White Paper

Creating safety.
With passion.

NewTec

WHITE PAPER

Industrial Internet of Things and Industry 4.0: New challenges for manufacturers and users

Industrial Internet of Things and Industry 4.0: New challenges for manufacturers and users

Contents

Management Summary

Industry 4.0 and the Industrial Internet of Things (IIoT) create significant challenges for users and manufacturers of systems and devices. Most machine and system manufacturers as well as most production companies lack adequate experience when it comes to using smart networks.

Even though, modular automation concepts with increasingly decentral distribution of control intelligence have already been around for some time. The decentral components – including safety controllers – communicate more and more via network technologies. However, many manufacturers and users hardly think about security issues. Cybercriminals use this fact to sabotage or extort companies, or to carry out espionage.

Industry 4.0 will force each company to put security on its agenda. Production machines communicating autonomously; interdepartmental networks of machines, material and people; customers and partners seamlessly integrated into business and production processes – the digitalization of the industry asks for new concepts with safe solutions.

Security in interconnected industrial systems includes two aspects which used to have little to do with each other: protecting people and the environment from dangers which are caused by operating a system (safety) and protecting systems from attacks from their environment (security). Two different worlds meet, the world of industrial automation and the world of IT.

Traditionally, functional safety was the responsibility of engineering departments which look back on decades of experience in the field. Security, on the other hand, the protection of IT systems against attacks from the outside, lies in the hands of the IT department. Conventional tools of IT security – firewalls, intrusion detection, virus scanners, etc. – are not enough to protect the interconnected Industry 4.0 production. Even worse: they might cause problems. Moreover, safety and security interact in interconnected production companies: Security measures can put the functional safety at risk and vice versa. Both areas have different protection targets which must be harmonised with each other.

The present white paper shows why Industry 4.0 calls for a new, integrated concept of security including both safety and security aspects. The implementation of such a security concept calls for a structured and integrated process, already considering the following aspects while developing an IoT product or an Industry 4.0 application, and during its complete life cycle: "Security & Safety by Design".

For companies lacking know-how and/or resources for functionally safe and protected developments, the technology and security specialist NewTec offers a wide range of services and products.

1 Introduction

1.1 Industrial Internet of Things (IIoT) and Industry 4.0

Industry 4.0 and the (Industrial) Internet of Things (IoT or IIoT) increasingly gain importance. Many producers, primarily in machine and system production and the automotive industry, already use digital technologies for producing more efficiently but also for their own products and new services. Smart, interconnected systems continuously support activities in the entire value chain. To remain competitive, it is essential to keep up with the digital transformation.

IIoT technologies are especially useful where process relevant data incur, such as product, operational, state, environmental or location data. That includes all elements of the value chain: Production systems, materials and parts, logistical systems and vehicles, employees, suppliers and customers as well as finished products. This data can be used in multiple ways: to efficiently control all production and logistic operations, to optimise servicing and maintenance or to exploit new business activities with innovative information-based business models.

An example: A customer configures his individual product online, e.g. a motor bike. He selects a model, style, frame design, colour, tank size etc., clicks on the order button and is thus automatically generating a production order. The production systems are interconnected in turn: Inventories and positions of the required parts as well as utilization and free capacities of machines are known. All parts on the parts list reach assembly accurately, possible problems in production and logistics are detected immediately and considered already in production control. Few hours later, the ordered motor bike is already assembled.

That is no futuristic image: Harley-Davidson produces machines in more than one thousand different configurations in its factory in York, Pennsylvania – within a time frame of six hours from ordering.

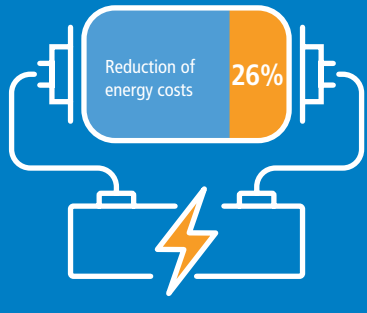
1.2 Technical and Organisational Challenges

According to a current survey by IDG, companies in the region of Germany, Austria and Switzerland expect multiple positive impulses for their businesses from IoT but see significant organisational and technical challenges at the same time: e.g. concerning the adaptation of the business processes, the complexity of the topic IoT, the IT infrastructure or the communication between departments (see next page).

The respondents consider guaranteeing security and compliance to be the biggest challenges. 44 % of the respondents consider the Internet of Things as a possible gateway for DDoS attacks (Distributed Denial of Service) or hacker attacks. Respondents were worried about issues such as data security / disaster recovery (39 %), industry espionage (32 %) and compliance (28 %).

