Industrie 4.0 – safe and smart

PILZ
THE SPIRIT OF SAFETY

White paper

Disclaimer

Our white paper has been compiled with great care. It contains information about our company and our products. All statements are made in accordance with the current status of technology and to the best of our knowledge and belief. While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, it should be noted that statements do not have the legal quality of assurances or assured properties. We are grateful for any feedback on the contents.

Copyright

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

Contents

1. About Industrie 4.0 4
1.1. History and background – from steam engine to Smart Factory 4
1.2. Smart Factory 4
1.2.1. Smart Factory^{KL} 5
1.2.2. The Pilz Smart Factory demonstrator 6
1.3. Safety & Security 7
1.4. Modular machinery and decentralisation 7

2. Industrie 4.0 and Pilz 9
2.1. Pilz's contribution 9
2.2. Industrie 4.0 in Pilz production 9
2.2.1. IT in integrated production 10
2.2.2. "Pilz Think Tank 4.0" 10
2.3. Action area – Industrie 4.0 10

3. Action area – safety & security 11
3.1. Safety 11
3.1.1. Safety – from static to dynamic safety 12
3.1.2. Safety 4.0 – from monolithic structures to modular solutions 12
3.1.3. Modular certification 13
3.2. Security 13
3.2.1. Solution approaches in the field of security 14
3.2.2. Automation solutions 14
3.3. Interaction between safety & security 15

4. Action area – modular approach 16
4.1. Distributed intelligent systems – automation system PSS 4000 16
4.2. Engineering tool PAS4000 16
4.3. PASvisu visualisation 17

Glossary 18

1. About Industrie 4.0

Industrie 4.0 is more than a vision of the future. Intelligent networking is a huge opportunity for industry. Flexible production can help to optimise the use of industrial plants. Customised products can be made on mass production terms, increasing the productivity of the plant. Nevertheless, many companies are still hesitant to embrace Industrie 4.0 for their own production operations. According to the McKinsey Institute study “Industry 4.0 – How to navigate digitization of the manufacturing sector, 2015”[1] only six out of ten companies in Germany feel they are ready for Industrie 4.0, even though 91 per cent perceive the digitisation of industrial production as an opportunity. We would like to change all that, and offer solutions and products for Industrie 4.0 to companies worldwide. Because the topic of Industrie 4.0 is coming increasingly sharply into focus in the international arena, too: the continuing process of globalisation in particular renders it necessary to prepare the way for integration through the digitisation of production processes along the entire value chain.

1.1. History and background – from steam engine to Smart Factory

The first industrial revolution involved mechanisation using water and steam power; this was followed by the second industrial revolution: mass production using conveyors and electrical energy. Then came the digital revolution, which is also referred to as “Industrie 3.0”. Computer-based working became the norm and the first programmable logic control system was introduced.
The term “Industrie 4.0” denotes the fourth industrial revolution, which permits cyber-physical systems, the Internet of Things and the Smart Factory. For Pilz, however, Industrie 4.0 is more of an evolution, because unless all the parties concerned are prepared to change it will not become a reality.

The term Industrie 4.0 was first made public at Hannover Messe 2011. In October 2012, the Industrie 4.0 working group from the Research Alliance’s communication promoters’ group presented implementation recommendations to the German government. The final report from the Industrie 4.0 working group was presented to leading representatives of the German government at Hannover Messe in April 2013. At the same time, the Industrie 4.0 platform set up by the three industry associations Bitkom[2], VDMA[3] and ZVEI[4] started work. Its objective is to coordinate activities in this future area. Pilz has been involved in these activities since the outset and draws on its many years of experience in automation technology to support projects.

1.2. Smart Factory

Smart Factory is the intelligent factory of the future. This is a term from research in the field of manufacturing engineering. The Smart Factory is the objective of the German government’s high-tech strategy within the Industrie 4.0 initiative[5]. It describes the vision of a production

[1] https://www.mckinsey.de/sites/mck_files/files/mck_industry_40_report.pdf
[2] Bitkom (Digitalverband Deutschlands / Germany's digital association) https://www.bitkom.org/EN/index-EN.html
[3] VDMA (Verband Deutscher Maschinen- und Anlagenbau, Mechanical Engineering Industry Association) http://www.vdma.org/ueber-uns
[4] ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e.V.,
Electrical and Electronic Manufacturers’ Association) http://www.zvei.org/en/Pages/default.aspx
[5] http://www.hightech-strategie.de/de/Industrie-4-0-59.php

environment in which manufacturing plants and logistics systems largely organise and optimise themselves. The products that are made in the Smart Factory always know where they are, as well as their history, their current status and the production steps that are still needed before they become the finished article. But how do they achieve that?
The technical basis is cyber-physical systems[6] that communicate with each other via the Internet of Things[7]. Communication between the product (e.g. workpiece) and manufacturing plant remains part of this future scenario: the product brings its manufacturing information with it in machine readable form, e.g. on an RFID chip. The product's route through the manufacturing plant and the individual manufacturing stages are controlled based on this data. Universities and research institutions are working on the Smart Factory within so-called model factories.

