Honeywell

Advanced

SICHERHEITSLEITFADEN

Warum Sie Advanced Controller sichern sollten 5

Systemübersicht 6

Internet/Intranet/Unternehmensnetzwerk 7
BAS-Netzwerk 7
BAS-Firewall 7
Niagara 4 Workstation 7
Ethernet-Switch 7
Advanced Plant Controller 7
HMI 7
E/A-Modul 7

Netzwerkplanung und -sicherheit 8

Ethernet-Netzwerk 8
Webserver 8
BACnet IP-Netzwerk 8
MS/TP (NC-Lizenzen) 8
USB 8
RS485 (inklusive Modbus-Lizenzen) 8
Modbus IP-Netzwerk (INT-Lizenzen) 8

Sicherheitssystem für Advanced Controller, HMI und E/A-Modul 9

Sicherheit im unkonfigurierten Zustand 9
Schutz vor nicht autorisierten Geräten 9
Kontoverifizierungscode 9
Systemkonten 9
Engineering-Systemkonto 9
Engineering-Rolle 10
Administrator-Rolle 10
Geräte-Systemkonto 10
Erstellung von Systemkonten 10
Synchronisierte Kontoverwaltung 10
Ändern des Netzwerkschlüssels für einen Advanced Controller 11
Lokale Sicherheit 11
Zugriff auf Webseiten 11
Erster Zugriff 11
Angemeldete Benutzer 12
Wiederherstellen des Kennworts 12

® U.S. Eingetragene Marke
Copyright © 2023 Honeywell Inc. • Alle Rechte vorbehalten

Schützen des Niagara Betriebssystems 12
Bewährte Verfahren 12
Firewall-Einstellung 12
Betriebssystemversion 12
Virenschutz 12
Einbruchschutz 13
Datenschutz-Grundverordnung (DSGVO) 13
Sichere Kommunikation 14
Client-Server-Beziehungen 14
Zertifikate 15
Selbst-signierte Zertifikate 15
Namenskonvention 16
Zertifikatsspeicher 16
Verschlüsselung 16
Übersicht über das Security Dashboard 16
Planung und Installation 17
Empfohlene Installation und Konfiguration 17
Nur BACnet 17
BACnet und Niagara 18
Empfehlung für Local Area Networks (LAN) 18
Dokumentation 19
Dokumentieren physischer Geräte und Konfigurationen, inklusive wichtiger Sicherheitsinformationen 19
Dokumentieren externer Systeme, insbesondere die Interaktion zwischen Advanced Plant Controller und zugehörigen Systemen 19
Zugangskontrolle und physische Sicherheit 20
Physischer Schutz von Advanced Plant Controller, HMI und E/A-Modul 20
Aufkleber am Zugangspaneel oder Gehäuse des Reglers 20
Trennen und Schützen der Netzwerke 20
Schützen von Advanced Controller, HMI und E/A-Modul 21
Bereitstellen der Anmeldedaten zum Admin-Systemkonto für den Benutzer 21
Entwickeln eines Sicherheitsprogramms 21
Physische Voraussetzungen und Umgebungsbedingungen 21
Sicherheits-Updates und Servicepakete 21
Benutzer und Kennwörter 21
Benutzer 21
Kennwörter 22
Konfigurieren eines Advanced Plant Controller 23
Erstellen und Verwalten einer Basiskonfiguration 23

Ändern der Standardkennwörter 23
Weitere Hinweise 23
Service Level Agreement 23
Konfiguration des IT-Netzwerks 23
Konfigurieren der BAS-Firewall 24
Einrichten der Authentifizierung 25
Vorgehensweise 25
Systembereitstellung 25
USB-Sicherung und Installation der CleanDist-Datei 25
Ausserbetriebnahme des Systems 25
Sicherheit von auf Advanced Niagara basierenden Produkten 26
Checkliste zum Prüfen der Installationssicherheit 27

Disclaimer

Wir haben die Richtigkeit und Genauigkeit dieses Dokuments nach bestem Wissen und Gewissen sichergestellt. Honeywell haftet jedoch nicht für Schäden jeglicher Art, einschliesslich jedoch nicht beschränkt auf Folgeschäden, die sich aus der Anwendung oder Verwendung der hierin enthaltenen Informationen ergeben. Sämtliche Informationen und Spezifikationen in diesem Dokument entsprechen dem aktuellen Stand zum Zeitpunkt der Veröffentlichung und können sich jederzeit ohne vorherige Ankündigung ändern. Die jeweils aktuellen Produktspezifikationen finden Sie auf unserer Website oder kontaktieren Sie unsere Geschäftsstelle in Atlanta, Georgia.

In den meisten industriellen Anwendungen ist die RS-485-Kommunikation standardmässig ab Werk deaktiviert, um die grösstmögliche Sicherheit zu gewährleisten. Grund dafür ist, dass diese ältere Generation von Kommunikationsbussen aus Kompatibilitätsgründen ältere Technologie verwenden und mit schwachem Sicherheitsschutz ausgestattet sind. Um einen maximalen Schutz Ihres Systems zu gewährleisten, hat Honeywell daher proaktiv die Kommunikationsanschlüsse dieser älteren industriellen Bussysteme deaktiviert (bei Auslieferung ab Werk), und Sie müssen diese explizit in der Station für jedes Netzwerk aktivieren. Sie sollten sich bei der Aktivierung dieser Anschlüsse jedoch des Risikos von Sicherheitsverletzungen bewusst sein, die durch die Verwendung von Legacy-Technologie entstehen können, darunter: Panel Bus, C-Bus, BACnet, M-Bus, CP-IO Bus, NovarNet, XCM-LCD-Protokoll, SBC S-Bus und Modbus usw.

Entwicklung gemäss ISA-62443

Honeywell wendet seit vielen Jahren die Norm ISA 62443-4-1 und entsprechende Begleitnormen an, um sichere Produkte für die Gebäudetechnik zu entwickeln. So dient in Honeywell Gebäudeprodukten die Norm ISA/IEC 62443-4-2 als Grundlage für die technischen Sicherheitsanforderungen von Komponenten und die Norm ISA/IEC 62443-3-3 als Grundlage für komplette Systeme. Diese Einhaltung der ISA/IEC 62443-Normen seitens Honeywell bietet Systemintegratoren und Kunden bei der Auswahl von Gebäudetechnologien ein hohes Mass an Sicherheit, dass unsere Produkte sich nicht nur Cyber Security auf die Fahne schreiben – sie wurden von Anfang an für höchste Cyber Security entwickelt, getestet und validiert.

Honeywell entwickelt seine Produkte streng nach ISA/IEC 62443-4-1 und wurde von einer unabhängigen Stelle nach dieser Norm bewertet und geprüft.

Einführung und Zielgruppe

Honeywell weist hiermit ausdrücklich darauf hin, dass die Regler nicht von Haus aus gegen Cyber-Angriffe aus dem Internet geschützt sind und daher ausschliesslich für die Verwendung in privaten Netzwerken vorgesehen sind. Aber auch private Netzwerke können Ziel böswilliger Cyber-Angriffe durch versierte und gut ausgerüstete IT-Spezialisten sein und müssen entsprechend geschützt werden. Kunden sollten daher die bewährten Installations- und Sicherheitsverfahren für IP-basierte Produkte des Advanced Plant Controller anwenden, um das Risiko solcher Angriffe zu minimieren.

Die folgenden Richtlinien beschreiben die allgemeinen Sicherheitsvorkehrungen für IP-basierte Produkte des Advanced Plant Controller. Sie sind aufsteigend in der Reihenfolge ihrer Risikominderung aufgelistet.

Die spezifischen Anforderungen jedes Standorts sind für jeden Fall separat zu prüfen. In den allermeisten Installationen würde eine Implementierung aller hierin beschriebenen Sicherheitsvorkehrungen weit über das für eine angemessene Systemsicherheit erforderliche Mass hinaus gehen. Die Umsetzung der Punkte 1 bis 5 (für Local Area Networks) – Siehe *„Empfehlung für Local Area Networks (LAN)“ auf Seite 18.* – erfüllt normalerweise die Anforderungen in den meisten Automations- und Leitnetzwerkinstallationen.

Dieses Handbuch enthält Anleitungen zur sicheren Installation und Konfiguration von Advanced Plant Controller, HMI und E/A-Modulen für das Personal von Honeywell Händlern. Sicherheitsrelevante Informationen zu Betrieb, USB-Sicherung und -Wiederherstellung und Installation der CleanDist-Dateien des Reglers finden Sie in der Installations- und Inbetriebnahmeanleitung (31-00584).

NOTE:

Bitte nehmen Sie sich die Zeit, alle relevanten Installations-, Konfigurations- und Betriebsanleitungen zu lesen und zu verstehen, und stellen Sie sicher, dass Sie regelmässig die neuesten Versionen abrufen

.

Tabelle 1. Produktinformationen

Produkt	**Produktnummer**	**Beschreibung**
Anlagenregler	N-ADV-134-H	Niagara Advanced Controller mit vier Ethernet-Anschlüssen, einem Anschluss für die HMI und vier RS485-Anschlüssen
	N-ADV-133-H	Niagara Advanced Controller mit vier Ethernet-Anschlüssen, einem Anschluss für die HMI und drei RS485-Anschlüssen
	N-ADV-112-H	Niagara Advanced Controller mit zwei Ethernet-Anschlüssen, einem Anschluss für die HMI und zwei RS485-Anschlüssen
HMI	HMI-DN	HMI mit DIN-Schienen-Montage
	HMI-WL	HMI mit Wand-/Schaltschrankmontage
E/A-Modul	IO-16UIO-S-S	E/A-Modul mit 16 UIO ohne HOA-Display, serielle Kommunikationsanschlüsse, Schraubklemmen
	IOD-16UIO-S-S	E/A-Modul mit 16 UIO und mit HOA-Display, serielle Kommunikationsanschlüsse, Schraubklemmen
	IO-16UI-S-S	E/A-Modul mit 16 UI, serielle Kommunikationsanschlüsse, Schraubklemmen
	IO-16DI-S-S	E/A-Modul mit 16 DI, serielle Kommunikationsanschlüsse, Schraubklemmen
	IO-8DOR-S-S	E/A-Modul mit 8 DO ohne HOA-Display, C/O-Relais, serielle Kommunikationsanschlüsse, Schraubklemmen
	IOD-8DOR-S-S	E/A-Modul mit 8 DO und mit HOA-Display, C/O-Relais, serielle Kommunikationsanschlüsse, Schraubklemmen
	IO-16UIO-S-P	E/A-Modul mit 16 UIO und mit HOA-Display, serielle Kommunikationsanschlüsse, Push-In-Klemmen
	IO-16UI-S-P	E/A-Modul mit 16 UIO, serielle Kommunikationsanschlüsse, Push-In-Klemmen
	IO-16DI-S-P	E/A-Modul mit 16 DI, serielle Kommunikationsanschlüsse, Push-In-Klemmen
	IO-8DOR-S-P	E/A-Modul mit 8 DO ohne HOA-Display, C/O-Relais, serielle Kommunikationsanschlüsse, Push-In-Klemmen
	IOD-8DOR-S-P	E/A-Modul mit 8 DO und mit HOA-Display, C/O-Relais, serielle Kommunikationsanschlüsse, Push-In-Klemmen

1. WARUM SIE ADVANCED CONTROLLER SICHERN SOLLTEN

- Sie schützen die Anlagen und Systeme Ihrer Kunden vor unbefugten Änderungen an betriebsrelevanten Sollwerten, Übersteuerungen und Zeitplänen.
- Sie verhindern den Zugriff auf Benutzerkontodaten, z. B. Benutzernamen, Kennwörter, E-Mail-Adressen, Mobiltelefonnummern (SMS) usw.
- Sie verhindern den Zugriff auf vertrauliche Geschäftsdaten, z. B. Energieverbrauchszahlen, spezielle Steuerungsstrategien und -lösungen usw.
- Sie verhindern den unbefugten Zugriff auf Regler, Computer und Netzwerke, auf denen BMS-Software und Steuergeräte installiert sind.
- Sie gewährleisten die Datenintegrität und erfüllen Ihre Rechenschaftspflichten.

