genua.

Secure Remote Access to Production Systems in the Process Industry

genubox Meets All Relevant NAMUR Recommendations

Secur|Ty made in Germany

Secur|Ty made in EU

> The aim of the **NAMUR Recommendation 135 (NE135)** is to provide the basis for secure planning, implementation, and operation of remote access solutions in the field of automation technology from the user‘s perspective. The relevant requirements are presented to manufacturers, integrators, and operators of remote access solutions for the entire system life cycle.
>
> NAMUR Recommendation “Remote Access”

The NAMUR Recommendation for Secure Remote Access to Systems in the Process Industry

Remote access is an important tool for gaining quick and cost-effective access to automation technology in the process industry. For example, it enables the maintenance of production systems and thus ensure trouble-free operational processes.

However, remote access also poses a significant risk: through inadequately secured access to the target system, unauthorized persons or malware can get into the network and cause serious damage.

From risks and protection goals to specific requirements and architectural aspects/target architectures, the “NAMUR Recommendation: Remote Access” offers a recognized expert guidance in eight chapters developed by process industry experts.

The precautions defined therein are equally relevant for manufacturers, system integrators, and operators: If possible, the requirements should be taken into account during planning and implementation as well as over the entire life cycle of the system. However, a significant improvement in system safety can also be achieved by networking older existing systems.

Remote Maintenance Solution genubox fulfills all relevant requirements

As a manufacturer of a highly secure remote maintenance solution, genua covers all solution-specific requirements for a secure architecture for process industry remote access, which result from chapters 5 to 7 of the NAMUR Recommendation. We offer a detailed overview on the following pages.

For implementing the processes recommended in chapter 7, you can receive consulting and support from genua or from specialized partners in your area upon request.

genubox Meets All NAMUR Recommendations for a Secure Access Architecture in Accordance with Chapters 5 to 7 *

Overview derived from: NAMUR Recommendation:
Remote Access - IT Security Requirements for Remote Access, Edition: 2023-07-10

Chapter 5: Requirements

5.1. Remote Access Solution Requirements (Manufacturer)

Solution from genua

Extensive support functions for system integrators and operators

5.1.1. IT Security Functions

	Solution from genua
Authentication	• Service provider: Two-factor authentication via Keycloak, Microsoft Active Directory, Microsoft Entra ID (formerly Azure Active Directory), OKTA, and RADIUS • Central management and operators: Multi-factor authentication via RADIUS, smart card or Yubikey
Fine-grained central rights management	Fine-grained multi-client capability with user/role concept
Operator consent and impact on access	• Communication must be confirmed by the receiving party • Operator can terminate communication at any time • Blocking of maintenance provider input devices • Assign/remove write access for maintenance providers
Logging, connection to central monitoring systems	• Logging in Common Event format for import via SIEM systems • Logging on central management system • Syslog output

* For implementing specific processes in accordance with chapter 7 of the NAMUR Recommendation, you can receive consulting and support from genua or from specialized cooperation partners in your area upon request.

Chapter 5: Requirements

5.1.1. IT Security Functions

	Solution from genua
Use of cryptographic procedures and protocols	• High-quality encryption such as AES256, SSH, IPsec, HTTPS (SSL/TLS)

5.1.2. Documentation

	Solution from genua
Providing detailed documentation	• Manuals • Release notes • Specific use cases (available as service)
Constant updates	Check for necessary updates with every release

5.1.3. Vulnerabilities and Security Updates

	Solution from genua
Secure development methods	Development quality assurance according to ISO 9001
Evidence of safe development processes	• Oriented to ISO 62443-4-1 • Certified according to ISO 27001
Information about possible vulnerabilities	• Highest prioritization for fixes of identified vulnerabilities • Information about vulnerabilities and provision of patches via direct communication

Chapter 5: Requirements

5.1.3. Vulnerabilities and Security Updates

	Solution from genua
Elimination of vulnerabilities without negative impact on target system accessibility	Quality assurance also for patches
Description of the impact of a security update	Release notes for security updates, especially if they have a functional impact
Security updates after discontinuation	Several years of security updates for the product core, even after discontinuation

5.1.4. Operator Support

	Solution from genua
Providing relevant information for risk analysis	Available via service
Training offer	• Company-owned training center • On-site and remote trainings • Trainings for solutions and products

Chapter 5: Requirements

5.1.4. Operator Support

	Solution from genua
Customer support	• Update support • Latest features/functionalities • Protection against attacks on the update mechanism • Hotline support • 1st to 3rd level • Staff in Germany • Availability up to 24/7 • Security system management according to ITIL
Support in auditing users (e.g. through ISO/IEC documents)	Available as service
Operator has data sovereignty	• Data is fully maintained in operator hands (supported by solution) • Logging into operator SIEM • 4-eyes principle • Live view of access • Revision-optimized recording funktion • Checking incoming data traffic using an optional virus scanner via ICAP interface • Support of zero-trust concepts • Minimally invasive access • Use of a software-defined perimeter • Enforcement of the least privilege principle
Compliance with data protection regulations	Consent request for recording function

