CYBER SECURITY

CYBER SECURITY

We recognize that any vulnerability weakens the entire system, much like the weakest link in a chain.

Security in breadth covers a wide range of protective measures, while security in depth ensures thorough defense.

IN MASCHINENFABRIK REINHAUSEN AUTOMATION PRODUCTS & DIGITAL SERVICES

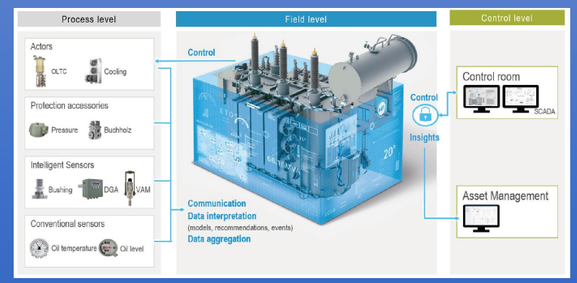
Maschinenfabrik Reinhausen (MR) from Germany is a company specializing in power engineering equipment which is used by our customers to build and operate transformers. In the realm of Cyber Security & critical infrastructure, safeguarding our systems is of ultimate importance. We recognize that any vulnerability weakens the entire system, much like the weakest link in a chain. Security in breadth covers a wide range of protective measures, and in addition security in depth ensures thorough defense. This principle applies not only to product development but also to day-to-day operations of our products in the field.

Photo: Maschinenfabrik Reinhausen

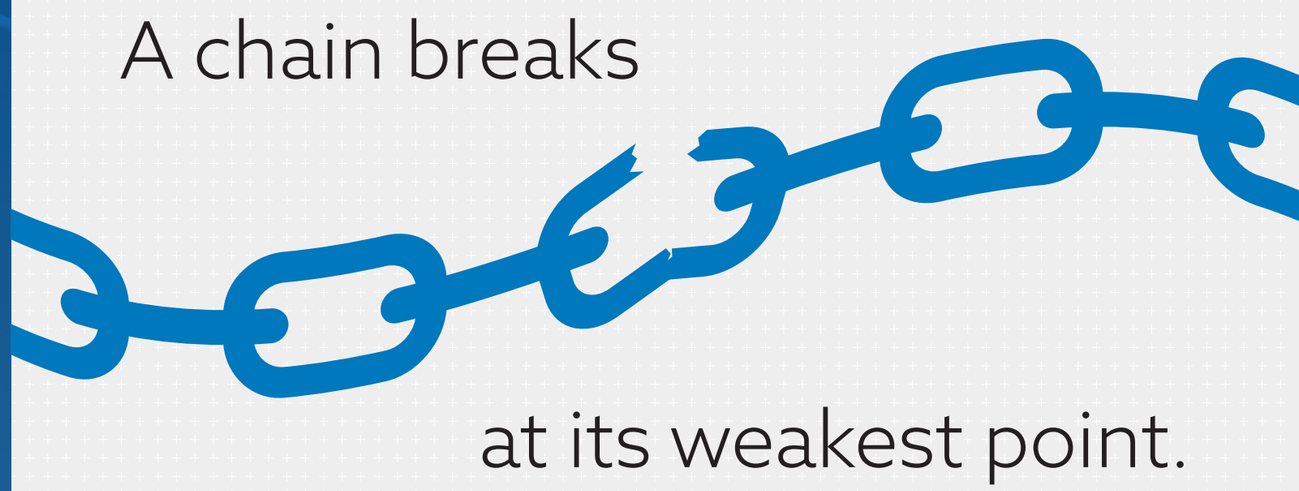
Our security journey begins at the development process, where security takes center stage. From design considerations to development practices, we explore how to create secure products that withstand real-world challenges throughout their lifecycle. In this article, we provide a detailed account of our vulnerability management process that is important when products are in operation. Specifically, we highlight its implementation for two critical components: the ETOS® transformer automation system as shown in Box 1, and our myReinhausen customer portal and TESSA APM as digital services.