2. SYSTEMÜBERSICHT

Die Übersicht zeigt eine typische Systeminstallation.

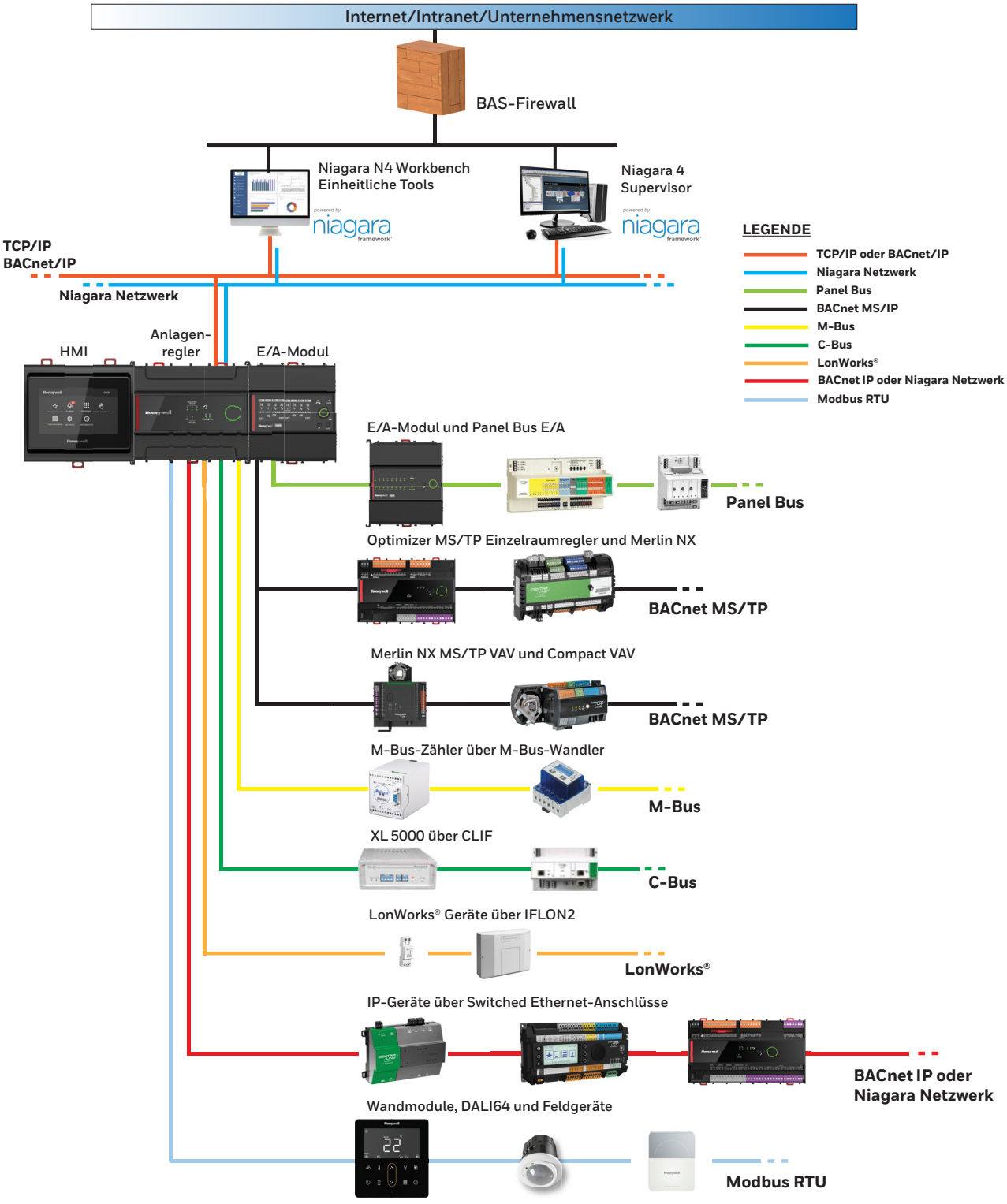

Abb. 1 Systemübersicht

2. 1 Internet/Intranet/Unternehmensnetzwerk

Hierbei handelt es sich um eine vereinfachte, logische Darstellung aller Netzwerke ausserhalb des Gebäudeautomationssystems (BAS). Der Zugriff auf die BAS-Verwaltungsschnittstellen (z. B. die Web-Benutzerschnittstelle der primären Niagara Workstation) hierüber ist optional. Es muss jedoch Zugriff auf das Internet bestehen, damit Niagara-Computer nach Betriebssystem- und Virenscanner-Updates suchen und diese herunterladen können; es sei denn, es ist eine andere Möglichkeit dafür vorgesehen.

2. 2 BAS-Netzwerk

Dieses Netzwerk wird ausschliesslich für BAS-Protokolle verwendet. Dazu gehören BACnet/IP, BACnet/Ethernet und alle Protokolle, die von den Niagara Integration Services auf einem Advanced Plant Controller verwendet werden können. Es darf sich dabei nicht um das gleiche Netzwerk wie für das Internet/Intranet/Unternehmensnetzwerk handeln.

2. 3 BAS-Firewall

Zum Trennen und Schützen des BAS muss eine Firewall zwischen Internet/Intranet/Unternehmensnetzwerk und allen verbundenen BAS-Geräten, z. B. der primären Niagara Workstation, den weiteren Niagara Workstations und dem Advanced Plant Controller, verwendet werden. Diese Firewall schränkt den Zugriff auf das BAS auf berechtigte Computer ein und kann dazu beitragen, das Risiko eines Angriffs (z. B. eines Denial-of-Service-Angriffs) zu verringern.

2. 4 Niagara 4 Workstation

Die primäre Niagara Workstation ist der Computer, auf dem die Niagara Software ausgeführt wird. Dieser benötigt zwei Netzwerkverbindungen: eine für die Verbindung mit der Web-Benutzerschnittstelle für die Verwaltung über einen Webbrowser (normalerweise im Internet/Intranet/ Unternehmensnetzwerk) und eine weitere für die Verbindung mit dem BAS-Netzwerk.

2. 5 Ethernet-Switch

Ein Ethernet-Switch erstellt Netzwerke und verwendet mehrere Anschlüsse für die Kommunikation zwischen Geräten im LAN. Ethernet-Switches unterscheiden sich von Routern, die Netzwerke verbinden und nur einen einzigen LAN- und WAN-Anschluss verwenden. Eine umfassende Infrastruktur für drahtgebundene und drahtlose Unternehmensnetzwerke bietet drahtgebundene Verbindungen und drahtlose Verbindungen über WLAN.

2. 6 Advanced Plant Controller

Der Advanced Plant Controller ist ein globaler Regler, der mit einem Ethernet-Netzwerk sowie mit BACnet IP- und Host MS/TP-Netzwerksegmenten verbunden ist. MS/TP ist eine Verbindung mit geringer Bandbreite, die für die Verbindung von Reglern und Sensoren verwendet wird.

2. 7 HMI

Die HMI wird an die Advanced Niagara Plant Controller angeschlossen und von diesen mit Strom versorgt. Sie verfügt über ein kapazitives Touchscreen-Display, das eine Auswahl mit dem blossen Finger unterstützt und Funktionen für die Anzeige, den Zugriff und die Fehlerbehebung von Reglerpunkten, E/A-Modulen und anderen verbundenen Geräten bietet.

2. 8 E/A-Modul

Die E/A-Module können über die Touchflake-Anschlüsse (Strom und Kommunikation) mit dem Regler verbunden werden. Alternativ können die E/A-Module mit einem Kabeladapter verbunden werden, der mit Strom versorgt und an eine der RS485-Schnittstellen des Reglers angeschlossen wird. Die E/A-Module sind mit den vorhandenen Engineering-Tools wie ComfortPoint Open Studio und Niagara 4 Workbench programmierbar.

3. NETZWERKPLANUNG UND -SICHERHEIT

3. 1 Ethernet-Netzwerk

Es wird empfohlen, das vom Gebäudemanagementsystem verwendete Ethernet-Netzwerk vom normalen Büronetzwerk zu trennen,

zum Beispiel

durch einen Luftspalt («air-gapped») oder ein Virtual Private Network. Der physische Zugriff auf die Ethernet-Netzwerkinfrastruktur muss eingeschränkt werden. Zudem müssen Sie sicherstellen, dass die Installation den IT-Richtlinien Ihres Unternehmens genügt.

Die Advanced Controller dürfen nicht direkt mit dem Internet verbunden sein.

3. 2 Webserver

Der Advanced Controller bietet sowohl HTTP- als auch HTTPS-Webserver. Wenn kein Webserver benötigt wird, empfiehlt es sich, beide Webserver zu deaktivieren.

3. 3 BACnet IP-Netzwerk

Aufgrund der geringen Sicherheit des BACnet-Protokolls dürfen Advanced Controller, HMI und E/A-Module, die BACnet verwenden, unter keinen Umständen mit dem Internet verbunden werden. Das Advanced Controller-Sicherheitssystem bietet keinen Schutz vor BACnet-Schreibzugriffen. Der physische Zugriff auf die BACnet IP-Netzwerkinfrastruktur muss eingeschränkt werden. Wenn keine BACnet IP-Kommunikation benötigt wird, muss das (BACnet IP) Netzwerkmodul der Advanced Controller deaktiviert werden, indem der Parameter «Disable Module» auf «1» gesetzt wird.

Ist eine BACnet-Kommunikation erforderlich, empfiehlt es sich dringend, die Services «BACnet Backup/Restore», «Reinitialize Device» und «BACnet Writable» zu deaktivieren. Dies bedeutet jedoch, dass die entwickelte Strategie nicht BTL-konform ist. Siehe *„Lokale Sicherheit“ auf Seite 11.*

3. 4 MS/TP (NC-Lizenzen)

Der physische Zugriff auf die MS/TP-Netzwerkinfrastruktur muss eingeschränkt werden. Wenn kein MS/TP-Netzwerk benötigt wird, muss das (BACnet MSTP) Netzwerkmodul der Advanced Controller deaktiviert werden, indem der Parameter «Disable Module» auf «1» gesetzt wird.

E/A-Bus (CAN-Lizenzen)
Der physische Zugriff auf den E/A-Bus muss eingeschränkt werden.

3. 5 USB

Der physische Zugriff auf den lokalen USB-Konfigurationsport des Advanced Controller muss eingeschränkt werden.

3. 6 RS485 (inklusive Modbus-Lizenzen)

Der physische Zugriff auf den RS485-Port des Advanced Controller muss eingeschränkt werden. Falls nicht erforderlich, sollten mit dem Anschluss verbundene Netzwerkmodule nicht in die Strategie einbezogen werden.

