issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Maintenance via remote access – IT-security aspects

In the last twenty years, the degree of automation of machines and industrial plants has increased ever faster and more comprehensively. In particular, the use of programmable electronic controls and computer systems with constantly increasing processing speed, complexity and extended interfaces to sensors and actuators is continuously enabling new applications. At first, IT-security at machine level has not been a problem because, although the degree of automation of machines and industrial plants has increased, the interconnection of different production plants has only occurred successively. To fully achieve the intended production goals, many machines are configured remotely via network interfaces. As a result of the increasing dynamics of networking via the internet, security aspects of industrial networking shall be considered.

The increasing use of remote maintenance (remote access facility) also leads to a higher risk of malicious interventions from outside.

These malicious interventions can not only impair the availability of the systems but also have serious consequences for machine safety. This means that security-relevant threats can become risks to safety where, for example, safety-relevant functions are corrupted. Therefore, IT-security must be kept up to date and constantly reassessed, and unauthorized access from outside must be prevented by security measures. From the safety point of view the aim of these measures is to prevent hazardous events, such as the unexpected start-up of the machine, exceeding safety-critical limits, disabling safety devices, etc.

Risk assessment

A risk assessment and suitable safety measures are crucial to ensure safe remote maintenance practices and to minimize the risk of hazards to an acceptable residual risk. The result of the risk assessment determines whether the machine manufacturer may actively access the machine via remote maintenance, e.g. to install software-updates to enable fault finding and for preventive maintenance (e.g. by identifying those elements which may fail in foreseeable time).

This includes aspects such as the safe identification of machines, on-site validation of safety functions, etc. From an occupational health and safety perspective, both the security aspects and the safety aspects, as shown in Figure 1, must be considered during the risk assessment.

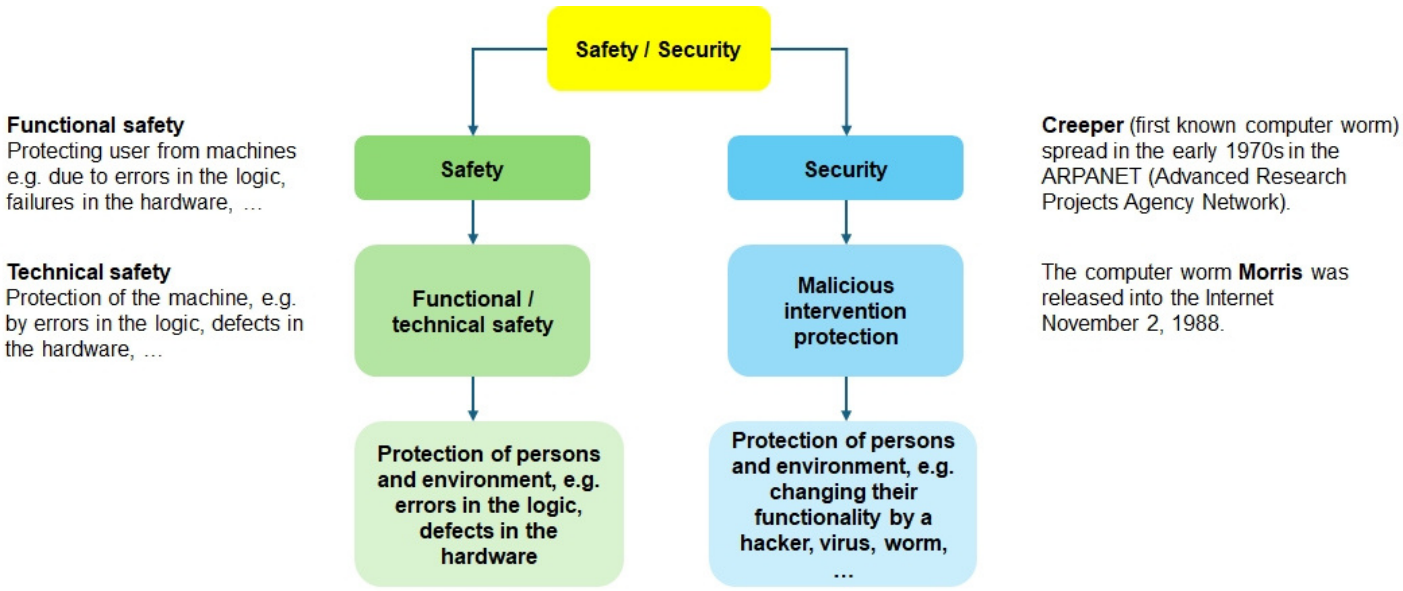

Figure 1: Definition safety – security © *Thomas Schulz Basten, BGHM*

A **comprehensive and documented risk assessment** for remote maintenance shall identify possible risks to take appropriate measures to reduce risks of security and safety. The risk assessment shall contain the following steps:

