atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 09 2022

Peer-Review: 24.03.2022

Fernwartung und OT-Security

Anforderungen und Implementierungsansätze

Philipp Langreder, Hochschule Hannover, Frank Schmidt, onoff engineering gmbh, Karl-Heinz Niemann, Hochschule Hannover

Die technische Betreuung von Produktionsanlagen durch den Anlagenhersteller oder einen Dienstleister ist in der Industrie häufig anzutreffen. Die Durchführung solcher Wartungsarbeiten erfolgt zum Großteil vor Ort an der jeweiligen Anlage. Mit der Fernwartung gibt es jedoch die Möglichkeit, die jeweiligen Arbeiten aus der Ferne durchzuführen. Unternehmen stellen sich bei der Einrichtung einer Fernwartungslösung die Frage, wie ein solches System zu planen ist. Der vorliegende Artikel beleuchtet daher, welche Anforderungen an Fernwartungssysteme zu stellen sind, welche Fernwartungskonzepte es gibt, was allgemein bei dem Einsatz eines Fernwartungssystems insbesondere aus Sicht der OT-Security zu beachten ist und wie die NOA Verification of Request bei der Fernwartung einzusetzen ist.

#Fernwartung #OT-Security #Verification of Request

Remote maintenance and OT security

Requirements and implementation approaches

Technical support for production plants is frequently provided by the plant manufacturer or a service provider. For the most part, such maintenance work is carried out on site at the plant in question. With remote maintenance, however, there is the option of performing the work remotely. This article considers what requirements need to be met by remote maintenance systems, and what remote maintenance concepts are available. We also consider what should generally be taken into account when using a remote maintenance system, particularly from the point of view of OT security, and how the NOA Verification of Request should be used for remote maintenance.

#remote maintenance #OT security #Verification of Request

1. Einleitung

Mit der 2020 in Deutschland beginnenden Coronapandemie und der daraus resultierenden Notwendigkeit zur Kontaktreduzierung gehen Unternehmen verstärkt dazu über, Dienstleistungen „remote“ ausführen zu lassen. Gleichzeitig hat sich in dieser Zeit die Anzahl der Angriffe durch Cyberkriminelle deutlich erhöht [1]. Dieser Trend führt verstärkt zu Überlegungen in Unternehmen, wie ein Fernwartungssystem effizient betrieben werden kann und wie gleichzeitig die OT-Security der Anlage gewährleistet werden kann. Im vorliegenden Artikel wird daher dargelegt, welche Punkte bei der Planung und dem Einsatz eines Fernwartungssystems zu beachten sind, um die OT-Security bei einem Fernzugriff zu gewährleisten.

Die vorliegenden Erkenntnisse basieren auf der Masterarbeit von Philipp Langreder. In dieser wurden neben den Anforderungen an die Fernwartung mögliche Fernwartungskonzepte und sonstige Punkte untersucht, die beim Einsatz der Fernwartung zu beachten sind. Dieser Beitrag gibt die allgemeinen Aspekte der Arbeit wieder. Ein Produktvergleich und Preisangaben zu den betrachteten Systemen sind jedoch nur Bestandteil der Masterarbeit, nicht jedoch dieses Beitrages.

In diesem Beitrag werden die folgenden Begriffe verwendet, die nachfolgend kurz erläutert werden sollen:

- **Demilitarisierte Zone (DMZ):** Bei der DMZ handelt es sich um einen Bereich vor dem Intranet eines Unternehmens, der zum Schutz des Unternehmensnetzwerks durch eine Firewall vom restlichen Unternehmensnetzwerk getrennt ist. In der DMZ befinden sich beispielweise Web-Server, die dauerhaft aus dem Internet erreichbar sein sollen. [2]

- **Fernwarter:** Person, die sich mithilfe eines Fernwartungssystems zu einer Anlage eines fernzuwartenden Unternehmens verbindet, um diese zu warten oder sonstige Arbeiten durchzuführen.

- **Fernzuwartendes Unternehmen**: Industrielles Unternehmen, dessen Anlagen teilweise von dritten Unternehmen

Tabelle 1: Auflistung der betrachteten Fernwartungssysteme.

Hersteller	Fernwartungssystem	Website des Herstellers
ads-tec Industrial IT GmbH	» Fernwartungsrouter *IRF 1000/2000 Serie* » Cloud-Server *Big-LinX®*	https://www.ads-tec-iit.com/
BeyondTrust	» Fernwartungsrouter *Bomgar Box* » Fernwartungssoftware *Bomgar Remote Support*	https://www.beyondtrust.com/
genua GmbH	» Fernwartungsrouter *genubox* » Fernwartungsapp *ReSi* » Verwaltungssystem *genucenter*	https://www.genua.de/
HMS Industrial Networks	» Fernwartungsrouter *Ewon-Cosy+* » Cloud-Server *Talk2M*	https://www.hms-networks.com/
INSYS icom	» *Insys*-Fernwartungsrouter » Cloudplattform *icom Connectivity Suite*	https://www.insys-icom.com/
ISL Online AG	» ISL *Remote-Desktop-Software*	https://www.islonline.com/
LUCOM GmbH	» *SmartFlex*-Fernwartungsrouter » Cloud-Server *Digicluster V3*	https://www.lucom.de/
MB connect line GmbH	» Fernwartungsrouter *mbNET* » Cloud-Server *mbCONNECT24*	https://mbconnectline.com/
Phoenix Contact Deutschland GmbH	» Fernwartungsrouter *mGuard* » Cloud-Server *mGuard Secure Remote Service*	https://www.phoenixcontact.com/
Sabo Elektronik	Keine Angabe	https://www.sabo.de/
Siemens AG	» Fernwartungsrouter *SCALANCE* » Rendezvous-Server *SINEMA Remote Connect*	https://www.siemens.com/
symmedia GmbH	» Softwarelösung *symmedia SP/1 Remote Service*	https://www.symmedia.de/
TeamViewer AG	» Softwarelösung *TeamViewer*	https://www.teamviewer.com/
Tosibox Oy	» Fernwartungsrouter *TOSIBOX-Lock* » Hardwarezertifikat *TOSIBOX Key*	https://www.tosibox.com/
Wieland Electric GmbH	» *Wieland*-Fernwartungsrouter » Cloud-Server *Wie-Service24 Portal*	https://www.wieland-electric.com/
Zedas GmbH	» Individuell auf den Kunden angepasste Lösung *zedas®secure*	https://www.zedas.com/

aufgebaut wurde. Die Wartung dieser Anlagenteile kann damit ggf. dem Aufgabenbereich dieses dritten Unternehmens zufallen.