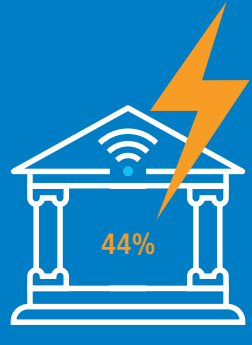
Industry 4.0

Primary objectives are an increase of productivity, shorter set-up times and reduction of energy costs.



New gateway for hackers

44 % of the companies consider security issues to be the biggest technical challenge for IoT projects.



source: IDG

In the scope of its online survey "Internet of Things 2018" in the autumn of 2017, IDG interviewed 385 IT managers from companies in the region Germany, Austria, Switzerland, including strategic (IT) decision-makers in the C-level area and departments, IT decision makers and IT specialists from the IT area.

What are the biggest technological challenges concerning IoT or the implementation of IoT projects?

Information in percent. Multiple answers possible. Basis: n = 310

Security (new gateway)	43.9
Data security / disaster recovery	39.0
Complexity of the topic	32.9
Safety / operational safety	29.7
ITC infrastructure	29.4
IT systems with obsolete operation systems without patching possibilities	26.5
Deficient network quality	25.2
Integration of the devices (sensors /actuators) into the IT infrastructure	24.2
Finding a suitable IoT platform	23.2
Missing technologies / platforms / standards	22.9
Availability / system stability	21.6
Excessive amounts of data	20.3
Missing or inefficient big data solutions / lacking analytics	19.7
Network access for isolated production systems	16.1
Missing updates for existing production system(s)	7.7
Other technical challenges	1.3

What are the biggest organisational challenges concerning IoT or the implementation of IoT projects?

Information in percent. Multiple answers possible. Basis: n = 310

Business process must be modified and adapted	40.6
Insufficient communication between involved departments	31.3
Members of staff are lacking skills	30.3
Restructuring the organisational structure to IoT interests	29.4
Issue "Interface IT and specific department (e.g. production)"	29.4
Development of a business model	27.1
Missing IT professionals	26.8
Missing openness for partnerships	25.5
Return on investment of IoT projects is unclear	25.5
Missing resources (not enough positions)	21.9
Missing acceptance by business partners and service providers	19.7
Lacking management support	18.7
Missing acceptance by customers	17.7
External partners are lacking skills (e.g. system house)	17.1
Research budget not sufficient for topics concerning IoT	14.5
Concerns of members of staff	13.2
Other technical challenges	1.9

2 The Security Challenge

Often, IoT systems have (severe) security flaws – in routers, printers or cameras, alarm systems or pace makers, or even in power plants. Such security issues for IoT devices are not limited to consumer products. IT systems for production include routers, switches, control components or workstations which can also have weak points.

The industry also relies on the interconnection of multiple embedded systems which are only inadequately protected against attacks. The interconnection of production with other areas in the supply chain, such as mobile unites or even external systems, is increasing. Therefore, the future "Industry 4.0" creates several potential weak points and gateways for malware.

It is important not to forget that an increasing number of attacks is carried out without internet connection, such as infected USB sticks or social engineering (see box). There are forms of malware that systematically exploit security flaws of industrial controls. It doesn't need more than one single vulnerable component to compromise the entire network.

Interconnection facilitates new threats with severe impact on all security aspects pertaining to functionality, failure and manipulation. Those risks include theft of critical information up to sabotage.
Conclusion: Interconnected devices must be secure, independent from their location.

2.1 Targeted Attacks are Increasing

Most cyber attacks spread widely so that they are also successful in the industrial environment: Ransomware such as WannaCry has compromised production in countless companies in the past. The attacks are increasingly targeted on specific business applications, e.g. accounting software (Petya/NotPetya). Malware is even spread via infected firmware updates for industrial components on hacked producer sites (so-called watering hole attacks).

At the same time, individual companies have become the target of specific attacks. A survey of B2B International (2017) on behalf of Kaspersky Lab, warns about this fact. No less than 27 percent of the companies interviewed confirm a targeted attack on their infrastructure (compared to 21 percent in the previous year).

For targeted attacks, hackers gain access to the company's network, either by technical means such as automatically scanning for weak (or unprotected) access points, or by tricking employees with things such as phishing/malware emails that mimick the look of the company's emails. If a flaw has been identified, the malware for espionage or ransom is installed manually. This specifically targets an increasing number of industrial control systems (ICS) to compromise them (Stuxnet, Havex, BlackEnergy2). SCADA servers, HMIs (human machine interfaces), workstations, programmable logic controllers (PLC) or network components are at risk. By interfering with the control systems, the safety of employees is also compromised. New malware such as Trisis/Triton is directly manipulating safety-relevant systems and puts lives at risk.

