiduels en provenance d'une machine ou d'une installation ne dépassent pas des valeurs acceptables. Cela inclut à la fois les dangers liés à l'environnement de l'installation (exemple : dommages causés à l'environnement) et les dangers au sein de l'installation (exemple : les personnes qui se trouvent dans l'installation). La sûreté concerne la protection d'une machine ou d'une installation contre un accès non autorisé de l'extérieur ainsi que la protection des données sensibles contre une falsification, une perte ou un accès non autorisé au niveau interne. Cela inclut aussi bien les attaques explicites que les incidents involontaires liés à la sûreté.

La protection complète des données de commande importantes pour la production et la sûreté lors du transfert, du traitement et de l'enregistrement doit considérer les domaines suivants de la sûreté :

- ▶ sécurité physique et disponibilité des systèmes informatiques
- ▶ sécurité du réseau
- ▶ sécurité d'utilisation du logiciel
- ▶ protection des données
- ▶ sécurité de fonctionnement

1.4. Machine modulaire et décentralisation

Depuis de nombreuses années, la construction modulaire des machines et installations est la clé d'une augmentation de la flexibilité dans la production. Une installation complète est composée de plusieurs modules de machines autonomes. Un module reproduit dans ce cadre une ou plusieurs étapes de production standardisées et peut être combiné avec d'autres modules pour former un procédé complet. Pour cela, tous les modules sont raccordés à un réseau dorsal qui alimente les modules aussi bien en énergie (courant triphasé 400 VAC, air comprimé, ...) qu'avec les données de processus et de commande. Si un procédé de fabrication doit être modifié ou si la productivité augmente, on peut remplacer un ou plusieurs modules ou ajouter des modules identiques.

Sur la voie vers l'avenir des automatismes, la modularisation et la décentralisation sont donc deux des principaux facteurs du succès. Il est indispensable que les systèmes d'automatismes soient en mesure de commander de manière conviviale l'intelligence répartie dans les modules de la machine. Toutes les machines et installations peuvent ainsi être découpées en unités dont le fonctionnement est transparent et indépendant.

L'architecture modulaire des machines et installations suit l'approche mécatronique. La philosophie de cette approche est de réunir globalement toutes les disciplines impliquées dans le process de création d'une machine : la mécanique, l'électricité et les techniques d'automatismes. L'interaction entre divers composants individuels pour les automatismes et les logiciels correspondants est définie de manière universelle pour constituer une solution d'automatismes. Cette universalité s'étend sur quatre niveaux de la pyramide des automatismes (gestion, fonctionnement, commande et terrain). L'approche mécatronique requiert la possibilité de « migration » des fonctions de commande dans les différents modules mécatroniques. C'est ici que les systèmes actuels se heurtent souvent à leurs propres limites. Les modules de fonction peuvent certes être créés, mais s'ils doivent être exécutés par de grands systèmes de commande centralisés, la mise en service des différents modules devient rapidement coûteuse du fait de la complexité. De même, des coûts supplémentaires apparaissent en cas de modifications ultérieures dans la configuration et la programmation des modules de fonctions individuels. À l'aide de systèmes créés de manière décentralisée, la mise en service des modules est simplifiée. De même, la création de la configuration est très conviviale car on peut utiliser des programmes et sous-fonctions de commande identiques pour différents modules.

Les automatismes du futur requièrent des solutions qui, d'une part, sont en mesure de répartir l'intelligence de commande et, d'autre part, garantissent pour l'utilisateur la facilité d'utilisation lors de la mise en réseau de plusieurs systèmes de commande. Une telle solution est proposée par Pilz avec son système d'automatismes PSS 4000.

2. L'Industrie 4.0 et Pilz

2.1. La contribution de Pilz

Susanne Kunschert, associée gérante de Pilz, a été recommandée en 2010 par le gouvernement allemand pour représenter personnellement les PME auprès de l'Organisme Officiel pour la Recherche. Il s'agissait de la commission consultative centrale du gouvernement en faveur de la politique d'innovation qui visait la mise en œuvre et la poursuite du développement de la stratégie de la haute technologie. Il a été demandé à Susanne Kunschert de présenter au sein de cet organisme les perspectives des PME innovantes.

En tant que membre du groupe de promoteurs de la sécurité, l'associée gérante de Pilz se consacre à la protection efficace des réseaux de communication et au développement de l'Allemagne comme marché leader des technologies de sécurité. Pour répondre à ce besoin identifié, l'Organisme Officiel pour la Recherche élaborait des projets d'avenir dans des groupes de travail. L'un des plus importants est l'« Industrie 4.0 ».