» **Fernwartungssystem:** Ein System bestehend aus mehreren Fernwartungskomponenten, dass dazu entwickelt wurde, die Wartung einer industriellen Anlage zu ermöglichen, ohne dass sich die Fernwarte vor Ort befindet. Das System soll dabei definierte OT-Security-Anforderungen erfüllen, um die zu wartende Anlage nicht zu gefährden.

» **Fernwartungskomponenten:** Alle Bestandteile, die das verwendete Fernwartungssystem hat. D. h. Fernwartungsrouter, Fernwartungsserver, Fernwartungssoftware.

2. Stand der Technik

Eine große Herausforderung ist derzeit vor allem das große Angebot an verschiedenen Fernwartungssystemen. Da es keinen festgelegten Standard gibt, nachdem ein Fernwartungssystem zu entwickeln ist, unterscheiden sich diese teilweise signifikant voneinander. [3] Damit ist es nicht ohne weiteres möglich zu differenzieren, welches System für den jeweiligen Einsatz am besten geeignet ist.

Im Rahmen der Masterarbeit von Philipp Langreder wurden insgesamt 16 verschiedene Fernwartungssysteme verschiedener Hersteller näher betrachtet, die in der voranstehenden Tabelle 1 in alphabetischer Reihenfolge aufgelistet sind. Die Auswahl soll einen Überblick auf verfügbare Produkte liefern und stellt keine Wertung da.

Bei einer ersten Betrachtung der Tabelle ist nicht ersichtlich, welches der genannten Systeme beispielweise am besten für den Einsatz in kritischen Infrastrukturen geeignet ist. In Kapitel 4 wird daher aufgezeigt, worauf bei der Auswahl eines Fernwartungssystems zu achten ist.

Aufgrund der steigenden Anzahl von Angriffen durch Cyberkriminelle [1], stellt die Sicherstellung, dass zur Fernwartung verwendete Computer nicht kompromittiert werden,

eine weitere große Herausforderung dar. Im Rahmen eines Fernwartungskonzeptes werden in Kapitel 5 daher Möglichkeiten aufgezeigt, mit denen das Risiko einer Systemkompromittierung deutlich verringert werden kann.

3. Anforderungen an Fernwartungssysteme

Laut dem BSI zählt die Kompromittierung einer Anlage über einen Fernwartungszugang zu den Top 10 Risiken der OT-Security [4],[5]. Damit Fernwartungssysteme sicher implementiert werden können, haben das BSI und weitere Institutionen Anforderungskataloge herausgegeben, die bei der Implementierung von Fernwartungssystemen zu beachten sind. Dies sind:

- **„Fernwartung im industriellen Umfeld v2.0“:** In diesem Dokument des BSI werden Empfehlungen aufgeführt, die ein Fernwartungssystem im industriellen Bereich erfüllen sollte. Dabei handelt es sich um Empfehlungen hinsichtlich der OT-Security der eingesetzten Fernwartungskomponente und um Empfehlungen für den Umgang mit diesen [3].

- **„Grundregeln zur Absicherung von Fernwartungszugängen v2.0“:** Dieses Dokument des BSI zeigt technische Lösungsmöglichkeiten und einige Regeln auf, die bei der Fernwartung zu beachten sind. Dies Lösungsmöglichkeiten und Regeln sind nicht explizit für den industriellen Einsatz gedacht, können daraus jedoch abgeleitet werden [6].

- **„Fernwartung bei Systemen der Automatisierungstechnik in der Prozessindustrie“**: Das NAMUR Arbeitsblatt NA 135 stellt Randbedingungen für die Fernwartung von Systemen der Automatisierungstechnik in der Prozessindustrie dar. Außerdem werden technische und methodische Anforderungen an den Ablauf einer Fernwartung aufgezeigt [7].

- **Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – DIN EN IEC 62443-3-3 (Systemanforderungen zur IT-Sicherheit und Security-Level):** Dieser Teil der Norm soll die IT-Sicherheit von industriellen Automatisierungssystemen sicherstellen. Dazu werden in mehreren Abschnitten allgemeine IT-Security-Anforderungen an OT-Systeme aufgelistet. Diese Anforderungen werden entsprechend des erreichbaren Security Level nach IEC 62443-1-1 gefordert (SL-C) [8].

Im Rahmen der Masterarbeit wurden die Anforderungen aus den o. g. Anforderungskatalogen gesammelt, bewertet und in einem generischen Satz von Security-Anforderungen in Tabelle 2 zusammengefasst.

4. Implementierungsalternativen von Fernwartungssystemen

Bei den verschiedenen Fernwartungssystemen, die auf dem Markt zur Verfügung stehen, lässt sich zwischen den reinen Softwaresystemen und Hardwaresystemen unterscheiden.

Tabelle 2: Security-Anforderungen für Fernwartungssysteme.

Nr	Kurzbeschreibung	Security-Anforderung
1	Einheitliche Lösung	Es ist eine einheitliche Lösung zu verwenden. D. h. innerhalb eines Unternehmens ist möglichst nur ein Fernwartungssystem einzusetzen. Systeme unterschiedlicher Hersteller sind zu vermeiden.
2	Fernwartungskomponente in einer DMZ	Die Fernwartungskomponenten sollten sich in der demilitarisierten Zone (DMZ) des fernzuwartenden Unternehmen befinden und nicht direkt im Produktionsnetz.
3	Fernwartungsverbindung feingranular pro IP und Port	Das Fernwartungssystem soll eine Fernwartungsverbindung nicht pro (Sub-)Netz, sondern feingranular pro IP-Adresse und Port aufbauen.
4	Verbindungsaufbau aus dem fernzuwartenden Unternehmen heraus initiiert	Der Aufbau einer Fernwartungsverbindung soll nur erfolgen, wenn das fernzuwartende Unternehmen die Verbindung freigibt (z.B. durch Schlüsselschalter am Fernwartungsrouter). Der Aufbau einer Verbindung soll dadurch ohne das Wissen des fernzuwartenden Unternehmens nicht möglich sein.
5	Keine offenen Ports	Das über das Internet erreichbare Netzwerk des fernzuwartenden Unternehmens sollte möglichst keine dauerhaft offenen Ports für einen Verbindungsaufbau von außen aufweisen.
6	Verwendung sicherer Protokolle	Das Fernwartungssystem soll etablierte Protokolle (in aktuellster Version) wie IPsec, SSH oder SSL/TLS für einen sicheren Tunnel zwischen zwei Endpunkten verwenden. Wenn möglich, ist das SSH-Protokoll zu verwenden, da es die Kopplung einzelner Geräte ermöglicht, während IPsec für die Kopplung ganzer Netze gedacht ist.
7	Verwendung sicherer Verschlüsselungsverfahren	Das Fernwartungssystem soll hinreichend starke kryptografische Verfahren zur Verschlüsselung verwenden; Z. B. AES mit mindestens 192 Bit Schlüssellänge.
8	Verwendung starker Authentisierungsmechanismen	Das Fernwartungssystem soll die Verwendung starker Authentisierungsmechanismen. Z. B. die 2-Faktor-Authentisierung unter Verwendung einer nicht kopierbaren Hardwarekomponente (z.B. Smart Cards, USB Token, …) verwenden.