3. 7 Modbus IP-Netzwerk (INT-Lizenzen)

Aufgrund der geringen Sicherheit des Modbus-Protokolls dürfen Advanced Controller, die Modbus IP unterstützen, unter keinen Umständen mit dem Internet verbunden werden. Der physische Zugriff auf die Modbus IP-Netzwerkinfrastruktur muss eingeschränkt werden. Wenn keine Modbus IP-Kommunikation benötigt wird, sollte das (Modbus IP) Netzwerkmodul des Advanced Controller nicht in die Strategie einbezogen werden.

4. SICHERHEITSSYSTEM FÜR ADVANCED CONTROLLER, HMI UND E/A-MODUL

Das Sicherheitssystem des Advanced Controller entspricht ISA 62433-3-3 SL 3 und bietet einen sicheren Systemstart, ein authentifiziertes und verschlüsseltes Netzwerk, eine Verschlüsselung während der Speicherung und eine synchronisierte Kontenverwaltung.

Um Zugriff auf die Advanced Controller-Produkte zu erhalten oder eine der oben genannten Aufgaben auszuführen, müssen Sie einen gültigen Benutzernamen und ein Kennwort für ein Engineering-Systemkonto oder ein Geräte-Systemkonto angeben.

4. 1 Sicherheit im unkonfigurierten Zustand

Für die Interaktion mit Advanced Controller, HMI und E/A-Modulen müssen gültige Anmeldedaten angegeben werden. Der Regler wird werksseitig ohne Anmeldedaten (Systemkonten oder Benutzermodule) ausgeliefert. Dadurch ist sichergestellt, dass er beim ersten Einschalten vor unbefugtem Zugriff geschützt ist. Wenn Sie zum ersten Mal eine Verbindung zu einem vCNC in einem der Advanced Produkte innerhalb des Niagara Netzwerks herstellen, müssen Sie ein Engineering-Systemkonto mit einer Administratorrolle erstellen.

4. 2 Schutz vor nicht autorisierten Geräten

Durch einen eindeutigen Schlüssel (Netzwerkschlüssel) wird sichergestellt, dass nur autorisierte Geräte dem Niagara Netzwerk beitreten können. Alle Regler, die ein Niagara Netzwerk bilden sollen, müssen den gleichen Netzwerkschlüssel und UDP-Port haben. Diese werden bei der Erstkonfiguration mit dem IP Tool konfiguriert.

Zum Beispiel

Vier Advanced Plant Controller haben den gleichen Netzwerkschlüssel (112233) und ein fünfter hat einen anderen Netzwerkschlüssel (222). Wenn diese mit demselben Ethernet-Netzwerk verbunden werden, werden die vier Regler mit demselben Netzwerkschlüssel zu einem einzelnen Netzwerk zusammengefasst. Der fünfte Regler kann diesem Netzwerk jedoch nicht beitreten, da er einen anderen Netzwerkschlüssel (222) hat.

Gleiches gilt, wenn der fünfte Regler neu ist (ab Werk) und zum Ethernet-Netzwerk hinzugefügt wird. Auch dann kann er keine Verbindung zum Niagara Netzwerk herstellen, da er keinen Netzwerkschlüssel hat.

4. 2. 1 Kontoverifizierungscode

Wenn ein Admin-Systemkonto zu einem der Regler im Netzwerk hinzugefügt wird, generiert der Regler, zu dem das Systemkonto hinzugefügt wurde, automatisch einen Kontoverifizierungscode. Dieser Code wird auf allen anderen Reglern mit demselben Netzwerkschlüssel und UDP-Port im Ethernet-Netzwerk synchronisiert.

Sobald ein Kontoverifizierungscode generiert wurde, müssen ALLE Regler im Netz denselben Kontoverifizierungscode sowie denselben Netzwerkschlüssel und UDP-Port verwenden.

Zum Beispiel

Bei fünf Reglern haben alle Advanced Controller denselben Netzwerkschlüssel. Vier haben zudem den gleichen Kontoverifizierungscode (Account Verification Code, AVC) und bilden somit ein Netzwerk. Der fünfte Regler hat einen anderen Kontoverifizierungscode, und obwohl er denselben Netzwerkschlüssel hat, kann er nicht mit den anderen Reglern zusammengeschlossen werden.

4. 3 Systemkonten

Systemkonten ermöglichen es Personen und Geräten, mit dem Advanced Controller zu interagieren. Die Zugriffsrechte sind von der Art des Kontos und der Rolle abhängig.

Es gibt zwei Arten von Systemkonten:

1. Engineering-Systemkonto
2. Geräte-Systemkonto

4. 3. 1 Engineering-Systemkonto

Engineering-Systemkonten sind für die Nutzung durch Techniker vorgesehen. Jedes Engineering-Systemkonto verfügt über einen Benutzernamen und ein Kennwort, die bei der Anmeldung am Regler angegeben werden müssen. Wenn ein gültiger Benutzername und ein gültiges Kennwort eingegeben werden, wird der Zugriff auf den Regler gewährt.

Für jede Person muss ein separates Engineering-Systemkonto angelegt werden. Engineering-Systemkonten können für eine von zwei Rollen eingerichtet werden:

- Engineering-Rolle
- Administrator-Rolle

Engineering-Rolle
Die Engineering-Rolle bietet den notwendigen Zugriff für das Engineering des Advanced Systems, die Erstellung/Verwaltung von Geräte-Systemkonten und die Verwaltung der eigenen Kontodaten des jeweiligen Benutzers (E-Mail-Adresse, Kennwort usw.).

Administrator-Rolle
Die Administrator-Rolle bietet dieselben Zugriffsrechte wie die Engineering-Rolle und zusätzlich die Möglichkeit, alle Engineering- und Geräte-Systemkonten zu verwalten.

4. 3. 2 Geräte-Systemkonto

Geräte-Systemkonten ermöglichen es Geräten wie Niagara, sich mit dem Netzwerk zu verbinden, um die erforderlichen Informationen abzurufen und Änderungen vorzunehmen. Es wird empfohlen, für jedes Gerät, das auf das Netzwerk zugreifen soll, ein separates Geräte-Systemkonto zu erstellen. Ihre Rolle ist die eines «Supervisor».

IMPORTANT:
Wichtig: Das Sicherheitssystem des Supervisors selbst muss so konfiguriert werden, dass die Zugriffsrechte des jeweiligen Supervisor-Benutzer eingeschränkt werden.

4. 3. 3 Erstellung von Systemkonten

Wenn zum ersten Mal eine Verbindung zu einem vCNC im Niagara Netzwerk hergestellt wird, muss ein Engineering-Systemkonto mit Administrator-Rolle angelegt werden. Dieses Konto wird anschliessend auf die anderen Regler im Niagara Netzwerk synchronisiert.

Siehe *„Synchronisierte Kontoverwaltung“ auf Seite 10.* Zusätzliche Konten können bei Bedarf mit Niagara Workbench erstellt werden.

NOTE:
Bei der erstmaligen Erstellung eines Engineering-Systemkontos in einem Regler wird automatisch ein Kontoverifizierungscode generiert und mit den anderen Reglern im Ethernet-Netzwerk, die denselben Netzwerkschlüssel und UDP-Port haben, synchronisiert. Wenn ein Regler einen Kontoverifizierungscode hat, kann er nur einem Netzwerk mit Reglern beitreten, die den gleichen Kontoverifizierungscode verwenden. Siehe *„Kontoverifizierungscode“ auf Seite 9.*

4. 4 Synchronisierte Kontoverwaltung

Die synchronisierte Kontoverwaltung synchronisiert auf einfache und sichere Weise die Systemkonten, einschliesslich des Kontoverifizierungscodes, auf allen Advanced Controllern im selben Niagara Netzwerk. Dies ermöglicht:

- Einmalige Anmeldung für das gesamte Netzwerk
- Geringerer Aufwand für Konfiguration und Verwaltung des Zugriffs am gesamten Standort ohne Beeinträchtigung der Sicherheit

Alle Advanced Controller im selben Netzwerk haben dieselben Systemkonten.

Wenn ein Advanced Controller ohne Systemkonten mit dem Ethernet-Netzwerk verbunden und mit dem Netzwerkschlüssel und dem UDP-Port für das Niagara Netzwerk konfiguriert wird, tritt er dem Netzwerk bei und bezieht die Systemkonten automatisch von den anderen Controllern im Niagara Netzwerk.

Zum Beispiel:

Wenn ein Advanced Controller ohne Systemkonten zum obigen System hinzugefügt wird und über den Netzwerkschlüssel für das Niagara Netzwerk (112233) und den UDP-Port verfügt, tritt er dem Netzwerk bei und bezieht die Systemkonten (Benutzer 1, Benutzer 2, Benutzer 3) von den anderen Advanced Controllern im Niagara Netzwerk.

Sobald die Synchronisierung abgeschlossen ist, können Sie Verbindungen zu allen vCNCs herstellen, Webseiten anzeigen und sich bei allen Advanced Controllern im Niagara Netzwerk mit einem der Systemkonten anmelden.

Werden Änderungen an den Systemkonten vorgenommen, z. B. wenn ein Konto hinzugefügt, gelöscht oder bearbeitet wird, werden diese Änderungen automatisch auf allen Advanced Controllern im Niagara Netzwerk synchronisiert.

Zum Beispiel:

Es sind fünf Advanced Controller vorhanden. Auf Controller (1) werden die Systemkonten bearbeitet, um Benutzer 2 zu entfernen, Benutzer 3 in Benutzer 3a umzubenennen und Benutzer 4 hinzuzufügen. Diese Änderungen werden auf Controller (2), Controller (3), Controller (4) und Controller (5) synchronisiert.

NOTE:
Wird während der Synchronisierung ein Konflikt festgestellt, hat die letzte Änderung Vorrang.

4. 5 Ändern des Netzwerkschlüssels für einen Advanced Controller

Wenn der Netzwerkschlüssel eines Advanced Controller geändert wird, werden alle zugehörigen Systemkonten gelöscht und er wird aus dem aktuellen Niagara-Netzwerk entfernt. Die Änderung des Netzwerkschlüssels muss von einem berechtigten Engineer- oder Administrator-Systemkonto autorisiert werden.

Sobald die Änderung vorgenommen wurde, tritt der Regler mit dem neuen Netzwerkschlüssel, sofern vorhanden, einem Niagara-Netzwerk bei und bezieht die Systemkonten vom Advanced Controller im neuen Niagara-Netzwerk, vorausgesetzt, es verwendet denselben UDP-Port.

4. 6 Lokale Sicherheit

Die lokale Sicherheit verwendet lokale Benutzer (Benutzermodule), um den Zugriff auf die Webseiten des Advanced Controller oder ein lokal angeschlossenes Display zu ermöglichen und die angezeigten Informationen oder einstellbaren Werte zu steuern.

Um Zugriff zu erhalten und Änderungen vorzunehmen, müssen ein gültiger Benutzername und ein Kennwort für einen lokalen Benutzer angegeben werden. Die PIN-Ebene des Benutzers bestimmt, welche Parameter dieser sehen und anpassen kann.

NOTE:
Lokale Benutzer werden NICHT mit anderen Advanced Controllern im Niagara Netzwerk synchronisiert.