Pilz a soutenu activement dans différents projets le travail réalisé par l'agence nouvellement créée « Industrie 4.0 » avec le parrainage des associations Bitkom, ZVEI et VDMA et a participé à l'élaboration des recommandations. Ces dernières ont été transmises au gouvernement au Salon de Hanovre 2013.

Pilz est actuellement active dans les commissions et initiatives suivantes :

- ▶ Collaboration au sein de la plate-forme Industrie 4.0
- ▶ Collaboration dans le groupe de direction de l'Industrie 4.0 dans la ZVEI
- ▶ Collaboration dans le réseau national allemand Mechatronik BW
- ▶ Membre du Comité exécutif Allianz Industrie 4.0 Bade-Wurtemberg
- ▶ Membre de la plate-forme de démonstration et de recherche Smart Factory^{KL} indépendante de tout fabricant
- ▶ Membre de ARENA2036 – l'avenir de la construction automobile

2.2. L'Industrie 4.0 au niveau de la production chez Pilz

Au-delà de son implication au sein de l'Organisme allemand pour la Recherche et de la plate-forme de recherches SmartFactory^{KL}, Pilz voit en l'Industrie 4.0 non seulement un projet d'avenir, mais aussi un concept intégré dans son propre procédé de fabrication.

Avec la mise en réseau croissante des machines et des infrastructures dans la production à l'aide de la technologie de l'information, Pilz répond à ses exigences en tant que leader technologique dans ses propres lignes de production. Au sens de l'Industrie 4.0, l'infrastructure nécessaire a été créée pour obtenir une production intelligente, et des éléments de l'Industrie 4.0 ont été mis en œuvre de manière précoce. On utilise déjà un transport intelligent des pièces à usiner qui a été développé dans les propres locaux de Pilz. Ce moyen de transport accélère et simplifie par exemple le garnissage des cartes imprimées et les opérations de soudage. Les supports de pièces à usiner trouvent leur chemin de manière autonome à partir d'une puce RFID intégrée, du soudage à la vague à l'unité de montage.

Pilz poursuivra la mise en œuvre de la production intelligente pas à pas : pour la commande de la production, les données sur les machines seront collectées et traitées de façon ciblée. Grâce à l'analyse, des informations importantes seront obtenues à partir de modifications des états et de

l'usure des machines. Ainsi, la maintenance peut être effectuée de manière préventive. La « maintenance préventive » évite des dysfonctionnements et des temps d'arrêt. Un enregistrement des documents de travail les plus récents dans un cloud Pilz sera également mis en place. L'ensemble des données et des documents sera alors disponible en temps réel et toujours actualisé et pourra être consulté de n'importe où, à partir de terminaux mobiles dans la production.

2.2.1. La technologie de l'information dans la production en réseau

Pilz est conscient des défis à relever en termes de sûreté des technologies de l'information grâce à sa production entièrement mise en réseau. C'est pourquoi Pilz investit dans une infrastructure complète de sûreté en vue de la surveillance de l'ensemble du flux de données. Cela comprend aussi un centre de données autonome qui satisfait aux standards les plus évolués. Une analyse permanente et un stockage de tous les paramètres de fabrication importants permettent une détection précoce des anomalies. Par ailleurs, différents systèmes de pare-feu ont été installés pour chaque domaine de production permettant de définir le niveau de sûreté nécessaire par zone. Les défaillances et les risques de sécurité sont réduits et le savoir-faire est protégé.

2.2.2. « Groupe de réflexion Pilz 4.0 »

Le travail en partenariat si important pour l'Industrie 4.0, en particulier entre les services Technologies de l'information et Techniques de fabrication est également la plus grande priorité chez Pilz. Au sein d'un « groupe de réflexion Pilz 4.0 » spécialement mis en place, les collaborateurs issus de la production et des technologies de l'information unissent leurs forces et reçoivent les ressources nécessaires afin de planifier et de mettre en œuvre des projets communs sur le thème de l'Industrie 4.0.

2.3. Champs d'action de l'Industrie 4.0

L'une des bases de l'acceptation durable sur le marché est la création de mécanismes normalisés pour la communication entre les machines et au sein de la machine. Si les exigences imposées par les deux mondes (celui des automatismes et l'univers informatique) sont prises en compte, on peut alors obtenir des solutions pratiques et acceptées par l'utilisateur.