Nr	Kurzbeschreibung	Security-Anforderung
9	Hohe Passwortsicherheit	Mittels einer Passwort-Policy soll im Fernwartungssystem ein Mindestniveau der Passwortqualität sichergestellt werden. D. h. es sind Vorgaben zur Verwendung von Sonderzeichen, Passwortlänge, etc. zu machen.
10	Vorhandene Benutzerverwaltung	Es soll die Möglichkeit bestehen, mehrere Benutzer mit verschiedenen Rechten anzulegen.
11	Zuweisung von Benutzerrechten	Benutzerrechte sollen auf bestimmte Geräte beschränkbar sein. Werden z. B. mehrere Fernwartungsrouter eingesetzt, soll es möglich sein, dass ein Fernwarter nur auf festgelegte Router bzw. Anlagenteile hinter einem Fernwartungsrouter Zugriff hat.
12	Fehlgeschlagene Anmeldeversuche erkennen	Fehlgeschlagene Anmeldeversuche sollen erkannt und protokolliert werden.
13	Logging der Fernwartung	Fernwartungssitzungen (wer, wann, wie lang) sind zu protokollieren.
14	Aktive Fernwartungssitzungen erkennbar	Aktive Fernwartungssitzungen sind deutlich erkennbar zu machen.
15	Fernwartungssitzungen unterbrechbar	Aktive Fernwartungssitzungen sollen jederzeit unterbrechbar sein.
16	Unterbrechung bei Inaktivität	Fernwartungszugänge sollen sich nach einer vorgebbaren Zeit automatisch schließen.
17	Bildschirmaufzeichnung der Fernwartung	Bei Fernwartungsvorgängen mit Bildschirmübertragung soll diese Übertragung aufgezeichnet werden, um die Fernwartung später nachvollziehen zu können.
18	Kundennetze nicht verknüpfen	Sollte ein Fernwarter mehrere Kunden fernwarten, muss gewährleistet sein, dass die Netze seiner Kunden nicht miteinander verbunden werden.
19	Fernwartungsobjekt isolieren	Das Fernwartungsobjekt sollte zumindest während einer Fernwartungssitzung soweit wie möglich vom Rest des Netzes isoliert werden. Z. B. mittels Paketfiltern.
20	Online-Dienste beschränken	Online-Dienste zur Fernwartung, bei denen die Verbindung über einen externen Dienstleister hergestellt wird, sind auf möglichst wenige Fälle beschränken, da die Kontrolle über die eigenen Daten kurzzeitig abgegeben wird. Außerdem ist nicht gewährleistbar, dass die Server jederzeit erreichbar sind.
21	Sicherheitsgateways möglichst wenig modifizieren	Für die Implementierung des Fernwartungssystems sollen Modifikationen an zentralen Sicherheitsgateways so gering wie möglich gehalten werden.
22	Regelmäßige Updates	Das Fernwartungssystem muss regelmäßige Sicherheitsupdates erhalten.
22	Regelmäßige Updates	Das Fernwartungssystem muss regelmäßige Sicherheitsupdates erhalten.

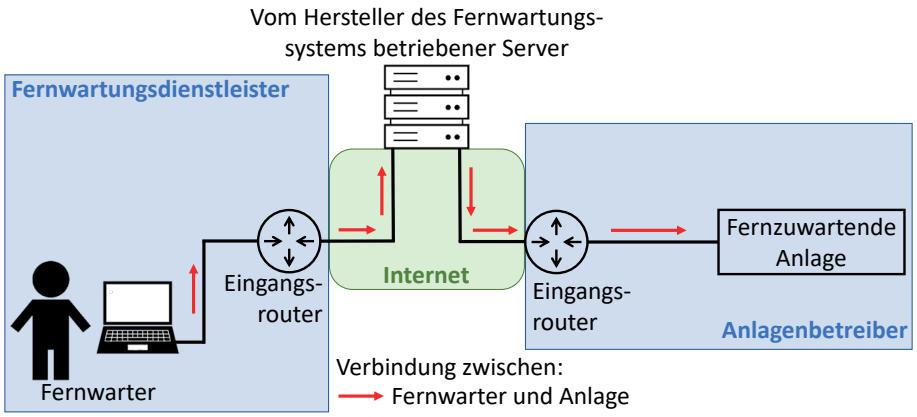

Abbildung 1: Fernwartung mit einem Softwaresystem.

Die Hardwaresysteme sind außerdem noch in die Systeme mit Rendezvous-Server und die Systeme mit Cloud-Server unterteilt. Die verschiedenen Systemtypen werden im Folgenden näher beschrieben [9], [10].

