

Creating safety.
With passion.

NewTec



NTSecuritySolutions

Services and solutions for the development
of secure components and systems

www.newtec.de

Security for Industry 4.0 and IoT – for the entire product life cycle

The demand for Industrial Security is growing. Increasing integration of embedded system within the framework of IoT and Industry 4.0 comes with increased vulnerability for cyber threats. Manufacturers and suppliers must act to remain competitive and to avoid liability risks.

Nowadays, security is an important quality feature of integrated systems and components. The resulting security requirements for component manufacturers, system integrators and operators (OEMs) are listed in the international series of standards 62443. Companies affected by this will face the following challenges:

- 1. Security from the start:** Already in the development stage, security must be integrated into the system architecture (Security by Design), since subsequent security measures for insecure architectures are costly, complex and ineffective in the long run.
- 2. Security over the entire life cycle:** Securing integrated systems is not finished when the development has been completed – it must be guaranteed during operation, even for new threats and operational scenarios.
- 3. Complex, diverting requirements:** Security requirements often contradict functional and safety requirements.

The solution: an integrated security-management-process which synchronises all areas of product development (system, security and safety development).

NTSecuritySolutions

With NTSecuritySolutions, NewTec supports component manufacturers, system integrators and operators (OEMs) with securing their products and systems – from design to operation.



Integrated process consultation

Security management process according to 62443-4



Security services

Consulting: Analyses, concepts, trainings
Development support: System integration/engineering
Operational support: Secure operation

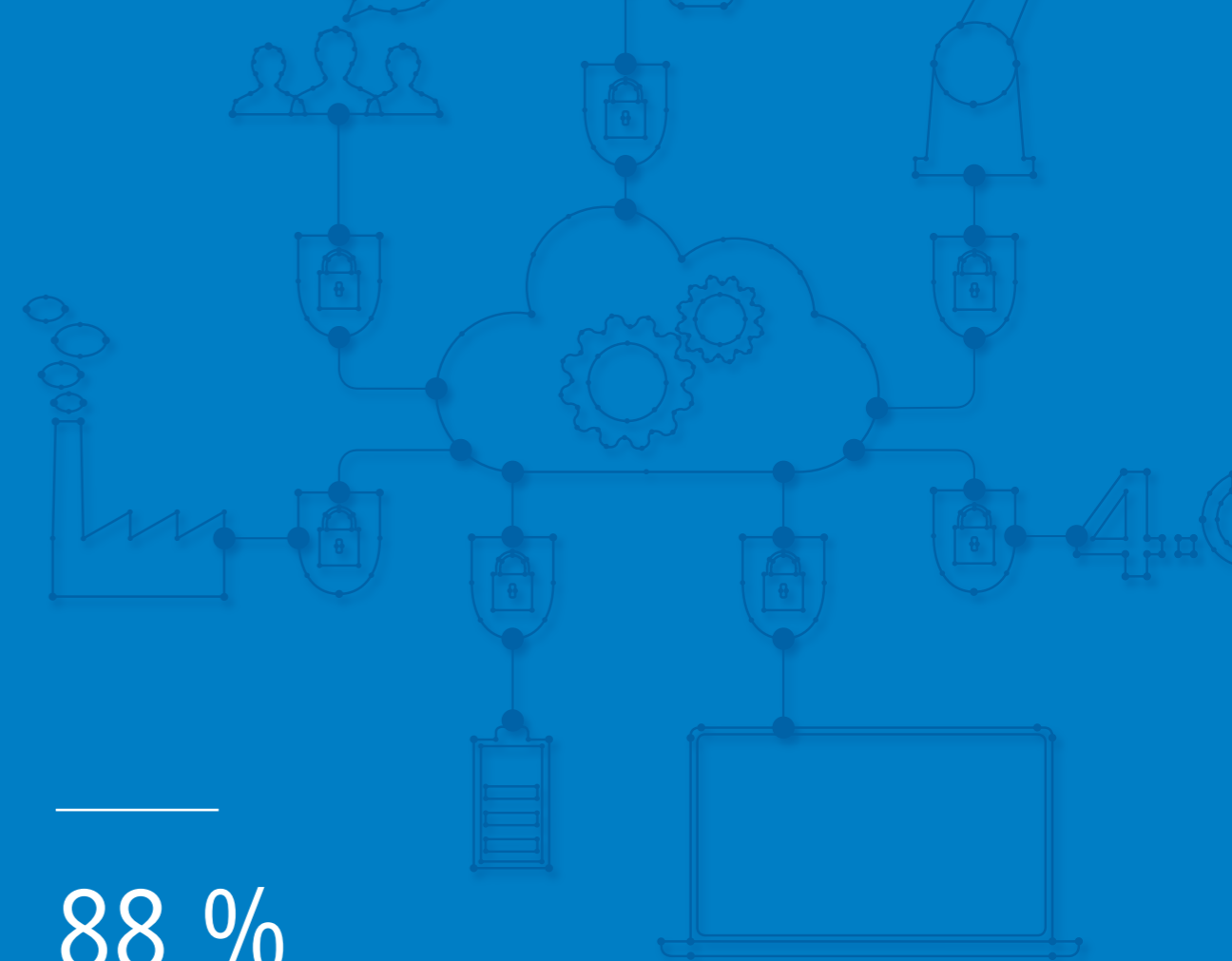


Hardware platforms (NTSecureCloudSolutions)