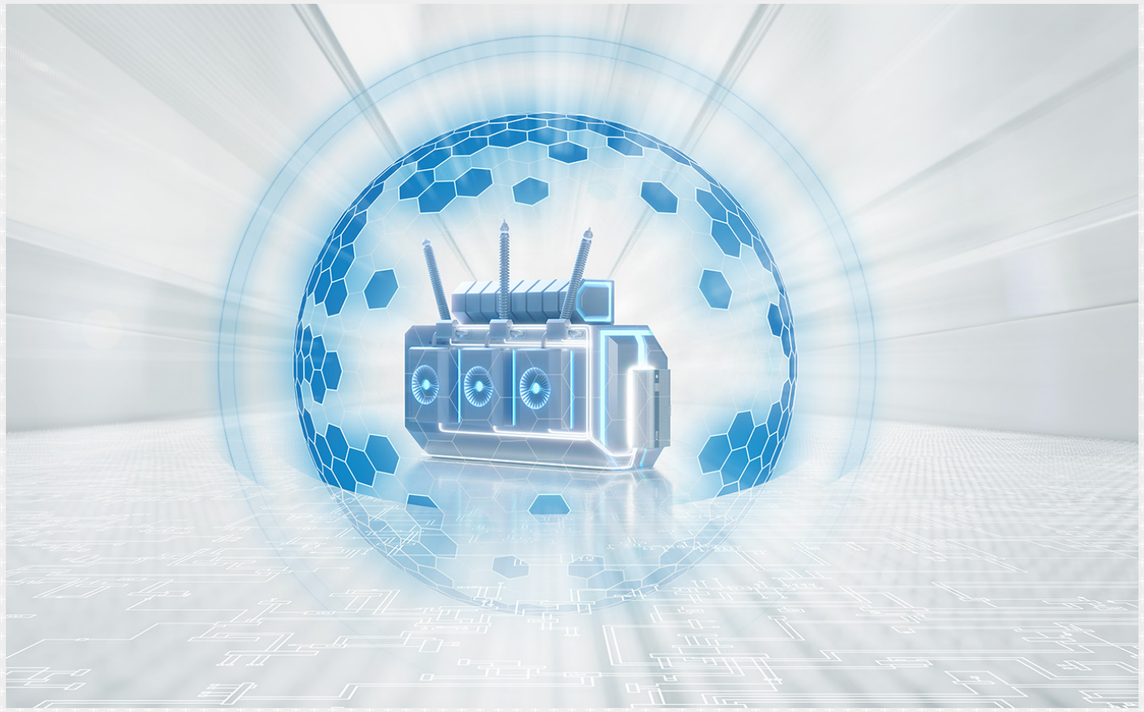
Box 1: What is ETOS®?

Acting as the bridge between the physical process and the control systems, the field level incorporates sensor information that monitor the transformer's condition and actuators that control its operation. ETOS® plays a vital role at this level, gathering data from various sensors and applying algorithms to analyze and interpret it as well as ensuring an efficient control of the temperature and the voltage. To suit different utility requirements, it supports the modular integration of functions in the areas of control, regulation, monitoring, and the tap-changer drive. By seamlessly integrating sensors, communication devices, and advanced algorithms, ETOS® creates a digital twin of the transformer. This digital twin serves as a comprehensive virtual representation of the transformer's condition and performance, providing operators with unprecedented insights into its health and operation. This holistic approach empowers operators to make informed decisions about maintenance schedules, optimization strategies, and overall asset management.



