genua.

Sicherer Fernzugriff auf Anlagen in der Prozessindustrie

genubox erfüllt alle relevanten NAMUR-Empfehlungen

Secur|Ty made in Germany

Secur|Ty made in EU

> Das Ziel der **NAMUR-Empfehlung 135 (NE135)** ist es, die Grundlage für eine sichere Planung, Umsetzung und den Betrieb von Fernzugriffslösungen im Umfeld der Automatisierungstechnik aus Anwendersicht zu bieten. Dazu werden die relevanten Anforderungen an Hersteller sowie Integratoren von Fernzugriffslösungen und die Betreiber über deren gesamten Lebenszyklus dargelegt.
>
> NAMUR-Empfehlung 135 Fernzugriff (Remote Access)

Die NAMUR-Empfehlung zum sicheren Fernzugriff auf Anlagen in der Prozessindustrie

Fernzugriffe sind ein wichtiges Instrument, um schnell und kosteneffizient Zugang zu Automatisierungstechnik in der Prozessindustrie zu erhalten. Sie ermöglichen beispielsweise die Wartung von Produktionssystemen und gewährleisten damit störungsfreie betriebliche Abläufe.

Fernzugriffe stellen jedoch auch ein erhebliches Risiko dar: Über einen unzureichend gesicherten Zugang zum Zielsystem können Unbefugte oder Malware in das Netzwerk gelangen und schwerwiegende Schäden verursachen. Daher sind wirksame Maßnahmen und Mechanismen zur Absicherung eines Fernzugriffs zu implementieren.

Von Risiken und Schutzzielen über konkrete Anforderungen bis hin zu architektonischen Aspekten/ Zielarchitekturen bietet die „NAMUR-Empfehlung: Fernzugriff (Remote Access)“ in acht Kapiteln eine anerkannte, fachkundige Orientierung, die von Branchenexperten der Prozessindustrie erarbeitet wurde.

Die darin definierten Vorkehrungen sind gleichermaßen für Hersteller, Systemintegratoren und Betreiber relevant: Die Anforderungen sollten möglichst bereits bei der Planung und Umsetzung sowie über den gesamten Lebenszyklus der Anlage berücksichtigt werden. Eine deutliche Verbesserung der Anlagensicherheit lässt sich jedoch auch bei der Vernetzung älterer Bestandssysteme erzielen.

Fernwartungslösung genubox erfüllt alle relevanten Anforderungen

Alle lösungsspezifischen Anforderungen an eine sichere Architektur für Fernzugriffe in der Prozessindustrie, die sich aus den Kapiteln 5 bis 7 der NAMUR-Empfehlung ergeben, deckt genua als Hersteller einer hochsicheren Fernwartungslösung ab. Dazu bieten wir Ihnen auf den folgenden Seiten einen detaillierten Überblick.

Bei der Umsetzung der im Kapitel 7 empfohlenen Abläufe erhalten Sie auf Anfrage Consulting und Support von genua oder von spezialisierten Kooperationspartnern in Ihrer Nähe.

Fernwartungslösung genubox erfüllt alle NAMUR-Empfehlungen für eine sichere Zugriffsarchitektur gemäß Kapitel 5 bis 7 *

Übersicht abgeleitet aus: NAMUR-Empfehlung: Fernzugriff (Remote Access) – Anforderungen an die IT-Sicherheit von Fernzugriffen, Ausgabe: 2023-07-10

Kapitel 5: Anforderungen

5.1. Anforderungen an die Fernzugriffslösung (Hersteller)

	Lösung von genua
	Breite Unterstützungsfunktionen für Integratoren und Betreiber

5.1.1. IT-Sicherheitsfunktionen

	Lösung von genua
Authentifizierung	• Fernwarter: Zwei-Faktor-Authentifizierung über Keycloak, Microsoft Active Directory, Microsoft Entra ID (vormals Azure Active Directory), OKTA und RADIUS • Zentrale Verwaltung und Betreiber-Operatoren: Multi-Faktor-Authentifizierung über RADIUS, Smart Card oder Yubikey
Feingranulare, zentrale Rechteverwaltung	Feingranulare Multi-Mandanten-Fähigkeit mit Benutzer-/Rollen-Konzept
Betreiber-Zustimmung und Einfluss auf Zugriffe	• Kommunikation muss von Empfangsseite bestätigt werden • Betreiber kann die Kommunikation jederzeit beenden • Sperrung von Eingabegeräten des Wartungsanbieters • Zuweisung/Entzug Schreibzugriff für Wartungsanbieter
Logging, Anbindung an zentrale Überwachungssysteme	• Logging im Common Event-Format zum Import durch SIEM-Systeme • Protokollierung auf zentralem Management-System • Syslog-Ausgabe

* Bei der Umsetzung spezifischer Abläufe gemäß Kapitel 7 der NAMUR-Empfehlungen erhalten Sie auf Anfrage Consulting und Support von genua oder von spezialisierten Kooperationspartnern in Ihrer Nähe.