Chapter 6: Architectural Aspects/Target Architectures

	Solution from genua
Purdue model to represent hierarchical arrangement and grouping: fieldbus level, control level, process control level, operations control level, company level, and Internet	• Flexible implementation of the solution across different appliances • (also in hybrid setups) depending on requirements • Server and industrial hardware • Virtual appliances • Hypervisor support

6.1. “Segmented Network” Assumption

	Solution from genua
Segmentation, grouping, and zoning of the network	• Basic firewall functionality of genubox (roles: Rendezvous Server and Service Box), Service Box includes Application Level Gateway (ALG) • Dedicated application access without network coupling • genubox is suitable due to the distribution of instances in the system (role: Service Box) especially for zoning tasks • Event-based switching in the event of remote maintenance to isolate the target system for maximum protection
Transitions (routers, firewalls)	• Basic firewall function of genubox (roles: Rendezvous Server and Service Box), Service Box includes Application Level Gateway (ALG) • No network transition between remote service provider and target systems, remote maintenance via Application Level Gateway (ALG)
Active network components: Network division into internal segments (lower level), outer segment (higher level) and neutral segment (DMZ)	Firewall function of genubox (placed in DMZ, role: Rendezvous Server) separates external and internal segments
Exclusive accessibility of intended remote maintenance targets	• Connection configurations for (sub)nets with target systems • Configuration option for fine-grained remote maintenance relationships per IP and port up to batch size 1

Chapter 6: Architectural Aspects/Target Architectures

6.2. Defense In Depth

Segmented networks follow the concept of Defense in Depth, in which access from internal to external systems are allowed, but not the other way around

Solution from genua

- genua's portfolio offers various network segmentation solutions
- Using genubox as a packet data firewall
- Rendezvous Server: Segmentation of the remote server and target networks
- Service Box: In the case of desired access, switch the rule set to "remote maintenance" (also ALG only allows permitted protocols)

In the case of remote access, the reverse occurs because the service provider is usually in a lower-protected security zone and accesses a higher-protected security zone

Solution from genua

The connection is always established from within to the Rendezvous Server (dedicated server as a central remote maintenance gateway in the DMZ)

- Continuous maintenance connection only with confirmed rendezvous
- Response of the target system is configured and controlled
- Connection of virus scanners to protect against malicious code in the event of data transfer

To prevent unauthorized data traffic in this direction, multi-factor authentication should be used, e.g. telephone agreement or one-time passwords

Solution from genua

- Individual agreement channels possible
- Multifactor or OTP authentication of the remote operator

Chapter 6: Architectural Aspects/Target Architectures

6.3. Security Consideration of the Remote Access Variants

6.3.1. Remote Diagnosis

	Solution from genua
Data flow direction from the target system to the remote access device or service: Securing through network architecture (e.g. with the help of a data diode or firewall)	• Opening to the outside can be configured using timed or manual triggers (temporary or permanent) • Optimal and optional: Data diode cyber-diode with permanent one-way communication exclusively for data output

6.3.2. Remote Monitoring

	Solution from genua
• **Data flow direction of process information and maintenance information to the outside** • **No change to the target system** • **Connection only in the required time frame**	• Opening to the outside can be configured using timed or manual triggers (temporary or permanent) • Optimal and optional: Data diode cyber-diode with permanent one-way communication exclusively for data output

6.3.3. Remote Control

	Solution from genua
If the connection is permanent, the requirement is checked regularly	• Application-sensitive SSH remote maintenance access without network coupling • Comprehensive governance with full control of all remote access • Temporal, spatial, role-specific, target system-restricted access can be configured

Chapter 6: Architectural Aspects/Target Architectures

6.3.4. Remote Access

	Solution from genua
• **Access from neutral to the inside, but limited in time** • **Also applies to "passive remote maintenance": Active system access by operators under the guidance of the remote service provider**	• Central administration with complete control at all times over maintenance action, access time, target and accessing instance • High operational reliability through confirmation of the connection from the inside, e.g. via Windows app, operator GUI in the central management system or key switch • Simple and uniform operation of a variety of services and integration of third-party solutions possible • Virus/malware protection of data transfer using external virus scanners via ICAP interface • Security level adaptable from open and continuous access to full control • Temporal, role-specific access restricted to the target system can be configured (ready for "geo-local restrictions") • Comprehensive rights and roles system • Maximum security and control through application-specific access to the target system isolated from the rest of the system as well as a rendezvous point in the DMZ or in the cloud • Video recording function and logging • All productive and management systems are available as hardware and virtualized systems; the Service Box is also available as an industrial hardware with a suitable temperature range and form factor as well as convenience features such as key switch • Highly secure update mechanism protects genubox software from quantum computer attacks • The service provider's input devices can be deactivated for screen sharing and verbal instructions only

6.4. Central Remote Access Point

	Solution from genua
• **Few remote access solutions in use** • **Ideally via existing communication channels**	• Representation of uniform governance for a variety of different remote maintenance services • Integration of third-party solutions possible