System components for secure IoT solutions
(sensor nodes, gateways, cloud services)

Your competitive benefits

- **Strengthening your market position** by professional security processes and secure systems
- **Accelerated development** thanks to ready-to-use IoT platforms (sensor nodes and gateways)
- **Robust systems** that can be operated securely even in years to come
- **Fit for the future** and securing your investments



88 %

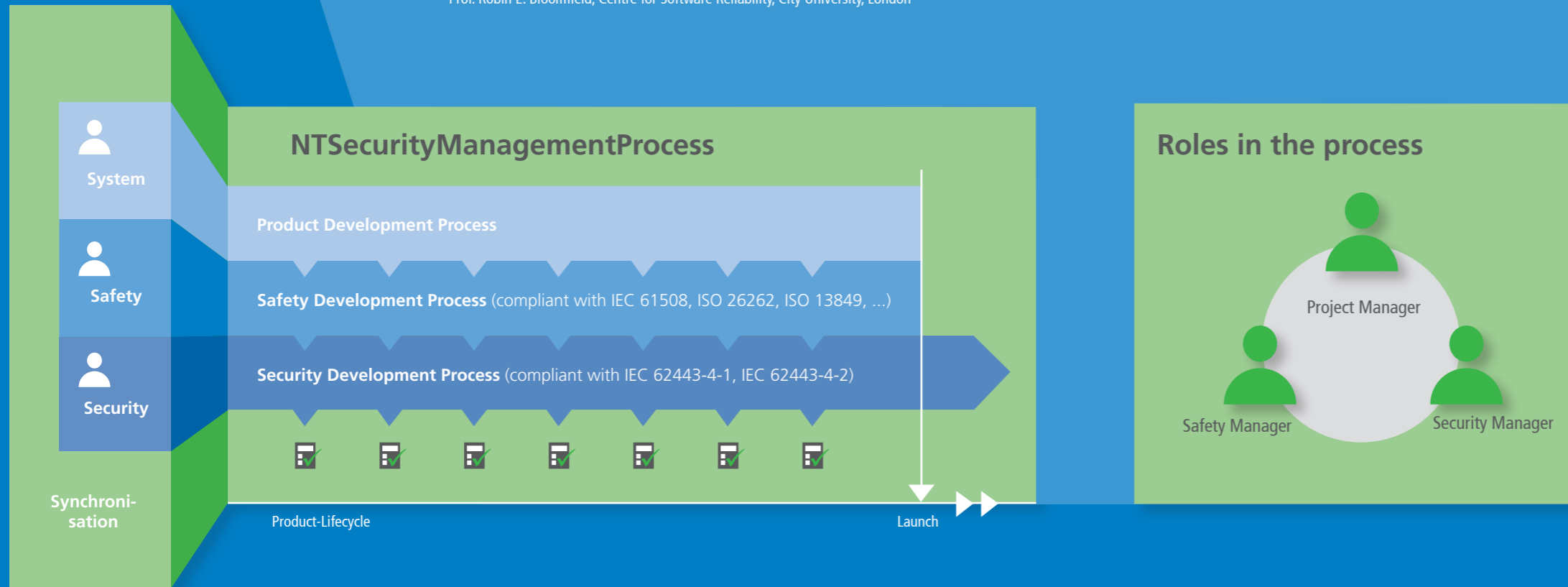
of the companies worry that digitalisation will increase security threats

Cyber security for companies

- Threat potential: 76% of the institutions consider cyber threats as relevant risks for their operability.
- Digitalisation increases the threat of becoming a target: 88% expect an increase in vulnerability to cyber crime due to digitalisation.
- Real threat: 43% of big enterprises and 26% of SMEs have been hit by cyber security incidences in 2018 (detected incidences)

Source:

German Federal Office for Information Security, Cyber Security Survey 2018 (IT security experts from 1093 institutions)



NTSecurityManagementProcess

- Objective: Support of secure product development with focus on embedded security
- 3 roles: project manager, security manager, functional safety manager
- 7 synchronisation points at strategic steps in the project life cycle: from initial project planning (Agreement on Scope) to design, implementation and tests up to operation (regular security reviews)
- Checklists to compare all requirements and documents in order to identify contradictions and test for completeness/availability
- Based on the series of standards IEC 62443 and 61508

Integrated process consultation: NTSecurityManagementProcess

Synchronise your development, safety and security processes!

NTSecurityManagementProcess - our proven security management process - completes your product development processes. The structural approach combines all requirements for system development, security and safety to safeguard system implementation. We can train and advise your staff on how to implement the security management process or we can join your project team on site..

Diverting requirements

When developing safe products, requirements from different areas must be implemented which may partially contradict each other.

Security vs. functionality:

Security requirements may compromise functionality and operability. For example, it is not always easy to combine usability and comfort with the required access restrictions.