2.2 Problems when Securing IT for Production Lines

Many IoT devices are easy targets for hackers: Open ports without authentication, pre-set standard logins with passwords such as "admin" or "1234" or missing security updates are only a few of the widespread mistakes of manufacturers. In an industrial environment, certain special properties of IT systems close to production complicate their protection significantly. This includes the heterogeneity of IT systems close to production, their significance critical to the business, the requirements for functional safety but also the limited capacities of embedded systems. Therefore, measures for IT security in Industry 4.0 require other solutions than standard IT systems.

Heterogenic systems

IT close to production is often not standardised. There are thousands of products of countless providers who all have their own software stacks. Experts estimate that the industry actively uses approx. 2,000 different protocols. Binding standards for production system software is still in its early phase of development. In contrast to an office environment where products of few companies such as Microsoft or Adobe are dominating on the market, these security issues cannot be eliminated globally with an update.

Updates and security checks are complicated

In contrast to an office environment, IT systems close to production must be available around the clock. To install software updates, production operations might need to shut down. Many systems effecting the functional safety – e.g. control systems – might even require recertification when installing a security update. The life cycle of control systems tends to be a lot longer than the life cycle of classical IT systems. Conventional, resource-hungry security technologies such as virus scans and network analyses are often not suitable for embedded systems in production since they might compromise real-time control.

2.3 Increased Liability Risks

Providers and operators of IoT systems must be prepared for stricter liability rules. Unsecured IoT devices misused as gateway into company networks or as part of bot networks for attacks are a threat to security. Security includes both the protection against attacks (security) and the protection of people and the environment (safety). Possible consequences of cyberattacks do not only include the economic loss but also dangers for life and health when hackers gain control of interconnected vehicles, fire prevention systems, industrial robots or power plants.

Therefore, it is obvious that the legal situation for IoT products must and will change. In the US and the EU, legislative proposals are being discussed, such as the IoT Cybersecurity Improvement Act which must guarantee for a minimum standard for IT security. Various committees, among others the Committee on Internal Affairs of the German Bundestag and the German Interior Minister's Conference, demand the creation of binding IT security standards on EU level and provisions for product liability in IoT products.

Currently, general provisions from the following acts are often applicable in Industry 4.0 scenarios in Germany: Liability in Damages (art. 823 et. seq. German Civil Code) or the Contractual Liability between Cooperation Partners (art. 280 et. seq. German Civil Code). Provisions of the product liability (German Act for Product Liability) might additionally apply. Considering the new framework factors due to digitalising and IoT, amendments of law are discussed intensely.

New acts set the agenda

IT security Act and NIS directive

The IT Security Act (Act for Increasing the Security of Information Technology Systems), in force since July 2015, obligates manufacturers or operators of critical infrastructures to take organisational and technical precautions ("state of the art" according to IEC 62443) to prevent problems concerning availability, integrity, authenticity and confidentiality of their information technology systems, components or processes. Critical infrastructures include equipment and systems for energy, information technology, transport/traffic and health. The new European Directive to guarantee a high network and information security (NIS-Directive) and the corresponding German implementation act will also make providers of digital services (such as cloud providers) responsible, from May 2018 onwards. However, most companies are not within the scope of this existing legislation. Therefore, the survey by the German Federal Ministry for Economic Affairs and Energy (BMWI) "IT security for Industry 4.0" sees the need for further legislation.

EU Data Protection Regulation

The General Data Protection Regulation of the EU (GDPR) mandatory in all EU member states from May 2018 onwards, demands for effective technical and organisational measured to protect personal data (Privacy by Design and Default). Violations of the data protection regulation can result in rigorous sanctions such as claims for damages worth millions (art. 83 GDPR). This applies directly to IoT devices when they collect personal data.

New liability subject in traffic laws

For strict liability in traffic, the German legislation has already taken action. Since June 2017, the German Road Traffic Act specifies a legal framework for autonomous driving. Thus, new potential liability subjects appear: If damages are caused by a driving error while in autonomous driving mode and the system has not prompted the driver to take over control, recourse can be taken to vehicle manufacturer and suppliers. This gives a glimpse of the direction the legal development might take: So far, liability lies with the one causing the damage and being responsible for it. Now, someone might be held liable who has not prevented the damage from occurring. This increases the liability risk for operators, manufacturers and developers.