6.5. Rendezvous System

	Solution from genua
• **Communication partners connect to a third system** • **Permission to connect on a case-by-case basis** • **Meeting point in the operator's DMZ or cloud environment** • **No VPN connection directly to target systems**	• Temporal, spatial, role-specific access restricted to the target system can be configured (activation by recipient) • Powerful rights and roles system • Application-specific SSH instead of network-wide VPN access

Chapter 6: Architectural Aspects/Target Architectures

6.6. Jump Server (Jump Host)

	Solution from genua
If connections to the target system are not possible, a jump server should serve as a proxy for the target system	Possible, e.g. on Windows Server (e.g. engineering workstation) via RDP, from there access to controls

6.7. Data Transfer

	Solution from genua
• **Possibility of interrupting data transmission through solution components** • **Data lock via additional system (with anti-malware)**	• Virus/malware protection of data transfer using external virus scanners via ICAP interface • Prevention of transmission upon detection

6.8. Example Architectures

	Solution from genua
Use of the rendezvous instance on-premises or via Internet/cloud	Remote access only via Rendezvous Server e.g. in a demilitarized zone (DMZ) or a cloud (please see the illustration on the back cover of this brochure*)

6.9. Decentralized Infrastructure

	Solution from genua
Integrated solutions (e.g. from the manufacturer of the target system) with their own VPN end-points do not meet the require-ments of increased protection due to a lack of control options	• Integration of manufacturer solutions possible • Implementation of uniform governance for a variety of different remote maintenance services

* Information on further use cases and application scenarios available upon request.

Chapter 7: Accompanying Processes

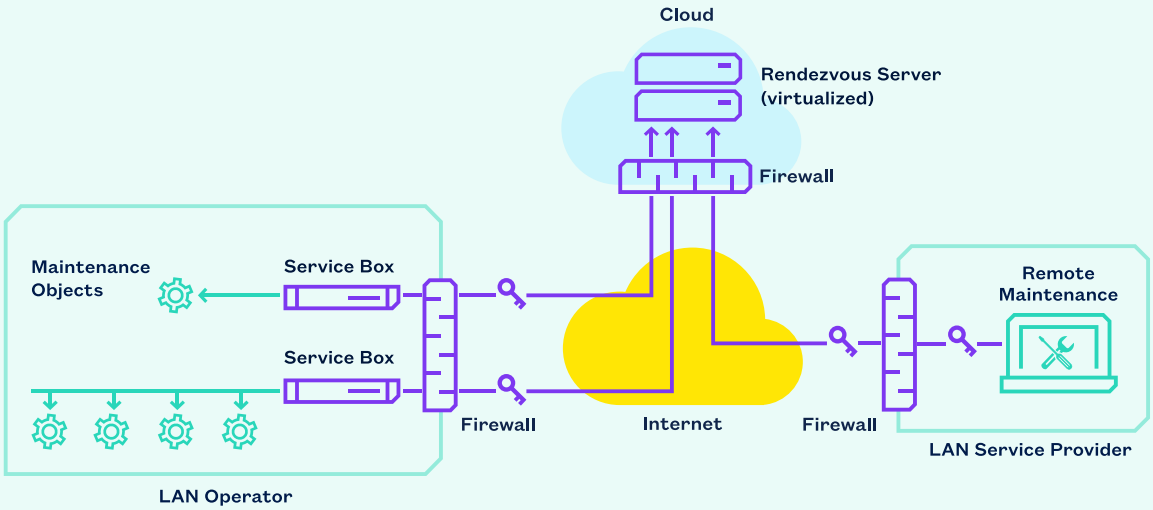
Processes based on an ISMS

Solution from genua

genua also offers consulting:

- ISMS assessment – maturity level analysis of the current status
- Support services in setting up an ISMS
- ISMS awareness training

Interested? Contact us:
+49 89 991950-902 or sales@genua.de



Exemplary implementation: The secure rendezvous solution from genua in accordance with NAMUR recommendation

The rendezvous solution from genua: No one-sided access from the remote maintenance service provider to customer networks is permitted. Instead, all maintenance connections run via a Rendezvous Server, e.g. in a demilitarized zone (DMZ) or a cloud. Both the maintenance service provider and the operator establish connections here at the agreed time.

The maintenance connection is only established through rendezvous on the server. The service can now use this to address the machine system, which is separated from the rest of the customer network by the Remote Maintenance Solution genubox. The rendezvous solution allows operators to maintain complete control over maintenance access to their networks.

Reasons Why

- Experts for the IT security of companies and public organizations
- Offer of a comprehensive, modular IT security portfolio
- Quality without compromise for all products, services, and processes

genua – Excellence in Digital Security

genua develops innovative, reliable as well as markets-haping products and solutions. Whether in the public sector, for the operators of critical infrastructures, in industry or in the protection of classified information: we provide answers to the IT security challenges of today and of tomorrow.

Further information:
www.genua.eu/genubox

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim, Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu

0224-02-EN