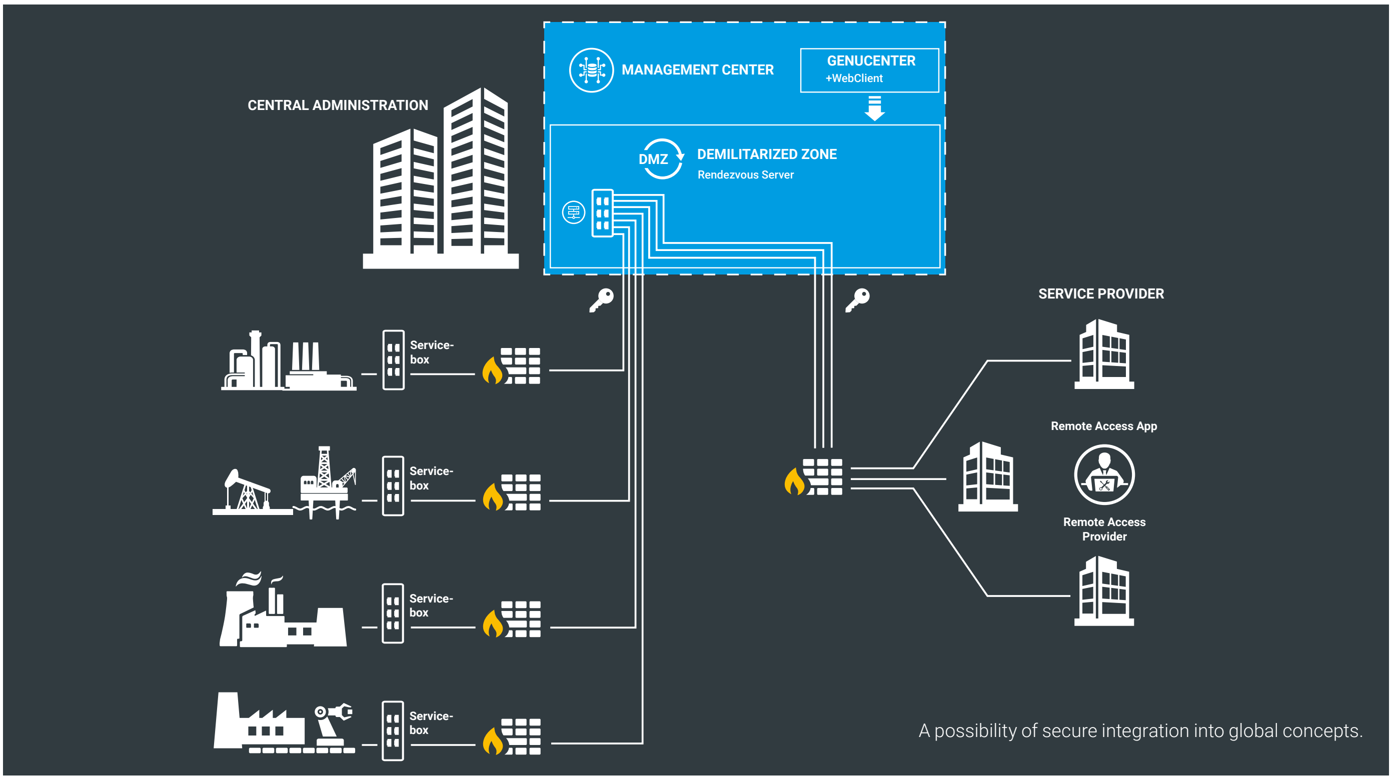
Technical Fact
HIMA Cybersecurity Solutions

Secure remote maintenance in an industrial environment

Challenges in industrial applications – today and in future

On the one hand, the remote maintenance of process plants via public networks in an industrial environment enables considerable cost advantages. On the other hand, significant security risks can be expected by accessing control system networks remotely. If your process network does not have an effective protective shield, a single security gap can make your production processes vulnerable to attacks – with potentially catastrophic consequences. It is necessary to reduce this vulnerability to a minimum and it requires considerable know-how to manage this problem efficiently. Ideally, this know-how is available in your own company or should be acquired through cooperation with a trustworthy partner. Doing nothing could be a serious mistake.

The consequence of a vulnerability in a process network is a reduction in safety and security, and there is an increased risk of personal, environmental and economic damage. It is important to weigh up the opportunities against the risks. The advantages of remote maintenance are obvious, but the risks imposed must be managed appropriately, given the potential consequences.