4. 7 Zugriff auf Webseiten

Der Zugriff auf die Webseiten des Reglers ist durch das Sicherheitssystem des Advanced Controller geschützt. Beim Zugriff auf den Webserver des Reglers wird eine Webseite angezeigt, die einige grundlegende Informationen enthält und die Anmeldung des Benutzers ermöglicht. Siehe *„Erster Zugriff“ auf Seite 11.*

Nach der Anmeldung werden die Benutzer wie angemeldete Benutzer behandelt. Siehe *„Angemeldete Benutzer“ auf Seite 12.* Benutzer, die ohne Anmeldung auf die Webseiten zugreifen, erhalten eingeschränkten Zugriff, wie unter *„Erster Zugriff“ auf Seite 11* beschrieben.

4. 7. 1 Erster Zugriff

Beim ersten Zugriff auf den Webserver des Reglers hängen die angezeigte Begrüssungsseite und der gewährte Zugriff von der aktuellen Sicherheitskonfiguration des Reglers ab:

- Keine Engineering-Systemkonten und keine Benutzermodule (Werkseinstellung)
  Die Begrüssungsseite wird angezeigt. Sie erhalten vollen Zugriff auf die Webseiten des Reglers und können Änderungen vornehmen.

NOTE:
Da es keine Engineering-Systemkonten oder Benutzermodule gibt, ist eine Anmeldung nicht möglich.

- Engineering-Systemkonten und keine Benutzermodule
  Die Begrüssungsseite wird angezeigt. Der Regler ermöglicht nur den Zugriff auf Sensor, Digitaleingang, Drehknopf, Schalter, Treiber, Zeitprogramm, Zeitplan, Zeit, Plot-Module, Alarmprotokoll und Grafiken und lässt keine Änderungen zu.

NOTE:
Sie können sich mit den Engineering-Systemkonten anmelden.

- Engineering-Systemkonten und Benutzermodule
  Anzeige und Zugriff bei der ersten Verwendung werden durch die Benutzermodule gesteuert. Wenn ein Benutzermodul namens «Guest» (Gast) ohne Kennwort vorhanden ist und auf die Webseiten des Advanced Controller ohne Anmeldung zugegriffen wird, gewährt der Regler die vom Benutzermodul «Guest» festgelegten Zugriffsrechte (Benutzerebene, Startseite und Standardansichten).

  Standardmässig bietet das Benutzermodul «Guest» nur Zugriff auf die Begrüssungsseite des Advanced Controllers und hat die Benutzerebene «0». Ein Benutzer, der ohne Anmeldung auf den Regler zugreift, kann somit nur die Begrüssungsseite sehen. Um weitere Zugriffsrechte zu gewähren, kann der Benutzer «Guest» wie jedes andere Benutzermodul des Typs 0 konfiguriert werden.

NOTE:
Die Niagara Workbench verhindert, dass dem Benutzer «Guest» ein Kennwort, eine PIN oder eine Benutzerebene höher als «0» zugewiesen wird. Sie können jedoch eine Startseite und Standardansicht konfigurieren.

Es wird dringend empfohlen, für den Benutzer «Guest» die Standardkonfiguration beizubehalten (Benutzerebene «0» und keine Anzeigeberechtigung).

Wenn kein Benutzermodul namens «Guest» vorhanden ist oder dieses mit einem Kennwort konfiguriert wurde, wird die Begrüssungsseite angezeigt und der Regler bietet nur Zugriff auf Sensor, Digitaleingang, Drehknopf, Schalter, Treiber, Zeitprogramm, Zeitplan, Zeit, Plot-Module, Alarmprotokoll und Grafiken, ohne dass Änderungen zulässig sind.

NOTE:
Sie können sich mit den Engineering-Systemkonten und allen vorhandenen Benutzermodulen anmelden.

4. 7. 2 Angemeldete Benutzer

Um sich bei den Advanced Controller-Webseiten anzumelden, müssen Sie einen Benutzernamen und ein Kennwort für eines der Engineering-Systemkonten oder eines der Benutzermodule vom Typ 0 am Advanced Controller eingeben.

4. 8 Wiederherstellen des Kennworts

Wenn ein Benutzer sein Kennwort vergessen hat, kann es mit Hilfe von Niagara Workbench wiederhergestellt werden. Einzelheiten zur Wiederherstellung eines vergessenen Kennworts mit Niagara finden Sie im Niagara Workbench Nutzungsleitfaden.

5. SCHÜTZEN DES NIAGARA BETRIEBSSYSTEMS

5. 0. 1 Bewährte Verfahren

Befolgen Sie die allgemein bekannten, bewährten Verfahren zum Schutz des Betriebssystems, wie z. B.:

- Kennwortgeschützter Bildschirmschoner
- Software zur Laufwerksverschlüsselung

5. 0. 2 Firewall-Einstellung

Das Betriebssystem muss so konfiguriert sein, dass eine Firewall verwendet und diese automatisch aktualisiert wird. Die Konfiguration muss den Zugriff (IN/OUT) an allen Ports verhindern, sofern kein Zugriff erforderlich ist; lassen Sie KEINE ungenutzten Ports offen.

5. 0. 3 Betriebssystemversion

Sie MÜSSEN sicherstellen, dass auf allen Geräten, auf denen Niagara Anwendungen ausgeführt werden oder die mit demselben IP-Netzwerk verbunden sind, die neuesten Betriebssystem-Updates installiert sind. Es empfiehlt sich, die automatische Installation von Windows-Updates zu aktivieren und diese zeitnah zu installieren.

5. 0. 4 Virenschutz

Sie MÜSSEN sicherstellen, dass auf allen Computern, auf denen die Niagara Anwendungen ausgeführt werden oder die mit demselben IP-Netzwerk verbunden sind, eine Virenschutzsoftware verwendet wird, und dass die Virendefinitionen auf dem neuesten Stand sind.

5. 0. 5 Einbruchschutz

Es wird empfohlen, auf allen Computern, auf denen Niagara Anwendungen ausgeführt werden, ein Einbruchmeldesystem (Intrusion Detection System, IDS) eines renommierten Sicherheitsproduktanbieters einzusetzen. Beachten Sie die bewährten Verfahren für die verwendeten Produkte sowie die IT-Richtlinien des Unternehmens, in dem die Installation erfolgt.

Viele IDS- und Firewall-Produkte bieten eine Komplettlösung für die Aufzeichnung des gesamten ein- und ausgehenden Datenverkehrs, sodass Benutzer alle Aktivitäten auf kleinster Ebene aufzeichnen können.

6. DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Die Datenschutz-Grundverordnung oder kurz DSGVO (EU)2016/679 ist eine EU-Rechtsverordnung zum Schutz der Daten und Privatsphäre aller Bürgerinnen und Bürger in der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR). Sie regelt zudem die Übermittlung personenbezogener Daten in Länder ausserhalb der EU und des EWR. Die DSGVO enthält Bestimmungen und Vorgaben hinsichtlich der Verarbeitung personenbezogener Daten von Einzelpersonen (betroffenen Personen) innerhalb des EWR und gilt für alle im EWR tätigen Unternehmen (unabhängig von deren Standort und der Staatsangehörigkeit der betroffenen Personen) sowie für alle Unternehmen, die personenbezogene Daten von betroffenen Personen innerhalb des EWR verarbeiten.

Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die zur Identifizierung einer Person dienen können. Dazu gehören unter anderem:

- Benutzernamen
- Kennwörter
- Telefonnummern
- E-Mail-Adressen
- Geschäftliche oder private Anschriften

Alle Informationen dieser Art, die in den Advanced Controller, die HMI und das E/A-Modul eingegeben werden, werden verschlüsselt und in den Advanced Produkten in den Räumlichkeiten des Kunden gespeichert. Honeywell ist in keiner Weise an der Speicherung und/oder Verarbeitung personenbezogener Daten in den Advanced Produkten von Honeywell beteiligt.

Die Verantwortung für die Einhaltung der DSGVO liegt in vollem Umfang beim Systemintegrator oder Systemadministrator. Dieser muss sicherstellen, dass geeignete technische und organisatorische Systeme vorhanden sind, um die Anforderungen der DSGVO zu erfüllen. Konkret heisst dies:

- Von jeder betroffenen Person ist die ausdrückliche Zustimmung zur Speicherung, Nutzung und/oder Verarbeitung personenbezogener Daten einzuholen.
- Die betroffenen Personen müssen Zugriff auf ihre personenbezogenen Daten haben, um deren Richtigkeit zu überprüfen.
- Die betroffenen Personen müssen die Möglichkeit haben, ihre Einwilligung jederzeit zu widerrufen und ihre personenbezogenen Daten dauerhaft zu löschen.
- Die Sicherheit und Integrität der Datenspeicherung und des Datenzugriffs muss jederzeit gewährleistet sein.
- Jegliche Verletzung der Datensicherheit (die sich auf den Datenschutz der Benutzer auswirken kann) muss innerhalb von 72 Stunden nach Eintreten der Verletzung an die zuständige Behörde gemeldet werden.

7. SICHERE KOMMUNIKATION

Eine Public-Key-Infrastruktur (PKI) unterstützt die Verteilung und Identifizierung von öffentlichen Schlüsseln, die zum Schutz des Datenaustauschs über Netzwerke, wie z. B. das Internet, verwendet werden. Die PKI prüft die Identität der Gegenseite und verschlüsselt die eigentliche Datenübertragung. Die Identitätsprüfung sorgt für eine unwiderlegbare Bestätigung der Serveridentität. Die Verschlüsselung sorgt für die Vertraulichkeit der Übertragung im Netzwerk. Die Notwendigkeit von Modulen mit signiertem Code gewährleistet, dass nur zu erwartender Code im System ausgeführt wird.

Um sichere Netzwerke mittels PKI bereitzustellen, unterstützt Niagara das TLS-Protokoll (Transport Layer Security) in den Versionen 1.0, 1.1 und 1.2. TLS ersetzt den Vorgänger SSL (Secure Sockets Layer).

Jede Niagara Installation erstellt automatisch ein Standardzertifikat, mit dem die Verbindung sofort verschlüsselt werden kann. Diese Zertifikate erzeugen jedoch Warnungen im Browser und in der Workbench und sind im Allgemeinen für Endbenutzer nicht geeignet. Das Erstellen und Signieren benutzerdefinierter digitaler Zertifikate ermöglicht hingegen eine nahtlose Verwendung von TLS im Browser und gewährleistet sowohl Verschlüsselung als auch Server-Authentifizierung.

Neben der Kommunikationssicherheit wird jedes Modul des Computercodes, das im System ausgeführt wird, durch eine digitale Signatur geschützt. Hinzugefügte Programmobjekte benötigen diese Signatur, sonst können sie nicht ausgeführt werden.

Die Verifizierung des Servers, die Verschlüsselung der Übertragung und die Gewährleistung, dass nur signierter Code ausgeführt wird, bieten jedoch keinen Schutz für die auf einem Speichergerät gespeicherten Daten. Sie müssen daher zusätzlich den physischen Zugang zu den Computern und Reglern, die Ihr Gebäudemodell verwalten, beschränken, eine Benutzerauthentifizierung mit sicheren Kennwörtern einrichten und die Komponenten durch eine Berechtigungskontrolle schützen.

Niagara unterstützt dies, indem standardmässig eine sichere Kommunikation und signierter Code verwendet werden. Sie müssen keine zusätzliche Lizenz erwerben.