Kapitel 5: Anforderungen

5.1.1. IT-Sicherheitsfunktionen

	Lösung von genua
Einsatz kryptografischer Verfahren und Protokolle	• Hochwertige Verschlüsselung, u. a. AES256, SSH, IPsec, HTTPS (SSL/TLS)

5.1.2. Dokumentation

	Lösung von genua
Bereitstellung ausführlicher Dokumentation	• Handbücher • Release Notes • Spezifische Szenarien (über Dienstleistung möglich)
Stetige Aktualisierung	Bei jedem Release Überprüfung auf Aktualisierungsbedarf

5.1.3. Schwachstellen und Sicherheitsupdates

	Lösung von genua
Sichere Entwicklungsmethoden	Qualitätssicherung der Entwicklung gemäß ISO 9001
Nachweis über sichere Entwicklungsprozesse	• Orientierung an ISO 62443-4-1 • Zertifiziert nach ISO 27001
Information über etwaige Schwachstellen	• Höchste Priorisierung für Fixes erkannter Schwachstellen • Information über Schwachstelle und Bereitstellung von Patches via direkter Kommunikation

Kapitel 5: Anforderungen

5.1.3. Schwachstellen und Sicherheitsupdates

	Lösung von genua
Behebung der Schwachstellen ohne negativen Einfluss auf Zielsystem-Erreichbarkeit	Qualitätssicherung auch für Patches
Beschreibung der Auswirkungen eines Sicherheitsupdates	Release Notes für Sicherheitsupdates, im Besonderen falls funktionale Auswirkungen
Abkündigungen mit weiterhin bereitgestellten Sicherheits-updates	Mehrere Jahre Sicherheitsupdates des Produktkerns auch nach etwaiger Abkündigung

5.1.4. Unterstützung des Betreibers

	Lösung von genua
Bereitstellung von relevanten Informationen für Risikoanalysen	Über Dienstleistung möglich
Angebot von Schulungen	• Eigenes Schulungszentrum • On-Site und Remote-Schulungen • Lösungs- und Produktschulungen

Kapitel 5: Anforderungen

5.1.4. Unterstützung des Betreibers

	Lösung von genua
Support für Benutzer	• Update-Support • Neueste Features/Functionalities • Schutz vor Angriffen auf Update-Mechanismus • Hotline-Support • 1st bis 3rd Level • Eigenes Personal in Deutschland • Verfügbarkeit bis hin zu 24/7 • Security System Management nach ITIL

	Lösung von genua
Unterstützung bei Auditierung der Benutzer (z. B. durch Belege zu ISO/IEC)	Über Dienstleistung möglich

	Lösung von genua

Datenhoheit beim Betreiber	• Daten sind vollständig in Betreiberhand haltbar (unterstützt durch Lösung)
	• Logging in Betreiber-SIEM
	• 4-Augen-Prinzip
	• Live-View des Zugriffs
	• Aufzeichnungsfunktion zur Revisionsoptimierung
	• Überprüfung eingehenden Datenverkehrs durch optionalen Virenscanner via ICAP-Schnittstelle
	• Unterstützung von Zero-Trust-Konzepten
	  • Minimal-invasive Zugriffe
	  • Einsatz von genubox als Software-Defined Perimeter
	  • Durchsetzung des Least-Privilege-Prinzips

	Lösung von genua
Beachtung der Vorgaben zum Datenschutz	Zustimmungsabfrage bei Aufzeichnungsfunktion

Kapitel 6: Architektonische Aspekte/Zielarchitekturen

	Lösung von genua
Purdue-Modell zur Darstellung hierarchischer Anordnung und Gruppierung: Feldbusebene, Steuerungsebene, Prozessleitebene, Betriebsleitebene, Unternehmensebene und Internet	• Flexible Implementierung der Lösung über verschiedene Appliances (auch in hybriden Setups) je nach Anforderungen • Server- und industrielle Hardware • Virtuelle Appliances • Hypervisor-Support