4.1 Softwaresysteme zur Fernwartung

Bei Softwaresystemen ist lediglich eine Fernwartungs-Software auf dem Computer des Fernwarters (links in Abbildung 1) und der fernzuwartenden Anlage (rechts in Abbildung 1)

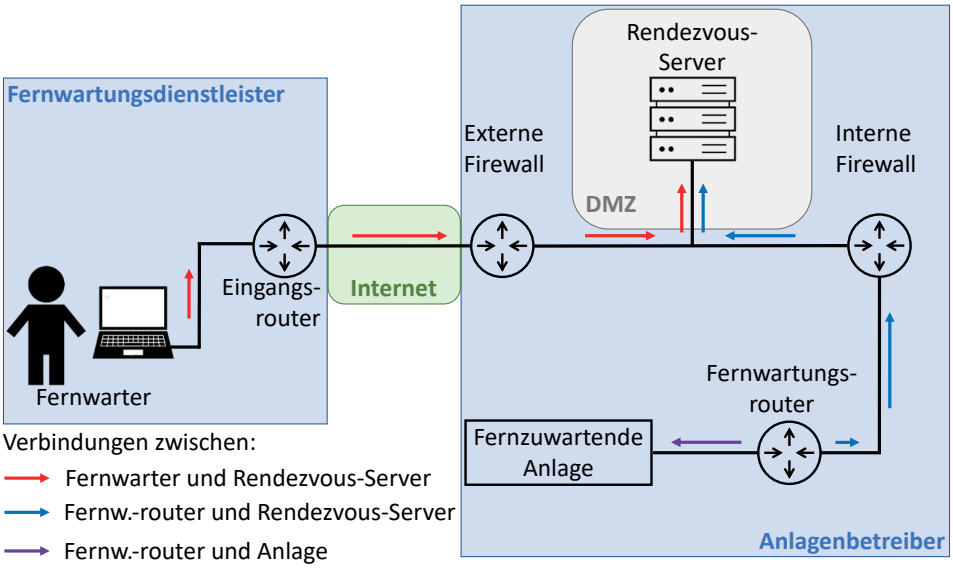

Abbildung 2: Fernwartung mit einem Hardwaresystem – Rendezvous-Server.

zu installieren. Bei der fernzuwartenden Anlage handelt es sich z. B. um eine Engineering Workstation des Automatisierungssystems. Bei Softwaresystemen wird außerdem ein Server benötigt (in der Mitte von Abbildung 1), der die gesamte Fernwartung abwickelt. Dieser wird in der Regel vom Hersteller des Fernwartungssystems betrieben. Die Fernwartungsverbindung muss immer den Eingangsrouter des Anlagenbetreibers und Fernwarters durchlaufen. I. d. R. sind dazu keine Anpassungen der Firewall notwendig, da Softwaresysteme mittels TCP und UDP eine Direktverbindung aufbauen und die dafür notwendigen Ports 80 oder 443 i. d. R. schon freigegeben sind. Sind diese Ports nicht freigeben, bzw. sollen diese nicht freigegeben werden, können für das jeweilige Softwaresystem i. d. R. auch andere, vom Hersteller des Systems definierte Ports freigegeben werden. Alle dargestellten Komponenten innerhalb eines Unternehmens werden i. d. R. über eine Ethernetleitung miteinander verbunden.
Zum Aufbau der Fernwartungsverbindung (rote Pfeile in Abbildung 1) erhält der Fernwarter eine ID und ein Passwort vom Anlagenbetreiber, die er in der Fernwartungs-Software eingibt und danach den vollständigen Zugriff zu dem fernzuwartenden System hat. Aufgebaut wird die Verbindung hierbei i. d. R. über die Server des verwendeten Fernwartungssystems, die von dem jeweiligen Hersteller des Fernwartungssystems betrieben werden. Die in Abbildung 1 dargestellte Hardware ist i. d. R. vorhanden, wodurch keine zusätzlichen Hardware-Beschaffungen notwendig sind.

4.2 Hardwaresysteme mit Rendezvous-Server

Ein Rendezvous-Server ist ein in der DMZ des Fernwarters oder in der DMZ des Anlagenbetreibers stehender Server (s. Abbildung 2). Dabei ist zu beachten, dass mehrere Kunden nur über einen Rendezvousserver ferngewartet werden dürfen, wenn dieser beim Fernwarter steht, da ansonsten die Netzwerke von mehreren Kunden miteinander verbunden werden (s. Nr. 18 in Tabelle 1). Bei dem Rendezvous-Server handelt sich entweder um eine separate Hardware oder um eine Software, die in einer virtuellen Maschine (VM) auf einem evtl. schon vorhandenen Server betrieben wird. Da der Rendezvous-Server innerhalb der DMZ betrieben wird, ist er dauerhaft aus dem Internet erreichbar.
Für eine erhöhte OT-Security ist für Hardwaresysteme mit Rendezvous-Server vorzugsweise eine zweistufige DMZ zu verwenden, mit einem Router in Richtung des Intranets des Unternehmens (interne Firewall in Abbildung 2) und einem Router in Richtung des Internets (externe Firewall in Abbildung 2). Im Gegensatz zu der einstufigen DMZ (ein Router, der über Firewalleinstellungen eine DMZ realisiert), besteht hierbei der Vorteil, dass ein Angreifer zwei Router/Firewalls überwinden muss, bevor er in das Unternehmensnetzwerk eindringen kann.
Zusätzlich zu dem Rendezvous-Server wird ein Fernwartungsrouter (unten rechts in Abbildung 2) direkt vor der fernzuwartenden Anlage benötigt. Damit ist sichergestellt, dass ein Fernwarter nur Zugriff auf die Anlage hinter dem Router hat. Das restliche Netzwerk des Anlagenbetreibers wird durch die integrierte Firewall des Fernwartungsrouters abgetrennt. Außerdem benötigt der Fernwarter einen Computer mit der dem Fernwartungssystem zugehörigen Fernwartungssoftware (links in Abbildung 2).
Wie bei den Softwaresystemen sind auch hier alle Komponente innerhalb eines Unternehmens über Ethernet verbunden. Ebenfalls gibt es auch hier einen Eingangsrouter beim Fernwartungsdienstleister, der bei einer Fernwartung durchlaufen wird, aber ansonsten keinerlei Anpassungen bedarf.
Für den Aufbau einer Fernwartungsverbindung muss der Fernwarter zunächst mithilfe der Fernwartungssoftware eine VPN- oder SSH-Verbindung zu dem Rendezvous-Server aufbauen (rote Pfeile in Abbildung 2). Dafür muss in der externen Firewall der Port für das verwendete Tunnelprotokoll (VPN oder SSH) freigegeben sein. In der internen Firewall dürfen diese Ports jedoch nicht freigegeben werden, da dies die IT-Sicherheit des Automatisierungsnetzwerks des Anlagenbetreibers negativ beeinträchtigen würde.