Sicherheit verlangt kontinuierliche Aufmerksamkeit. In den Themen zur sicheren Kommunikation finden Sie viele wertvolle Informationen dazu, allerdings müssen Sie mit neuen Entwicklungen und Änderungen in der Zukunft rechnen.

Nachstehend finden Sie eine Übersicht über die sichere Kommunikation. Ausführliche Informationen entnehmen Sie bitte dem Sicherheitsleitfaden für die Niagara Station.

- Client-Server-Beziehungen
- Zertifikate
- Zertifikatsspeicher
- CSR-Ordnerstruktur
- Einrichtung von Zertifikaten
- Zertifikats-Assistent
- Signieren mehrerer Zertifikate
- Konfigurieren der sicheren Kommunikation für Plattformen
- Konfigurieren der sicheren Kommunikation für Stationen
- Aktivieren von Clients und Konfigurieren für den richtigen Port
- Installieren einer Stationskopie auf einer anderen Plattform
- Schützen von E-Mails
- Beheben von Fehlern bei der sicheren Kommunikation

7. 1 Client-Server-Beziehungen

Client-Server-Beziehungen identifizieren die zu schützenden Verbindungen. Die Client-Server-Beziehungen variieren je nachdem, wie Sie das System konfigurieren und verwenden. Eine Workbench ist immer ein Client. Eine Plattform ist immer ein Server. Eine Station kann sowohl ein Client als auch ein Server sein.

Folgende Systemprotokolle regeln die Kommunikation:

- Plattformverbindungen zwischen Workbench (Client) und Regler- oder Supervisor-PC-Plattform-Daemon (Server) verwenden Niagara. Eine sichere Plattformverbindung wird manchmal auch als «platformtls» bezeichnet. Sie aktivieren «platformtls» in der Ansicht «Platform Administration».
- Lokale Stationsverbindungen (Supervisor und Plattform) verwenden Foxs. Sie aktivieren diese Verbindungen im FoxService der Station (Config > Services > FoxService).
- Browser-Verbindungen verwenden Https sowie Foxs, wenn Sie Web Launcher mit einem WbWebProfile verwenden. Sie aktivieren diese Verbindungen im WebService der Station (Config > Services > WebService).
- Client-Verbindungen erfolgen zum E-Mail-Server der Station, falls zutreffend. Sie aktivieren sichere E-Mails im Email-Service der Station (Config > Services > EmailService).

8. ZERTIFIKATE

Ein Zertifikat ist ein elektronisches Dokument, das eine digitale Signatur verwendet, um einen öffentlichen Schlüssel mit einer Person oder Organisation zu verknüpfen. Zertifikate können verschiedenen Zwecken dienen, je nachdem, wie Sie die Eigenschaft «Key Usage» des Zertifikats konfigurieren. Ihr primärer Verwendungszweck in diesem System besteht darin, die Identität eines Servers zu verifizieren, damit die Kommunikation vertrauenswürdig ist. Ausführliche Informationen entnehmen Sie bitte dem Abschnitt zu Zertifikaten im Sicherheitsleitfaden für die Niagara Station.

Niagara unterstützt die folgenden Zertifikatstypen:

- Ein **CA-Zertifikat** (Certificate Authority) ist ein selbst-signiertes Zertifikat einer Zertifizierungsstelle. Dies kann eine Drittpartei sein oder das Unternehmen fungiert als seine eigene Zertifizierungsstelle.
- Ein **Root-CA-Zertifikat** ist ein selbst-signiertes CA-Zertifikat, dessen privater Schlüssel zum Signieren anderer Zertifikate verwendet wird, wodurch eine vertrauenswürdige Zertifikatsstruktur entsteht. Ein Root-CA-Zertifikat kann zusammen mit seinem privaten Schlüssel exportiert, auf einem USB-Stick in einem Tresor gespeichert und nur dann herausgeholt werden, wenn Zertifikate signiert werden müssen. Der private Schlüssel eines Root-CA-Zertifikats erfordert die Erstellung eines Kennworts beim Export und die Angabe desselben Kennworts, wenn Sie es zum Signieren anderer Zertifikate verwenden.
- Ein **Zwischenzertifikat** ist ein CA-Zertifikat, das durch ein Root-CA-Zertifikat signiert ist und zum Signieren von Serverzertifikaten oder anderen zwischengeschalteten CA-Zertifikaten verwendet wird. Durch die Verwendung von Zwischenzertifikaten kann eine Gruppe von Serverzertifikaten getrennt werden.
- Ein **Serverzertifikat** stellt die Serverseite einer sicheren Verbindung dar. Sie können ein separates Zertifikat für jedes Protokoll (Foxs, Https, Webs) einrichten. Sie können ebenso eine Plattform und eine Station (als Server) mit separaten Serverzertifikaten konfigurieren. Die meisten Systeme verwenden der Einfachheit halber jedoch das gleiche Serverzertifikat.
- Ein **Code Signing- oder Codesignierungszertifikat** ist ein Zertifikat, das zum Signieren von Programmobjekten und Modulen verwendet wird. Systemintegratoren verwenden dieses Zertifikat, um bei der Anpassung des Frameworks die Einführung von böswilligem Code zu verhindern.

8. 1 Selbst-signierte Zertifikate

Ein selbst-signiertes Zertifikat ist ein Zertifikat, das standardmässig mit seinem eigenen privaten Schlüssel und nicht mit dem privaten Schlüssel eines Root-CA-Zertifikats einer Zertifizierungsstelle signiert ist.

Das System unterstützt zwei Arten von selbst-signierten Zertifikaten:

- Ein **Root-CA-Zertifikat** ist implizit vertrauenswürdig, da es keine höhere Instanz als die Zertifizierungsstelle (CA) gibt, die Herausgeberin dieses Zertifikats ist. Aus diesem Grund legen die Zertifizierungsstellen, deren Geschäft die Bestätigung von Fremdzertifikaten ist, grossen Wert auf die Sicherheit ihrer Root-CA-Zertifikate und privaten Schlüssel. Wenn Ihr Unternehmen als seine eigene Zertifizierungsstelle fungiert, sollten Sie deshalb ebenfalls das Root-CA-Zertifikat, das Sie zum Signieren anderer Zertifikate verwenden, streng überwachen.
- Ein **standardmässiges selbst-signiertes Zertifikate**: Beim ersten Start einer Instanz der Workbench, Plattform oder Station nach der Installation (Inbetriebnahme) erstellt das System ein standardmässiges, selbst-signiertes Serverzertifikat mit dem Alias «tridium».

NOTE:

Dieses Zertifikat darf nicht exportiert und in einen Speicher einer anderen Plattform oder Station importiert werden. Wenngleich dies möglich ist, verringert es die Sicherheit und erhöht die Angriffsfläche.

Um das Risiko von Man-in-the-Middle-Angriffen bei der Verwendung selbst-signierter Zertifikate zu minimieren, sollten sich alle Ihre Plattformen in einem sicheren privaten Netzwerk befinden, das offline ist und keinen öffentlichen Zugang aus dem Internet ermöglicht.

⚠ CAUTION

Wenn Sie selbst-signierte Zertifikate verwenden möchten, stellen Sie vor dem ersten Zugriff auf die Plattform oder Station von der Workbench aus sicher, dass Ihr Computer und die Plattform nicht mit einem Unternehmensnetzwerk oder dem Internet verbunden sind. Wenn die Verbindung sicher getrennt ist, schliessen Sie den Computer direkt an die Plattform an, öffnen Sie die Plattform über die Workbench und genehmigen Sie ihr selbst-signiertes Zertifikat. Erst dann sollten Sie die Plattform wieder mit dem Unternehmensnetzwerk verbinden.

8. 2 Namenskonvention

Der **User Key Store**, der **User Trust Store** und der **System Trust Store** bilden das Herzstück der Konfiguration. Die Zertifikate sehen sich sehr ähnlich, und die verschiedenen selbst signierten Standardzertifikate verwenden die gleichen Namen.

8. 3 Zertifikatsspeicher

Die Zertifikatsverwaltung verwendet vier Speicher: einen **User Key Store**, einen **System Trust Store**, einen **User Trust Store** und eine Liste der zulässigen Hosts oder Englisch **Allowed Hosts**.

Der **User Key Store** ist der Serverseite in der Client-Server-Beziehung zugeordnet. In diesem Speicher befinden sich Zertifikate zusammen mit ihren öffentlichen und privaten Schlüsseln. Ausserdem enthält dieser Speicher das selbst-signierte Zertifikat, das beim ersten Start der Workbench oder beim ersten Booten der Plattform erstellt wurde.

Der **User Trust Store** und der **System Trust Store** sind der Clientseite in der Client-Server-Beziehung zugeordnet. Im System Trust Store sind bereits einige standardmässige öffentliche Zertifikate enthalten: Root-CA-Zertifikate von bekannten Zertifizierungsstellen wie VeriSign, Thawte und Digicert. Der **User Trust Store** enthält Root-CA- und Zwischenzertifikate für Unternehmen, die als ihre eigene Zertifizierungsstelle fungieren.

Die Liste der **Allowed Hosts** enthält Serverzertifikate für zulässige Hosts, für die im **System Trust Store** oder **User Trust Store** des Clients kein vertrauenswürdiges Root-CA-Zertifikat vorhanden ist, die aber trotzdem zur Verwendung freigegeben wurden. Dazu gehören Server, deren Hostname nicht mit dem «Common Name» im Serverzertifikat übereinstimmt. Die Verwendung dieser Zertifikate wird jeweils individuell genehmigt. Obwohl sie eine sichere Kommunikation gewährleisten, ist es besser, signierte Serverzertifikate zu verwenden.

8. 4 Verschlüsselung

Bei der Verschlüsselung werden die übertragenen Daten so verschlüsselt, dass sie von unbefugten Dritten nicht gelesen werden können. TLS verwendet Verschlüsselung für die Datenübertragung zwischen Client und Server. Zwar ist es möglich, eine unverschlüsselte Verbindung nur mit dem fox- oder http-Protokoll herzustellen, doch wird dringend davon abgeraten, diese Möglichkeit zu nutzen. Ohne Verschlüsselung besteht die Gefahr, dass Ihre Kommunikation einem Angriff zum Opfer fällt. Übernehmen Sie immer die standardmässigen Foxs- oder Https-Verbindungen.

9. ÜBERSICHT ÜBER DAS SECURITY DASHBOARD

In Niagara 4.u5 und höher bietet das Security Dashboard (für Administratoren und andere autorisierte Benutzer) einen Gesamtüberblick über die Sicherheitskonfiguration Ihrer Station. So können Sie mühelos die Sicherheitskonfiguration in mehreren Stationsservices überwachen und eventuelle Schwachstellen in der Sicherheitskonfiguration der Station erkennen.

⚠ CAUTION

Im Security Dashboard werden möglicherweise nicht alle verfügbaren Sicherheitseinstellungen angezeigt. Es bietet somit keine Garantie dafür, dass alles sicher konfiguriert ist. Insbesondere Module von Drittanbietern können Sicherheitseinstellungen haben, die nicht im Dashboard registriert werden.

Das Security Dashboard ist die Hauptansicht des SecurityService der Station. Die Übersicht informiert Sie über Sicherheitsmängel, wie z. B. unzureichende Einstellungen für die Kennwortstärke, abgelaufene, selbst-signierte oder ungültige Zertifikate, unverschlüsselte Transportprotokolle usw., und zeigt Bereiche auf, in denen die Konfiguration sicherer sein sollte. Andere gemeldete Daten sind: Systemzustand, Anzahl der aktiven Konten, inaktive Konten, Anzahl der Konten mit Superuser-Berechtigungen usw. Optional kann das Attribut «system» der Lizenzfunktion «securityDashboard» auf «true» gesetzt werden, um die Systemansicht der Station zu aktivieren, die Sicherheitsinformationen für jede untergeordnete Station im Niagara Netzwerk liefert.

