Source: ONTRAS

Safety plus cyber security equals maximum protection for critical infrastructure

Words: Andreas Michael, Michael Pfeifer, Jens Gerlach and Sven Kalmeier

Digitalisation is bringing change, including the operation of supply networks that form part of the critical infrastructure. Current vulnerabilities demonstrate how important it is for this to be in compliance with the IT security catalogue in accordance with the German Energy Industry Act. TÜV SÜD is supporting the transmission system operator (TSO) ONTRAS by providing a new risk assessment concept that considers both safety and IT and OT security, as well as possible interactions.

Recently, the 'Log4Shell' vulnerability threatened data centers, company servers, and connected systems among others. Experts assessed its risk level at the highest possible severity. The vulnerability also affected operators of energy supply networks and other critical infrastructures (KRITIS).

To limit the consequences of this type of vulnerability, the regulator requires KRITIS companies in the energy sector to establish and maintain an information security management system (ISMS). This comprises all systems necessary to ensure secure operation and is specified by further regulations. Its applicable normative requirements are those of DIN ISO/IEC 27001, expanded by DIN ISO/IEC 27019.

The German Energy Industry Act (EnWG) also requires operators of KRITIS supply networks and/or energy systems to comply with a catalogue of IT security

requirements. Section 11 of the EnWG, for example, reads: 'The operation of a resilient and reliable energy supply network in particular also covers adequate protection from threats against telecommunication and electronic data processing systems that are needed for secure network operation. Adequate protection of operation is deemed to be provided when the catalogue of IT security requirements issued by the regulatory authority/BSI is complied with and compliance documented accordingly by the operator.'

Natural gas pipeline network

Leipzig-based ONTRAS Gastransport GmbH started working to meet the above requirements at an early stage. The company operates the gas pipeline network in eastern Germany, spanning roughly 7,700 kilometers and comprising approximately 450 coupling points. ONTRAS uses electronic data processing, in other words, information technology (IT), for the control and monitoring of its pipeline network and hardware and software for the operation of its systems, known as 'operational technology' (OT). Focal topics in this context include cyber security, protection against unauthorised access, but also safety, i.e. the protection of people and the environment.

For safety and security solutions as well as concepts to work, they need to be initiated by company management and actively applied by the people in a company. This is the case at ONTRAS. After all, for a concept to be effective, a great number of disciplines must be brought to the table and work together. Suitable protective measures for an identified risk need not necessarily come from the world of security. Sometimes simple safety measures may be suitable alternatives, such as physical access restrictions or mechanical components not accessible or modifiable via the network. What matters is keeping the overall context in mind.

Enhanced risk assessment

Traditional risk assessment methods for safety and security are separate and have no points of connection. However, the previously separate faculties are connected through the industrial practice of networking at OT level. The task is to bring these different risk assessment methods together in a holistic approach that looks at all requirements and interactions. To achieve this, Enhanced Risk Assessment (ERA) combines classical safety assessment with cyber security assessment. The approach resulted from a TÜV SÜD innovation project that merged traditional and new methods of analysis. At ONTRAS the new concept was successfully implemented into practice for the first time.

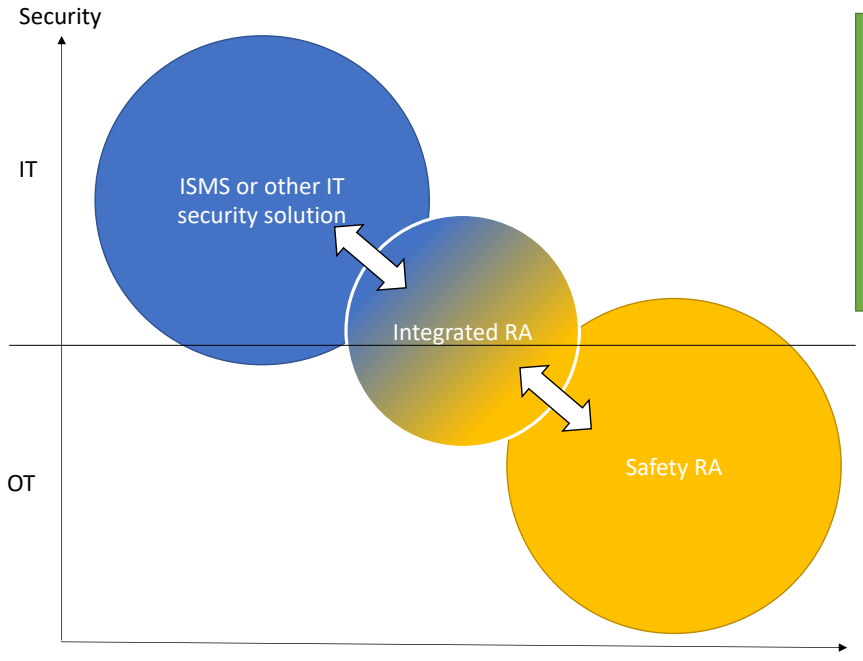
TÜV SÜD and ONTRAS used Enhanced Risk Assessment to analyse the interaction of IT and OT security and safety. The first successful application and implementation of the method concerned a gas pressure gauge and regulator system. The challenge: Cyber-risks are not quantifiable in analysis. Given this, the security level (SL) is not as predictable as the safety risk level for machinery safety.