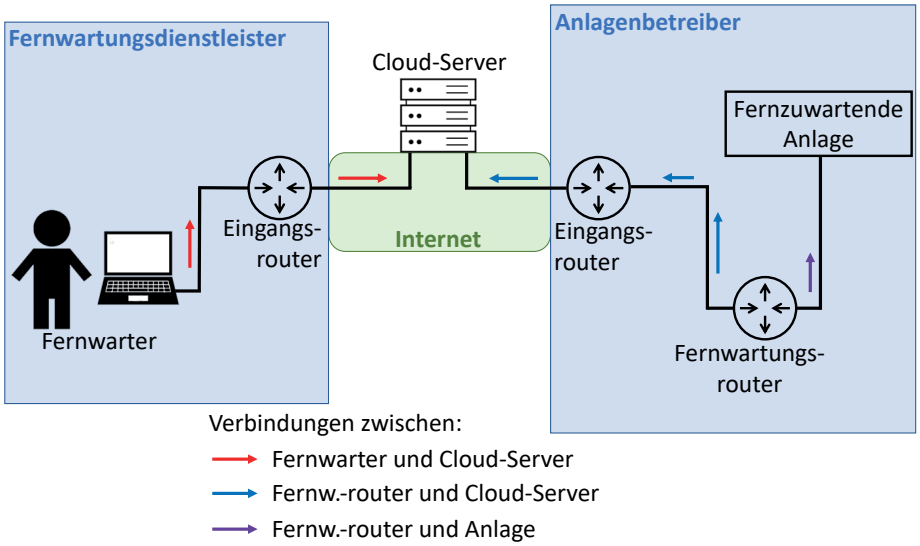

Abbildung 3: Fernwartung mit einem Hardwaresystem – Cloud-Server.

Nach dem Aufbau der Verbindung zum Rendezvous-Server werden dem Fernwarter in der Fernwartungssoftware alle Fernwartungsrouter angezeigt, zu denen er sich verbinden kann. Damit es keine offene Verbindung in das Automatisierungsnetzwerk des Anlagenbetreibers gibt, die ein Angreifer nutzen könnte, besteht zur Sicherheit keine permanente Verbindung von den Fernwartungsroutern zum Rendezvous-Server. Diese Verbindung (ebenfalls VPN oder SSH; s. blaue Pfeile in Abbildung 2) muss manuell vom Personal des Anlagenbetreibers aufgebaut werden, nachdem der Fernwarter die gewünschte Verbindung ausgewählt hat. Dazu haben die Fernwartungsrouter i. d. R. einen Schlüsselschalter, der betätigt werden muss oder eine Software-Komponente, in der diese Verbindung freigegeben werden.
Sobald von der fernzuwartenden Anlage und vom Fernwarter eine Verbindung zum Fernwartungsserver besteht, werden diese Verbindungen automatisch miteinander verknüpft. Über diese verknüpfte Verbindung werden alle Daten, die mit der Fernwartung zusammenhängen, übertragen. Dabei ist zu beachten, dass die Pfeilrichtung nur für den Verbindungsaufbau zwischen Fernwarter und Fernwartungsrouter entscheidend ist. Sobald die Verbindung besteht, ist diese entlang der Pfeile bidirektional, womit eine Kommunikation in beide Richtungen möglich ist.
Nach erfolgreichem Verbindungsaufbau wird dem Fernwarter vom Fernwartungsrouter der Zugriff auf die Anlagen freigegeben, mit denen er sich verbinden darf (violetter Pfeil in Abbildung 2). Verbindungen zu Anlagen, die der Fernwarter nicht warten darf, lässt der Fernwartungsrouter nicht zu. Zu beachten ist hierbei, dass es sich bei der Verbindung zwischen Fernwartungsrouter und Anlage i. d. R. nicht um eine VPN- oder SSH-Verbindung handelt.

4.3 Hardwaresysteme mit Cloud-Server

Im Gegensatz zu dem in Kapitel 4.2 beschriebenen Rendezvous-Server wird für einen Cloud-Server keine Hardware oder Software in der DMZ des Anlagenbetreibers benötigt. Ein Cloud-Server wird von dem Hersteller des Fernwartungssystems auf einem aus dem Internet erreichbaren Server betrieben (s. Abbildung 3). Je nach Fernwartungssystem kann dieser Server in Deutschland, anderen EU-Staaten oder einem anderen Land stehen. Aus diesem Grund ist in Abbildung 3 keine DMZ beim Anlagenbetreiber eingezeichnet sondern nur ein Eingangsrouter. Der sonstige Aufbau des Fernwartungssystems mit Cloud-Server ist identisch mit dem Aufbau eines Fernwartungssystems mit Rendezvous-Server. Es gibt ebenfalls einen Fernwartungsrouter vor der fernzuwartenden Anlage (rechts in Abbildung 3), eine Fernwartungssoftware auf dem Computer des Fernwarters (links in Abbildung 3), einen Eingangsrouter beim Fernwartungsdienstleister, den eine Fernwartungsverbindung durchlaufen muss, der aber ansonsten keinerlei Anpassungen bedarf und eine Verkabelung der Komponente mittels Ethernetleitungen.
Das Konzept zum Aufbau einer Fernwartungsverbindung ist dem Konzept des Rendezvous-Servers sehr ähnlich. Zunächst muss der Fernwarter über die Fernwartungssoftware eine VPN- oder SSH-Verbindung zum Cloud-Server aufbauen (rote Pfeile in Abbildung 3). Wie beim Rendezvous-Server können in der Fernwartungssoftware alle Fernwartungsrouter eingesehen werden, mit denen sich der Fernwarter verbinden kann. Nachdem der Fernwarter die gewünschte Verbindung ausgewählt hat, muss wie bei der Lösung mit Rendezvous-Server das Personal des Anlagenbetreibers durch Betätigung eines Schlüsselschalters oder Freigabe in einer Software, eine VPN- oder SSH-Verbindung mit dem Cloud-Server aufbauen (blaue Pfeile in Abbildung 3). Danach werden die beiden Verbindungen wie beim Rendezvous-Server miteinander verknüpft und es ist wieder eine bidirektionale Kommunikation entlang der Pfeile möglich. Wie bei dem Konzept des Rendezvous-Servers wird dem Fernwarter danach auch hier im Fernwartungsrouter der Zugriff auf die Anlagen freigegeben, mit denen er sich verbinden darf (violetter Pfeil in Abbildung 3). Es handelt sich bei der Verbindung zwischen Fernwartungsrouter und Anlage ebenfalls nicht um eine VPN- oder SSH-Verbindung.
Im Gegensatz zum Rendezvous-Server-Konzept müssen jedoch dauerhaft Ports am Eingangsrouter des fernzuwar-

Tabelle 3: Security-Anforderungen für Fernwartungssysteme.