Das Security Dashboard ist die Hauptansicht für die Sicherheitsservices. Ausführliche Informationen zu dieser Ansicht finden Sie unter «nss-SecurityDashboardView» im Sicherheitsleitfaden der Niagara Station.

10. PLANUNG UND INSTALLATION

Dieser Abschnitt enthält Informationen zur Planung und Durchführung einer Installation von Advanced Plant Controller.

10. 1 Empfohlene Installation und Konfiguration

Im folgenden Abschnitt werden zwei empfohlene Konfigurationen für die Installation beschrieben.

- Nur BACnet
- BACnet und Niagara

10. 1. 1 Nur BACnet

Wenn der Advanced Plant Controller nur für die BACnet-Kommunikation verwendet wird, verbinden Sie nur Ethernet 1 mit dem BAS-Netzwerk, in dem BACnet (BACnet/IP oder BACnet/Ethernet) ausgeführt wird.

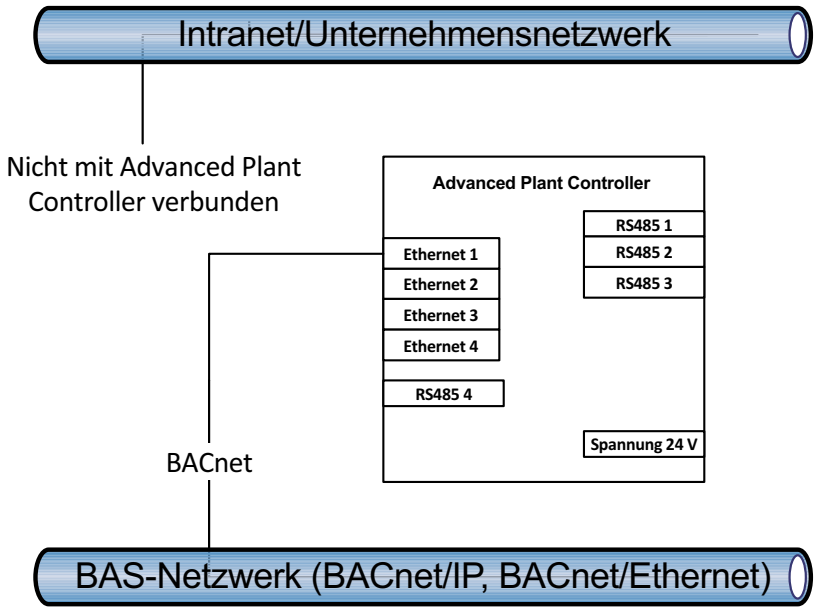

Abb. 2 BACnet-Verbindung

10. 1. 2 BACnet und Niagara

Wenn auf dem Advanced Plant Controller Niagara verwendet wird, kann das System so konfiguriert werden, dass Services, wie z. B. Webservices oder Niagara FOXS, für das Internet/Intranet/Unternehmensnetzwerk bereitgestellt werden. Verbinden Sie in diesem Fall Ethernet 2 über die BAS-Firewall mit dem Internet/Intranet/Unternehmensnetzwerk, um Services für dieses Netzwerk bereitzustellen.

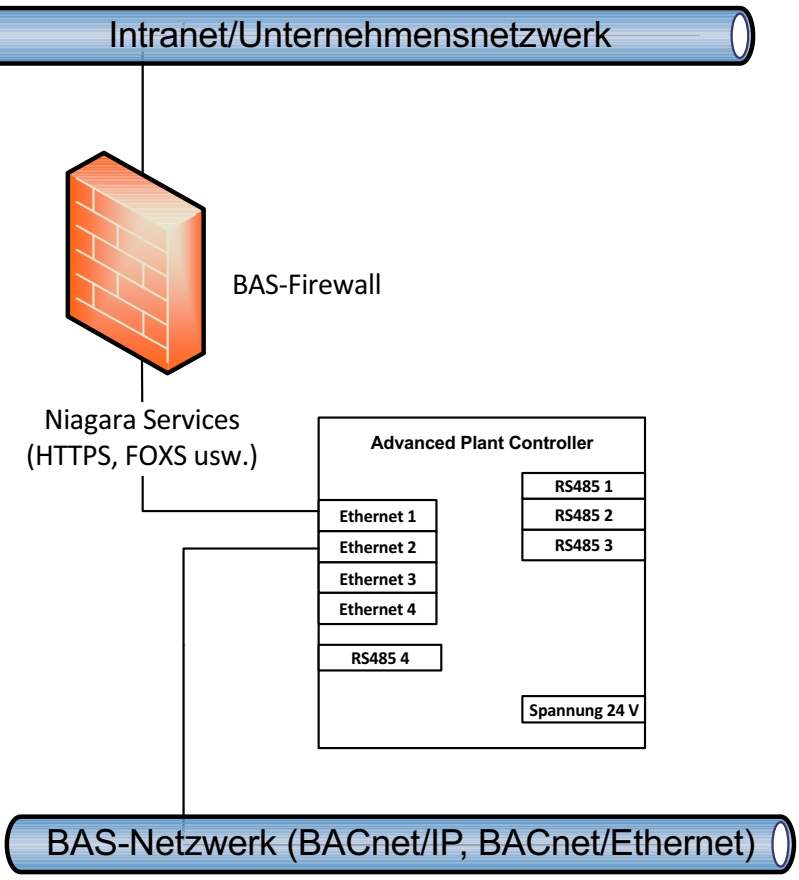

Abb. 3 BACnet- und Niagara-Verbindungen

10. 2 Empfehlung für Local Area Networks (LAN)

Stellen Sie sicher, dass die Systeme eine angemessene Kennwortrichtlinie für den Benutzerzugriff auf die Servers verwenden. Diese Richtlinie sollte unter anderem Folgendes beinhalten:

1. Verwendung starker Kennwörter.
2. Empfohlenes Kennwortänderungsintervall.
3. Eindeutige Benutzernamen und Kennwörter für jeden Systembenutzer.
4. Regeln für die Offenlegung von Kennwörtern.
5. Für einen ggf. benötigten Remotezugriff auf IT-basierte Gebäudesteuerungssysteme sollte VPN-Technologie (Virtual Private Network) verwendet werden, um die Gefahr, dass Daten abgehört werden, zu verringern und um zu verhindern, dass die Steuerungsgeräte direkt mit dem Internet verbunden sind.

11. DOKUMENTATION

Die Dokumentation der Entwurfs- und Konfigurationsinformationen ist unerlässlich, um die für die Sicherheit des Systems zu gewährleisten.

11. 1 Dokumentieren physischer Geräte und Konfigurationen, inklusive wichtiger Sicherheitsinformationen

Die Dokumentation zu Geräten und Konfigurationen muss immer auch die relevante Sicherheitsinformationen enthalten, um die nötigen Sicherheitskontrollen einzuführen und aufrechtzuerhalten. Wenn beispielsweise Änderungen an den Standard-services oder -ports des Advanced Plant Controller vorgenommen werden, müssen diese eindeutig dokumentiert werden, damit die Einstellungen zu einem späteren Zeitpunkt wiederhergestellt werden können.

11. 2 Dokumentieren externer Systeme, insbesondere die Interaktion zwischen Advanced Plant Controller und zugehörigen Systemen

Für die Funktionen des BAS werden häufig externe Systeme benötigt bzw. genutzt, z. B. die bestehende Netzwerkinfrastruktur, VPN-Zugang, VM-Hosts (virtuelle Maschinen) und Firewalls. Wenn es für die Sicherheit des BAS erforderlich ist, dass diese Systeme auf eine bestimmte Weise konfiguriert werden, z. B. eine Firewall, die bestimmte Ports freigibt oder sperrt, oder ein Netzwerk, das den Zugriff auf bestimmte Systeme erlaubt, dann müssen Sie diese Informationen dokumentieren. Diese Dokumentation hilft Ihnen bei der Wiederherstellung der Systeme auf der vorherigen Sicherheitsstufe, sollten die Systeme zu einem späteren Zeitpunkt wiederhergestellt werden müssen, **z. B.** aufgrund eines Geräteausfalls, oder wenn Änderungen an den externen Systemen vorgenommen werden müssen, **z. B.** die Aktualisierung einer Firewall.

12. ZUGANGSKONTROLLE UND PHYSISCHE SICHERHEIT

Bei der Zugangskontrolle geht es darum, den Zugang zu Geräten oder Funktionen auf autorisierte Benutzer zu beschränken.

12. 1 Physischer Schutz von Advanced Plant Controller, HMI und E/A-Modul

Verhindern Sie einen unbefugten Zugang zu Netzwerkgeräten, die in Verbindung mit den von Honeywell bereitgestellten Systemen verwendet werden. Wie bei allen Systemen verringern Sie die Gefahr unbefugter Eingriffe, indem Sie den physischen Zugang zum Netzwerk und zu den Geräten unterbinden. Eine Best Practice für die Sicherheit von IT-Installationen ist es, Serverräume, Patchpanels , und IT-Geräte in geschlossenen Räumen unterzubringen. Honeywell Geräte müssen dementsprechend in geschlossenen Schaltschränken installiert werden, die sich wiederum in sicheren Anlagenräumen befinden.

12. 2 Aufkleber am Zugangspaneel oder Gehäuse des Reglers

Zur Erkennung von Manipulationen kann ein Aufkleber am Zugangspaneel oder Gehäuse des Advanced Plant Controller, der HMI und des E/A-Moduls angebracht werden.

Wenn ein Kunde zusätzliche Sicherheit benötigt, dass der physische Zugang zu Advanced Plant Controller, HMI und E/A-Modul nicht manipuliert wurde, bringen Sie ein manipulationssicheres Siegel bzw. einen Aufkleber über dem Zugangspunkt an.

12. 3 Trennen und Schützen der Netzwerke

1. Verwenden Sie eine Firewall zwischen dem Internet/Intranet/Unternehmensnetzwerk und dem BAS.
2. Verwenden Sie für die BACnet-Kommunikation ein separates dediziertes physisches Netzwerk (getrennte Leitungen) oder ein virtuelles Netzwerk (VLANs). Hierbei muss es sich um ein anderes Netzwerk als für das Internet/Intranet/Unternehmensnetzwerk handeln.
3. Verbinden Sie EN2 am Advanced Plant Controller nur dann mit einem Netzwerk, wenn Sie Niagara Services benötigen (Plattform, Station und/oder Webserver). Wenn Sie EN2 mit dem Internet/Intranet/Unternetzwerk verbinden müssen, verwenden Sie eine externe BAS-Firewall zwischen dem Advanced Plant Controller und dem Internet/Intranet/Unternetzwerk.

13. SCHÜTZEN VON ADVANCED CONTROLLER, HMI UND E/A-MODUL

13. 1 Bereitstellen der Anmeldedaten zum Admin-Systemkonto für den Benutzer

Die Anmeldedaten für das Systemkonto «Admin» müssen dem verantwortlichen Benutzer bereitgestellt werden, damit er die Systemkonten verwalten kann.