3 Minimise Risks: Security & Safety

Security has strategic significance

When providers and users of interconnected devices and solutions want to prevent business losses and a negative image and also consequences based on liability and criminal laws, they need to consider the factor security and safety already in the design and development stage. To mitigate risks, it is essential to consistently comply with standards and directives during the entire product life cycle and verify it by certifying components, software and processes.

This clarifies the strategic dimension of security processes: When manufacturers adapt and develop their development and security processes accordingly, they improve both the security of their products and their compatibility. Companies lacking the required know-how must learn or purchase it.

Reliable systems need safety and security

Most companies consider primarily functional or operational safety. Safety includes the protection of people and the environment from dangers which are caused by operating a system. Security, i.e. the protection of systems from their environment, used to be no real issue. However, with the digital transformation and IoT, the situation has changed significantly. Therefore, companies must nowadays adopt a new, integrated concept of "Security" that includes both aspects – Security & Safety – to the same extent.

New security concepts for Industry 4.0

The flexible production in Industry 4.0 scenarios requires more flexible, decentralized security concepts. Modern machines are complex, modular and allow for flexible configurations. Close cooperation with other machines, robots and most importantly people is increasingly important. Therefore, security systems are developing away from rigid protection walls towards equipping machines with sensors, safety logic and actuators, that can bring the system into a hazard-free condition. Machines, sensors, actuators and decentralised controls are increasingly interconnected via Ethernet; and safety controllers are often used in connection and are thus required to exchange information safely. This provides for a close integration of safety with security.

Security and safety affect each other

No safety without security. There is no doubt about the fact that security flaws are a risk for functional safety, e.g. when hackers infiltrate critical infrastructures, manipulate medical devices or shut down systems in production. Furthermore, in Industry 4.0 applications, functions critical to security are realised with distributed and interconnected components. Every interconnected component could provide potential access to the network and must thus be secured.

The protection goals of security & safety might even contradict each other. On the one hand, security measures can be complicated when data must be collected, and additional points of intervention must be created for safety reasons. On the other hand, security measures such as encrypting or authenticating can affect functional safety by binding required system resources or delaying time-sensitive functions.

➔ Reliable systems need safety and security. Both security and safety are intertwined, affect each other and must therefore be considered together from the start.

4 Integrated Safety Development: Implementation Recommendations

4.1 Security & Safety by Design

Security and safety from the start

Product and application developers can use the approach "Security by Design" as a guideline. It has been tried and tested several times, e.g. at Microsoft, Google, Adobe or Oracle.

In short, this approach provides for an analysis of the security and safety requirements before development of the product so that they can be considered at a later stage. Only required functionalities are implemented and the concept of the product already provides security and safety measures for all scenarios identified in the threat and risk analysis.

For the provision of functional safety, this basic procedure has been the standard for years. For integrated safety and security, make sure that the measures from the safety and security standards and guidelines listed above are implemented. In addition, the interaction of the security and safety threats and measures must be analysed and considered.

Retrospective and external protection measures are inappropriate

The task force "Industry 4.0", initiated by the Industry-Science Research Alliance from the German Federal Ministry of Education and Research considers it vital to integrate all aspects of security and safety from the start: Industry 4.0 requires "a far more proactive approach considering security and safety (especially Security by Design) than before" because questions concerning security are nowadays only raised after concrete security- or safety-related issues have occurred.

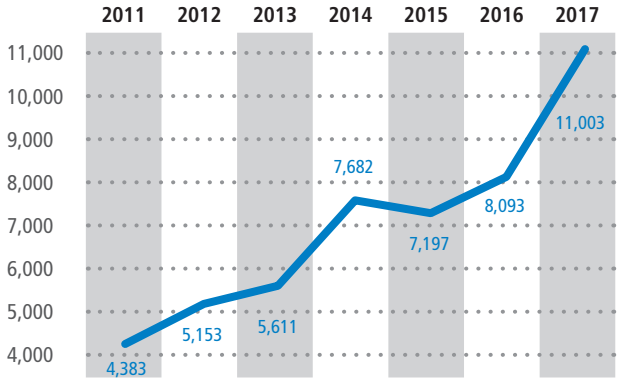
To implement security and safety measures at a later stage in the product life cycle is both more complex and more expensive and it only protects inadequately – i.e. up to the following flaw. For interconnected embedded systems in the industrial area, retrospective improvement is complicated: If a system is already in operation, changes to its basic architecture are not possible anymore. The complexity of updating a firmware depends on the system. And often – e.g. for security-related applications – retrospective changes are not intended and could require extensive re-certifications. Conclusion: To keep closing new safety flaws in elaborate patch cycles is a lot more expensive than developing a secure and safe product from the start. However, retrospective system updates must be possible, of course.