Nr	Security-Anforderungen (Kurzbeschreibung)	Softwaresysteme	Hardwaresysteme	
			Rendezvous-Server	Cloud-Server
1	Einheitliche Lösung	+	+	+
2	Fernwartungskomponente in einer DMZ	–	+	–
3	Fernwartungsverbindung feingranular pro IP und Port	–	+	+
4	Verbindungsaufbau aus dem fernzuwartenden Unternehmen heraus initiiert	+	+	+
5	Keine offenen Ports	0	+	–
6	Verwendung sicherer Protokolle	+	+	+
7	Verwendung sicherer Verschlüsselungsverfahren	+	+	+
8	Verwendung starker Authentisierungsmechanismen	0	+	+
9	Hohe Passwortsicherheit	0	+	+
10	Vorhandene Benutzerverwaltung	0	+	+
11	Zuweisung von Benutzerrechten	0	+	+
12	Fehlgeschlagene Anmeldeversuche erkennen	0	+	+
13	Logging der Fernwartung	0	+	+
14	Aktive Fernwartungssitzungen erkennbar	+	+	+
15	Fernwartungssitzungen unterbrechbar	+	+	+
16	Unterbrechung bei Inaktivität	–	+	0
17	Bildschirmaufzeichnung der Fernwartung	–	0	–
18	Kundennetze nicht verknüpfen	+	+	+
19	Fernwartungsobjekt isolieren	–	+	0
20	Online-Dienste beschränken	–	+	–
21	Sicherheitsgateways möglichst wenig modifizieren	+	+	–
22	Regelmäßige Updates	+	+	+
	Summe von **+**	9	21	15
	Summe von **0**	7	1	2
	Summe von **–**	6	0	5

tenden Unternehmens freigegeben werden, damit eine VPN- oder SSH-Verbindung überhaupt möglich wird. Sofern diese Ports nicht nach jeder Fernwartung manuell geschlossen werden, sind diese auch freigegeben, wenn vom Fernwartungsrouter keine aktive Verbindung zum Cloud-Server besteht.

4.4 Bewertung der Konzepte anhand der Security-Anforderungen

Die Bewertung der verschiedenen Konzepte erfolgt mittels der voranstehenden Tabelle 3 anhand der Bewertungskriterien aus Tabelle 2. In der Tabelle werden folgende Symbole verwendet:

- **+** : Kriterium erfüllt
- **0** : Kriterium wird nur eingeschränkt erfüllt
- **–** : Kriterium wird nicht erfüllt

Wie in Tabelle 3 zu sehen ist, können Hardwarelösungen mit Rendezvous-Server fast alle Anforderungen erfüllen, während vor allem die Softwarelösungen mehrere Kriterien nicht oder nur teilweise erfüllen können.

Aus Sicht der OT-Security sind Softwaresysteme damit am wenigsten für eine Fernwartung geeignet. Je nach verwendetem System besteht oft keine Möglichkeit der Strukturierung von Benutzergruppen und der Zuweisung von Rechten. Durch die Verbindung über einen externen Server sind Fernwartungsdaten außerdem kurzzeitig unter der Kontrolle eines Dritten. Dabei kann nicht sichergestellt werden, was dort mit den Daten geschieht. Außerdem kann nicht garantiert werden, dass der Server des Fernwartungsanbieters zu jedem Zeitpunkt erreichbar ist. Ein weiterer Nachteil ist hierbei, dass die Möglichkeit besteht, vom fernzuwartenden System auf den Rest der Anlage zuzugreifen, da die ferngewarteten Anlagen nicht vom restlichen Anlagennetzwerk isoliert werden.

Tabelle 4: Organisatorische Maßnahmen zur Fernwartung.

Nr	Konzeptvorschläge
1	Festlegen, welche Personen dazu befugt sind, eine Fernwartung durchzuführen.
2	Festlegen, welche Personen Zugang zu den Fernwartungskomponenten haben.
3	Fernwartungssoftware nur auf IT-Systemen installieren, auf denen sie benötigt wird.
4	Fernwartern vorgeben, welche IT (Computer, Mobiltelefone, …) zur Fernwartung verwendet werden darf, welche Schutzmechanismen auf der verwendeten IT einzusetzen sind (z. B. aktueller Virenschutz, Firewall, …) und wie diese aktuell gehalten wird.
5	Fernwartungssysteme ausschließlich zur Fernwartung verwenden: » Computer anschaffen, die ausschließlich zur Fernwartung verwendet werden » Wird ein Computer gerade nicht verwendet, sollte dieser in einem verschlossenen Raum, zu dem nur befugtes Personal zugangsberechtigt ist, aufbewahrt werden.
6	Es sind Richtlinien zum Umgang mit externen Speichermedien (z. B. USB-Sticks) zu erarbeiten. D. h. unter welchen Bedingungen diese eingesetzt werden dürfen, was bei dem Einsatz zu beachten ist, usw.
7	Fernwartungskomponenten (z. B. Fernwartungsrouter) möglichst unzugänglich (in verschließbaren Schaltschränken/Räumen) platzieren. » Nur befugtem Personal den Zugriff erlauben.
8	Alle Komponente, die bei der Fernwartung verwendet werden (Fernwartungsrouter, Rendezvous-Server, Computer), sind auf dem neusten Software-Stand zu halten.
9	Nur unbedingt erforderliche Fernwartungszugriffsmöglichkeiten implementieren. » Den Zugang zu nicht erforderlichen Anlagenteilen beschränken. » Z. B. über Benutzereinstellungen auf den ferngewarteten Systemen beschränken, welche Software ein Fernwarter verwenden kann.
10	Etablieren von Prozessen, die Freigaben von Verbindungen, Sperrungen, Notfallprozeduren und regelmäßige Wechsel von Authentisierungsdaten regeln.
11	Für jeden Benutzer einen eigenen Benutzerzugang anlegen. Gruppen-Accounts sind zu vermeiden.
12	Regelmäßige Funktionsprüfungen durchführen.
13	Nach dem Fernzugriff müssen Fernwartungsverbindungen getrennt werden. Die automatische Trennung ist zu testen.
14	Eine Fernwartungsverbindung muss immer manuell vom Anlagenbetreiber aus aufgebaut werden.
15	Sämtliche Fernwartungszugänge sind im Rahmen eines Sicherheitsmanagements zu erfassen und zu dokumentieren (Art des Zugangs, betroffene Systeme, berechtigte Personen und zugehöriger Vorgang/Prozess)
16	Genaue Dokumentation des Fernwartungskonzeptes. Sicherstellen, dass die Dokumentation aktuell bleibt.

