RECOMMENDATION: Secure use of IT IN PRODUCTION

Remote maintenance in industrial environments

Systems for process control, production and automation, subsumed under the term “industrial control systems” (ICS), are meanwhile exposed to the same threats as conventional IT systems. Due to operational or economic reasons, it is often required to be able to perform remote maintenance of the systems via public networks. Remote maintenance accesses designed in such a way mean that industrial systems are exposed much more and thus at the same time lead to an increased threat situation. Today, industrial remote maintenance components must therefore reach an adequate security level.

The range of available solutions on the market for remote maintenance in the industrial environment is very wide. The offers range from VPN solutions via cloud-based approaches to provider solutions in the field of machine-to-machine (M2M). There are significant differences between the product features of individual solutions. This recommendation provides an overview of the generic requirements for industrial remote maintenance according to the state of the art. It is explicitly pointed out that established solutions on the basis of analogue or ISDN modems as well as the direct Internet connection of components such as programmable logic controllers (PLCs) do not comply with the state of the art.

1 Architecture

The following requirements should already be taken into consideration when planning and integrating a remote maintenance solution:

✔ Consistent solution: Especially in larger infrastructures, a consistent solution should preferably be used. This reduces both the number of attack vectors and the complexity (no “uncontrolled growth”).

✔ DMZ: The remote maintenance component should preferably be in a separate zone (DMZ) and not localised directly in the production network. Remote maintenance accesses must not lead to existing firewalls being bypassed. Rather, firewalls are suitable to define, for example, allowed IP address ranges for remote maintenance.

✔ Granularity of the communication connections: The remote maintenance access should preferably not be performed generally per (sub)network, but rather it should be possible to control remote maintenance access per IP and port in a fine-grained manner. This minimises the “range” of remote maintenance accesses and thus also limits the consequence of compromising. One possible approach is for example to establish 1:1 connections by means of SSH instead of coupling entire networks by means of IPsec.

✔ Connection establishment: remote access should, if possible, only be initiated from the company (outbound). There should be no open ports for establishing a connection from outside. As an alternative, remote maintenance accesses can be activated temporarily. This requires adequately secure authentication and an up-to-date patch level as well as organisational processes to ensure subsequent deactivation.

✔ Dedicated systems: The components used for remote maintenance should only be used for this application purpose and not be mixed with other functionalities.
2 Secure communication

The security of the communication in the case of remote maintenance is primarily ensured by means of established standard solutions.

✔ Secure protocols: Only established protocols such as IPsec, SSH or SSL/TLS in current versions are used in order to establish a tunnel between two end points or networks. Only the current versions of the respective protocols are to be recommended. Additional information in this respect can be found in the BSI's minimum standard TLS 1.2\(^1\). Furthermore, up-to-date reports regarding vulnerabilities such as Heartbleed\(^2\) or Poodle should be observed.

✔ Secure procedures: Sufficiently strong cryptographic procedures are used for encryption, for example AES with a key length of at least 196 bits\(^3\). Using the recommended minimum key length, such as 128 bits for AES, is not recommended due to the typically long service life. The strength of the keys used should be checked at regular intervals as part of the security management and adjusted if necessary.

3 Authentication mechanisms

Only by complying with the following requirements for user authentication, an adequate security level can be reached for a remote maintenance solution.

✔ Granularity of the accounts: Only one user per account should be provided. Group accounts must be avoided under all circumstances.

✔ Strong authentication mechanisms: The best security level is provided by two-factor-methods in which not only knowledge (e.g. a password), but also ownership (e.g. X.509 certificate) has to be proven. In the case of hardware-based solutions, such as generators for one-time passwords, smart cards or USB tokens, for which copying the hardware component is impossible, the security level is particularly high. In every case, using such mechanisms must be preferred to simple authentication using a password.

✔ Password security: Using password-based authentication requires a password policy which ensures the minimum level of the password quality. It must be possible to implement such a policy by the respective remote maintenance solution (e.g. use of special characters, password length etc.). A remote maintenance solution should preferably also be able to technically force a password policy. It must explicitly be pointed out that using only password-based authentication methods cannot provide more than a basic level of protection. In any case, the related organisational processes must be implemented (see below).

✔ Attack detection: Using mechanisms to detect attacks on password-based authentication methods (e.g. brute-force or dictionary attacks) would be preferable. Precautions are necessary against repeated trying (online brute-force), such as by activating temporary blocking after a defined number of failed attempts. Unlike in conventional IT, such blocking, however, must be performed for example only after 20 instead of already after three failed attempts with regard to the special requirements in terms of availability and safety.