6.1. Annahme „segmentiertes Netzwerk“

	Lösung von genua
Segmentierung, Gruppierung und Zonierung des Netzwerks	• Grundsätzliche Firewall-Funktion von genubox (Rollen: Rendezvous Server und Servicebox), Servicebox zudem mit Application Level Gateway (ALG) • Dedizierter Anwendungszugriff ohne generelle Netzkopplung • Aufgrund Verteilung von Instanzen in der Anlage eignet sich genubox (Rolle: Servicebox) besonders für Zonierungsaufgaben • Event-basierte Umschaltung im Fernwartungsfall zur Isolation des Zielsystems für maximalen Schutz der Anlage

	Lösung von genua
Übergänge (Router, Firewalls)	• Grundsätzliche Firewall-Funktion von genubox (Rollen: Rendezvous Server und Servicebox), Servicebox zudem mit Application Level Gateway (ALG) • Kein Netzwerkübergang zwischen Fernwarter und Zielsystemen, Fernwartung über Application Level Gateway (ALG)

	Lösung von genua
Aktive Netzwerkkomponenten: Teilung Netzwerk auf interne Segmente (niedrigere Ebene), äußeres Segment (höhere Ebene) und neutrales Segment (DMZ)	Firewall-Funktion in genubox (in DMZ platziert, Rolle: Rendezvous Server) trennt externe und interne Segmente

	Lösung von genua
Exklusive Erreichbarkeit beabsichtigter Fernwartungsziele	• Verbindungskonfigurationen für (Sub-)Netze mit Zielsystemen • Konfigurationsmöglichkeit feingranularer Fernwartungsbeziehung pro IP und Port bis hin zu Losgröße 1

Kapitel 6: Architektonische Aspekte/Zielarchitekturen

6.2. Tiefengestaffelte Verteidigung (Defence in Depth)

Segmentierte Netzwerke folgen dem Konzept der tiefengestaffelten Verteidigung, bei dem Zugriffe von inneren Systemen auf äußere erlaubt sind, aber nicht umgekehrt

Lösung von genua

- Das Portfolio von genua bietet verschiedene Lösungen zur Segmentierung
- Nutzen von genubox als Paketdaten-Firewall
- Rendezvous Server: Segmentierung der Fernwarter- und Zielnetze
- Servicebox: Im Fall erwünschter Zugriffe Regelsatz auf „Fernwartung“ umstellen (zudem lässt ALG nur erlaubte Protokolle zu)

Bei Fernzugriffen erfolgt die Umkehrung, da der Zugreifende sich in der Regel in einer niedriger geschützten Sicherheitszone befindet und auf eine höher geschützte Sicherheitszone zugreift

Lösung von genua

Verbindungsaufbau immer von innen zum Rendezvous-Server (dedizierter Server als zentrales Fernwartungs-Gateway in der DMZ)

- Durchgängige Wartungsverbindung erst mit bestätigtem Rendezvous
- Ansprechen der Maschinenanlage, bzw. des Zielsystems konfiguriert und kontrolliert
- Anbindung von Virenscanner zum Schutz vor Schadcode im Fall von Datenübertragung

Um unbefugten Datenverkehr in dieser Richtung zu verhindern, sollte eine Multi-Faktor-Authentifizierung eingesetzt werden, z. B. telefonische Anrufe oder Einmal-Passwörter

Lösung von genua

- Individuelle Abstimmungskanäle möglich
- Multifaktor- oder OTP-Authentifizierung des Fernwarters

Kapitel 6: Architektonische Aspekte/Zielarchitekturen

6.3. Security-Betrachtung der Fernzugriffsvarianten

6.3.1. Ferndiagnose

	Lösung von genua
Datenfluss-Richtung vom Zielsystem zum Fernzugreifenden oder Dienst: Sicherstellung durch Netzwerkarchitektur (z. B. mit Hilfe einer Datendiode oder Firewall)	• Durch zeitliche oder manuelle Auslöser konfigurierbare Öffnung nach außen (zeitlich begrenzt oder auch dauerhaft) • Optimal und optional: Datendiode cyber-diode mit dauerhafter One-Way-Kommunikation ausschließlich nach außen

6.3.2. Fernüberwachung

	Lösung von genua
• **Datenflussrichtung von Prozessinformationen und Instandhaltungsinformationen nach außen** • **Keine Änderung am Zielsystem** • **Verbindung nur in benötigtem Zeitrahmen**	• Durch zeitliche oder manuelle Auslöser konfigurierbare Öffnung nach außen (zeitlich begrenzt oder auch dauerhaft) • Optimal und optional: Datendiode cyber-diode mit dauerhafter One-Way-Kommunikation ausschließlich nach außen