1.2.1. Smart Factory^{KL}

SmartFactory^{KL} is pioneering the Smart Factory of the future. As a leading centre of excellence and manufacturer-independent demonstration and research platform, it develops innovative factory systems where the vision of Industrie 4.0 already becomes a reality[8]. The aim is to form a network of high-profile partners from industry and research to work on new concepts, standards and solutions that will provide the basis for highly versatile automation engineering.
As a full member, Pilz gives its wholehearted backing to this goal of the initiative. Pilz follows up findings obtained from the joint work on the development platform and feeds them into its own products.
SmartFactory^{KL} already has the world's first manufacturer-independent Industrie 4.0 plant[9]. Safety and modularisation are important issues here. Firstly, with its experience in the field of machinery safety, Pilz advocates standardisation and a common approach to safety, which comprises the dual facets of safety (machinery safety) and security (IT security).
Secondly, Pilz is involved with the issue of modularisation. The construction of plants in accordance with the mechatronic approach enables complete modularisation in the form of machine elements. Functions can be standardised and re-used across a range of modules. Automation systems such as PSS 4000 from Pilz, which can distribute control functions, are the foundation. Such automation concepts can be tested in the Smart Factory. For some years now, SmartFactory^{KL} has been exhibiting a modular, cross-manufacturer production plant in which individual modules made by a range of manufacturers with various control architectures work together seamlessly. Pilz expands this Smart Factory^{KL} demonstrator plant with an intelligent, automated storage module.

[6] Definition in Glossary, page 20f.
[7] Definition in Glossary, page 20f.
[8] http://www.smartfactory.de/
[9] http://www.smartfactory.de/

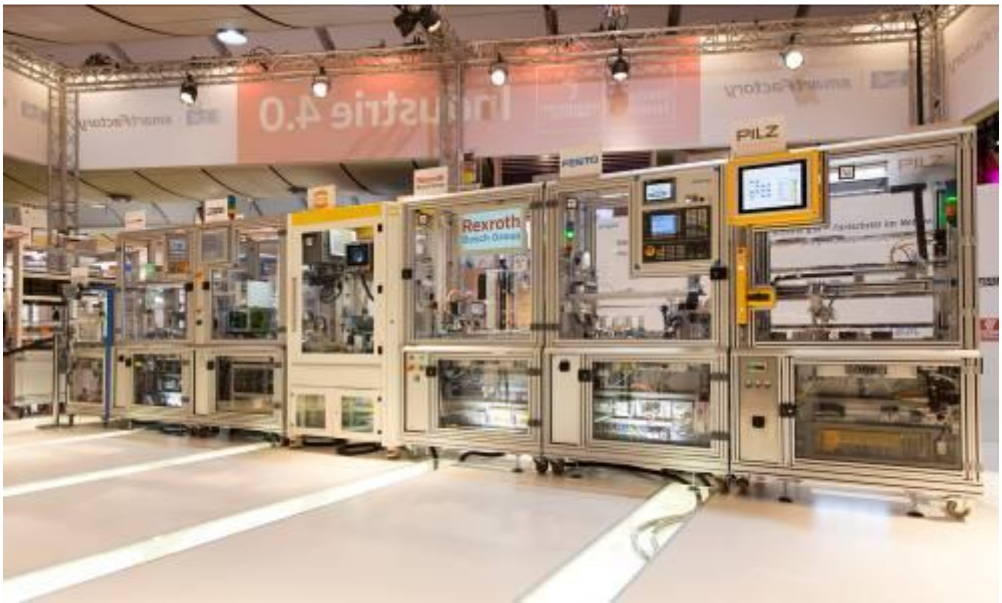

Figure 1: SmartFactory^{KL} *at Hannover Messe 2015*

1.2.2. The Pilz Smart Factory demonstrator

The Smart Factory demonstrator enables us to show how customised products can be manufactured swiftly, flexibly and cost-effectively. The modular production line illustrates communication between distributed automation systems in cooperation with actuator and sensor technology. The Industrie 4.0-compatible automation system PSS 4000 coordinates the sequence of all networked components – safety and automation, from engineering to visualisation.
Our intelligent production line produces personalised business card holders and ballpoint pens. One priority is to keep the production processes transparent. With our solutions it is simple to represent complex plant and machinery with sophisticated functions, such as those featuring in the digitally networked systems of Industrie 4.0.

The demonstrator comprises three different function modules:

- Store for workpiece carriers
- Robot with workpiece magazine/product handover station
- Laser station

A customer data record (contact, address...) is generated via a PC, where customers can choose between a business card box or a ballpoint pen. They then can then either have the pen inscribed with their name or have a digital business card box produced with their name lettering. The data is stored digitally on an RFID chip located on the workpiece carrier. This ensures that all the information is available in every module. At the individual modules, the information required is then read out from the chip and the appropriate processes are performed. Once the product has been produced the RFID chip is erased at the product issuing station, and is then ready to be written with the next data record.
After this erasing process the workpiece carrier with the RFID chip is either returned to the store if no further data record is available, or alternatively is fed straight back into the production cycle.