4 Organisational requirements

Secure maintenance access can never be ensured by technical safeguards alone. Therefore, the following requirements are essential for the integration and operation phase.

✔ Risk analysis: The designed solution is subjected to a formal risk analysis.

✔ Principle of minimalism: Only the absolutely necessary remote access options must be implemented. The necessity of a remote access must be documented by the respective person responsible (“business justification”).

✔ Processes: The operator of the system has established processes which for example govern the release of connections, locking (e.g. when employees leave the organisation), emergency procedures and the regular change of authentication data.

✔ Inventory: All remote access options are identified as part of a security management. This includes the type of the access, the affected systems, the authorised persons as well as the corresponding specifications and processes.

✔ Time window: Remote access is only enabled when needed or in a defined maintenance window (e.g. key-operated switches). Activation and/or deactivation must be logged.

✔ Functional test: The proper functioning of the remote maintenance is checked at regular intervals.

---

\(^1\) Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung [Minimum standard of the BSI for the use of the SSL/TLS protocol in federal administration], https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll.html

\(^2\) BSI stuft Heartbleed-Bug als kritisch ein [BSI classifies Heartbleed bug as critical], https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Heartbleed_11042014.html

Guidelines for persons performing the maintenance work: Especially in the case of remote maintenance by third parties (manufacturers, integrator etc.), guidelines are made for the IT used (e.g. no smartphones) and protection mechanisms of the remote clients (e.g. latest virus protection, firewall, system hardening, latest patch level etc.). These guidelines are contractually agreed upon.

Patch process: For functional industrial components (e.g. PLC), it is often not possible to install updates and patches. Notably remote maintenance components are exposed very much, eliminating the known vulnerabilities there in a timely manner is of central importance for security aspects. Since a remote maintenance component does usually not have a direct impact on aspects in terms of time, such as real-time capability or system availability, in most cases such updates are also possible as part of a defined patch process.

Logging & alerting: Available logging functions must be used to track for example connection data and also failed login attempts. It must be ensured that the log data is evaluated automatically and an alarm is generated if necessary. Moreover, manual inspection should be performed periodically. To ensure auditing acceptability, it is absolutely necessary that the log data is collected at the operator instead of at the person performing the maintenance work.

5 Miscellaneous

Depending on the specific application, further requirements can be useful. As it is hardly possible to make general statements in this respect, some examples are listed below:

Scalability: Primarily in larger infrastructures, the costs for operation, maintenance and servicing can be reduced significantly by a central management, bulk roll-out, bulk configuration, or bulk actions, such as executing scripts.

Investment protection: By taking possible future requirements into account, such as the support of IPv6, it makes sense to choose products with regard to investment protection and sustainability.

High availability: Provided that there are corresponding requirements, functions for implementing high-availability concepts, such as the redundant use of several mobile communication networks for the communication by means of Dual SIM, are useful.

Depending on the requirements as well as on the remote maintenance solution to be assessed, further criteria must be examined in an individual assessment. For example, the corresponding recommendations of the BSI\(^4\) should be followed in the case of cloud-based products. Especially public cloud-based solutions imply a higher security risk, which is why rather a private cloud or a sufficiently trusted provider should be chosen by taking security aspects into account.

The recommendations described above apply to the widespread case of remote maintenance within the meaning of a maintenance case in which changes are made to the system or which requires at least an interaction. For a merely passive remote access, for example for only reading status information, measured values or system states, other solutions may be used. Thus, the information can for example be decoupled via a web or FTP server to which the data is supplied from the ICS network per push method and which cannot establish a connection to this server itself.

A more in-depth insight in the security of remote maintenance in IT can be found in the basic rules for protecting remote maintenance accesses\(^5\). Additional information, especially regarding organisational regulations can be found in IT-Grundschutz\(^6\) safeguards S 2.415, S 2.416, S 2.417, S 2.418, S 2.419, S 2.420, S 4.224, S 4.319, S 4.320, S 4.321, S 4.322, S 6.109 as well as S 5.33. Furthermore, the BSI publication ISi-Fern [publication on secure remote access to the internal network] provides supplementing information regarding technical and architecture-related issues.

---


6 IT-Grundschutz, BSI, [https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html)