6.3.3. Fernsteuerung

	Lösung von genua
Dauerhafte Verbindung besteht, Notwendigkeit wird regelmäßig überprüft	• Anwendungssensitive SSH-Fernwartungszugriffe ohne Netzkopplung • Umfassende Governance mit vollständiger Kontrolle über alle Fernzugriffe • Zeitliche, räumliche, rollenspezifische, auf das Zielsystem beschränkte Zugriffe konfigurierbar

Kapitel 6: Architektonische Aspekte/Zielarchitekturen

6.3.4. Fernwartung

	Lösung von genua
• **Zugriff von neutral nach innen, aber zeitlich begrenzt** • **Gilt auch für „passive Fernwartung“: Aktive Tätigkeiten durch Betreiber unter Anleitung des Fernzugreifenden**	• Zentrale Verwaltbarkeit mit jederzeit vollständiger Kontrolle über Wartungsaktion, Zugriffszeitpunkt, Ziel und zugreifende Instanz • Hohe Betriebssicherheit durch Bestätigung der Verbindungsaufnahme von innen, z. B. per Windows-App, Operator GUI im zentralen Managementsystem oder Schlüsselschalter • Einfache und einheitliche Bedienung einer Vielzahl von Services und Integration von Fremdlösungen möglich • Viren-/Malware-Schutz durch Datenprüfung mittels externer Virenscanner über ICAP-Schnittstelle • Sicherheitsniveau an Bedarf anpassbar, „offener“ und fortlaufender Zugriff bis hin zu vollständiger Kontrolle • Zeitliche, rollenspezifische, auf das Zielsystem beschränkte Zugriffe konfigurierbar (bereit für „geolokale Einschränkungen“) • Leistungsstarkes Rechte- und Rollensystem • Höchste Sicherheit und Kontrolle durch anwendungsgenauen Zugriff auf das vom Rest der Anlage isolierte Zielsystem sowie Rendezvous-Punkt in der DMZ oder in der Cloud • Video-Aufzeichnungsfunktion und Logging • Alle Produktiv- und Management-Systeme sind als Hardware- und virtualisierte Appliances erhältlich, Servicebox-Hardware ist auch als Industrial-Variante mit zweckgemäßem Temperaturbereich und Formfaktor sowie Komfort-Features wie z. B. Schlüsselschalter verfügbar • Hochsicherer Update-Mechanismus schützt genubox-Software vor Angriffen mit Quantencomputern • Eingabegeräte des Zugreifenden deaktivierbar, lediglich Screen Sharing und mündliche Anweisung

6.4. Zentraler Fernzugriffspunkt

	Lösung von genua
• **Nutzung weniger Fernzugriffslösungen** • **Bestenfalls über bereits bestehende Kommunikationswege**	• Abbildung einer einheitlichen Governance für eine Vielzahl von verschiedenen Fernwarter-Services • Integration von Fremdlösungen möglich

6.5. Rendezvous-System

	Lösung von genua
• **Kommunikationspartner verbinden sich zu drittem System** • **Fallweise Freischaltung der Verbindung** • **Treffpunkt in DMZ des Betreibers oder dessen Cloud Umgebung** • **Kein direktes VPN auf Zielsysteme**	• Zeitliche, räumliche, rollenspezifische, auf das Zielsystem eingeschränkte Zugriffe konfigurierbar (Freischaltung durch Empfänger) • Leistungsstarkes Rechte- und Rollensystem • Anwendungsgenaues SSH statt netzwerkumfassender VPN-Zugriff

Kapitel 6: Architektonische Aspekte/Zielarchitekturen

6.6. Sprungserver (Jump Host)

	Lösung von genua
Sind Verbindungen auf Zielsystem nicht möglich, soll ein Sprungserver als Proxy für das Zielsystem dienen	Ist möglich, z. B. auf Windows-Server (bspw. Engineering Workstation) per RDP, von dort Zugriff auf Steuerungen

6.7. Dateiübertragung

	Lösung von genua
• **Unterbrechungsmöglichkeit von Datenübertragung durch Lösungskomponenten** • **Datenschleuse über Zusatzsystem (mit Anti-Schadsoftware)**	• Viren-/Malware-Schutz durch Datenprüfung mittels externer Virenscanner über ICAP-Schnittstelle • Verhinderung der Übertragung im Fall einer Detektion

6.8. Beispielarchitekturen

	Lösung von genua
Platzierung der Rendezvous-Instanz On-Premises oder Internet/Cloud	Fernzugriff nur über Rendezvous Server z. B. in einer Demilitarisierten Zone (DMZ) oder einer Cloud (vgl. Darstellung der Rendezvous-Lösung auf der Rückseite des Flyers*)