- **Determination of limits of the remote maintenance access:** Enable and perform preventive maintenance, software updates in the safety-relevant part of the control system.
- **Identification of remote maintenance access points**: Identify all elements that are accessible for remote maintenance and the required software.
- **Consideration of the safety-relevant factors:** Consider the possible effects of a malicious intervention to the safety of the machine, e.g., such as the unexpected start-up of the machine, exceeding of safety-critical limits, disabling safety devices, etc.
- **Threat analysis:** Analyze possible threats that could jeopardize remote maintenance, such as malware, unauthorized access, phishing attacks, insider threats, social engineering, etc.
- **Vulnerability assessment**: Identify potential vulnerabilities in the remote maintenance infrastructure, communication protocols and software, e.g. insecure authentication, lack of encryption, outdated software versions, etc.

- **Identification of vulnerable entry points:** Identify how attackers could potentially try to penetrate the remote maintenance system, identify vulnerabilities and how they could exploit them.
- **Compliance and legal aspects:** Consider the legal requirements in your country and industry standards that apply to your industry and ensure that your remote maintenance practices comply with them.
- **Risk estimation:** Estimate the potential harm and probability of its occurrence for the identified risks to determine the priority of the risks to be reduced.
- **Develop security measures:** Based on the risk assessment, develop a strategy to improve the security of remote maintenance, such as implementing additional control procedures, updating the remote maintenance software, training for staff, etc.
- **Assess security controls:** Review the security countermeasures in place, such as encryption, firewall, access restrictions, logging, etc., to ensure that they adequately withstand known threats.
- **Continuous monitoring and improvement:** Continuously monitor IT-systems to identify potential security incidents or new threats. Update and improve security countermeasures regularly to keep up with changing threat landscapes.

Applicable techniques to achieve secure and safe remote maintenance

To ensure adequate risk reduction for remote maintenance on machines, one or more of the following measures shall be applied as a result of the risk assessment:

- **VPN connection:** Establish a Virtual Private Network (VPN) connection between the remote maintenance server and the machine. Use only state-of-the-art VPN technology to ensure a secure transmission of data.
- **Authentication and authorization:** Implement strong authentication and authorization methods to ensure that only authorized users can access the machine. For example, use strong passwords and, if reasonably possible, a two-factor authentication.
- **Firewall, intrusion prevention system (IPS) and intrusion detection system (IDS):** Apply a firewall system in order to protect the production site. Eventually use IPS or IDS depending on the results of the risk analysis.
- **Access control:** Define clear policies on who may access the machine and what permissions they have. Limit access to only the necessary people and functions applying the principle of least privilege.
- **On-site initiation:** The remote maintenance session shall only be enabled on site by the local machine user, having direct access to the machine control devices and must be confirmed at the machine by an active action (‘from the

inside to the outside'). It shall not be possible to initiate a remote maintenance session without further confirmation on site.