Concept of an intelligent transformer with ETOS®





LEGISLATION

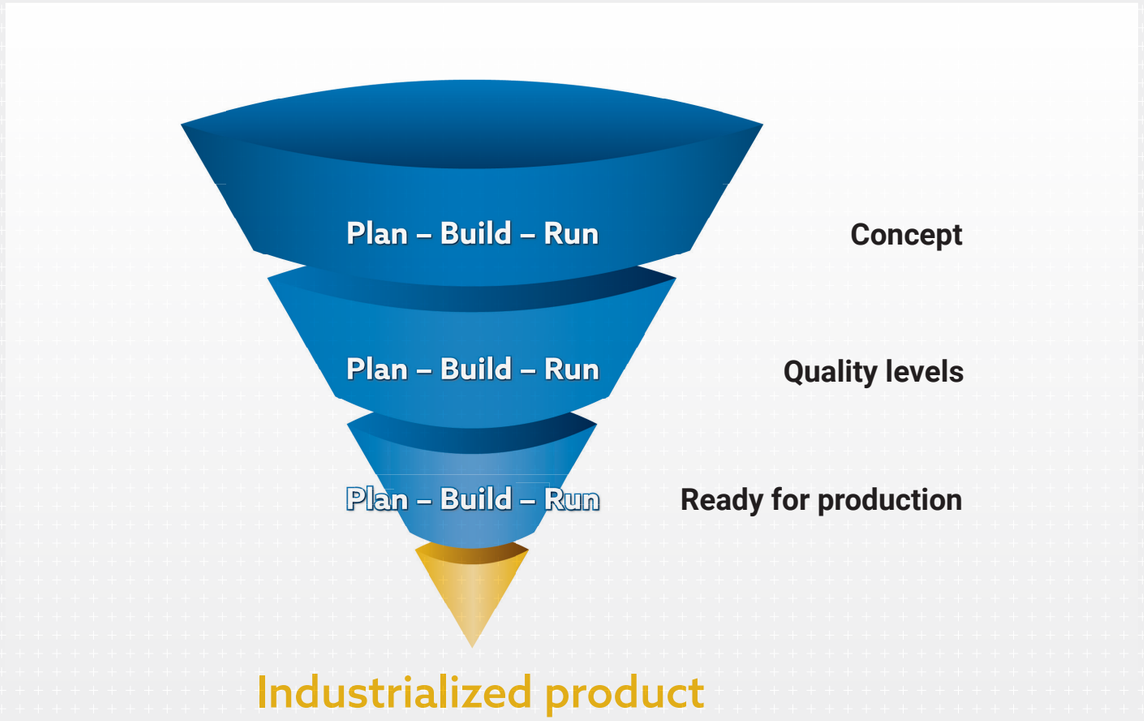
Alongside established security practices, there's a noticeable surge in regulatory and legal demands. Examples include the EU General Data Protection Regulation (GDPR), the EU Network Information Security (NIS-2) directive, and the forthcoming EU Cyber Resilience Act. These regulations particularly target products integrating digital components and their cyber security.

Moreover, existing mandates such as the US NERC CIP for the energy sector in the United States and the NIST Cybersecurity Framework further underscore the importance of adherence to security protocols. With such a diverse array of regulations, it is important to compile them into a unified framework for Information and Cyber Security. This framework serves as a comprehensive guide to pinpoint requirements and mitigate potential risks effectively and on the spot in the form of our Information Security Management System (ISMS), which is based on ISO 27001. In essence, it provides a structured approach to navigate the complex web of regulations and safeguard against emerging threats towards selected services and products with digital elements.

DEVELOPMENT PROCESS

Product funnel

The components introduced here adhere to the principle of "security by design." This means that potential cybersecurity threats are identified early, during the planning phase, and are factored into implementation, ongoing operation, and product maintenance. But MR doesn't easily release fully developed products onto the market in one go. Instead, we use our product funnel. This means that concepts undergo several iterations, progressing from the initial idea to a functional model, through various quality checkpoints, and from a pilot series to full-scale industrialization. Throughout this process, both the product and its manufacturing methods are continuously refined. The following image illustrates those two concepts.



Considering cybersecurity from the start does not necessarily mean all measures are immediately implemented. For instance, while a prototype might demonstrate functionality, aspects like user roles and access rights might only become mandatory at later stages of development. This approach is an integral part of our Product Lifecycle Management (PLM) strategy, ensuring that cybersecurity is an intrinsic consideration at every step of the product's evolution, from conception to market readiness.

Security in the Software Development Life Cycle (SDLC / SSDLC)

Security is a part of the whole Maschinenfabrik Reinhausen GmbH Software Development Life Cycle (SDLC) and in particular the Security SDLC (SSDLC) for products incorporating digital elements. With phases encompassing planning, building, and running, MR has established a written policy to embed security into development and operation. An internal design rule for IT-Security aids project managers in defining cybersecurity measures that need to be implemented, while quality management ensures the measures that were defined during the design phase are implemented to guarantee operational security measures as products mature for market deployment. This structured approach ensures that cybersecurity is seamlessly integrated into every stage of product development at MR.

Supply Chain Security

At MR, ensuring robust security standards is a fundamental aspect of our product development. This commitment extends to our suppliers, especially those providing software components that are integrated into our products. Recognizing the role of our suppliers in maintaining overall security, we engage them from the beginning of security management processes. This collaboration is essential to establish and uphold supply chain security, guaranteeing that our products meet the highest standards of cybersecurity. By involving suppliers early on, we can proactively address potential security risks, reinforcing the integrity and reliability of our offerings throughout the supply chain.