13. 2 Entwickeln eines Sicherheitsprogramms

Siehe «Allgemeine Sicherheitsvorkehrungen»

13. 3 Physische Voraussetzungen und Umgebungsbedingungen

Advanced Controller, HMI und E/A-Modul müssen in einer geschlossenen Umgebung installiert werden, z. B. in einem gesicherten Anlagenraum oder abschliessbaren Schaltschrank.

NOTE:
Sorgen Sie für eine ausreichende Belüftung.

13. 4 Sicherheits-Updates und Servicepakete

Stellen Sie sicher, dass auf dem Advanced Controller, der HMI und dem E/A-Modul die neueste Firmwareversion ausgeführt wird.

14. BENUTZER UND KENNWÖRTER

14. 1 Benutzer

Stellen Sie sicher, dass die Anzahl der Benutzer und deren Zugriffsebenen für die von ihnen ausgeführten Tätigkeiten angemessen sind.

- **Konfigurieren Sie Systemkonten auf Ebene der Steuergeräte oder Benutzer in Reglern für Web-Client, Supervisor und Peer-to-Peer-Zugriff.**

  Wenn Sie in den Advanced Controllern Benutzermodule konfigurieren, bedeutet dies, dass sich ein Benutzer mit gültigen Anmeldedaten bei einem Gerät anmelden muss, bevor er Einstellungen vornehmen kann. Stellen Sie sicher, dass den Systemkonten und Benutzern die richtigen Zugriffsrechte zugewiesen werden.

- **Nutzung eines separaten Kontos für jeden Benutzer**

  Verwenden Sie eindeutige Namen und Kennwörter für jeden Benutzer bzw. jedes Konto im System anstelle eines generischen Zugriffs. Verschiedene Personen sollten niemals dasselbe Konto benutzen. Anstelle eines allgemeinen «Managerkontos», das von mehreren Managern genutzt wird, sollte jeder Manager über ein eigenes, separates Konto verfügen.

Es gibt viele Gründe für die Verwendung eines separaten Kontos für jeden Benutzer:

- Wenn jede Person ein eigenes Konto hat, sind Prüfprotokolle aussagekräftiger. Es lässt sich dann leicht feststellen, welcher Benutzer welche Aktion durchgeführt hat. So kann erkannt werden, ob ein Konto manipuliert wurde.

NOTE:
Nicht alle Produkte verfügen über eine Prüfprotokollfunktion. Sofern vorhanden, sollte diese nicht deaktiviert werden.

- Wird ein Konto gelöscht oder geändert, hat dies keine Auswirkungen für andere Personen. Soll zum Beispiel eine Person keinen Zugriff mehr haben, ist es einfach, ihre individuellen Zugangsdaten zu löschen. Bei einem gemeinsamen Konto bleibt nur die Möglichkeit, das Kennwort zu ändern oder das Konto zu löschen und alle anderen Benutzer entsprechend zu informieren. Das Konto unverändert zu lassen ist keine Option. Ziel ist es, den Kontozugriff der betreffenden Person zu widerrufen.
- Wenn jede Person ein eigenes Konto hat, ist es viel einfacher, die Berechtigungen genau auf deren Bedürfnisse abzustimmen. Ein gemeinsames Konto könnte dazu führen, dass Personen mehr Rechte erhalten, als sie haben sollten.

  - Ein gemeinsames Konto heisst auch ein gemeinsames Kennwort. Die Weitergabe von Kennwörtern ist jedoch eine extrem schlechte Sicherheitspraxis. Die Wahrscheinlichkeit, dass ein Kennwort in die falschen Hände gerät, wird dadurch deutlich erhöht, und es wird in vielen Fällen schwieriger, die bewährte Verfahren für Kennwörter umzusetzen, wie z. B. ein Ablaufintervall für Kennwörter.

- **Nutzung eindeutiger Engineering-Benutzer für Projekte**

  Es ist gängige Praxis, dass Unternehmen für jedes Projekt die gleichen Kontodaten verwenden. Sollte diese Information an die Öffentlichkeit gelangen, verfügt der Angreifer, der ein einzelnes System kompromittiert hat, potenziell über Zugangsdaten für zahlreiche weitere Projekte, die von demselben Unternehmen installiert wurden.

- **Deaktivieren allgemein bekannter Konten (wenn möglich)**

  Einige Produkte verfügen über Standardkonten. Diese sollten so konfiguriert werden, dass das Kennwort nicht mehr der Standardeinstellung entspricht.

- **Zuweisen der minimalen erforderlichen Berechtigungen für Benutzer**

  Stellen Sie sicher, dass anstelle eines Vollzugriffs im System nur die tatsächlich benötigten Konten mit der minimal erforderlichen Sicherheitsebene eingerichtet werden. Wenn Sie ein neues Konto erstellen, überlegen Sie, welche Aufgaben die betreffende Person im System ausführen muss, und weisen Sie ihr dann nur die für diese Aufgabe minimal erforderlichen Berechtigungen zu. Beispielsweise benötigt eine Person, die nur Alarme einsehen muss, keinen Administratorzugriff. Die Erteilung von nicht erforderlichen Berechtigungen erhöht das Risiko einer Sicherheitsverletzung. Der Benutzer könnte zum Beispiel versehentlich (oder absichtlich) Einstellungen ändern, die nicht verändert werden sollten.

- **Verwenden möglichst weniger Systemadministrator-Konten**

  Weisen Sie Systemadministrator-Berechtigungen nur zu, wenn dies unbedingt erforderlich ist. Diese Art von Konto hat extrem weitreichende Berechtigungen – es ermöglicht einen vollständigen Zugriff auf das gesamte System. Nur der Systemadministrator sollte Zugriff auf das Konto haben. Ziehen Sie auch in Erwägung, dem Systemadministrator zwei Konten zur Verfügung zu stellen, eines für den täglichen Gebrauch, um die laufenden Aktivitäten zu verwalten, und ein zweites Konto für den Zugriff auf höherer Ebene, das nur dann benötigt wird, wenn administrative Änderungen erforderlich sind.

14. 2 Kennwörter

Das Trend-System und die von Trend-Produkten verwendeten Betriebssysteme nutzen Kennwörter, um «Benutzer» am Supervisor, Display, Tool oder Betriebssystem zu authentifizieren. Der richtige Umgang mit Kennwörtern ist hierbei besonders wichtig. Wird diese erste Sicherheitsstufe nicht korrekt angewendet, kann jede Person, die über ein Display, einen Web-Client oder einen Supervisor auf das System zugreift, Einstellungen vornehmen. Stellen Sie daher sicher, dass das Niagara Systeme eine angemessene Kennwortrichtlinie für den Benutzerzugriff anwendet. Dies beinhaltet unter anderem Folgendes:

- **Verwendung starker Kennwörter** – Es müssen sichere Kennwörter verwendet werden. Informationen darüber, was ein sicheres Kennwort ausmacht, finden Sie in den neuesten Sicherheitsstandards.
- **Empfohlenes Kennwortänderungsintervall** – In einigen Niagara Produkten kann der Systemadministrator einen Zeitraum festlegen, nach dem ein Kennwort geändert werden muss. Zwar wird dieses Kennwortänderungsintervall derzeit nicht von allen Produkten durchgesetzt, aber es kann in einer Standortrichtlinie empfohlen werden.
- **Regeln für die Offenlegung von Kennwörtern** – Der Benutzer MUSS sicherstellen, dass er seinen Benutzernamen und sein Kennwort nicht an Dritte weitergibt und dass er diese Daten nicht aufschreibt.

15. KONFIGURIEREN EINES ADVANCED PLANT CONTROLLER

Informationen zur Konfiguration eines Advanced Plant Controller finden Sie in der Installations- und Inbetriebnahmeanleitung (31-00584). Informationen zur HMI finden Sie in der HMI Treiberanleitung (31-00590) und zum E/A-Modul in der PanelBus Treiberanleitung (31-00591).

15. 1 Erstellen und Verwalten einer Basiskonfiguration

Erstellen und verwalten Sie eine Basiskonfiguration eines Advanced Plant Controller, dessen Sicherheitseinstellungen korrekt konfiguriert wurden. Stellen Sie sicher, dass diese Basiskonfiguration auch DCF-Dateien und Niagara Komponenten enthält. Übernehmen Sie keine unsicheren Konfigurationen in die Basiskonfiguration. So verhindern Sie, dass diese in Zukunft versehentlich angewendet werden. Bei Konfigurationsänderungen sollte stets die gesamte relevante Dokumentation aktualisiert werden.

15. 2 Ändern der Standardkennwörter

Ändern Sie alle Standardkennwörter: für die Konsolenkonfiguration, für Sicherung/Wiederherstellung/Neustart/Steuerung und für die Niagara Plattform. Stellen Sie sicher, dass das Gerät mit einem Kennwort geschützt ist, sobald Sie die Inbetriebnahme abschliessen. Vergewissern Sie sich, dass den Benutzern entsprechende Benutzerebenen zugewiesen wurden.

15. 3 Weitere Hinweise

15. 3. 1 Service Level Agreement

Wenden Sie eine geeignete Aktualisierungsrichtlinie für die installierte Infrastruktur als Bestandteil eines Service Level Agreements an. Die Richtlinie sollte u. a. die Aktualisierung der folgenden Systemkomponenten auf die neueste Version beinhalten:

- Geräte-Firmware für Controller, E/A-Module, HMI usw.
- Supervisor-Software, wie Arena NX
- Computer-/Serverbetriebssysteme
- Netzwerkinfrastruktur und alle Remote-Zugriffssysteme

15. 3. 2 Konfiguration des IT-Netzwerks

Konfigurieren Sie separate IT-Netzwerke für die Automations- und Leitsysteme und für das unternehmensinterne IT-Netzwerk des Kunden. Dies kann durch die Konfiguration von VLANs (Virtual LANs) innerhalb der IT-Infrastruktur des Kunden oder durch die Installation einer
separaten, «air-gapped» Netzinfrastruktur für die Automations- und Leitsysteme erfolgen.

Wenn an der Schnittstelle zu den Reglern ein zentraler System-Supervisor (z. B. Niagara) eingesetzt wird und das System keinen direkten Zugriff auf die Webserver einzelner Geräte benötigt, sollte der Webserverzugriff in der Konfiguration der Netzwerkinfrastruktur eingeschränkt werden.

Dynamische VLANs mit MAC-Adressenzuordnung können eine unbefugten Verbindung von Geräten mit dem System verhindern und die Gefahr minimieren, dass Informationen aus dem Netzwerk von Fremden abgehört werden.

16. KONFIGURIEREN DER BAS-FIREWALL

Die folgende Tabelle gibt einen Überblick über die Netzwerkanschlüsse in einem Advanced Plant Controller. Siehe *„Systemübersicht“ auf Seite 6.*, um ein Beispiel für eine Installationsarchitektur zu sehen. Die Tabelle enthält folgende Spalten:

- Standardport und Protokoll (TCP oder UDP)
- Zweck des Ports
- Ändern des Standardports erforderlich
- Zulassen eingehender Verbindungen oder Datenverkehr über die BAS-Firewall
- Zusätzliche Hinweise sind unter der Tabelle aufgeführt.