IoT manufacturers can learn from experiences in the software industry that applications cannot be protected completely by external protection measures such as firewalls. On the one hand, security flaws in components cannot always be corrected by external systems without suffering a loss of functionality. On the other hand, experience shows that attackers succeed time and again in bypassing external security measures and invading the network.

"A retrospective implementation of safety measures is far more expensive and offers generally less protection than security integrated from the start into the system development process and/or selection process for a product. Therefore, security and safety should be integrated components of the entire life cycle of an IT system or a product" (German Federal Office for Information Security (BSI), basic protection)

Continuous security management

Safety measures are implemented and certified once and must not be modified afterwards. IT security, on the contrary, requires continuous observation of the threat condition and constantly new defence measures. While the safety threat remains relatively constant – new risks arise only when machines and processes are modified – threats concerning security are changing constantly. A statistic by the Hasso-Plattner-Institute in Potsdam, Germany, reveals for 2017 a record number of more than 11,000 identified new software security flaws globally – in contrast to approx. 8,100 in 2016 and approx. 5,000 in 2010. The number of new weak points with "medium" severity (according to the common vulnerability scoring system CVSS), has even increased by 50 percent compared to 2016, flaws with "high" severity by 17 percent.



Record new number of weak points (source: HPI)

Security is a condition of the entire system
Since one single component can compromise the security of the entire system and has diverse influences on the interaction between and within systems, interconnected systems must always be considered as a whole.

As an integrated and methodological approach, "Security & Safety by Design" aims to control threats and hazards in a systematic and structured way. For this purpose, all relevant levels of a system must be included:

- People (awareness, qualifications)
- Technology (complexity, network)
- Organisation (processes, responsibilities)

Some of the guiding principles are:

- Include the entire safety chain
- Measures on process, system and component level
- Multi-level security barriers (the "knight's castle")
- Security from inside to the outside on all levels – from operational to field level, from access control to copy protection.

4.2 Standards and Instructions

The implementation of integrated security and safety developments is not that easy. This is due to the fact that most companies in the industrial area – solution providers and users – have hardly any experience in that area and applicable standards for integrated security and safety are missing.

Generally, companies know the specific requirements for functional safety in their specific industry and they can use detailed standards as a base, such as the basic safety standard IEC 61508 for safety relevant electrical and electronic systems as well as sector specific standards such as EN ISO 13849 and IEC/EN 62061 for machines or ISO 26262 for the automotive industry.

For IT security in companies, there is the ISO standard 27001 for office IT, ISO/IEC 27034 (application security) and, most importantly, IEC 62443 for "Industrial Communication Networks", i.e. the IT security of industrial automation and control systems.

Nowadays, most industrial branches use the standard IEC 62443 for IT security, which makes it the most important standard for Industry 4.0. IEC 62443 can be considered as the basic standard for industrial security by analogy with the basic safety standard IEC 61508 (the latter refers to IEC 62443 concerning the security requirements to be determined). This means that an integrated security and safety development must consider both standards (or sector specific forms, if applicable) simultaneously.

Tip

Generally, we recommend the extensive IT Basic Protection (Grundschutz) standards and catalogues by the German Federal Office for Information Security (BSI). There are no comparable instructions for an integrated implementation of safety and security measures which consider the described interaction. The IT basic protection by BSI, expressly excludes functional safety. For the security of "industrial control systems" in the producing industry and critical infrastructures, the BSI published an "ICS Security Kompendium" in 2013, amended by a section for component manufacturers in 2014. Here, the institute refers nearly exclusively to security and only refers to the listed safety standards instead of covering functional safety.

4.3 Risk and Threat Analysis

The basis for every safe and secure development is an extensive risk analysis. It should identify and assess both safety risks (hazards) and security risks (threats). All risks exceeding a tolerable residual risk must be eliminated with corresponding protection measures.

Define protection targets
Different potential protection targets apply for every case that should be considered and checked for relevance for every specific application.

For **Safety**, it is important to secure correct procedures (reliability) and – most importantly – to protect people and the environment from dangers caused by malfunctions of machines and systems (functional safety). Specifics depend on the corresponding application.

Security measures should protect people and systems and/or infrastructures from attacks from unauthorized use, manipulation, sabotage or data theft and secure the regulation and control of relevant processes. This includes the integrity of data and services (security against loss and manipulation of data; correct function), reliability (protection against misuse; certain data and services are only available for an authorized user circle) and availability (reaction with tolerable delay). Further protection targets within the scope of security are data protection (protection of personal data from misuse) and protection of intellectual property.