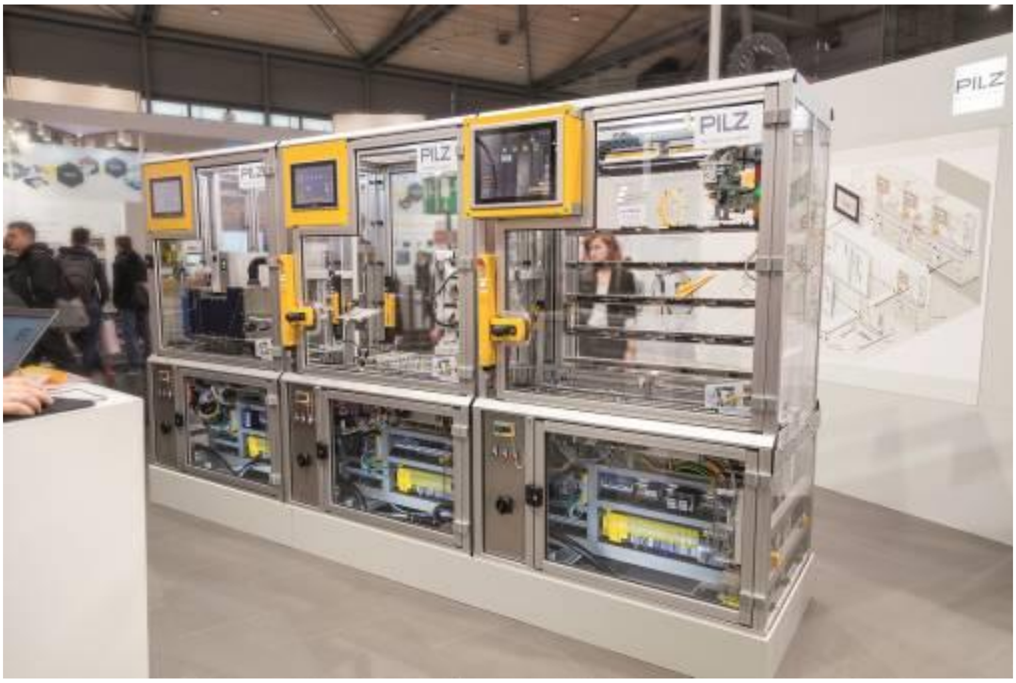

Figure 2: The Pilz Smart Factory demonstrator at Hannover Messe 2016

1.3. Safety & Security

The ongoing development of the automation landscape with Industrie 4.0 means that companies are faced with new safety and security challenges. The world of automation is merging with the IT world. Specific perspectives on the issue of safety/security differ significantly: the internationally used terms are “Safety” for machinery safety and “Security” for IT and data security; this helps with the basic differentiation.

Safety demands that residual risks arising from a plant or machine do not exceed acceptable values. This includes hazards to the plant environment (e.g. environmental damage) as well as hazards within the plant (e.g. people inside the plant).

Security concerns the protection of a plant or machine from unauthorised access from outside as well as the protection of sensitive data from corruption, loss and unauthorised access from within. This includes explicit attacks as well as unintentional security incidents.

Comprehensive protection of production and safety-relevant control data during transfer, processing and storage must address the following areas of security:

- Physical security and availability of the IT systems
- Network security
- Software application security
- Data security
- Operational safety

1.4. Modular machinery and decentralisation

For several years now, modular mechanical and plant engineering has been seen as the key to greater flexibility in production. A complete plant comprises multiple autonomous machine modules. Each of these modules represents one or more standardised production steps and can be combined with other modules to create a complete process. This involves connecting all modules to a backbone that supplies each of them with energy (400 VAC three-phase current, compressed air, ...) as well as with process and control data. If the production method needs to be changed or productivity ramped up, one or more modules can be exchanged or identical modules added.

Modularisation and decentralisation are consequently two of the key success factors en route to the future of automation. A prerequisite for this is automation systems that are able to control the distributed intelligence in the machine modules in a user-friendly way. All plant and machinery can then be broken down into manageable, independently functioning units.

The modular structure of plant and machinery follows the mechatronic approach. The philosophy here is to universally merge all the disciplines involved in a machine's development process: mechanics, electrics and automation technology. The interaction between diverse, individual, automation technology components and associated software tools to form an automation solution is universally defined. This universality extends across the four levels of the automation pyramid (management level, operational level, control level and field level). The mechatronic approach requires even control functionalities to be able to migrate into individual mechatronic modules.

This is where systems so far meet their limits. Although function modules can be created, when these are to be executed by powerful, central control systems, the commissioning of individual modules rapidly becomes a laborious process because of its complexity. Subsequent configuration changes and programming of the individual function modules likewise increase the workload.