Tabelle 2. Konfigurieren der BAS-Firewall

Standardport/ Protokoll	Zweck	Ändern des Standardorts?	Verbindung über BAS-Firewall?	Hinweise
80/TCP	HTTP	Nein	Nein	
443/TCP	HTTPS	Nein	Möglich, wenn Webzugriff aus dem Internet/Intranet/ Unternehmensnetzwerk erforderlich ist	1
1911/TCP	Fox (nicht gesicherte Version des Niagara Anwendungsprotokolls)	Ja	Nein	
4911/TCP	Fox + SSL (gesicherte Version des Niagara Anwendungsprotokolls)	Ja	Nein	
3011/TCP	NiagaraD (nicht gesicherte Version des Niagara Plattformprotokolls)	Ja	Nein	
5011/TCP	NiagaraD + SSL (gesicherte Version des Niagara Plattformprotokolls)	Ja	Nein	
2601/TCP	Zebra-Konsolenport	Nein	Nein	2
2602/TCP	RIP-Konsolenport			2
47808/UDP	BACnet/IP-Netzwerkverbindung	Ja	Nein	3

NOTE:

1. Wenn eine direkte Remote-Web-Benutzerschnittstelle unterstützt wird, muss dieser Port in der BAS-Firewall freigegeben werden.
2. Der Port wird von diesem Daemon automatisch freigegeben; diese Funktion kann nicht deaktiviert werden. Der Daemon ist so konfiguriert, dass keine Anmeldungen über diesen Port möglich sind.
3. Befolgen Sie die in diesem Leitfaden angegebenen Richtlinien für die Netzwerkkonfiguration, damit der Advanced Plant Controller niemals UDP-Datenverkehr über die BAS-Firewall übertragen muss.

17. EINRICHTEN DER AUTHENTIFIZIERUNG

Das Google Authentication Scheme ist ein Zwei-Faktor-Authentifizierungsmechanismus, bei dem der Benutzer sein Kennwort sowie ein Einmal-Token eingeben muss, wenn er sich bei einer Station anmeldet. Dadurch ist das Konto des Benutzers auch dann geschützt, wenn sein Kennwort kompromittiert wurde.

Dieser Authentisierungsmechanismus basiert auf einem zeitbasierten Einmal-Kennwort (Time-based OneTime Password, TOTP) und der Google Authenticator-App auf dem Mobilgerät des Benutzers, um Authentisierungs-Token für den einmaligen Gebrauch zu generieren und zu verifizieren. Die Google-Authentifizierung erfolgt zeitbasiert, d. h. es besteht keine Notwendigkeit für eine Netzwerkverbindung zwischen dem Mobilgerät des Benutzers, der Station oder externen Servern. Aufgrund der Zeitabhängigkeit des Authentifikators müssen die Uhrzeit in der Station und im Mobiltelefon möglichst übereinstimmen. Die App hat einen Puffer von plus/minus 1,5 Minuten, um Zeitunterschiede auszugleichen.

Voraussetzungen: Auf dem Mobiltelefon des Benutzers muss die Google Authenticator-App installiert sein. Sie arbeiten in Workbench. Der Benutzer ist in der Stationsdatenbank vorhanden.

17. 1 Vorgehensweise

1. Öffnen Sie die Palette «gauth» und fügen Sie in der Navigationsstruktur unter **Services** > **Authenticationservice** das **GoogleAuthenticationScheme** hinzu.
2. Klicken Sie mit der rechten Maustaste auf **Userservice** und doppelklicken Sie dann in der Tabelle auf den Benutzer. Die Bearbeitungsansicht für den Benutzer wird geöffnet.
3. Setzen Sie die Eigenschaft «Authentication Scheme» auf **GoogleAuthenticationScheme** und klicken Sie auf **Save**.
4. Klicken Sie auf die Schaltfläche neben dem geheimen Schlüssel unter dem Authentifikator des Benutzers und folgen Sie den Eingabeaufforderungen.
5. Klicken Sie zum Abschliessen der Konfiguration auf **Save**. Je nachdem, welche Ansicht Sie verwenden, müssen Sie den Benutzer nach dem Speichern erneut öffnen oder die Ansicht aktualisieren.

18. SYSTEMBEREITSTELLUNG

Dieser Abschnitt enthält Informationen, die Sie dem Systemeigentümer bei der Bereitstellung des BAS übergeben müssen.

- Dokumentation mit Sicherheitsinformationen, Konfigurationseinstellungen, Benutzernamen und Kennwörtern für den Administrator, Notfall- und Wiederherstellungsplänen sowie Sicherungs- und Wiederherstellungsverfahren.
- Endbenutzerschulung zu Sicherheits- und Verwaltungsaufgaben.

19. USB-SICHERUNG UND INSTALLATION DER CLEANDIST-DATEI

Informationen zur USB-Sicherung und Installation der CleanDist-Dateien finden Sie in der Installations- und Inbetriebnahmeanleitung (31-00584).

20. AUSSERBETRIEBNAHME DES SYSTEMS

Wenn Geräte ausser Betrieb genommen werden, müssen sensible Daten von diesen gelöscht werden; dies kann durch Zurücksetzen auf die Werkseinstellungen geschehen. Weitere Informationen finden Sie in den Abschnitten zur Wartungstaste/Wartungsalarm-LED und zur Installation der CleanDist-Dateien in der Installations- und Inbetriebnahmeanleitung (31-00584).

NOTE:

Durch Installation der CleanDist-Datei «clean4» können die Einstellungen auf die Werkseinstellungen zurückgesetzt werden.

21. SICHERHEIT VON AUF ADVANCED NIAGARA BASIERENDEN PRODUKTEN

Für Advanced Produkte von Honeywell, die auf den Niagara N4 und Niagara AX Frameworks basieren (z. B. Advanced Plant Controller, HMI und E/A-Modul), müssen Sie die Hinweise von Tridium zum Schutz des Niagara Frameworks beachten.

In Niagara können eine Reihe von Konfigurationsänderungen vorgenommen werden, um die Sicherheit der Advanced Produkte von Honeywell zu maximieren.

- Verwenden der Funktion für starke Kennwörter
- Aktivieren der Kontosperrfunktion
- Ablaufende Kennwörter
- Verwenden der Kennworthistorie
- Verwenden der Funktion zum Zurücksetzen des Kennworts
- Deaktivieren des Kontrollkästchens «Remember These Credentials»
- Ändern der standardmässigen System-Passphrase
- Verwenden von TLS zum Einstellen der System-Passphrase
- Auswählen einer starken System-Passphrase
- Schützen der System-Passphrase
- Sicherstellen, dass der Plattformeigentümer die System-Passphrase kennt
- Verwenden eines separaten Kontos für jeden Plattformbenutzer
- Verwenden eindeutiger Kontonamen für jedes Projekt
- Sicherstellen, dass der Plattformeigentümer die Plattform-Anmeldedaten kennt
- Verwenden eines separaten Kontos für jeden Stationsbenutzer
- Verwenden eindeutiger Servicekonten für jedes Projekt
- Deaktivieren allgemein bekannter Konten (wenn möglich)
- Einrichten von temporären Konten, die automatisch ablaufen
- Ändern der Anmeldedaten für Systemkonten
- Verbieten gleichzeitiger Sitzungen, sofern angemessen
- Konfigurieren von Rollen mit den minimal erforderlichen Berechtigungen
- Zuweisen von Rollen mit den minimal erforderlichen Berechtigungen an Benutzer
- Verwenden möglichst weniger Superuser
- Voraussetzung von Superuser-Berechtigungen für Programmobjekte
- Verwenden der minimal erforderlichen Berechtigungen für externe Konten
- Verwenden eines für den Kontotyp geeigneten Authentifizierungsmechanismus
- Entfernen unnötiger Authentifizierungsmechanismen
- TLS und Zertifikatsverwaltung
- Modulinstallation
- Anfordern signierter Programmobjekte und Roboter
- Deaktivieren von SSH und SFTP
- Deaktivieren nicht benötigter Services
- Sicheres Konfigurieren benötigter Services
- Aktualisieren von Niagara 4 auf die neueste Version
- Installieren des Produkts an einem sicheren Ort
- Sicherstellen, dass die Stationen über ein VPN gesichert sind

Spezielle technische Publikationen sind verfügbar, die eingehalten werden müssen, um die grösstmögliche Sicherheit des Systems zu gewährleisten. Hierzu gibt es zahlreiche Möglichkeiten, wie z. B. SSL-Verschlüsselung und zusätzliche Massnahmen zum Schutz von Elementen wie Programmmodulen. Weitere Informationen finden Sie im Niagara 4 Hardening Guide (für Niagara N4-basierte Produkte) und im Niagara Hardening Guide (für Niagara AX-basierte Produkte) auf der Tridium-Website.

Dieses Dokument dient nur zu Informationszwecken. Der Inhalt und das beschriebene Produkt können ohne Vorankündigung geändert werden. Honeywell übernimmt keine Gewähr in Bezug auf dieses Dokument. Honeywell haftet unter keinen Umständen für technische oder redaktionelle Auslassungen oder Fehler in diesem Dokument. Ebenso wenig haftet Honeywell für etwaige Schäden, die sich direkt oder indirekt aus der Verwendung dieses Dokuments ergeben oder damit zusammenhängen. Dieses Dokument darf ohne vorherige schriftliche Genehmigung von Honeywell weder ganz noch teilweise in irgendeiner Form vervielfältigt werden.

Honeywell Building Technologies

715 Peachtree Street, N.E.,
Atlanta, Georgia, 30308, United States.
https://buildings.honeywell.com/us/en

® U.S. Eingetragene Marke
©2023 Honeywell International Inc.
31-00594-01 Rev. 07-23

Honeywell

22. CHECKLISTE ZUM PRÜFEN DER INSTALLATIONSSICHERHEIT

Advanced Plant Controller Geräteinstanz: _____

Advanced Plant Controller Beschreibung: _____

Advanced Plant Controller Ort: _____

Installateur:_____ Datum: _____

Für jeden installierten Advanced Plant Controller sind die folgenden Sicherheitsmassnahmen auszuführen.

- ☐ Installation einer Firewall zwischen dem Advanced Plant Controller und externen Netzwerken. Siehe *„BACnet und Niagara“ auf Seite 18.*
- ☐ Physische Sicherung des Advanced Plant Controller. Siehe *„Physischer Schutz von Advanced Plant Controller, HMI und E/A-Modul“ auf Seite 20.*
- ☐ Änderung des Standardkennworts in ein eindeutiges Kennwort für jede der folgenden Komponenten: Konsolenkonfiguration, Sicherung/Wiederherstellung/Neustart/Steuerung und Niagara Plattform. Siehe Installations- und Inbetriebnahmeanleitung (31-00584).
- ☐ Konfiguration eines ggf. erforderlichen Webservers, sodass dieser nur im HTTPS-Modus betrieben werden kann. Siehe Installations- und Inbetriebnahmeanleitung (31-00584).

Webserver-Status: Deaktiviert / Aktiviert.

Bei Aktivierung des Webservice führen Sie folgende Schritte aus:

- ☐ Stellen Sie «Http Enabled» = «false» ein.
- ☐ Stellen Sie « Https Enabled» = «true» ein.
- ☐ Stellen Sie « Https Only» = «true» ein.
- ☐ Konfigurieren Sie die BAS-Firewall. Siehe *„Konfigurieren der BAS-Firewall“ auf Seite 24.*
- ☐ Übergeben Sie dem Eigentümer des BAS-Systems bei der Lieferung alle erforderlichen Daten. Siehe *„Einrichten der Authentifizierung“ auf Seite 25.*