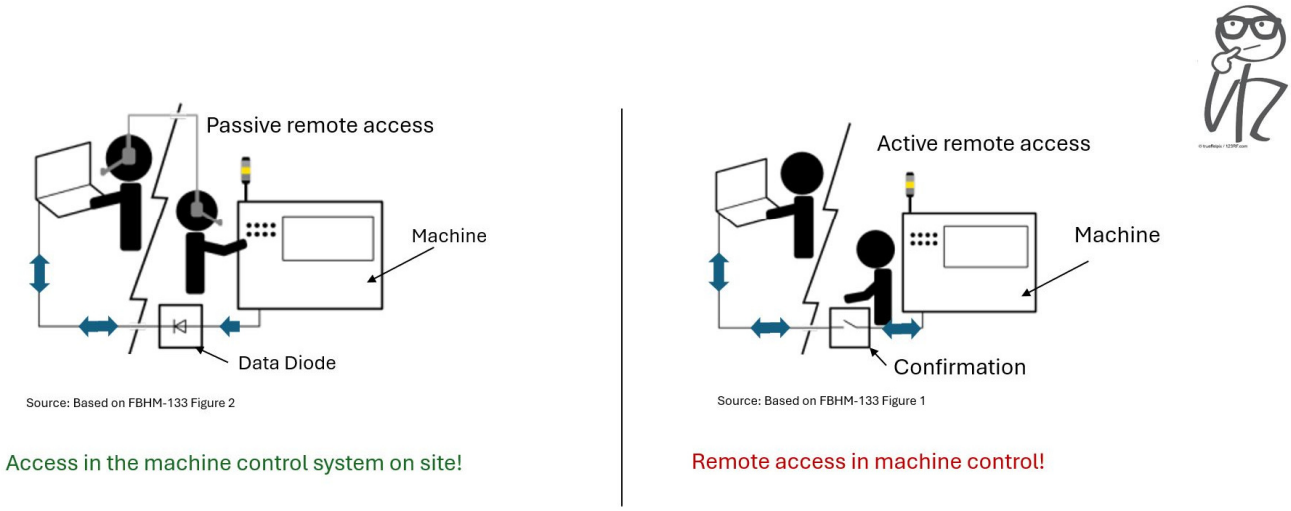

Figure 2: Types of remote maintenance session *© Jonas Stein, IFA*

- **Regular updates:** Ensure that the IT-systems and the machine control software are regularly updated with the latest security updates and patches to eliminate known security gaps and new threats.
- **Audit logs**: Activate detailed audit logs to log all activities during remote maintenance. This allows to detect and analyze suspicious activities.
- **User training:** Ensure that all users who have access to remote maintenance are adequately trained and aware of how to behave safely and minimize potential risks.
- **Time limit remote maintenance access:** Ensure that the remote maintenance access is time-limited by an initially defined timeout.
- **Local control of safety functions:** Ensure that the suspension or reset of safety functions is only possible from the local controls.
- **Local validation of safety functions:** Modified, added and deleted safety functions shall be validated and enabled locally.
- **Signalization:** The active status of the remote maintenance shall be signaled preferably with a visual signal.
- **Safety-related operating mode**: Ensure that the machine is provided with a specific operation mode for remote maintenance that enables all required safety and security functions and protective devices. This may include the application of additional risk reduction measures to be implemented by the user (e.g. barriers, personal protective equipment, see ISO 12100, figure 2). Remote

maintenance shall only be possible when this operating mode is locally selected and locally enabled.

Validation measures

If a software modification has been made in the safety-relevant part of the control system by remote maintenance, all measures to avoid systematic errors in the design shall be taken into account, considering ISO 13849-1 or IEC 62061 and the validation measures described therein.
Validation of software modifications through remote maintenance access can be done in several ways. Here are some measures that should be considered when designing a software modification:

- **Planning:** Ensure that all parties involved (e.g. developers, testers, stakeholders) are informed about the schedule and requirements of the software modifications.
- **Logging:** Carefully log all steps and actions during remote maintenance access. This will allow to track modifications and analyze any possible upcoming problem.
- **Test scenarios**: Define clear test cases and scenarios that cover the functionality of the software modifications. Define also the criteria for passing or failing the required tests. Ensure that these tests are carried out in a simulated or controlled environment to avoid hazardous situations derived from unintended effects on the related machine. The test results shall be documented.
- **Monitoring and feedback:** While the remote maintenance access is active, continuously monitor the execution of the software modifications. Ensure that all intended modifications and functions have been implemented properly.
- **Traceability**: Track all modifications and verify that all modifications comply with applicable requirements and document this. This will allow to check the progress and quality of the software modification.
- **Communication**: Keep all involved parties informed about the progress and outcome of the validation. If necessary, agree on further steps for troubleshooting or adjustments.
- **Final evaluation:** If all tests have been carried out successfully and all requirements have been met, the validation can be considered complete. Release and document the final version of the software modifications and inform the affected parties. The operation of the machine shall only be resumed after a successful final evaluation.

Summary

Applying appropriate technical and organizational measures is essential for health and safety while working with machines that are maintained via remote access.

Note: No legal claims can be derived from the content of this document.

The ISSA Section Machine and System Safety, Project Group “Control Devices”, declines any responsibility which derives from the use of this document. For more information, please refer to the relevant applicable national or international Standards as well as applicable national laws and regulations.

ISSA Section Machine and System Safety
Dynamostrasse 7 – 11
D – 68165 Mannheim
Contact: scholl@ivss.org

Oct. 6th, 2025