En résumé, cela signifie que Pilz s'engage activement en faveur d'architectures de commande modernes dans l'environnement de l'Industrie 4.0.

Les sujets suivants constituent nos points forts :

- ▶ **Sécurité & sûreté :**
 - Les deux concepts possèdent des parallèles évidentes dans la standardisation et la procédure à suivre dans le processus d'ingénierie. Forts de notre expérience dans les domaines de la sécurité des machines et de l'automatisation, nous entendons faire avancer ce travail important.
 - Tous les appareils et composants d'automatismes requis pour la fonction de commande reçoivent un accès direct à internet pour l'échange de données du processus et de données de paramétrage pour le diagnostic et la maintenance (à distance). Par conséquent, on assiste pour tous les appareils d'automatismes concernés à une augmentation des exigences en matière de sûreté et à une représentation homogène du diagnostic.

- Approche modulaire :
 - Nos fonctions de commande modernes sont conçues selon une distributivité et une orientation sur les objets – les capteurs et les actionneurs deviennent intelligents. Nous illustrons ainsi la tendance vers des objets de commande mécatroniques (composants d'automatismes) dans nos produits et les logiciels d'ingénierie correspondants.

3. Champ d'action – sécurité & sûreté

La sécurité et la sûreté sont indispensables pour le fonctionnement des installations de l'Industrie 4.0 qui, contrairement aux installations de production traditionnelles, disposent d'interfaces avec leur environnement.

À l'avenir, les installations de l'Industrie 4.0 pourront se reconfigurer et s'optimiser de manière autonome, ce qui requiert une nouvelle analyse de la sécurité (sécurité & sûreté) pendant la durée de fonctionnement – c'est-à-dire en cours de fonctionnement par l'installation elle-même. De plus, il faut s'assurer qu'aucun risque d'importance inacceptable au sens de la sécurité ne résulte des lacunes issues de la sûreté.

Finalement, cette thématique doit soutenir l'instauration d'un climat de confiance pour les petites et moyennes entreprises, base décisive pour la production dans des réseaux ad hoc. La transparence, la participation et la communication ouverte sont essentielles.

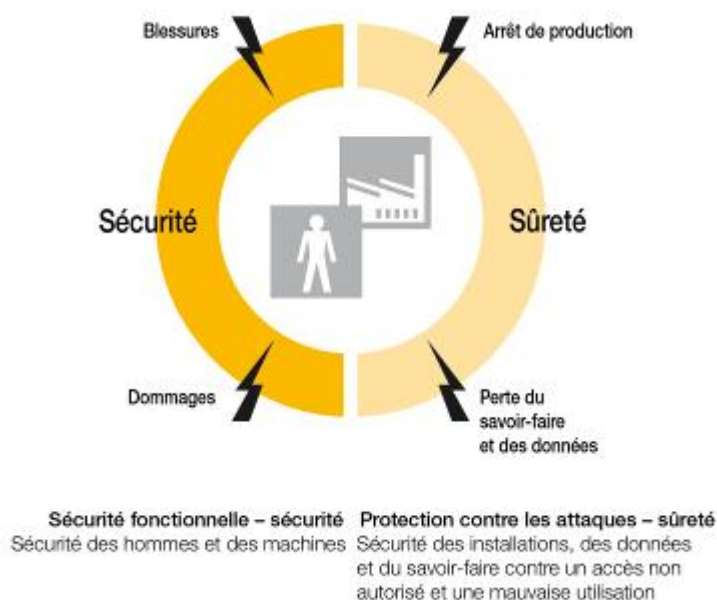


Illustration 3 : Interaction entre la sécurité et la sûreté

3.1. Sécurité

Le domaine de la sécurité se caractérise déjà par une grande sécurité des investissements et une sécurité juridique. Cela dépend aussi de l'organisation liée aux normes et standards. Toutes les procédures pour l'analyse et l'évaluation du risque ainsi que pour la réalisation de l'analyse sont ainsi clairement définies à l'aide des classements internationaux standardisés en niveaux d'intégrité de sécurité (SIL) et une comparaison légalement valable des solutions est possible.

3.1.1. Sécurité – de la sécurité statique à la sécurité dynamique

Le terme « sécurité » désigne la sécurité fonctionnelle des machines ou, en d'autres termes, la protection de l'homme et de l'environnement contre les menaces pouvant provenir des machines. La sécurité exige que des risques résiduels en provenance d'une machine ou d'une installation ne dépassent pas des valeurs acceptables. Cela inclut à la fois les dangers liés à l'environnement de l'installation (exemple : dommages causés à l'environnement) et les dangers au sein de la machine ou de l'installation (exemple : les personnes qui se trouvent dans l'installation).