Trotzdem haben auch Softwaresysteme ihre Berechtigung, da sie i. d. R. kostengünstig sind und für kurzzeitige Eingriffe keine eigene Hardware aufgebaut werden muss. Langfristig sind Hardwaresysteme jedoch zu bevorzugen.

Hardwaresysteme mit Cloud-Server können ebenfalls einige Kriterien von Tabelle 3 nicht erfüllen. Sie haben z. B. wie die Softwaresysteme den Nachteil, dass der Server unter der Kontrolle eines Dritten steht. Außerdem werden offene Ports im Eingangsrouter des fernzuwartenden Anlagenbetreibers benötigt, die ein Angriffspotenzial bieten. Dafür bieten diese Systeme i. d. R. eine Benutzerverwaltung mit Rechtezuweisung, einen durchgängigen Schutz der Daten mithilfe von VPN oder SSH (abhängig vom jeweiligen System), gute Verschlüsselungsalgorithmen und starke Authentifizierungsmechanismen. Außerdem wird die fernzuwartende Anlage durch den Fernwartungsrouter vom restlichen Netzwerk des Anlagenbetreibers abgetrennt, wodurch ein Fernwarter nur Zugriff auf die jeweilige Anlage hat. Je nach Fernwartungssystem besteht sogar die Möglichkeit, dem Fernwarter einzelne IP-Adressen zuzuweisen, mit denen er sich verbinden kann, falls sich mehrere Anlagen hinter einem Fernwartungsrouter befinden.

Damit sind Hardwaresysteme mit Cloud-Server, wie es auch Tabelle 3 anhand der erfüllten Anforderungen zu entnehmen ist, deutlich sicherer als Softwaresysteme und sind somit auch als langfristige Lösung oder z. B. für Inbetriebnahmen gut geeignet. Zu beachten ist dabei aber, dass durch die Nachteile, die Cloud-Server-Systeme mit sich bringen, diese bei Systemen aus dem kritischen Bereich nicht die erste Wahl darstellen sollten, da für diese eine höchstmögliche OT-Security zu gewährleisten ist.

Für Systeme aus dem kritischen Bereich eigenen sich somit Hardwaresysteme mit Rendezvous-Server am besten. Wie Tabelle 3 zeigt, können diese nahezu alle OT-Security-Anforderungen erfüllen. Im Gegensatz zu den Cloud-Server-Systemen hat der Anlagenbetreiber bei Hardwaresystemen mit Rendezvous-Servern durch den Server in der DMZ die vollständige Kontrolle über das gesamte Fernwartungssystem und die

Fernwartungsdaten sind durchgängig über eine VPN- oder SSH-Verbindung (abhängig vom jeweiligen System) geschützt. Des Weiteren kann ein Angreifer dadurch, dass die interne Firewall keine offenen Ports vom Internet in das Unternehmensnetzwerk benötigt, auch wenn er den Rendezvous-Server kompromittieren sollte, nicht in das Unternehmensnetzwerk eindringen. Darüber hinaus bietet das Hardwaresystem mit Rendezvous-Server dieselben Vorteile, wie ein Hardwaresystem mit Cloud-Server.

5. Erstellung eines Fernwartungskonzeptes

In Ergänzung zu den technischen Anforderungen an ein Fernwartungskonzept sind vorangehend weitere organisatorische Punkte aufgelistet (s. Tabelle 4). Diese organisatorischen Punkte sind aus den in Kapitel 3 aufgeführten Anforderungskatalogen abgeleitet.
Ohne passende Prozesse ist keine sichere Fernwartung möglich. Eine Abweichung von den Prozessen birgt Sicherheitsrisiken, die von der technischen Lösung der Fernwartung nicht kompensiert werden können. Je nach Anwendungsfall kann eine Ergänzung weiterer Maßnahmen erforderlich sein. Außerdem sollte das erstellte Sicherheitskonzept in ein Managementsystem für Informationssicherheit (ISMS) aufgenommen werden, sofern dies vorhanden ist.

6. Verification of Request

Die *Verification of Request* (VoR) ist ein Teil der *NAMUR Open Architecture* (NOA), die in der zukünftigen NAMUR-Empfehlung NE 178 näher spezifiziert wird. [11] Beim VoR handelt es sich um ein System, dass Änderungen an Produktionsanlagen von einem autorisierten Antragsteller entgegennimmt, diese anhand vorgegebener Anforderungen überprüft und dann entweder zulässt oder ablehnt. Außerdem gibt es an den Antragsteller den aktuellen Status zurück, d. h., dass die vorgeschlagenen Änderungen derzeit geprüft werden, die Änderungen akzeptiert/abgelehnt wurden.
Ein Antragsteller ist hierbei z. B. ein Systemintegrator, der einen Anlagenteil eines Unternehmens betreut und dafür Änderungen an der Programmierung vornimmt und vorhandene Störungen beseitigt. Bevor das VoR-System von dem Antragsteller Änderungen entgegennimmt, muss sich dieser zunächst autorisieren (z. B. mittels Einmalpasswort). [12]

6.1 VoR in der Fernwartung

VoR kann die Fernwartung und die erforderlichen Freigabevorgänge unterstützen. Beim Aufbau einer Fernwartungsverbindung kann das System durch die Authentisierung eines Antragstellers eine Remote-Service-Verbindung bestätigen oder ablehnen. Da Anlagenänderungen immer nur an das VoR-System übergeben werden, wird außerdem sichergestellt, dass ein Außenstehender nie direkten Zugriff auf die Anlage hat. Einem Angreifer wird damit die Kompromittierung einer Anlage deutlich erschwert. Des Weiteren stellt die automatisierte Prüfung von Änderungen sicher, dass eine Anlage nicht durch Fehler in der Programmierung ausfällt oder Schaden nimmt.