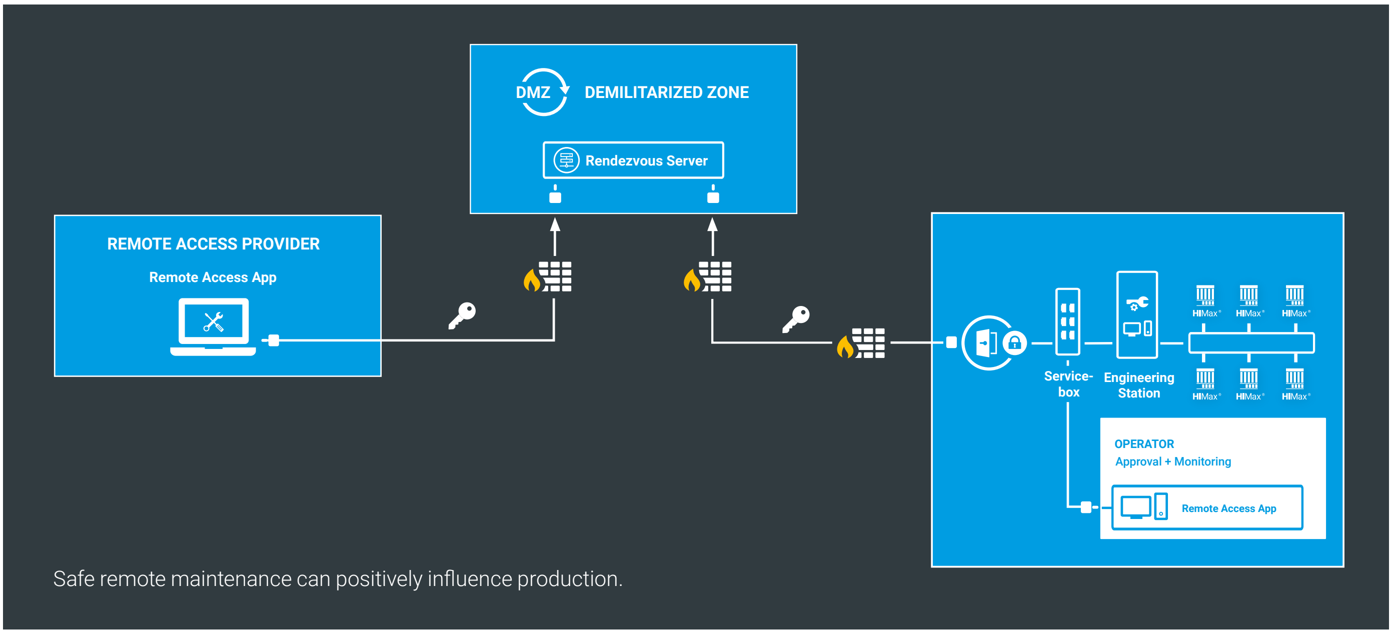


A possibility of secure integration into global concepts.

State-of-the-Art Solution

The German Federal Office for Information Security (BSI), the central point of contact for IT security issues in Germany, helps to avoid risks faced by plant owners and operators. The BSI publication on cyber security (BSI-CS 108 | Version 2.0 | 07.2018) provides an overview of the generic requirements for industrial remote maintenance according to the current state-of-the-art. A checklist for your investment decision can be derived from this. We have developed a checklist from the BSI report, based on our products, which will enable you to make an informed investment decision. You will also receive the official, detailed BSI publication on secure remote maintenance as an attachment.

In collaboration with genua, HIMA offers a solution that meets the highest requirements for secure remote maintenance in industrial environments. With the Rendezvous solution, no direct access from the remote maintainer to production environment is permitted. Instead, all maintenance connections run via a Rendezvous server installed in a demilitarised zone (DMZ), where both the maintenance service and the customer establish connections in an agreed time window. The Rendezvous Server maintains the continuous maintenance connection. Once securely established within the Rendezvous Server, the maintainer can now access the Remote Access App located in a segregated portion of the local engineering environment.



Safe remote maintenance can positively influence production.

Benefit of great importance

Through the implemented mechanisms you can build up a remote maintenance concept adapted to your needs, which fulfils the highest demands on safety and security. There are no real limits to scalability. From the individual solution connecting to a single critical system, to a global multiple site solution, all requirements are achievable. And all this with high availability. There are no restrictions regarding the integration of third-party automation solutions. The Rendezvous solution gives you complete control over maintenance access to your networks.