Identify hazard and threat scenarios

Identifying as many concrete hazard and threat scenarios for an application as possible helps to determine and assess risks. For every component of a system or an application, the specific damage potential must be identified so that the protection requirements can be determined. For this purpose, first analyse the type of risk: Which threat could be aimed directly at the respective component – e.g. manipulation, sabotage or data theft? Which hazard for people and the environment could be caused by errors or successful attacks?

An example is the use of industrial robots working directly with people (cobots). Depending on the application profile, an analysis will most probably identify that certain errors, e.g. a failed sensor, will put the health of users at risk. Simultaneously, consider all possible issues that could arise from a compromised infrastructure that is parametrising and controlling cobots. Especially in cases where hazardous substances are used in the manufacturing process or where high temperatures arise, a manipulable control component creates extreme risks.

Assess risks and determine security levels

To be able to assess risks adequately, evaluate the conditions for a certain error to arise or a specific attack to be carried out. Then, the severity of the consequences and the probability of them occurring must be assessed.

For **functional safety**, the basic functional safety standard IEC 61508 stipulates four Safety Integrity Levels (SIL 1 - 4). The Safety Integrity Level is a measure for the risk mitigating effect of safety functions to be reached. The SIL for every application depends on the extent of damage or the severity of the possible injury to be expected from the errors, the frequency and duration of the risk exposition, the probability of occurrence of the error and the possibilities to eliminate or mitigate the danger.

Sector-specific standards, e.g. 62061 for machines or ISO 26262 for the automotive industry can be used in the corresponding industry as a reference. For the assessment of the safety performance, the entire security chain must be considered, i.e. all possible errors for all components of a system.

For **Security**, the risk assessment must consider the known weak points, calculate the effort required for carrying out a successful attack and determine the severity of the consequences of such an attack. The analysis focuses on technological, infrastructural and organisational weak points e.g. user. The objective is to obtain an extensive list of the most probable and most harmful possible attacks which shows against which threats and attack vectors the product must be primarily protected.

Within the scope of the threat analysis, the risk for different attacker profiles and/or attack vectors is calculated. Potential attackers could include hackers, competitors, employees of a service provider (e.g. of a cloud provider) or an unhappy member of staff. This will result in assumptions about the procedure a potential attacker is using, the degree of motivation, the extent of the damage and the chances for success. From these aspects – means, resources, capabilities, motivation – the risk-based priorities are calculated: The primary protection of the product must fight off which attackers?

Based on that, the Industrial Security Standard IEC 62443 defines four Security Levels (SL) which are a measure for the expected threat to a system by attacks. SL-1 applies to the threat of accidental impairment or manipulation due to foreseeable misuse by any user, SL-2 to SL-4 refer to targeted attacks. SL-2 applies to an attack with simple means and limited resources (average capabilities, low motivation, e.g. hobby hacker). SL-3 applies to attacks with sophisticated means and limited resources (professional hacker, cost-effective attack scenarios) and SL-4 applies to attacks with sophisticated means and extensive resources (e.g. secret services with specific knowledge).

These Safety Levels are defined in IEC 62443 both as target (SL-Target/SL-T as result of the threat and risk analysis), achievable level of protection (SL-Capability/SL-C as capability for correct implementation) or the actually achieved protection level of the entire system (SL-Achieved/SL-A). To obtain a certain protection level LS-C for a component, the component manufacturer must consider certain functional and non-functional security requirements during development and guarantee an IT-secure development process. The integrator, e.g. machine producer, will achieve a certain protection level SL-A in a concrete project with the entirety of the used components (this SL-A must reach at least a SL-T defined by the operator). Furthermore, the standard includes the maturity level of the security processes of a company – security level of the technical solution and maturity level of the processes combined result in the Protection Level (PL-1 to PL-4) of a system.

4.4 Measures to Mitigate Risks

Knowledge of the risks, threats and hazards helps in defining suitable measures to mitigate risks for every component of the system. This includes both preventive measures which prevent all errors and attacks and measures helping to intercept errors or detect and fight attacks. For functional safety, there are measures from the listed safety standards: for security, use IEC 62443, the BSI basic protection documents and instructions by industry associations (e.g. VDMA, VDI, ZVEI) or the platform Industry 4.0. The platform Industry 4.0 is a network with experts

from the German Federal Ministries of Education and Research, of Economics and of Science.