Photo: Maschinenfabrik Reinhausen

PROTECTION

For the products introduced here, we approach cybersecurity with a focus on both breadth and depth. We adhere to the ISO 27001 standard to ensure a broad coverage of security measures across our operations. Additionally, we implement Cybersecurity risk management methodologies based on our Security Software Development Life Cycle (SSDLC), the concepts in the upcoming EU Cyber Resilience Act (CRA), and e.g. the IEC 62443 standards to dive deeper into specific areas of vulnerability. The following Image shows our overall SSDLC, how our Secure Development Policy gives general guardrails that are then put into action by our threat and risk analyses in the various phases.

Aspect	Plan	Build	Run	Secure development policy Security by design	
IT-security	– Involve MR ProductCERT for Cyber-security Risk Assessment (CS -RISK) – Data classification – Login – authentication – Access control – Autorisierung – Encryption – Cryptography – Logging – Disaster reaction & BCM – Data protection – Secure operations	– Secure codierung – Pentest – Involve MR Product -CERT for open risks	– Change management – Capacity management – Management of vulner -abilities and IT software updates	**Cyber security risk assessment**	**Product lifecycle management**

Understanding the interplay between attack surfaces and vulnerabilities is crucial in our approach to cybersecurity. By assessing and managing our attack surfaces, we can better identify and address potential vulnerabilities within our products. This proactive approach is further reinforced by robust vulnerability management processes, which are mandated by the ISO 27001 standard and by upcoming regulations such as the EU CRA.

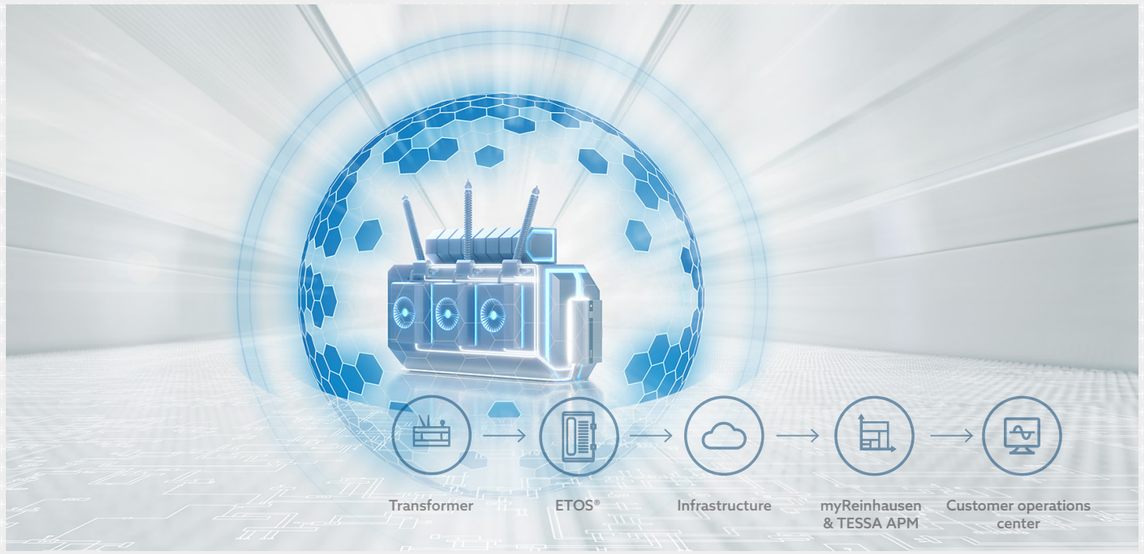


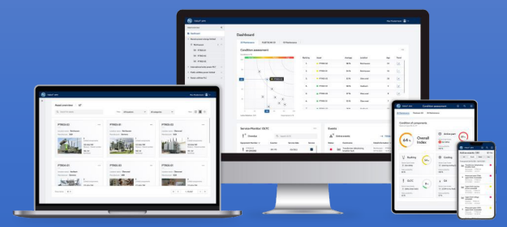
Photo: Maschinenfabrik Reinhausen

EXAMPLE OVERVIEW

In our technical environment, we have two distinct examples illustrating our approach: ETOS® serving as an edge device with embedded hardware development, and the myReinhausen customer portal with TESSA® APM for Asset Performance Management as shown in Box 2, functioning as software and digital service endpoints for data collection and analysis. The image on page 46 provides an overview of the data flow within this setup. Detecting vulnerabilities and implementing security updates are essential tasks in both scenarios, demonstrating our commitment to maintaining robust security measures across our technical landscape.