6.9. Dezentrale Infrastruktur

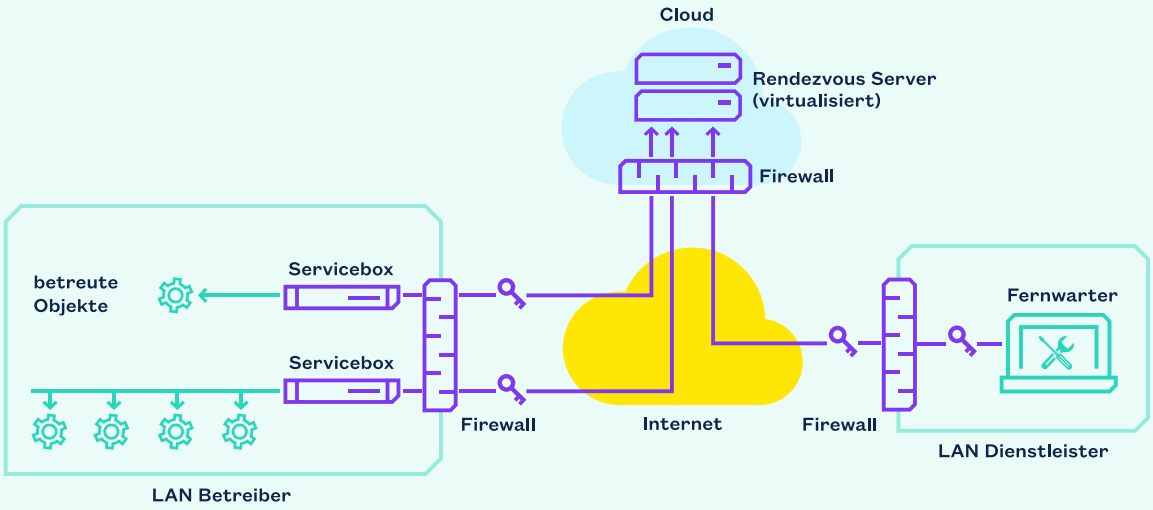
	Lösung von genua
Integrierte Lösungen (z. B. durch Hersteller des Zielsystems) mit eigenen VPN-Endpunkten erfüllen nicht den Anforderungen von erhöhtem Schutzbedarf durch mangelnde Kontrollmöglichkeit	• Integration von Herstellerlösungen möglich • Abbildung einer einheitlichen Governance für eine Vielzahl verschiedener Fernwarter-Services

* Informationen zu weiteren Einsatzmöglichkeiten und Anwendungsszenarien auf Anfrage.

Kapitel 7: Begleitende Prozesse

	Lösung von genua
Prozesse auf Basis eines ISMS	genua bietet auch Consulting: • ISMS Assessment - Reifegradanalyse des IST-Stands • ISMS Aufbau - Unterstützungsleistungen beim Aufbau eines ISMS • ISMS Awareness - Training

Interessiert? Kontaktieren Sie uns:
+49 89 991950-902 oder vertrieb@genua.de



Beispielhafte Darstellung: Die sichere Rendezvous-Lösung von genua gemäß NAMUR-Empfehlung

Die Rendezvous-Lösung von genua: Es werden keine einseitigen Zugriffe vom Fernwartungs-Service in Kundennetze zugelassen. Stattdessen laufen alle Wartungsverbindungen über einen Rendezvous Server z. B. in einer Demilitarisierten Zone (DMZ) oder einer Cloud. Hierhin bauen sowohl der Wartungs-Service als auch der Betreiber zum verabredeten Zeitpunkt Verbindungen auf.

Erst mit dem Rendezvous auf dem Server entsteht die durchgängige Wartungsverbindung. Über diese kann jetzt der Service die Maschinenanlage ansprechen, die durch die Fernwartungslösung genubox vom übrigen Kundennetz separiert wird. Durch die Rendezvous-Lösung behalten Betreiber die vollständige Kontrolle über die Wartungszugriffe in ihre Netze.

Reasons Why

- Experte für die IT-Sicherheit von Unternehmen und öffentlichen Organisationen
- Angebot eines umfangreichen, modularen IT-Security-Portfolios
- Kompromisslose Qualität bei allen Produkten, Dienstleistungen und Prozessen

genua – Excellence in Digital Security

genua entwickelt innovative, zuverlässige sowie marktprägende Produkte und Lösungen. Ob im öffentlichen Sektor, bei Betreibern kritischer Infrastrukturen (KRITIS), in der Industrie oder im Geheimschutz: Wir liefern Antworten auf die IT-Security-Herausforderungen der Gegenwart und Zukunft.

Mehr Produktinfos:
www.genua.de/genubox

genua GmbH
Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de

0224-02-DE