Si nécessaire, couper immédiatement l'alimentation en énergie et arrêter brusquement la machine représente une possibilité. De manière classique, cette solution est réalisée par un câblage de sécurité spécial et par des composants tels que des relais de sécurité. Comme cette approche est très liée au matériel et donc statique, elle est peu adaptée aux procédés de fabrication intelligents dans lesquels l'organisation de l'installation doit être régulièrement modifiée. Une coupure brusque s'accompagne généralement d'inconvénients supplémentaires, que ce soit une perte de productivité, des temps d'arrêt plus longs suite à des procédures plus complexes pour la remise en service ou une limitation du concept de commande et de maintenance de la machine.

Les concepts de la sécurité dynamique, fondés sur une considération globale des processus d'automatismes changeants et des exigences en matière de sécurité fonctionnelle, offrent une alternative. Cela implique une évolution de la conception de la sécurité en tant que telle ; de moins en moins considérée comme une propriété matérielle, elle est davantage perçue comme une fonction globale des appareils. Cette approche, déjà développée avant l'ère de l'Industrie 4.0, permet de contrôler les processus en toute sécurité, sans qu'il soit nécessaire de les couper immédiatement à chaque fois qu'une erreur apparaît. L'approche dynamique ne peut néanmoins être mise en œuvre efficacement que si la sécurité fonctionnelle est prise en compte dès le début de la planification dans les projets d'automatismes. Autrement, il faut éventuellement modifier ultérieurement le déroulement de certaines étapes de fabrication ou d'un processus complet, ce qui empêche la création de solutions optimales et entraîne des coûts importants.

Tandis que souvent seuls des signaux binaires sont transférés dans le cadre de la sécurité statique, afin par exemple de couper le mouvement de la machine après l'ouverture d'un protecteur mobile, des informations plus complètes sont requises pour la sécurité dynamique. En effet, cette procédure implique différents modes de fonctionnement de sécurité qui permettent par exemple le « fonctionnement avec un protecteur mobile ouvert ». Les informations sur les modes de fonctionnement de sécurité doivent cependant être présentes dans tous les composants concernés. En ce qui concerne l'exemple du protecteur mobile, l'ouverture d'un tel protecteur n'entraîne plus automatiquement – selon le niveau d'autorisation de l'utilisateur – la coupure immédiate de la machine, mais les mécanismes de sécurité

surveillent plutôt le respect d'une vitesse limite de rotation réduite ou alors ils génèrent et surveillent les consignes de sécurité de l'axe de rotation.

3.1.2. Safety 4.0 – des structures monolithiques aux solutions modulaires

Dans le cadre de l'usine intelligente, les installations avec une architecture modulaire doivent pouvoir être reconfigurées rapidement et en toute flexibilité ou être modifiées en tant qu'entité. La validation d'une solution de sécurité doit alors pouvoir gérer cette flexibilité (tardive). Les configurations qui n'ont pas été prises en compte dans le cadre du marquage CE ne peuvent pas non plus être établies simplement par l'opérateur. Le principe de transférabilité ne s'applique pas : $CE_{\text{module1}} + CE_{\text{module2}} = CE_{\text{machine complète}}$!

L'avantage fonctionnel des concepts modulaires d'une machine est évident. Vous gagnez en flexibilité dans le procédé de fabrication tout en augmentant la possibilité de standardisation au niveau de la fonction. Le plus haut niveau de possibilité de standardisation est atteint lorsque les limites de division des différents modules peuvent être organisées à l'identique – qu'il s'agisse d'un module de fonction mécanique, électrique, de commande ou de visualisation. L'approche mécatronique a pour objectif une telle formation standardisée des objets d'automatismes.

Les avantages de la modularisation sont souvent anéantis par des solutions d'amélioration rigides, avec éventuellement un câblage dur. De plus, les systèmes de commande de sécurité électroniques possèdent presque toujours une reproduction de la sécurité basée sur le matériel, et ce sous la forme de circuits de sécurité fixes, même si ceux-ci sont quasiment proposés dans une logique de raccordement librement configurable.

L'élément de base des architectures de commande modernes est de plus en plus le renoncement aux règlements liés au système. L'utilisateur doit pouvoir optimiser librement en fonction de ses niveaux de modularisation. Si la barrière des différentes approches est également supprimée pour les fonctions d'automatisation et de sécurité des machines, l'utilisateur accède à des niveaux de liberté essentiels.