7. Fazit

Fernwartung ist eine gute Möglichkeit, um Wartungsarbeiten effizienter zu gestalten, da das betreuende Personal ohne vorherige lange Anreisen direkt auf Anlagen zugreifen können.
Bei der Implementierung von Fernwartungssystemen ist zu beachten, dass diese aus Sicht der OT-Security ein Sicherheitsrisiko darstellen, weshalb entsprechende Sicherheitsanforderungen zu erfüllen sind. Dabei ist abzuwägen, wie hoch der Sicherheitsbedarf der jeweiligen Anlage ist, um ein geeignetes Fernwartungssystem auszuwählen. Hierbei ist zwischen den Systemen mit Rendezvous-Server, die nahezu alle genannten OT-Security-Anforderungen erfüllen, den Cloud-Server-Systemen, die nicht mehr alle OT-Security-Anforderungen erfüllen können, aber dennoch gut einsetzbar sind und den Softwaresystemen, die nur einzusetzen sind, wenn es sich nicht vermeiden lässt, da sie die wenigsten OT-Security-Anforderungen erfüllen können, zu unterscheiden.
Zusätzlich zu einem sicheren Fernwartungssystem ist die Definition zugehöriger Arbeitsprozesse unabdingbar. Nur so kann sichergestellt werden, dass die Integrität einer Anlage nicht durch eine unsachgemäße Nutzung des Fernwartungssystems verletzt wird.
Nach Herausgabe der NAMUR-Empfehlung NE 178 (liegt zur Zeit im Entwurf vor) ist außerdem eine weitere Betrachtung von VoR im Rahmen der Fernwartung zu empfehlen.

Referenzen

[1] Bundeskriminalamt. (2020). *Sonderauswertung – Cybercrime in Zeiten der Corona-Pandemie*. Abgerufen von: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html;jsessionid=A3FF890A532B758A7F55323BF332FD36.live302?nn=28110

[2] Dehn, S. (2019). Netzwerke Sicherheit. 11. Aufl. Bodenheim. Herdt

[3] Bundesamt für Sicherheit in der Informationstechnik. (2018). Fernwartung im industriellen Umfeld v2.0. Abgerufen von: https:// https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.html

[4] Bundesamt für Sicherheit in der Informationstechnik. (2022). *Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2022*. Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=5

[5] Kruglov, K., Goncharov, E. (2018*). Threats posed by using RATs in ICS*. Abgerufen von: https://ics-cert.kaspersky.com/media/KL_RAT_ICS_ENG.pdf.

[6] Bundesamt für Sicherheit in der Informationstechnik. (2018). *Grundregeln zur Absicherung von Fernwartungszugängen v2.0.* Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.html

[7] NA 135. (2011). Fernwartung bei Systemen der Automatisierungstechnik in der Prozessindustrie. NAMUR: www.namur.net

[8] DIN EN IEC 62443-3-3. (2020). Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit

und Security-Level. https://www.beuth.de

[9] SI | Sichere Industrie GmbH. (2022). *Fernwartungslösungen für Industrie und KRITIS Betreiber.* Abgerufen von: https://www.sichere-industrie.de/industrial-iiot-security-themen/industrie-fernwartung/.

[10] Iatrou, C. P., Hoppe, H., & Erni, K. (2022). NOA Verification of Request: Automatisierte Anlagenoptimierung mit Feedback aus Edge und Cloud. *atp magazin, 64*(1-2), 78-84. doi:10.17560/atp.v64i1-2.2592

[11] Tauchnitz, T. (2021). *Namur Open Architecture (NOA) – Das Konzept zur Öffnung der Prozessautomatisierung*. Vulkan Verlag

AUTOREN

Philipp Langreder, M.Eng., (geb. 1997) hat nach seinem abgeschlossenen Abitur mit dem Studium der Elektro- und Informationstechnik begonnen. Seine Abschlussarbeit schrieb er in Kooperation mit der onoff AG in Wunstorf und beendet sein Bachelorstudium an der Hochschule Hannover im August 2020. Anschließend begann er ebenfalls an der Hochschule Hannover den Masterstudiengang „Sensor- und Automatisierungstechnik“ zu studieren. Nebenbei war er in der onoff AG als Werkstudent tätig. Im Februar 2022 beendet er das Studium mit seiner Masterarbeit, die er wieder in Kooperation mit der onoff AG schrieb. Aktuell ist er für die enercity Netz GmbH tätig.

Philipp Langreder, M.Eng.
enercity Netz GmbH
30459 Hannover
Auf der Papenburg 18
@ philipp.langreder+atp@gmail.com

Dipl.-Ing. (FH) Frank Schmidt (geb. 1978) ist seit 2020 technischer Leiter der Forschung und Entwicklung der onoff engineering gmbh. Seit 2009 in mehreren Positionen bei der onoff engineering gmbh, unteranderem von 2014 bis 2020 Projektleiter für Standardisierung im Bereich der internen Modul- und Bibliotheksentwicklung für Automatisierungssysteme, sowie der Standardisierung von Engineering Prozessen.

Dipl-Ing. (FH) Frank Schmidt
onoff engineering gmbh
Niels-Bohr-Str. 6
31515 Wunstorf
✆ +49 5031 9686-225 0
@ frank.schmidt@onoff-group.de

Prof. Dr.-Ing. Karl-Heinz Niemann (geb. 1959) vertritt seit 2005 die Bereiche Industrieinformatik und Automatisierungstechnik an der Fachhochschule Hannover. Von 2002 bis 2005 war er an der Fachhochschule Nordostniedersachsen (heute Leuphana Universität) für den Bereich Prozessdatenverarbeitung zuständig. Zuvor war er in führenden Positionen in der Entwicklung von Prozessleitsystemen bei ABB, Elsag Bailey und Hartmann & Braun tätig.

Prof. Dr.-Ing. Karl-Heinz Niemann
Hochschule Hannover
Fakultät I - Elektro- und Informationstechnik
Postfach 92 02 61
30441 Hannover
✆ +49 511 92 96 12 64
@ karl-heinz.niemann@hs-hannover.de