Box 2: What is TESSA® APM?

"TESSA® APM, short for Asset Performance Management, is a comprehensive platform designed to provide an insightful overview of transformer fleets. By leveraging advanced algorithms and the latest standards, TESSA® APM stores and analyzes inspection and sensor data in a centralized database, enables automated evaluations and provides actionable recommendations. Users can generate individual assessments and define necessary actions with analytical support in the expert cockpit, optimizing their maintenance strategies. Seamlessly integrating with ETOS®, TESSA® APM detects irregularities early on and facilitates timely life-extending measures. Delve into the digital realm of MR through "myReinhausen," MR's central digital customer platform, to access TESSA® APM and explore additional services tailored to support your needs within the context of MR products and services."

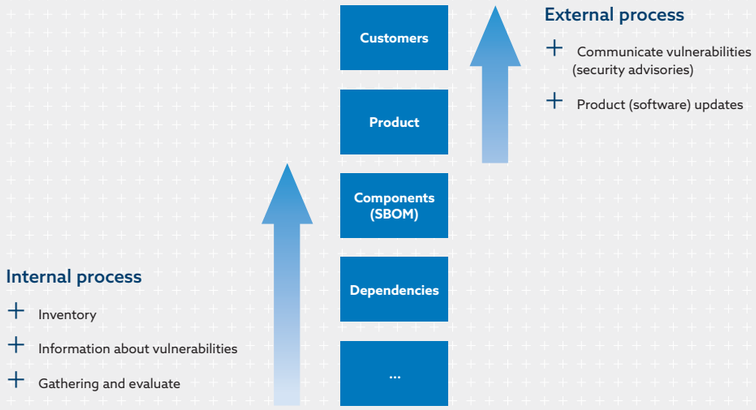


EXAMPLE 1: Vulnerability Management of MR ETOS® as Embedded device

In the development of ETOS®, we rely on a Linux-based System-on-Chip (SOC) architecture, incorporating various third-party components, hardware that was developed in-house as well as 3rd party sensors. The process of vulnerability management is shown in the image below. To ensure security integrity, we utilize our Software Bill of Materials (SBOM) as a comprehensive component list, which is used in the identification of vulnerabilities.

Critical to our security measures is the US NIST's National Vulnerability Database (NVD), serving as a one of the sources for vulnerability information. This database includes Common Vulnerability Enumerations (CVE) as unique identifiers, Common Platform Enumations (CPE) for component matching, and Common Vulnerability Scoring System (CVSS) scores for assessing vulnerability severity and impact in the target environment. Our CVE Search Server consolidates this data, continuously detecting new vulnerabilities and generating Jira tickets for immediate action.

Our vulnerability management process consists of both an internal as well as an external process. The internal process starts with weekly evaluations of newly discovered vulnerabilities. In our decision-making process, low to medium vulnerabilities are addressed in our semi-annual software releases. High or critical vulnerabilities are prioritized for immediate resolution and are accompanied by additional risk management actions. This is shown as part of external process from the following image. The external process and the corresponding communication strategy involves issuing security advisories on our webpage and directly contacting customers if appropriate.



This proactive approach ensures that not only the design and implementation of ETOS® remain secure, but also emphasizes the importance of providing software updates to devices in the field, accessible through the myReinhausen customer portal.

EXAMPLE 2: Vulnerability Management of myReinhausen & TESSA® APM as Digital Service platforms

In managing vulnerabilities for our myReinhausen portal and the TESSA® APM platform, MR follows a method similar to that used for ETOS® as shown in the above image. However, due to differing development environments and customer deployments, there are slight variations in the process. While ETOS® operation occurs at the customer/operator site, our software portals operate within MR's own data centers and a limited number of customer sites, which simplifies software updates. Nevertheless, software component analysis and vulnerability detection remain necessary. These tasks are facilitated by a commercial application that analyzes software components, identifies vulnerabilities and their potential impact, and suggests updates for these components if available, as shown in the lower-left part of the above image.