Le PSS 4000 est un système d'automatismes qui contient les aspects de modularisation et de flexibilisation comme deux de ses fonctions de base. Pour la première fois, toutes les variables du process (même celles des fonctions de sécurité) peuvent être entièrement gérées dans le système de manière symbolique et sans rapport avec le matériel. Cela est illustré par le fait que toutes les variables du process sont disponibles à travers le système et, grâce à l'architecture multimaître, leur disponibilité est automatique pour tous les systèmes de commande du système d'automatismes réparti.

3.1.3. Certification modulaire

Plus les machines sont conçues sous forme de modules, plus les composants doivent être reliés de manière décentralisée. La modularité des machines ou de parties de machines présente plusieurs avantages considérables : les modules de machines peuvent être à nouveau combinés et remplacés, on peut étendre les machines ou, par exemple, exécuter un changement d'outils pendant la production. Les machines sont plus flexibles. Le même nombre de machines permet à l'exploitant de fabriquer un plus grand nombre de produits. Les concepts de commande sont de plus en plus décentralisés à condition que cela représente un avantage pour l'exploitant. Une place importante est accordée à la question de la sécurité et de la sûreté. Dans ce cadre, le mot clé est la certification modulaire des différents modules de l'installation. Aujourd'hui, les machines sont homologuées par les organismes en tant qu'entité complète. Une petite modification, par exemple le remplacement de deux modules, requiert une nouvelle

homologation. On discute de différentes solutions à ce sujet, mais il n'existe actuellement pas de procédure homogène. L'une des approches consiste à considérer que la machine est sûre si ses différents modules le sont. Il s'agit de sensibiliser les entreprises et les décideurs politiques par le biais des associations, car sans un cadre légal adéquat, aucune avancée n'est envisageable sur la question.

3.2. Sûreté

Pour la question de la sûreté, le défi est que, contrairement à la sécurité fonctionnelle, les mécanismes de sûreté doivent toujours être adaptés au danger. Par exemple par une mise à jour traitée au cas par cas, car un virus, cheval de Troie, etc. se développe en permanence et les failles dans la sûreté peuvent finalement gêner la production et tous ses éléments fonctionnels.

Pour pouvoir réagir de manière flexible à un scénario de menace, il faut également encourager la protection des applications de sécurité par une stratégie de sûreté complète, composée de différentes couches : les composants d'automatismes sont au cœur de cette approche. Vient ensuite le réseau via lequel ces composants peuvent communiquer avec d'autres ou avec un système ERP (Enterprise Resource Planning). La couche supérieure est constituée de l'usine qui est protégée à l'extérieur par un concept de pare-feu spécial, appelé zone démilitarisée.

Les exigences que le monde informatique et le monde des automatismes imposent en termes de sûreté sont très différentes. Tandis que dans un environnement de bureau, la confidentialité des informations est une priorité absolue, la disponibilité des données occupe une place de premier plan dans le domaine de la production, car elles constituent une condition essentielle pour un procédé de fabrication sans incident. Une norme internationale (CEI 62443) est actuellement en cours de développement et vise à uniformiser les deux mondes de la sûreté. Comme les dangers du cybermonde sont dynamiques, la sûreté et la sécurité resteront encore à l'avenir deux questions séparées qui sont cependant étroitement liées.

Il est pour cela important de développer des méthodes et des outils à l'aide desquels la conséquence des failles de sûreté sur des risques résiduels supplémentaires peut être analysée au sens de la sécurité. Dans la mesure du possible, ces méthodes et outils doivent être intégrés dès la phase de développement des produits de systèmes cyberphysiques (SCP) : la sûreté par la conception.

Les aspects à prendre en compte sont :

- ▶ la protection des interfaces (API) vers l'extérieur (internet, réseau d'entreprise, ...)
- ▶ la protection des systèmes de communication dans la machine et l'installation selon les types d'utilisation (utilisation constante, maintenance à distance, diagnostic à distance, liaisons ad hoc)
- ▶ la sûreté en tant que « cible mobile », il n'existe pas de solution de sécurité constante

3.2.1. Approches proposées dans le domaine de la sûreté

Comment protéger les applications de sécurité contre les menaces du monde virtuel ? Voici une réponse rapide à la question : uniquement par la combinaison de différentes mesures et directives de sûreté qui sont strictement respectées par toutes les personnes concernées.