However, the interactions between safety and security aspects have not yet been considered exhaustively in these instructions. Nevertheless, it is very important to analyse this relationship, both on the risk level (security flaws of safety systems, possible effects of security attacks on functional safety, etc.) and on the level of the measures (e.g. effects of security measures on the availability of safety functions).

Module and system tests and network penetration tests will help to determine whether defined measures have been implemented correctly and whether they are effective. Furthermore, development and production processes and the safety and security measures taken must be documented carefully. Compliance with IEC 62443 and ISO 27001 and IEC 61508 or sector specific standards can be tested and certified, e.g. by the TÜV. This concerns compliance of safety standards for development and production processes, systems or system components incl. security functions or SIL.

4.5 Security Management

With Security & Safety by Design, manufacturers and operators of IIoT products can guarantee that their devices and applications offer state-of-the-art protection and fulfil all applicable safety and security standards. But things don't end at market introduction. A continuous and consequent security management must guarantee that security threats are recognized quickly and security flaws are closed immediately. For a number of components cooperating in the interconnected value chains of Industry 4.0, this is not a trivial issue. Due to liability reasons, manufacturers are requested to carefully observe new developments in standards and provisions.

Platform Industry 4.0 recommends establishing an Information Security Management System (ISMS) for this purpose. BSI standard 200-1 describes the structure of such a system with the four components security process, resources, employees and management principles. The security process as a central element of the management system is designed as a cyclic process according to the PDCA model (Plan, Do, Check, Act). In connection with Industry 4.0, an integrated approach is required that includes all company departments with office IT, product development and production IT.

To implement an ISMS, clear roles and responsibilities must be defined. In addition to a "Chief (Information) Security Officer (C(I)SO)", platform Industry 4.0 recommends appointing an "Industrial Security Officer" who makes sure that security is managed across all departments and that the "silo mentality" connected with the organisational separation of office and production IT will be overcome.

5 NewTec Supports "Security & Safety by Design"

Manufacturers and users must guarantee an high level of security in their IIoT systems. If they lack know-how and resources, they must establish it or seek help from experts.

As a technology and security specialist, NewTec supports companies in implementing security and safety requirements for Industry 4.0: Safety and security experts will carry out detailed hazard, threat and risk analyses, deduce required measures and help with the implementation, if required. For many requirements in the IIoT and cloud environment, NewTec provides ready solutions that can be customized to the individual requirements of the particular user.

Extract from the NewTec portfolio

5.1 NTSafetySolutions

Product development
according to applicable safety standards, e.g. IEC 61508, IEC 62061, ISO 26262, ISO 13849

- Design and implementation of safety-relevant, complex electronic systems
- As consultant or full-service contractor
- Product development for the entire life cycle of your product
- Incl. industrialising and series support, certification, and continuous improvement of existing systems

Platform solutions
incl. IP cores for quick realisation of functionally safe solutions up to SIL 3

- NTSafeDrive: Platform to control servo drives with extended safety functions
- NTMicroDrive: Compact software and hardware solution for driving electric motors up to 10W safely
- NTSafePLC: High-performance PLC platform for industrial controls up to SIL 3 / PL e Cat 4
- SafeFlex: Developing environment for FPGA based safety solutions with evaluation board

Consultancy & Services

- Hazard and risk analysis
- Error analysis (FMEA)
- Strategy consultation: Avoid errors, control errors

Know-how transfer

- Individual trainings, workshops and seminars
- Methodology of safe product development and manufacturing according to good practices

5.2 NTSecuritySolutions

Security process consultation and threat / risk analyses
according to applicable standards such as IEC 62443

- Process consultation in IT security
- Planning IT security
- Weak point analysis
- Trainings and workshops IEC 62443
- Consultation IEC 62443