Decentralised systems make commissioning modules a straightforward affair. The configuring task is also very user-friendly because identical control programs and subfunctions can be used for various different modules.

So the automation of the future demands solutions that are able to both distribute control intelligence and guarantee that the necessary networking of several control systems remains easy for the user to handle. Pilz offers such a solution with the PSS 4000 automation system.

2. Industrie 4.0 and Pilz

2.1. Pilz's contribution

Susanne Kunschert, Managing Partner of Pilz, was personally appointed to the Research Alliance by the German government in 2010, as the representative for small and medium-sized enterprises. This is the central, innovative policy body advising the Federal Government on the implementation and development of the high tech strategy. Susanne Kunschert was asked to bring the perspectives of the innovative small and medium-sized enterprise.

As a member of the safety promoters' group, Pilz's Managing Partner is concerned with effective protection for communication networks and the development of Germany as a leading market for safety technology. Where areas of need were identified, the Research Alliance developed initiatives within working groups. One of the most important is Industrie 4.0.

Pilz has actively supported the work of the newly founded Industrie 4.0 Administrative Office in various projects under the umbrella of the industry associations BITKOM, ZVEI and VDMA. It was also involved in developing recommendations for action. These were delivered to the Federal Government at Hannover Messe 2013.

Pilz is currently active in the following committees:
- Collaborates in the Industrie 4.0 Platform
- Collaborates in the Industrie 4.0 Management Team at ZVEI
- Collaborates in the Baden-Württemberg Federal Mechatronics Network
- Member of the Steering Committee of the Baden-Württemberg Industrie 4.0 Alliance
- Member of the manufacturer-independent demonstration and research platform Smart Factory^{KL}
- Member of ARENA2036 – The Future of Automotive Manufacturing

2.2. Industrie 4.0 in Pilz production

Moving beyond involvement in the Research Alliance and the research platform SmartFactory^{KL}, Industrie 4.0 is more than a mere initiative for Pilz; it has become an integral part of the production process**.**
With the growing integration of machinery and infrastructure through the use of IT in production, Pilz is also highlighting its profile as technology leader in its own production operations. In the spirit of Industrie 4.0, the necessary infrastructure for intelligent production has been created and elements of Industrie 4.0 have been swiftly implemented.
An intelligent workpiece conveyor developed in-house is already in use. It speeds up and simplifies the process of populating the circuit boards and the soldering process. The workpiece carriers find their way from the solder wave to the assembly unit automatically thanks to a built-in RFID chip.
Pilz will successively roll out intelligent production: machine data will be specifically gathered and processed for production control. Evaluating this data will yield important information about changes in the condition of machinery and levels of wear. Maintenance can then be carried out preventively. Predictive maintenance avoids malfunctions and downtimes.
The latest versions of work documents will also be saved in a Pilz cloud. All data and

documents will then be available in real time, always in the latest form, and can be accessed on mobile devices in production shops anywhere.

2.2.1. IT in integrated production

Pilz is aware of the challenges to IT security of a fully integrated production setup. That is why Pilz is investing in a comprehensive security infrastructure to monitor all data traffic. The measures include a separate computer centre reflecting the latest standards. By permanently analysing and logging all relevant production parameters, anomalies can be picked up early on. In addition, different firewall systems have been installed for individual production areas so that the necessary security level can be determined individually by zone. Stoppages and safety risks are minimised, and know-how is protected.

2.2.2. “Pilz Think Tank 4.0”

Cooperation specifically between the Information Technology and Production Technology departments, which is so pivotal to Industrie 4.0, is another top priority for Pilz. The specially created “Pilz Think Tank 4.0” brings together members of Production and IT and equips them with the necessary resources to plan and carry out joint projects for Industrie 4.0.

2.3. Action area – Industrie 4.0

One of the principles for sustained market acceptance is to create standardised mechanisms in communication between machines and within the machine. Practical solutions that are acceptable to users will only take shape if the requirements of both worlds (automation and IT) are considered.
In summary this means that Pilz is committed to modern control architectures in an Industrie 4.0 environment.

Our focus is on the following issues:

- Safety & security:
  - Both have clear parallels in terms of standardisation and procedure in the engineering process. We want to utilise the experience we have gained in machinery safety and automation to drive this important work forward.
  - All the devices and automation components necessary for the control function receive direct Internet access to exchange process data and parameter data for diagnostics and (remote) maintenance. As a result, the demands for all the automation devices involved increase in terms of security and a standardised diagnostic interface and display.
- Modular approach:
  - Our modern control functions are designed for distribution and object orientation – sensors and actors have intelligence. We hereby replicate the trend towards mechatronic control objects (automation components) in our products and the corresponding engineering tools.

3. Action area – safety & security

Safety & security is an important prerequisite for the function of Industrie 4.0 systems, which in contrast to traditional production plants have interfaces to their environment.