En ce qui concerne la mise en réseau, la clé de la réussite est la « défense en profondeur ». Un élément central, également appliqué depuis le Moyen-Âge dans la construction des châteaux,

est le modèle de sûreté des « zones et passages » qui est déjà défini dans la norme CEI 62443. Celui-ci prévoit de répartir un réseau d'automatismes dans différentes zones dans lesquelles des appareils peuvent communiquer ensemble. L'échange de données avec des appareils dans d'autres zones est uniquement possible via un passage unique qui est surveillé par un routeur sécurisé ou un pare-feu qui filtre le flux de données au moyen de règles fixes et bloque ainsi les accès non autorisés. Même si un assaillant parvenait à pénétrer dans une zone, seuls les appareils qui s'y trouvent seraient alors en danger et tous les autres seraient encore en sécurité.

3.2.2. Solutions d'automatismes

Pour la protection des solutions d'automatismes, la CEI 62443 (la série de normes pour la sécurité informatique dans les systèmes d'automatismes industriels) définit les sept « exigences fondamentales » pour la sécurité de ces systèmes d'automatismes :

- ▶ Identification and authentication control (IAC – identification et contrôle de l'authentification)
- ▶ Use control (UC – contrôle de l'utilisation)
- ▶ Data integrity (DI – intégrité des données)
- ▶ Data confidentiality (DC – confidentialité des données)
- ▶ Restricted data flow (RDF – flux de données restreint)
- ▶ Timely response to events (TRE – réponse rapide aux événements)
- ▶ Resource availability (RA – disponibilité des ressources)

Chaque exigence de base peut être répartie selon les éléments suivants :

- ▶ Identification & authentification
- ▶ Identification d'utilisateur humain
- ▶ Authentification multifacteur pour réseaux non approuvés
- ▶ Processus logiciel et identification d'appareil
- ▶ Identification unique et authentification
- ▶ Sécurité de l'authentification strictement basée sur mot de passe
- ▶ Génération de mot de passe et restrictions de la durée de vie pour les utilisateurs humains

Chacun des éléments possède quatre niveaux de sûreté qui peuvent être atteints en fonction des coûts de développement des solutions d'automatismes. On a besoin ici de l'intégrateur de systèmes et de l'exploitant de l'installation qui définissent les niveaux de protection correspondants pour l'application et le modèle de zone dérivé. Le niveau de protection le plus élevé, à savoir le « niveau 4 » ne sera certainement pas toujours applicable car il peut impliquer des frais très élevés.

Cependant, la meilleure mesure technique de sûreté ne sert à rien si elle n'est pas mise en pratique en raison du temps qu'elle implique ou souvent en raison de la non-compréhension ou de la méconnaissance, voire – pire – si elle est consciemment contournée. Des directives et mesures organisationnelles doivent accompagner les mesures techniques. À quoi servent les meilleurs réglages de pare-feu si le mot de passe par défaut, indiqué dans le manuel, n'est pas modifié ou si un lien peut être établi très facilement entre le mot de passe et l'appareil ? Le niveau de protection pour une partie de l'installation résulte de l'interaction entre les mesures techniques et organisationnelles.

3.3. Interaction entre la sécurité et la sûreté

Les solutions globales d'amélioration rendent l'interaction entre la sécurité et la sûreté nécessaire. Bien souvent, elles nécessitent une orientation spécifique vers des architectures systèmes en suivant les standards ouverts et en incluant les considérations des fabricants. Si on prend en compte l'aspect sécurité, il faut vérifier dans quelle mesure les thèmes liés à la sûreté influencent la sécurité fonctionnelle.

Des preuves d'identité claires et sécurisées pour les produits, les processus et les machines, y compris pour l'échange en toute sécurité des informations tout au long du procédé de fabrication, sont des thèmes fondamentaux.

Par ailleurs, des solutions conviviales sont demandées : la sûreté et la sécurité doivent devenir maîtrisables et s'orienter sur les besoins des utilisateurs. Du point de vue de l'entreprise, la sécurité est également un moteur d'innovation : elle englobe l'intégration de structures de coûts en rapport avec la productivité. La possibilité d'assurance du dommage et les méthodes de calculs nécessaires à ce sujet sont des éléments indispensables.

En ce qui concerne le facteur humain, on parle de « sûreté utilisable et confidentialité ». L'objectif est de réduire au maximum les efforts liés au temps et à la compréhension des mesures de sûreté nécessaires.