Updates for the portal software are conducted in fixed development cycles multiple times a year to introduce new features. Security enhancements are implemented based on their urgency, either through regular releases or as emergency updates occurring between regular cycles. This proactive approach underscores MR's commitment to maintaining the integrity and security of our software solutions. It ensures that our customers can rely on robust and up-to-date systems, enhancing their overall experience and satisfaction with our products and services.

PRODUCTCERT AS PSIRT

Maschinenfabrik Reinhausen's ProductCERT operates as the Product Security Incident Response Team (PSIRT), ensuring the implementation of product security measures. Beyond vulnerability management, the team plays a vital role in integrating "security by design" principles into the MR product lifecycle management process. This involves conducting cybersecurity risk assessments, performing vulnerability management activities, and publishing security advisories to inform our customers if necessary. Furthermore, our ProductCERT serves as the central point of contact internally as well as for customers and other third parties, facilitating effective communication, and coordination and addressing of security-related concerns.

CONCLUSION

Cybersecurity is a top priority for Maschinenfabrik Reinhausen GmbH and our customers. Implementing comprehensive measures across all aspects and stages of product development is essential to safeguarding against potential threats. From initial design to ongoing maintenance, we are committed to ensuring the security and integrity of our products and services.

This commitment is reflected in MR's ecosystem, encompassing a range of offerings from ETOS® as an edge device to our digital service platforms myReinhausen and TESSA® APM. By integrating robust cybersecurity measures into every aspect of our products, we strive to provide our customers with peace of mind and confidence in the security of their operations.

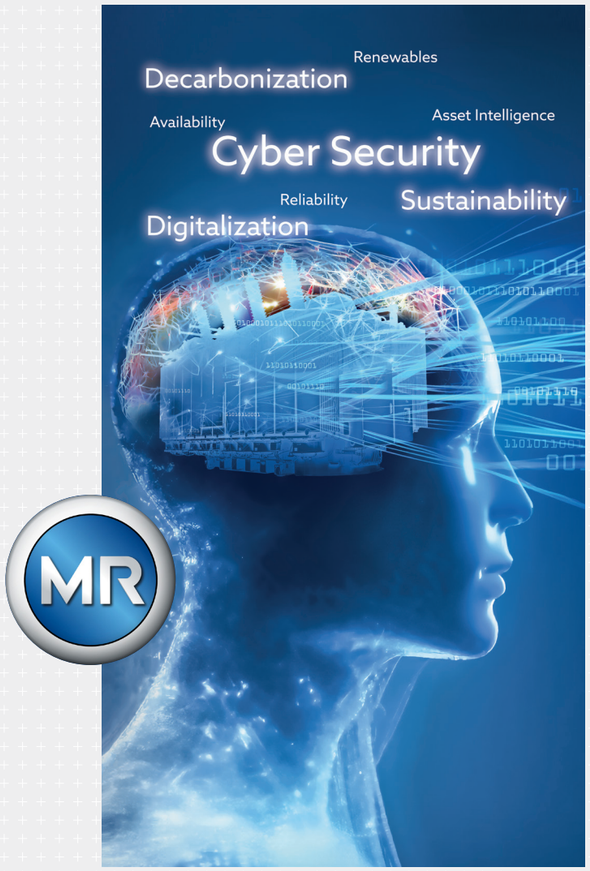


Photo: Maschinenfabrik Reinhausen

Dr. **Hubert Feyrer** has studied technical computer science at the University of Applied Sciences (FH) Regensburg. This was followed by employment as Unix/Solaris/NetBSD system administrator and as computer science teacher, both at the University of Applied Sciences Regensburg as well as Stevens Institute of Technology in Hoboken, NJ, USA. After receiving a PhD in Information Science from the University of Regensburg start as developer of hard-and software as well as network and security solutions, with later promotion to IT manager (CTO). As such, performing security consulting according to ISO 27001 and later changing into the automotive sector as Chief Information Security Officer (CISO). Recent occupations include working as CISO for one of Germany`s largest process-and people service provider and a major German car manufacturer, currently responsible as Cyber Security Expert for a supplier of the energy sector.