In future Industrie 4.0 systems will be reconfigured and optimised autonomously – i.e. by the system itself during operation – so this requires a reassessment of safety & security during runtime. It must also be ensured that no unacceptably high safety risks will arise as a result of residual security vulnerabilities.

Ultimately, confidence building on this issue should be supported among small and medium-sized enterprises, as the crucial basis for production in ad-hoc networks. Transparency, participation and open communication are important prerequisites in this regard.

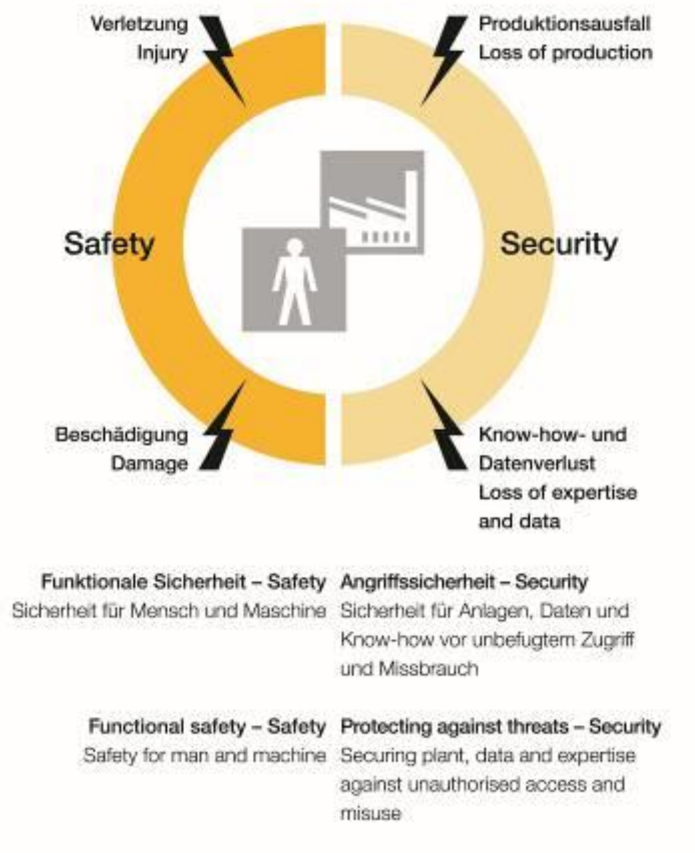
Verletzung
Injury
Produktionsausfall
Loss of production
Safety
Security
Beschädigung
Damage
Know-how- und Datenverlust
Loss of expertise and data
Funktionale Sicherheit – Safety
Sicherheit für Mensch und Maschine
Angriffssicherheit – Security
Sicherheit für Anlagen, Daten und Know-how vor unbefugtem Zugriff und Missbrauch
Functional safety – Safety
Safety for man and machine
Protecting against threats – Security
Securing plant, data and expertise against unauthorised access and misuse

Figure 3: The interplay of safety and security

3.1. Safety

The field of safety is already characterised by considerable security of investment and legal certainty. That is partly due to the need to comply with norms and standards.
For example, all risk analysis, risk assessment and execution processes are clearly defined using the internationally standardised Safety Integrity Level (SIL) classifications, permitting legally effective comparability of the various solutions.

3.1.1. Safety – from static to dynamic safety

The term safety denotes the functional safety of machinery or, put another way, the protection of people and the environment against threats that can proceed from machinery. Safety demands that residual risks arising from a plant or machine do not exceed acceptable values. This includes hazards to the plant environment (e.g. environmental damage) as well as hazards within the plant or machine (e.g. people inside the plant).
One option for the worst case is simply to interrupt the energy supply straight away and bring the machine to a hard stop. The traditional way of providing scope for this is by means of special safety wiring and components such as safety relays. Because this approach is very much hardware-based and therefore static, it is not particularly suitable for intelligent manufacturing processes where plant layouts continually need to be changed. A hard shutdown is generally associated with further disadvantages, whether these involve loss of productivity, extended downtimes due to more complex recommissioning procedures or a restriction in the machine's operating and maintenance concept.

An alternative is offered by dynamic safety concepts based on an integrated view of changing automation processes and functional safety requirements. This changes the view of safety itself; it is regarded less as a hardware characteristic and more as a cross-device function. This approach, which was already developed before the age of Industrie 4.0, allows processes to be operated in a safely controlled manner without any need to interrupt them immediately every time a fault occurs. But the dynamic approach can only be implemented efficiently if functional safety is built into automation projects from the moment they are planned. Failing that, the sequence of individual manufacturing stages or of an entire process may need to be changed retrospectively; this is a barrier to achieving the optimum solution and also incurs considerable costs.
While static safety often involves only transmitting binary signals, for instance to shut down the movement of a machine after a safety gate has been opened, more extensive information is required for dynamic safety. Because with this approach there are various safe operating modes that permit "operation with safety gate open", for example. But this information on the safe operating mode must be present in all the components involved. In the example of the safety gate, depending on the authorisation level of the user such actions as opening the safety gate no longer automatically result in the machine being shut down immediately; instead, safety mechanisms monitor whether a reduced limit speed is complied with, or generate and monitor the safe setpoint of the rotational axis.