On trouve ici des similarités avec la sécurité fonctionnelle : la disponibilité ne doit pas être entravée par des mesures de sécurité. Les principes de sécurité peuvent être appliqués à l'identique dans le domaine de la sûreté. La sécurité requiert une approche globale.

4. Champ d'action de l'approche modulaire

Du point de vue des défis, seule une « pensée en modules » interdisciplinaire stricte peut mener au succès à moyen et à long terme. Les systèmes de commande qui doivent prendre en charge cette approche jouent un rôle central.

4.1. Systèmes avec intelligence répartie – système d'automatismes PSS 4000

Avec son système d'automatismes PSS 4000, Pilz suit avec conviction l'approche mécatronique. L'idée principale du PSS 4000 est la fusion du standard et de la sécurité. Les données de process ou de commande, les données failsafe et les informations de diagnostic sont échangées et synchronisées via le système de communication multimaître SafetyNET p. L'emplacement pour le traitement de la partie du programme correspondante est ainsi sans importance pour la fonction de commande. Au lieu d'une commande centralisée, l'utilisateur dispose d'un programme dont l'exécution est répartie dans une vue centralisée du projet. Tous les abonnés du réseau sont configurés, programmés et diagnostiqués via cette création de projets centralisée. Une fois cette création de projets terminée, les différentes parties du programme sont affectées aux appareils de commande individuels. Cela s'effectue au moyen de prescriptions claires de l'utilisateur pour le regroupement d'unités fonctionnelles. Un fonctionnement simple et uniforme est ainsi possible dans le projet complet. En plus de la formation de modules et de la possibilité de standardisation, d'autres avantages apparaissent sous la forme d'une réaction plus flexible aux erreurs, d'une disponibilité plus élevée ainsi

qu'une productivité plus élevée suite à des temps de réponse plus courts de l'ensemble du système.

Tandis que, dans un système d'automatismes classique, une seule commande centralisée surveille la machine ou l'installation et traite tous les signaux, le PSS 4000 permet une répartition cohérente des fonctions de commande. Dans les détails, le système d'automatismes PSS 4000 est constitué de composants matériels et logiciels ainsi que d'Ethernet en temps réel SafetyNET p et de différents éditeurs de programmes utilisables pour divers secteurs d'activités, avec leurs blocs fonctions axés sur les applications. Les systèmes de commande de différentes classes de performance font partie du matériel. Les données de process ou de commande, les données failsafe et les informations sur le diagnostic sont échangées et synchronisées via Ethernet. Cette fusion conséquente des fonctions de sécurité et standard réduit la complexité dans le domaine de la communication et entraîne encore une optimisation des coûts.

4.2. Logiciel d'ingénierie PAS4000

Le système d'automatismes PSS 4000 a pour objectif de simplifier la décentralisation des fonctions de commande tout en conservant une utilisation claire. La plate-forme logicielle PAS4000 joue à ce propos un rôle essentiel. Elle comprend différents éditeurs pour la programmation d'API et leur configuration ainsi que des blocs logiciels. Dans le PAS4000, les outils de création de projets, de programmation, de mise en service et d'exploitation sont étroitement adaptés les uns aux autres.

Le PAS4000 prend en charge le découpage d'une fonction de la machine / l'installation en modules de fonction toujours plus petits qui suivent de la même manière les limites de division des unités mécatroniques. La modularisation est un aspect essentiel : les éléments sont créés à partir des fonctions de base, les modules à partir des éléments, et les machines et installations à partir des modules – tout simplement par l'emboîtement hiérarchique des blocs. Les fonctions de base, les éléments et les modules forment la colonne vertébrale de la création logicielle et peuvent être réutilisés de manière optimale en tant que composants logiciels grâce à l'encapsulation et à l'orientation de l'objet.

Le PAS4000 fournit des bibliothèques logicielles qui contiennent les fonctions de base, les éléments et les modules les plus courants. Le choix de composants finis de la bibliothèque n'est en soi pas une nouveauté. La particularité du PAS4000 est que ces composants ont été dotés de propriétés appelées « Properties ». Elles permettent de paramétrer en toute simplicité les fonctions souhaitées. Cela se traduit en particulier par des avantages pour une standardisation de fonctions.



Illustration 4 : Les installations peuvent être découpées en unités dont le fonctionnement est transparent et indépendant.

4.3. Visualisation PASvisu

La visualisation et le programme de commande peuvent être divisés selon le même principe dans la plus petite unité. Une base de données commune des différents modules permet aux modules de communiquer ensemble. L'architecture homogène permet la réutilisation en toute simplicité des données de la création de projets.