Assessment of a gas pressure gauge and regulator system

The experts started by bringing together the existing safety risk assessment and the security risk assessment established within the scope of the information security management system (ISMS). In doing so, they focused on questions such as: What is included in the ISMS? What does safety risk management look like? In which areas is interaction already ideal? The answers were considered in the evaluation of the status quo.

Workshops were held at which the protection objective and the scope of assessment were defined, potential hazards identified and vulnerabilities analysed. After the cyber-risk analysis, multi-disciplinary expert teams worked together to choose the right solutions for effectively addressing the specific risks from the countermeasures developed. Here, it was important to ensure that the actions chosen would not give rise to new risks at other points, freedom from interference. The TÜV SÜD experts and ONTRAS applied the Enhanced Risk Assessment (ERA) method to the risk assessment performed on the gas-pressure gauge and regulator system. Training of qualified persons ensures that the knowledge acquired will be passed on in the company over the long term.

Functioning and continuous communication between the people responsible for safety and security in the company is another key factor of success. This applies in particular to cases where components need to be removed, replaced, or added. The documentation developed indicates the interfaces and possible risks that need to be taken into account. It also serves to objectify assessments in order to maintain or increase the level of protection.



The Integrated Risk Assessment is not a new management system. It combines the existing management systems from the areas of IT and OT, as well as safety and security. It also takes into account interactions.

Source: IRB-ONTRAS

Enhanced Risk Assessment (ERA) not least supports targeted communication and documentation between the safety and security representatives and does so to a level extending beyond the legal framework.

From safety to security level

All cyber-security characteristics of an OT system component are assigned to a security level. The security levels 0 to 4 as defined in the IEC 62443-3-2 standard describe the strength of an attack, from which appropriate countermeasures can be deduced.

At security level 0 no special requirements or protection are required. At security level 1 protection against casual or coincidental violation is needed. For security level 2 protection against intentional violation using simple means with low resources, generic skills, and low motivation is necessary. In the case of security level 3 protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, industrial automation control and systems, and moderate motivation is required. Finally, when security level 4 is reached, protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation is needed.

Once the experts draw their focus away from the component and machine-level back to the system as a whole, the following questions arise: Which security level does the company expect, for example, from suppliers and service providers? Which security level target (SL-T) can be achieved for a particular system or section? What capability of carrying out security functions (SL-C) does a component offer? And how high is the actual security level achieved (SL-A)? The SL-A depends on factors including the vulnerability of the software used, making fixed classification difficult. A zero-day gap, for example, can result in a sudden reduction of SL-A. Zero-day gaps are software vulnerabilities that are still unknown to manufacturers, operators or security representatives, yet may already be exploited by cyber-criminals.

Precise and cost-effective security

In the case of the gas-pressure regulator and gauge, Enhanced Risk Assessment demonstrated that suitable countermeasures to address the risks were not limited to the IT/OT domain. Cyber security benefits to some extent from simple, non-connected, and non-digital safety measures such as mechanical overpressure valves or pressure regulators. This example shows how a protective measure can be beneficial across faculties and has not resulted in any new cybersecurity risks.

Authors

Andreas Michael, Industrial IT Security Expert at TÜV SÜD Industrie Service GmbH

Michael Pfeifer, Expert for Machine Safety and Industry 4.0 at TÜV SÜD Industrie Service GmbH

Jens Gerlach, Team Lead Automation and Electrical Engineering at ONTRAS Gastransport GmbH

Sven Kalmeier, Specialist Planning/ Technology at ONTRAS Gastransport GmbH.

Enhanced Risk Assessment (ERA) not least supports targeted communication and documentation between the safety and security representatives and does so to a level extending beyond the legal framework. Risks during system operation can thus be assessed more precisely and protection levels maintained and increased reliably and cost-effectively.

www.tuvsud.com/en/industries/manufacturing/enhanced-risk-assessment

ERA: core aspects at a glance

Safety concepts can no longer be implemented without security measures.

Companies understand that security concepts are needed. Management must initiate and drive holistic risk handling approaches to prevent blind spots.

Many measures can be implemented successfully and resource-efficiently during operation.

Using Enhanced Risk Assessment, safety, and security representatives will understand their systems and technical dependencies better than ever.

Sharing the same understanding of safety and security, safety and security representatives will ‘speak the same language’.