3.1.2. Safety 4.0 – from monolithic structures to modular solutions

The Smart Factory vision entails modular plant reconfigured quickly and flexibly or modified as an entity. The validation of a safety solution must then be in a position to accommodate this (late) widening of flexibility. Because any configurations that have not been considered in the CE marking process cannot simply be established by the operator. This is not a case of a simple equation which states that:
$CE_{module1} + CE_{module2} = CE_{complete\ machine}$!
The functional advantage of modular machine concepts is obvious. They introduce greater flexibility into the production process while at the same time increasing scope for standardisation at functional level. The highest degree of standardisation potential can be achieved when the boundaries of the various modules can be identical in design – regardless of whether a module handles a mechanical, electrical, control engineering or

visualisation function. The mechatronic approach has the goal of creating automation objects that are standardised in this way.
The advantages of modularisation are often cancelled out by a rigid safety concept that may still be based on hard wiring. Electronic safety control systems, too, almost always mimic hardware-based safety – in the form of fixed safety circuits – even if the product is offered with freely programmable circuit logic.
By contrast, a basic feature of modern control architectures is that they largely function without systemic rules. The intention is that the user can optimise them freely in keeping with their degrees of modularisation. Remove the barrier thrown up by different perspectives for the automation and machine safety functions and the user gains key degrees of freedom. PSS 4000 is an automation system that contains the aspects of modularisation and enhanced flexibility as two of its basic functions. For the first time it is now possible to manage all process variables – including for the safety functions – entirely symbolically and without any hardware correlations in the system. To reflect this, all process variables are available system-wide and, thanks to the multi-master architecture, are automatically available for all control systems in the distributed automation system.

3.1.3. Modular certification

The more machines are created out of modules, the more components need to be connected decentrally. A modular design for machinery or machine parts has several big advantages. Machine modules can be recombined and exchanged. You can extend machines or for example perform a tool change while production continues. Machines become more flexible. The operator can manufacture a larger number of products with the same number of machines. Working on the assumption that this is a benefit for the operator, control concepts become more decentralised. The issue of safety and security is important in this context. Modular certification of the individual plant modules is the key consideration. Today, machines are inspected and accepted by the certification bodies as complete entities. Even a minor change, such as exchanging two modules, means renewed acceptance is required. Although various solution approaches are under discussion, there is currently no standard practice. One such approach adopts the view that the machine is safe if its individual modules are safe. The task is now to sensitise companies and policymakers to this issue through the trade associations. Without a legal framework, progress in this domain is inconceivable.

3.2. Security

The challenge for security is that – unlike functional safety – security mechanisms need to adapt continually to new threats. This may be due to occasional updates, because viruses, worms, Trojans etc. keep evolving and security gaps can ultimately impair production along with all its functional elements.
In order to respond flexibly to the prevailing threat scenario, there must also be a comprehensive security strategy comprising multiple layers to underpin the protection of safety applications: the automation components are at the heart. This is followed by the network via which these components can communicate with other networks or, for example, with an ERP (enterprise resource planning) system. The outermost layer represents the factory, which is shielded from the outside world by a special firewall concept, the so-called demilitarised zone.

The demands that the spheres of IT and automation place on security vary considerably. While the confidentiality of information enjoys top priority in the office environment, in the production sphere data availability comes top of the list because this is a key prerequisite for smooth production processes. An international standard (IEC 62443) designed to bring both security worlds together is currently being drawn up. Because the threats from the cyber world are dynamic, safety and security will remain two separate issues, which are nevertheless closely related.

What matters is that we develop methods and tools with which we can analyse the impact of security gaps on additional residual risks to safety. These methods and tools should ideally already be applied in the product development of cyber-physical systems (CPS): security by design.

Aspects to take into account are:

- Protection of interfaces (PLC) from external influences (Internet, company network, …)
- Protection of communication systems in the plant and machinery depending on the usage methods (constant operation, remote maintenance, remote diagnostics, ad hoc connections, ...)
- Security is a “moving target”; there isn’t just one constant safety solution

3.2.1. Solution approaches in the field of security

How can safety applications protect against the threats from the cyber world? The short answer is: only by combining various measures and security guidelines, which are consistently observed by all parties.
For networking, the recipe for success is “defence in depth”. One core element that harks back to the way mediaeval castles were built is the “zones and conduits” security model, which is already defined in the standard IEC 62443. It envisages dividing an automation network up into different zones, within which devices are allowed to communicate with each other. Data exchange with devices in other zones is only possible via a single conduit, which is guarded by a secure router or a firewall to filter the data flow according to defined rules, thus blocking unauthorised access. Even if an attacker were able to penetrate into one zone, only the devices in that zone would be endangered and all others would remain safe.