Security strategy consultation
for system protection

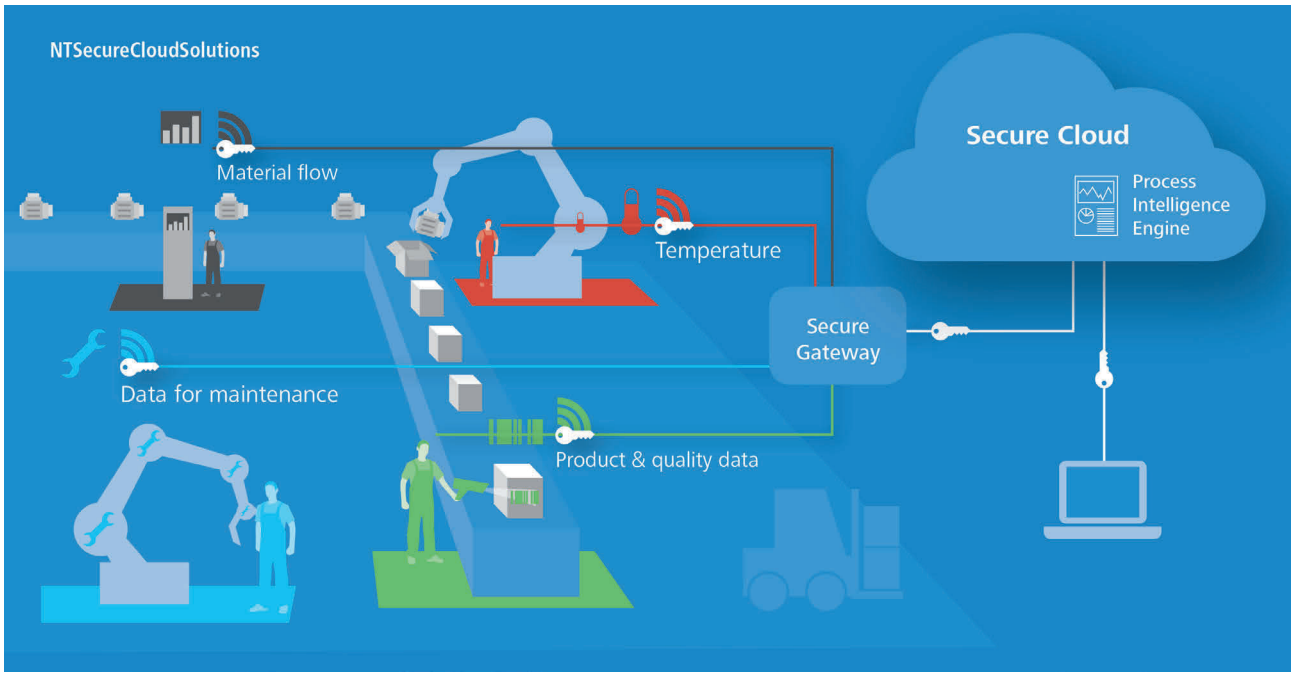
- Development of security concepts
- Secure data transmission
- Cryptography procedures
- Access control procedures
- Trainings and workshops
  - Identification of protection targets
  - Threat and risk analysis
  - Determination of security requirements

Verification and validation
of the effectiveness of the security measures

- Penetration tests
- IT security robustness test (DoS, CRC Violation, ...)
- Statistic code analysis (with e.g. poly space)
- Validation of the requirements and the security concept
- Evaluation of IT security
- Recommendation of actions

Security monitoring
of systems in running operation

- IT incident management in the security product life cycle
- Continuous identification and assessment of threats and weak points



5.3 NTSecureCloudSolutions

NTSecureCloudSolutions includes IoT solutions and services in development that support connection with other solutions from the safety and security portfolio of NewTec. These support companies in implementing products and services in the cloud environment and help integrating heterogeneous services, technologies and processes into a secure cloud architecture.

Solutions

The core of NTSecureCloudSolutions is a turn-key platform with certified, secure hardware and software solutions with essential security features such as end-to-end encryption, certificate management, policy management and wireless device updates. Included in the final expansion:

- NTSecureDevices: IoT terminals / sensor nodes
- NTSecureGateway: IoT gateways for the secure cloud connection
- NTSecureCloud: Modular system for secure cloud application (secure application framework)

Services

- IoT business model development
- Security consultation and trainings
- Safety consultation and trainings
- Managed services concerning secure operation.

NewTec is a leading design house providing customised system and product solutions in medical technology, industrial systems, automotive & transportation: NewTec provides guidance to its customers throughout the product lifecycle. The team of experts develops electronic products from the conceptual idea to industrialisation, including licensing.

Founded in 1986, NewTec looks back on more than three decades of project experience in developing complex hardware and software systems with a focus on functional safety and embedded security. NewTec aims to ensure the safety-relevant functionality of a system at all times as well as to protect embedded systems from sabotage attacks and manipulations from the outside.

Today, NewTec has more than 180 employees at five locations in Pfaffenhofen/Roth, Freiburg, Mannheim, Friedrichshafen, Bremen and Taipei/Taiwan.

Creating safety.
With passion.

NewTec

NewTec GmbH
Buchenweg 3
89284 Pfaffenhofen a. d.
Roth
Germany
Tel.: + 49 7302 9611-0
Fax: + 49 7302 9611-99
info@newtec.de
www.newtec.de

F807_0718