Security vs. safety:

Functional safety and IT security are strongly interconnected in integrated systems: hackers or malware can cause malfunctions, emergency exits can grant access to unauthorised persons or closing a security loophole with an update can change a system certified as „safe“.

Structured approach

To resolve these contradictions, it is required to synchronise all parts of the product engineering process – system development, security development and safety development, if required. An integrated security management process is required for this purpose, which safeguards the implementation of all requirements over the entire product life cycle.

We have defined synchronisation points at important steps in the process, where existing contradictions can be made visible. In close cooperation with the stakeholders in all relevant areas, we resolve these contradictions and adapt the corresponding development phase accordingly.

Our experienced consultants follow proven best practices, the specifications by the German Federal Office for Security in Information Technology (BSI) and the international standards for safe system development IEC 62443 (Security) and IEC 61508 (Safety). We have coordinated our security management process in close cooperation with the TÜV to simplify and speed up the certification process.

NewTec's security and safety experts consult and support manufacturers, system integrators and operators of integrated products in developing secure systems and implementing structured security management processes

Added value for your processes

- Processes compliant with IEC 62443
- Basis for conformity declaration or certification
- No liability risks
- Structured controlled process
- Transparency of development steps
- Higher product quality





Security services and platforms: From system concept to safe operation

NewTec offers a wide selection of services and platform solutions for security engineering which cover the complete life cycle of your secure product. Our offer includes services, platform solutions, trainings and consultation for all aspects of security – from risk and specification analyses, security concepts and tests for toughness and weak points, via support for the technical implementation of all requirements up to continuously securing your system during operation.

Your benefits

- Highly secure IoT applications with hardware-based end-to-end encryption
- Shorter time-to-market
- Cost savings for development and certification
- Flexibility due to numerous communication interfaces

NewTec security services

Expert services and know-how transfer

Security requirements for a product must already be analysed and considered in detail when designing the product (security by design). Our expert services help you in developing secure products effectively:

- System analyses (danger, risk and requirement analyses, static code analyses)
- Security concepts
- Trainings for developers and security managers
- Security reviews
- Interim security manager
- Penetration tests (internally/externally)
- Security toughness tests

Engineering and integration support

As experts for the safe system development with extensive safety and security knowledge, we are happy to support you with individual engineering services:

- System development
- Security & safety engineering
- System integration

Managed services for securing the operation

The secure operation of integrated products and cloud-based applications requires continuous attention to new cyber threats. Individual operational concepts and managed services by NewTec will support you in:

- Continuous check for weak points due to new threat situations
- Continuous check for conformity with current security standards
- Continuous maintenance of the desired level of protection
- Incidence management
- Obsolescence management for security-related system parts

NTSecureCloudSolutions: System components for secure IoT solutions

Our hardware platforms with end-to-end encryptions help you launch secure IoT systems more quickly and with minimum development efforts.

NTSecureNode

Secure nodes connect your existing devices with the highest level of security. They collect, buffer and filter data, merge it and provide it to cloud services via secure communication paths. Stored data can be encrypted immediately for a particular target which enables direct end-to-end encryption. In the other direction, these transmission paths can be used for configuration, control and update of applications. NTSecureNodes create wireless connections to Secure Gateways via Wifi, BLE or NB radio or directly to a secure cloud service via NB IoT.



NTSecureNode BLE100



NTSecureNode NB100

NTSecureGateway

The IoT Gateway is usually used to connect secure nodes with local services or cloud services. Due to multiple field bus options, it can also be used to connect current devices with cloud applications for secure detection, processing and transmission of data (e.g. sensors). Detailed configurable end-to-end encryption and anonymisation will reliably protect confidential data. NTSecureGateway supports ethernet, BLE, NarrowBand IoT and Wifi. Various radio standards are available as extension modules.



NTSecureGateway



Shield96

NTSecureCloudConnector (SCC)

The software stack SCC offers a reliable communication channel to secure cloud services while accounting for bi-directional authentication and stable, powerful encryption. SCC is compatible with various security elements, TPMs and HSMs. Apart from a highly secure connection to the NTSecureCloud, SCC will connect to IoT platforms of other manufacturers, such as Siemens Mindsphere, AWS IoT, Google Cloud IoT-Core and MS-Azure IoT-Hub.

NTSecureCloud

NTSecureCloud is an adaptive, highly secure database often used to provide encrypted or decrypted data for digital services such as internet applications, ERP or MES systems. In addition, it can be used as a secure cloud proxy to provide data to other cloud services.

NTCloudServices

NewTec operates as a full-featured system integrator for safety and security solutions. Apart from the basic components for secure cloud solutions, NewTec offers cloud-based data analysis and a safe user framework for platform-independent client/server applications. Typical applications are:

- Pattern detection
- Image processing
- Maintenance as required/preventive maintenance

Third-party suppliers cloud services

Siemens Mindsphere

NewTec is member of the Siemens Mindsphere Gold Partner program and operates as hardware integration partner for secure Mindsphere applications.



Compatible cloud suppliers

NewTecs secure cloud components support the cloud authentication and links with AWS IoT, Google Cloud IoT-Core and MS-Azure IoT-Hub.



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