3.2.2. Automation solutions

For the protection of automation solutions, IEC 62443 – the standards series on IT security in industrial automation systems – defines the seven “foundational requirements” for the security of such automation solutions:

- 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)

Each foundational requirement can be expanded into the following elements:

- 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

Each of the elements has four securityevels that can be achieved, based on the work invested in the development of automation solutions. The systems integrator and plant operator now need to define the protection levels that are appropriate to the application and the zone model derived from it. Certainly the highest protection level, “Level 4”, will not always be applicable, as this can involve a tremendous amount of work.

Even the best technical security measures are worthless if they are not put into practice or – worse still – are deliberately bypassed because they take up too much time or due to a lack of understanding and ignorance. The technical measures must be implemented hand in hand with organisational guidelines and measures. What is the point of secure firewall settings if the password is left set to the default given in the manual, or if it is easy to establish a link between the password and device? A protection level for a plant section is the result of technical and organisational measures working together.

3.3. Interaction between safety & security

Holistic security concepts not only require interaction between safety & security; rather, they call for system architectures geared specifically toward this consideration, based on open standards and incorporating cross-manufacturer considerations. As for the safety aspect, it is necessary to check the extent to which security issues influence functional safety.
Central issues include clear, secure proof of identity for products, processes and machines, as well as safe information exchange across the entire production process.

User-friendly solutions are also in demand: safety & security must be manageable and must reflect the needs of the user. From an economic perspective, safety is also an innovation driver: this encompasses the inclusion of cost structures with reference to productivity. The insurability of the damage and the required calculation methods are indispensable here.
As for the human factor, the issue at stake is “usable security and privacy”. The aim is to keep to a minimum the effort expended in time and understanding of the necessary security measures.

There are analogies here to functional safety: the safety measures must not adversely affect availability. Principles from the world of safety can be transferred one-to-one to the world of security. Safety requires a holistic approach.

4. Action area – modular approach

In terms of the challenges, only strict interdisciplinary “modular thinking” will succeed in the medium to long term. Control systems which support this approach will play a central role here.

4.1. Distributed intelligent systems – automation system PSS 4000

With its automation system PSS 4000, Pilz is pursuing a consistently mechatronic approach. The central idea of PSS 4000 is to merge automation and safety. Process or control data, failsafe data and diagnostic information are exchanged and synchronised via the multi-master communication system SafetyNET p. For the control function, therefore, it makes no difference where the respective program section is processed. Instead of a centralised control system, a user program distributed in runtime is made available to the user within a centralised project view. All network subscribers are configured, programmed and diagnosed via this central project configuration. If the project configuration is closed, the individual program components are assigned to the individual control devices. This is achieved based on clear user specifications for the clustering of functional units, enabling simple, standardised handling across the whole project. Advantages include not only module formation and standardisation but also more flexible error reaction, greater availability and higher productivity thanks to shorter response times for the overall system.

Whereas in classic automation a standalone, centralised control system monitors the plant or machine and processes all the signals, the PSS 4000 allows control functions to be distributed consistently. In detail, the automation system PSS 4000 consists of hardware and software components such as the real-time Ethernet SafetyNET p and various programming editors designed for use in different sectors, with their application-oriented function blocks. The hardware includes control systems of various performance classes. Process or control data, failsafe data and diagnostic information are exchanged and synchronised via Ethernet. This consistent merging of safety and automation functions reduces the complexity of communication and also optimises costs.

4.2. Engineering tool PAS4000

The aim of the automation system PSS 4000 is to simplify the decentralisation of control functionalities and still maintain clarity of operation. The software platform PAS4000 plays a key role in this. It comprises several editors for PLC programming and configuration as well as software blocks. In PAS4000, the tools for configuration, programming, commissioning and operation are closely compatible.

PAS4000 supports the breaking down of a plant/machine function into ever smaller function modules, according to the same principle as the boundaries of the mechatronic units. Modularisation is a key aspect: elements are created from basic functions; elements in turn give rise to modules and modules give rise to plant and machinery – quite simply through hierarchical block nesting. Basic functions, elements and modules form the backbone of the software development and are ideal to re-use as software components thanks to encapsulation and object orientation.

PAS4000 provides software libraries containing the most common basic functions, elements and modules. The selection of ready-made components from libraries is itself not new. A special feature of PAS4000 is that these components have been assigned “properties”. These allow the parameters for the required functions to be set quite simply. This is a particular benefit in terms of the standardisation of functions.