Le logiciel de visualisation permet de créer et de configurer en toute simplicité des projets de visualisation à partir du PASvisu Builder.

Grâce à l'accès à toutes les données d'un projet d'automatismes, y compris à toutes les variables du process et aux espaces de domaines OPC, la saisie manuelle qui est sujette à des erreurs, ainsi que l'affectation des variables sont inutiles. Il est ainsi possible, par exemple, d'obtenir des informations telles que la somme de contrôle du projet ou la version du firmware de la tête de commande.

L'Industrie 4.0 prend en considération la « valeur des données », dans ce cas celle des données pour la création de projets. Une base de données commune permet la réduction des sources d'erreurs possibles par la prise en charge automatique des données « appropriées », le contrôle automatique de la cohérence garantit une réduction des temps d'ingénierie : la formation homogène des modules dans la commande et la visualisation facilite la réutilisation des éléments et des modules de la machine.

Glossaire

Smart Product

Le produit intelligent est pourvu directement ou via une ID d'informations importantes sur sa fabrication et peut ainsi commander lui-même son procédé de fabrication. En tant qu'objet intelligent, il constitue la base de l'Internet des objets.

Internet des objets

Dans l'Internet des objets (IdO), les « objets » ou éléments intelligents communiquent ensemble via un réseau numérique universel. Les ordinateurs disparaissent de plus en plus en tant qu'appareils individuels et sont remplacés par des « objets intelligents ». Ceux-ci sont reliés à internet afin de communiquer de manière autonome via internet et de réaliser ainsi différentes tâches pour leur propriétaire.

La technologie Radio Frequency Identification (RFID) et la technique de localisation intelligente qu'elle représente permet ainsi que des objets s'identifient maintenant eux-mêmes et se commandent dans une certaine mesure. À leur tour, les objets comportent des informations sur leur utilisation. Les produits communiquent ainsi eux-mêmes l'opération suivante à leur installation de flux matériel ou de fabrication. L'intervention des personnes n'est plus nécessaire.

Systèmes cyberphysiques (SCP)

Les éléments essentiels sont des dispositifs, machines et appareils mobiles et portables (notamment des robots), des systèmes intégrés et des objets en réseau (Internet des objets). Le transfert et l'échange de données ainsi que le contrôle et la commande s'effectuent via une infrastructure telle qu'internet en temps réel.

Sans contact direct, ils peuvent être commandés et lus et, à l'aide de l'intelligence qui leur est affectée, ils peuvent prendre eux-mêmes des décisions. Un système cyberphysique se distingue par son haut niveau de complexité. Les systèmes cyberphysiques naissent de la mise en réseau de systèmes intégrés par des réseaux de communication câblés ou sans fil.

Modèle d'architecture de référence (RAMI)

Les automatismes étaient auparavant marqués par une structure orientée sur le matériel (pyramide des automatismes). Aujourd'hui, cette structure est obsolète car les automatismes ne concernent plus seulement le câblage de matériels, mais également des liaisons entre des clouds et des données. Par ailleurs, le processus ne fournit pas seulement des données de production, mais il est également possible d'accéder aux données de la commande depuis l'extérieur. C'est pourquoi le modèle d'architecture de référence (RAMI) a été créé en tant que pyramide modernisée des automatismes. L'association ZVEI a développé les idées et concepts du secteur des automatismes aux côtés de VDI/VDE-GMA, DKE et des partenaires sur la plate-forme des associations Industrie 4.0, Bitkom et VDMA.¹⁰ Le modèle regroupe dans un premier temps les éléments essentiels de l'Industrie 4.0 dans un modèle à couches en trois dimensions.¹¹ Cette structure de base permet ainsi d'organiser systématiquement l'Industrie 4.0 et de la développer. Le modèle définit également des normes pour l'Industrie 4.0. Cette standardisation est nécessaire car différentes entreprises doivent pouvoir communiquer ensemble dans le cadre des composants de l'Industrie 4.0.

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

Nous sommes représentés à l'échelle internationale. Pour plus de renseignements,
consultez notre site Internet www.pilz.com ou prenez contact avec notre maison mère.

Maison mère : Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Allemagne
Téléphone : +49 711 3409-0, Télécopie : +49 711 3409-133, E-mail : info@pilz.com, Internet : www.pilz.com

PILZ
THE SPIRIT OF SAFETY