Important benefits at a glance:

- Reduce complexity due to a single solution
- Full control by an upstream demilitarized zone (DMZ)
- Secure protocols and high-quality encryption: SSH, IPsec, SSL / TLS
- Investment-safe due to optional expandability, complete IPv6 support and constant product maintenance
- No limits through proprietary solutions
- Satisfy all requirements for a secure and BSI compliant remote maintenance solution in the industrial environment

At a glance: Safe Remote Maintenance in the Industrial Environment

BSI recommendation	Solution from HIMA & genua
Architecture	
Uniform solution (no "uncontrolled growth")	All remote maintenance cases can be covered uniformly as well as central management solution
Remote maintenance components in the DMZ	Dedicated server as central remote maintenance gateway in the DMZ
Connections not per (sub)network but fine-granular per IP and port	Remote maintenance relationship always per IP and port
Connection setup from inside to outside, no open ports	Machine operator controls remote maintenance channel (four-eyes principle)
Dedicated systems for remote maintenance	Dedicated system: Remote maintenance appliance genubox
Secure communication	
Secure protocols	SSH, IPsec, SSL/TLS
Secure cryptographic methods	High quality encryption, e.g. AES256
Authentication mechanisms	
Granularity of accounts	Guaranteed by user role concept
Strong authentication mechanisms	Authentication via password, OTP (with Yubikey token) together with RSA key
Password security	Guaranteed via password policy
Attack detection	Failed authentication detection
Organisational requirements	
Risk analysis*	Possible via service
Principle of minimalism	Access generally strictly limited to the remote maintenance object (IP and port)
Processes	Comprehensive support for processes and user roles
Inventory	Remote maintenance accesses are fully monitored and recorded
Time windows	Remote access can be limited in time
Functional test	Guaranteed via central monitoring
Specifications for remote service technicians	Testing of specifications by remote maintenance app
Patch process	Central Patch Management
Logging & Alerting	Central Logging & Alerting
Others	
Scalability	Easily scalable through central management, even for very large environments
Investment protection	Full IPv6 support, continuous product maintenance
High availability	Highly available provision of all components possible

Overview derived from: BSI-CS 108 | Version 2.0 dated 11.07.2018

* Offered by HIMA Consultancy

For further information, please contact us:

HIMA Automation Security Competence Center
Klaus Wagner / Heiko Schween
Phone: +49 (0) 6202 709-128 / -599
E-mail: k.wagner@hima.com / h.schween@hima.com

Or visit us online:
https://www.hima.com/en/about-hima/cybersecurity

About HIMA

The HIMA Group is the world's leading independent provider of smart safety solutions for industrial applications. With more than 35,000 installed TÜV-certified safety systems worldwide, HIMA qualifies as the technology leader in this sector. Its expert engineers develop customized solutions that help increase safety, cyber security, and profitability of plants and factories in the digital age. For over 45 years, HIMA has been a trusted partner to the world's largest oil, gas, chemical, and energy-producing companies. These rely on HIMA solutions, services and consultancy for uninterrupted plant operation and protection of assets, people, and the environment. HIMA's offering includes smart safety solutions that help increase safety and uptime by turning data into business relevant information. HIMA also provides comprehensive solutions for the efficient control and monitoring of turbomachinery (TMC), burners and boilers (BMC), and pipelines (PMC). In the global rail industry, HIMA's CENELEC-certified SIL 4 COTS safety controllers are leading the way to increased safety, security, and profitability. Founded in 1908, the family-owned company operates from over 50 locations worldwide with its headquarters in Brühl, Germany with a workforce of approximately 800 employees.

For more information please visit: *www.hima.com*

The content provided in this document is intended solely for general information purposes, and is provided with the understanding that the authors and publishers are not herein engaged in rendering engineering or other professional advice or services. Given the complexity of circumstances of each specific case and the site-specific circumstances unique to each project any use of information contained in this document should be done only in consultation with a qualified professional who can take into account all relevant factors and desired outcomes. This document has been prepared with reasonable care and attention. However, it is possible that some information in this document is incomplete, incorrect, or inapplicable to particular circumstances or conditions. Neither HIMA nor any of its affiliates, directors, officers or employees nor any other person accepts any liability whatsoever for any loss howsoever resulting from using, relying or acting upon information in this document or otherwise arising in connection with this document. Any modification of the content, duplication or reprinting of this document, as well as any distribution to third parties – even in parts – shall require the express written approval of HIMA.

HIMA SMART SAFETY.

www.hima.com

Reference number: 96 9000726 0719 V01

Federal Office
for Information Security

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 an 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

[3] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen [English version: BSI TR-02102 Cryptographic Procedures: Recommendations and Key Lengths], https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.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.

By means of the BSI publications, the Federal Office for Information Security (BSI) publishes documents about current topics in the field of cyber security. Comments and advice from readers can be sent to info@cyber-allianz.de.

[4] Cloud Computing, BSI, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Publikationen/CloudComputing-Studien.html

[5] Grundregeln zur Absicherung von Fernwartungszugängen [Basic rules for protecting remote maintenance accesses], BSI / Alliance for Cyber Security, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054.html

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