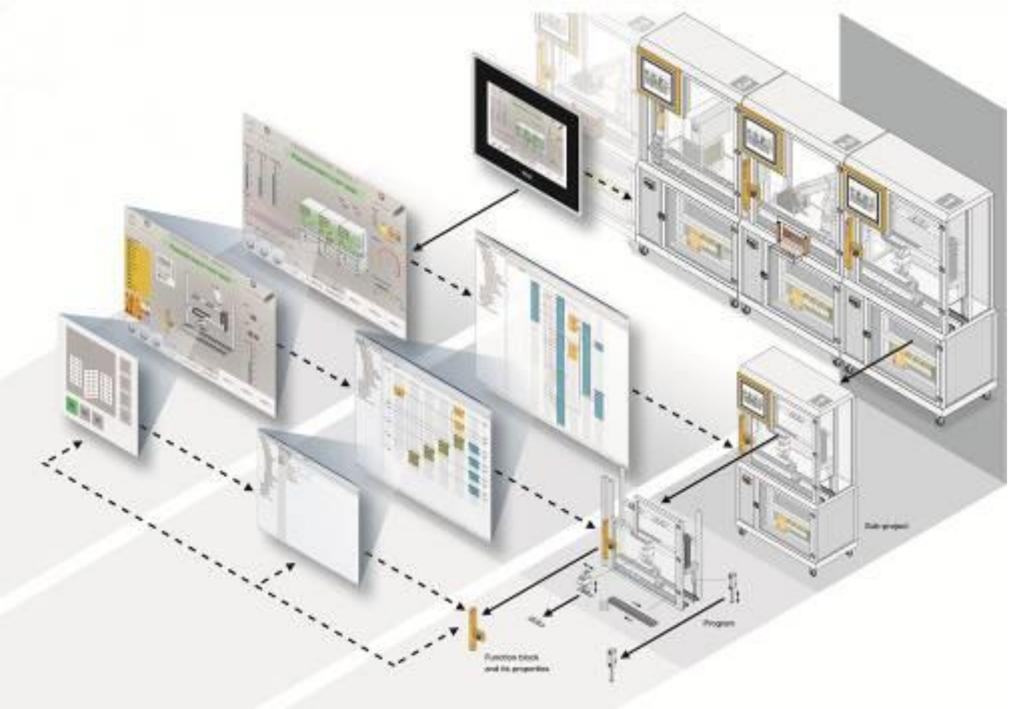

Figure 4: Plants can be broken down into manageable, independently functioning units.

4.3. PASvisu visualisation

According to the same principle, visualisation and control programs can be broken down into the smallest unit. A common data basis for the individual modules ensures that the modules can communicate with each other. Thanks to the uniform structure, project configuration data can easily be re-used.

The visualisation software enables visualisation projects to be created and configured simply via the PASvisu Builder.
As there is access to all data in an automation project, including all process variables and OPC namespaces, variables no longer need to be entered and assigned manually, a process which was error-prone. This means it is now possible to call up information such as the checksum of the project or the firmware version of the head unit.

Industrie 4.0 considers the “value of data” – in this instance, project configuration data. A common data basis helps to reduce potential error sources by automatically adopting “matching” data, while automated consistency checks reduce engineering times: uniform module formation in control and visualisation facilitates the re-use of machine elements and modules.

Glossary

Smart product
The smart product carries an ID or is marked directly with key information about its manufacturing, enabling it to control its production process itself. As a smart object, it forms the basis for the Internet of Things.

Internet of Things
On the Internet of Things (IoT), smart “things” or elements or objects communicate with each other via a universal, digital network. Computers as individual devices increasingly disappear and are replaced with “intelligent things”. These connect to the Internet so that they are able to communicate independently with the Internet in order to perform a variety of tasks for the owner.
Particularly thanks to the intelligent localisation technology of radio-frequency identification (RFID), objects can now already identify themselves, and in fact control themselves to some degree. These objects in turn carry certain information about what should happen to them. So the products themselves inform their material handling or production system of the next working steps. Human intervention is no longer necessary.

Cyber-physical systems (CPS)
Key components are mobile and movable installations, devices and machinery (including robots), embedded systems and networked objects (Internet of Things). The transfer, exchange, monitoring and control of their data are handled by an infrastructure such as the Internet in real time.
They can be activated and read out without any direct contact and draw on their assigned intelligence to make decisions independently. A cyber-physical system is characterised by its high degree of complexity. Cyber-physical systems are created by integrating embedded systems by means of wired or wireless communications networks.

Reference architecture model (RAMI)
Automation used to be characterised by a hardware-oriented structure (automation pyramid). Such a structure has today become obsolete because there is now more to automation than simply wiring up hardware devices; it also involves cloud connections and data connections. Furthermore, as well as production data being available in the process it is also possible to access external control data. That is why the reference architecture model (RAMI) was created as a modernised automation pyramid. The ZVEI developed the idea and concept of the automation industry together with the VDI/VDE-GMA, DKE and the partners in the Industrie 4.0 joint platform Bitkom and VDMA.[10] The model brings together the essential elements of Industrie 4.0 for the first time in a three-dimensional layer model.[11] With this framework, Industrie 4.0 can be systematically classified and developed further. The model defines standards for Industrie 4.0. Such standardisation is necessary because Industrie 4.0 means components from different companies need to be able to communicate with each other.

[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

We are represented internationally. Please refer to our homepage www.pilz.com
for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY