Honeywell

Advanced

GUIDA SULLA SICUREZZA

Perché proteggere gli Advanced Controller? 5

Panoramica del sistema 6

Rete aziendale / Internet / intranet 7
Rete BAS 7
Firewall BAS 7
Workstation Niagara 4 7
Switch Ethernet 7
Advanced Plant Controller 7
HMI 7
Modulo I/O 7

Pianificazione e protezione della rete 8

Rete Ethernet 8
Server Web 8
Rete BACnet IP 8
MS/TP (licenze NC) 8
USB 8
RS485 (incluse licenze Modbus) 8
Rete Modbus IP (licenze INT) 8

Sistema di sicurezza di Advanced Controller, HMI e modulo I/O 9

Sicurezza in mancanza di configurazione 9
Protezione dai dispositivi non autorizzati 9
"Account Verification Code" (Codice di verifica account) 9
Account di sistema 9
"Engineering System Account" (Account di sistema di ingegnerizzazione) 9
Ruolo "Engineering" (Ingegnerizzazione) 10
Ruolo "Administrator" (Amministratore) 10
"Device System Account" (Account di sistema del dispositivo) 10
Creazione di account di sistema 10
Gestione account sincronizzata 10
Modifica della chiave di rete di un Advanced Controller 11
Sicurezza locale 11
Accesso a pagine Web 11
Accesso iniziale 11
Utenti connessi 12
Recupero della password 12

Protezione del sistema operativo Niagara 12

® U.S. Registered Trademark
Copyright © 2023 Honeywell Inc. • Tutti i diritti riservati

Best practice generali 12
Impostazione del firewall 12
Versione del sistema operativo 12
Protezione antivirus 12
Protezione dalle intrusioni 13
Regolamento generale sulla protezione dei dati (GDPR) 13
Comunicazioni sicure 14
Relazioni client/server 14
Certificati 15
Certificati autofirmati 15
Convenzione di denominazione 15
Archivi di certificati 16
Crittografia 16
Panoramica della dashboard di sicurezza 16
Pianificazione e installazione 17
Installazione e configurazione consigliate 17
Solo BACnet 17
BACnet e Niagara 18
Consiglio sulle reti locali (Local Area Network, LAN) 18
Documentazione 19
Documentare dispositivi fisici e configurazioni, compresi i dati chiave correlati alla sicurezza 19
Documentare sistemi esterni, in particolare l'interazione fra l'Advanced Plant Controller e i sistemi correlati 19
Controllo dell'accesso e sicurezza fisica 20
Proteggere fisicamente l'Advanced Plant Controller, HMI e il modulo I/O 20
Adesivi sul pannello di accesso o l'alloggiamento del controller 20
Segregare e proteggere le reti 20
Protezione di Advanced Controller, HMI e modulo I/O 21
Credenziali dell'account di sistema amministratore fornite all'utente del sito 21
Sviluppo di un programma di protezione 21
Considerazioni di carattere fisico e ambientale 21
Aggiornamenti e service pack di sicurezza 21
Utenti e password 21
Utenti 21
Password 22
Configurazione di un Advanced Plant Controller 23
Creare ed eseguire la manutenzione di configurazioni di base 23

Modificare le password predefinite 23
Ulteriori considerazioni 23
Contratto sul livello di servizio 23
Configurazione della rete IT 23
Configurazione del firewall BAS 24
Impostazione dell'autenticazione 25
Procedura 25
Consegna del sistema 25
Backup via USB e installazione di file CleanDist 25
Dismissione del sistema 25
Sicurezza dei prodotti Advanced basati su Niagara 26
Lista di controllo della sicurezza dell'installazione 27

Esclusione di responsabilità

Nonostante l'impegno dedicato a garantire l'accuratezza del presente documento, Honeywell non si assume responsabilità per danni di qualsiasi tipo, inclusi, senza limitazione, danni consequenziali derivanti dall'applicazione o dall'utilizzo delle informazioni qui contenute. Le informazioni e le specifiche riportate in questo documento sono aggiornate alla data di pubblicazione e sono soggette a modifica senza preavviso. Le specifiche più recenti sul prodotto sono reperibili consultando il sito Internet di Honeywell o contattando la sede aziendale di Atlanta, Georgia.

Per molte comunicazioni basate su RS485 per l'industria, lo stato predefinito dell'interfaccia al momento della spedizione dalla fabbrica è "disabilitata" per garantire la massima sicurezza possibile, in quanto i bus di comunicazione sono legacy, usano tecnologie legacy per la migliore compatibilità e sono stati progettati con un basso livello di sicurezza. Pertanto, per massimizzare la protezione del sistema, Honeywell disabilita preventivamente le porte di comunicazione del bus industriale legacy (al momento della spedizione dalla fabbrica) e l'utente deve abilitare esplicitamente la rete in ciascuna stazione. Se si desidera abilitare queste porte, è necessario tenere presente il rischio di violazioni della sicurezza associato all'uso di tecnologie legacy. Ciò comprende, senza limitazione: Panel-Bus, C-Bus, BACnet, M-Bus, Bus CP-IO, NovarNet, il protocollo XCM-LCD, S-Bus e Modbus SBC, ecc.

Sviluppo conforme a ISA-62443

Da molti anni Honeywell si affida allo standard ISA 62443-4-1 e alle normative correlate per sviluppare soluzioni tecnologiche sicure per gli edifici. Ad esempio, i nostri prodotti per edifici utilizzano anche lo standard ISA/IEC 62443-4-2 come base per i requisiti di sicurezza tecnica all'interno dei componenti mentre per i sistemi completi l'azienda fa riferimento a ISA/IEC 62443-3-3. Grazie alla nostra aderenza alla famiglia di standard ISA/IEC 62443, gli integratori e i clienti che scelgono tecnologie per gli edifici possono fidarsi del fatto che i prodotti di Honeywell non sostengono semplicemente di essere resilienti agli attacchi informatici - ma sono stati progettati, testati e validati a tale scopo sin dall'inizio.

Honeywell sviluppa prodotti conformi a ISA/IEC 62443-4-1 ed è stata valutata da una terza parte e verificata in base a tale standard.

Introduzione e destinatari

Nel presente documento, Honeywell dichiara espressamente che i propri controller non sono dotati di protezione intrinseca dagli attacchi informatici via Internet e che, pertanto, sono intesi esclusivamente per l'uso nelle reti private. Tuttavia, anche le reti private possono essere vittima di attacchi informatici da parte di cyber-criminali competenti e dotati di attrezzature adeguate, quindi richiedono protezione. Per questo è essenziale che i clienti adottino le linee guida sulle best practice di installazione e sicurezza per i prodotti Advanced Plant Controller basati su IP, al fine di mitigare il rischio costituito da tali attacchi.

Le linee guida riportate di seguito descrivono le best practice di sicurezza generali per i prodotti Advanced Plant Controller basati su IP. Sono elencate in ordine di prevenzione crescente.

I requisiti specifici di ogni sito vanno valutati caso per caso. La grande maggioranza delle installazioni che implementano tutti i livelli di prevenzione qui descritti supera di gran lunga i criteri necessari per una protezione soddisfacente dei sistemi. In genere, integrando gli elementi 1-5 correlati alle reti locali (LAN), Vedere *"Consiglio sulle reti locali (Local Area Network, LAN)" a pag. 18.*, si soddisfano i requisiti della maggior parte delle installazioni delle reti di controllo automazione.

Il presente manuale contiene informazioni utili per orientare il personale dei rivenditori Honeywell su come installare e configurare in modo sicuro dispositivi quali Advanced Plant Controller, HMI e moduli I/O. Le informazioni di sicurezza relative al funzionamento, al backup e ripristino via USB e all'installazione dei file CleanDist del controller sono disponibili nella Guida di istruzioni per l'installazione e la messa in servizio (31-00584).

NOTE:

È importante prendersi il tempo necessario per leggere e comprendere tutti i manuali di installazione, configurazione e funzionamento pertinenti e assicurarsi di avere a disposizione sempre le versioni più aggiornate.

.

Tabella 1 Informazioni sui prodotti

Prodotto	Codice prodotto	Descrizione
Plant Controller	N-ADV-134-H	Advanced Controller Niagara con quattro porte Ethernet, una porta per HMI e 4 porte RS485
	N-ADV-133-H	Advanced Controller Niagara con quattro porte Ethernet, una porta per HMI e 3 porte RS485
	N-ADV-112-H	Advanced Controller Niagara con due porte Ethernet, una porta per HMI e 2 porte RS485
HMI	HMI-DN	HMI con montaggio su guida DIN
	HMI-WL	Montaggio su porta/a parete
Modulo I/O	IO-16UIO-S-S	Modulo I/O 16UIO senza HOA, com. seriali, morsetti a vite
	IOD-16UIO-S-S	Modulo I/O 16UIO con display HOA, com. seriali, morsetti a vite
	IO-16UI-S-S	Modulo I/O 16UI, com. seriali, morsetti a vite
	IO-16DI-S-S	Modulo I/O 16DI, com. seriali, morsetti a vite
	IO-8DOR-S-S	Modulo I/O 8DO senza HOA, relè C/O, com. seriali, morsetti a vite
	IOD-8DOR-S-S	Modulo I/O 8DO con display HOA, com, relè C/O, com. seriali, morsetti a vite
	IO-16UIO-S-P	Modulo I/O 16UIO con display HOA, com. seriali, morsetti a innesto
	IO-16UI-S-P	Modulo I/O 16UIO, com. seriali, morsetti a innesto
	IO-16DI-S-P	Modulo I/O 16DI, com. seriali, morsetti a innesto
	IO-8DOR-S-P	Modulo I/O 8DO senza HOA, relè C/O, com. seriali, morsetti a innesto
	IOD-8DOR-S-P	Modulo I/O 8DO con display HOA, relè C/O, com. seriali, morsetti a innesto

1. PERCHÉ PROTEGGERE GLI ADVANCED CONTROLLER?

- Proteggere i sistemi di impianto dei clienti dalle modifiche non autorizzate a setpoint operativi, override e pianificazioni orarie.
- Prevenire l'accesso ai dettagli degli account utente: ad esempio nomi utente, password, indirizzi e-mail, numeri SMS (cellulari), ecc.
- Prevenire l'accesso ai dati sensibili a livello commerciale: ad esempio, parametri di consumo energetico, soluzioni per strategie di regolazione specializzate, ecc.
- Prevenire l'accesso non autorizzato a controller, computer e reti che ospitano dispositivi di controllo e software BMS.
- Mantenere l'integrità dei dati e garantire l'assunzione di responsabilità.

2. PANORAMICA DEL SISTEMA

La panoramica della tipica installazione del sistema.

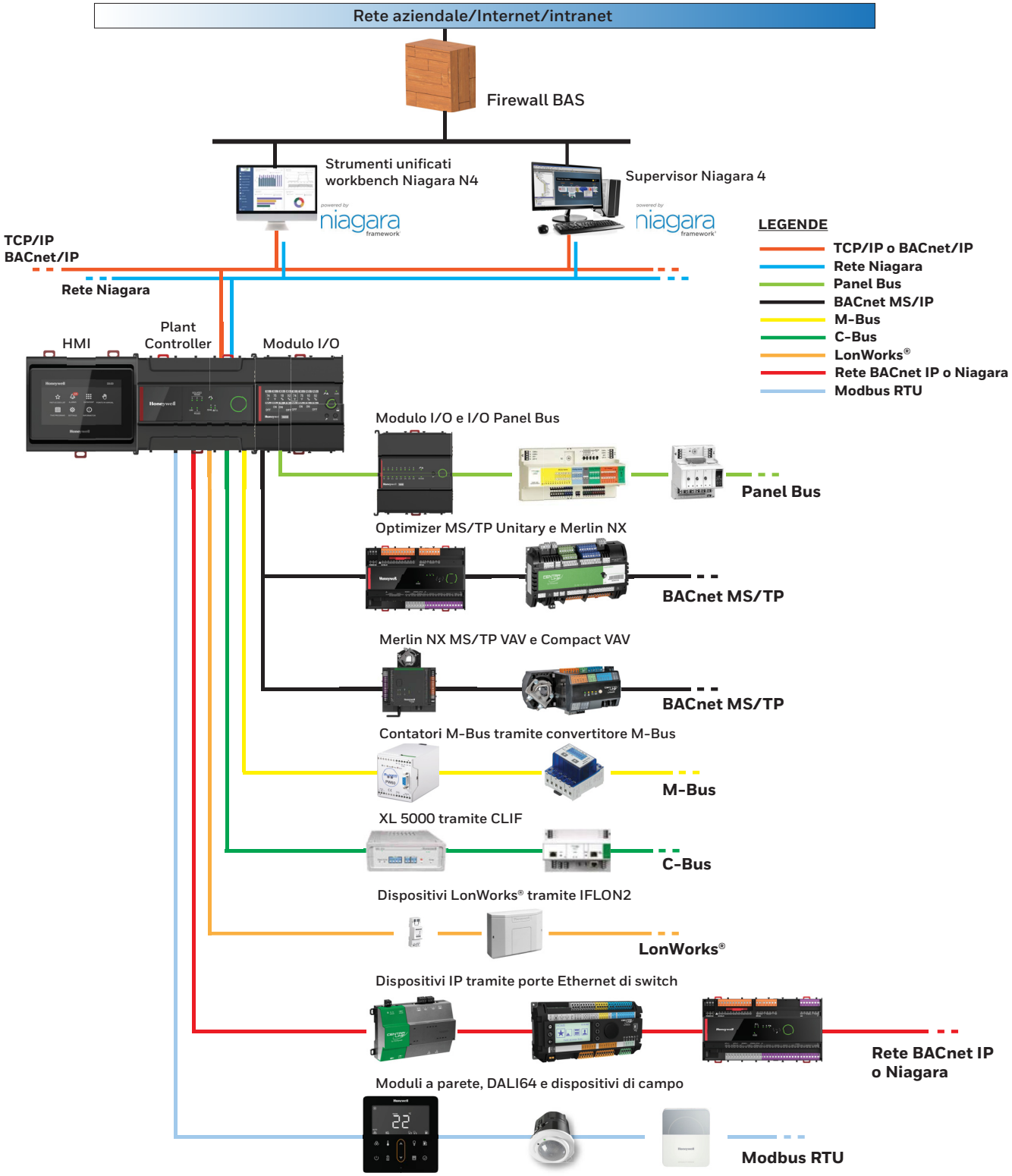

Fig. 1 Panoramica del sistema

2. 1 Rete aziendale / Internet / intranet

Questa è una rappresentazione di una rete logica semplificata applicabile a tutte le reti esterne all'ambito del sistema di automazione dell'edificio (BAS). Può fornire accesso alle interfacce di gestione BAS (ad es. l'interfaccia utente Web della workstation Niagara principale) ma deve consentire di accedere a Internet in modo che i computer Niagara possano verificare e scaricare aggiornamenti del sistema operativo e degli scanner antivirus, a meno che non si predisponga un metodo alternativo per farlo.

2. 2 Rete BAS

Questa rete viene utilizzata unicamente per i protocolli BAS, che comprendono BACnet / IP, BACnet / Ethernet e qualsiasi altro che Niagara Integration Services potrebbe utilizzare su un Advanced Plant Controller. Questa rete non deve essere la stessa utilizzata come rete aziendale / Internet / intranet.

2. 3 Firewall BAS

Per assicurare una maggiore separazione e protezione al BAS, è necessario predisporre un firewall fra la rete aziendale / Internet / intranet e gli eventuali dispositivi BAS che vi si connettono, come ad esempio la workstation Niagara principale, le workstation Niagara e l'Advanced Plant Controller. Questo firewall limita l'accesso al BAS ai soli computer autorizzati e può contribuire a ridurre il rischio di attacchi, ad esempio del tipo di negazione del servizio (denial-of-service).

2. 4 Workstation Niagara 4

La workstation Niagara principale è un computer che esegue il software Niagara. Richiede due connessioni di rete: una per collegarsi all'interfaccia utente Web di gestione, tramite un browser Web (solitamente all'interno della rete aziendale / Internet / intranet), e un'altra per collegarsi alla rete BAS.

2. 5 Switch Ethernet

Uno switch Ethernet crea reti e utilizza varie porte per la comunicazione fra i dispositivi della rete locale (LAN). Gli switch Ethernet sono diversi dai router, che connettono le reti e utilizzano solo una singola porta LAN e WAN. Un'infrastruttura completa, cablata e wireless aziendale fornisce la connettività via cavo e il Wi-Fi per la connettività wireless.

2. 6 Advanced Plant Controller

L'Advanced Plant Controller è un controller globale che si connette ai segmenti di rete Ethernet, BACnet IP e MS/TP host. La connessione MSTP è a bassa larghezza di banda e viene utilizzata per collegare controller e sensori.

2. 7 HMI

L'interfaccia HMI è connessa e alimentata dagli Advanced Plant Controller Niagara. Questi dispositivi sono dotati di un display touchscreen capacitivo sensibile al tocco delle dita che offre all'operatore le funzionalità necessarie per visualizzare, accedere e risolvere i problemi dei punti del controller, dei moduli I/O e di altre attrezzature collegate.

2. 8 Modulo I/O

I moduli I/O possono collegarsi al controller tramite connessioni TouchFlake (alimentazione e comunicazioni) oppure a un adattatore di cablaggio che viene alimentato e si collega a una delle interfacce RS485 del controller. I moduli I/O sono programmabili tramite lo strumento di ingegnerizzazione esistente, quale il tool ComfortPoint Open Studio e il workbench Niagara 4.

3. PIANIFICAZIONE E PROTEZIONE DELLA RETE

3. 1 Rete Ethernet

La rete Ethernet utilizzata dal sistema BMS deve essere tenuta separata dalla normale rete dell'ufficio.

Esempio:

Si può predisporre un'intercapedine o una rete virtuale privata (VPN). È necessario limitare l'accesso fisico all'infrastruttura della rete Ethernet. Inoltre, occorre garantire un'installazione conforme ai criteri informatici della propria azienda.

Gli Advanced Controller non devono essere connessi direttamente a Internet.

3. 2 Server Web

L'Advanced Controller fornisce entrambi i server Web HTTP e HTTPS. Se non occorre un server Web, si consiglia di disabilitare entrambi i server Web.

3. 3 Rete BACnet IP

A causa della natura poco sicura del protocollo BACnet, l'Advanced Controller, HMI e i moduli I/O che utilizzano BACnet non devono essere connessi a Internet in alcuna circostanza. Il sistema di protezione dell'Advanced Controller non protegge dall'accesso a BACnet in scrittura. È necessario limitare l'accesso fisico all'infrastruttura della rete BACnet IP. Se le comunicazioni BACnet IP non sono necessarie, il modulo di rete (BACnet IP) dell'Advanced Controller deve essere disabilitato impostando il parametro "Disable Module" (Disabilita modulo) su "1".

Se le comunicazioni BACnet sono necessarie, si consiglia fortemente di non abilitare i servizi "BACnet Backup/Restore" (Backup/Ripristino BACnet), "Reinitialize Device" (Reinizializza dispositivo) e "BACnet Writable" (BACnet scrivibile). Tuttavia, ciò significa che la strategia creata non sarà conforme a BTL - Vedere *"Sicurezza locale" a pag. 11.*

3. 4 MS/TP (licenze NC)

È necessario limitare l'accesso fisico all'infrastruttura della rete MS/TP. Se la rete MS/TP non è richiesta, il modulo di rete (BACnet MSTP) dell'Advanced Controller deve essere disabilitato impostando il parametro "Disable Module" (Disabilita modulo) su "1".

Bus I/O (licenze CAN)
È necessario limitare l'accesso fisico al Bus I/O.

3. 5 USB

È necessario limitare l'accesso fisico alla porta USB di ingegnerizzazione locale dell'Advanced Controller.

3. 6 RS485 (incluse licenze Modbus)

È necessario limitare l'accesso fisico alla porta RS485 del controller. Se non sono richiesti, i moduli di rete collegati alla porta non devono essere inclusi nella strategia.

3. 7 Rete Modbus IP (licenze INT)

A causa della natura poco sicura del protocollo Modbus, gli Advanced Controller che supportano Modbus IP non devono essere connessi a Internet in alcuna circostanza. È necessario limitare l'accesso fisico all'infrastruttura della rete Modbus IP. Se le comunicazioni Modbus IP non sono richieste, il modulo di rete (Modbus IP) dell'Advanced Controller non deve essere incluso nella strategia.

4. SISTEMA DI SICUREZZA DI ADVANCED CONTROLLER, HMI E MODULO I/O

La sicurezza degli Advanced Controller è conforme allo standard ISA 62433-3-3 SL 3 e offre l'avvio sicuro, una rete autenticata e crittografata, la crittografia a riposo e la gestione account sincronizzata.

Per avere accesso agli Advanced Controller o eseguire qualsiasi operazione fra le precedenti è necessario fornire un nome utente e una password validi per un "Engineering System Account" (Account di sistema di ingegnerizzazione) o un "Device System Account" (Account di sistema del dispositivo).

4. 1 Sicurezza in mancanza di configurazione

Per interagire con Advanced Controller, HMI e moduli I/O è necessario fornire credenziali valide. Il controller viene rilasciato dalla fabbrica senza alcuna credenziale (account di sistema o moduli utente), in modo da garantire che al primo avvio sia protetto dagli accessi non autorizzati. La prima volta in cui si tenta di connettersi a un vCNC in uno dei prodotti Advanced della rete Niagara occorre creare un "Engineering System Account" (Account di sistema di ingegnerizzazione) con il ruolo di amministratore.

4. 2 Protezione dai dispositivi non autorizzati

Per garantire che solo i dispositivi autorizzati possano connettersi alla rete Niagara si utilizza una chiave univoca ("Network Key", Chiave di rete). Tutti i controller che devono formare una rete Niagara devono condividere la stessa chiave di rete e la stessa porta UDP. Queste impostazioni vengono configurate tramite lo strumento IP durante il processo di configurazione iniziale.

Esempio:

Se quattro Advanced Plant Controller presentano la stessa chiave di rete (112233) e un quinto ha una chiave di rete diversa (222), quando vengono connessi alla stessa rete Ethernet i quattro controller con la stessa chiave di rete si uniscono gli uni agli altri per formare una rete singola, ma il quinto controller rimane escluso a causa della propria chiave di rete (222).

Analogamente, se il quinto controller è nuovo (appena ricevuto dalla fabbrica) e viene aggiunto alla rete Ethernet, non può connettersi alla rete Niagara perché privo di chiave di rete.

4. 2. 1 "Account Verification Code" (Codice di verifica account)

Quando si aggiunge un "Admin System Account" (Account di sistema amministratore) a uno dei controller nella rete, questo dispositivo genera automaticamente un codice di verifica account. Tale codice viene sincronizzato con tutti gli altri controller dotati della stessa chiave di rete e porta UPD nella rete Ethernet.

Una volta generato un codice di verifica account, TUTTI i controller nella rete DEVONO presentare lo stesso codice di verifica account, oltre alla stessa chiave di rete e porta UDP.

Esempio:

si supponga che vi siano cinque Advanced Controller con la stessa chiave di rete. Quattro presentano lo stesso codice di verifica account e pertanto formano una rete. Il quinto ha un codice di verifica account diverso e, nonostante presenti la stessa chiave di rete, non è in grado di unirsi agli altri controller.

4. 3 Account di sistema

Gli account di sistema consentono alle persone e ai dispositivi di interagire con l'Advanced Controller. L'accesso fornito dipende dal tipo di account e dal ruolo.

Esistono due tipi di account di sistema:

1. "Engineering System Account" (Account di sistema di ingegnerizzazione)
2. "Device System Account" (Account di sistema del dispositivo)

4. 3. 1 "Engineering System Account" (Account di sistema di ingegnerizzazione)

Questi account sono concepiti per i tecnici. Ciascuno è abbinato a un nome account e a una password che devono essere forniti quando richiesto dal controller. Se si forniscono il nome utente e la password corretti, il controller concede l'accesso.

Per ogni persona è necessario creare un account di sistema di ingegnerizzazione separato. Questi account possono essere impostati su un ruolo fra due disponibili:

- Ruolo “Engineering” (Ingegnerizzazione)
- Ruolo “Administrator” (Amministratore)

Ruolo “Engineering” (Ingegnerizzazione)
Questo ruolo fornisce l’accesso richiesto per eseguire interventi tecnici sul sistema dell’Advanced Controller, creare/gestire account di sistema del dispositivo e gestire i propri dettagli dell’account utente (indirizzo e-mail, password, ecc.).

Ruolo “Administrator” (Amministratore)
Questo ruolo fornisce lo stesso accesso del ruolo di ingegnerizzazione ma vi aggiunge la capacità di gestire tutti gli account di sistema di ingegnerizzazione e di dispositivo.

4. 3. 2 “Device System Account” (Account di sistema del dispositivo)

Questi account sono concepiti per permettere ai dispositivi quali Niagara di connettersi alla rete per ottenere le informazioni che occorrono e apportare modifiche. Si consiglia di creare un account di sistema del dispositivo per ciascun dispositivo che deve accedere alla rete. Il ruolo corrispondente è quello di “Saia PCD Supervisor” (Supervisore).

IMPORTANT:
Importante: il sistema di sicurezza Saia PCD Supervisor deve essere configurato in modo da limitare i diritti di accesso di ciascun utente Saia PCD Supervisor.

4. 3. 3 Creazione di account di sistema

È necessario creare un account di sistema di ingegnerizzazione con il ruolo di amministratore al primo tentativo di connettersi a un vCNC nella rete Niagara. L’account creato viene poi sincronizzato con altri controller nella rete Niagara.

- Vedere *“Gestione account sincronizzata” a pag. 10.* È possibile creare account aggiuntivi, in base alle esigenze, utilizzando il workbench Niagara.

NOTE:
La prima volta in cui in un controller si crea un account di sistema di ingegnerizzazione viene generato automaticamente un codice di verifica account e il controller viene sincronizzato con gli altri nella rete Ethernet che presentano la stessa chiave di rete e la stessa porta USB. Un controller che condivide con altri controller lo stesso codice di verifica account può entrare in una rete con tali dispositivi - Vedere *““Account Verification Code” (Codice di verifica account)” a pag. 9.*

4. 4 Gestione account sincronizzata

Questa funzionalità sincronizza in modo semplice e sicuro gli account di sistema, incluso il codice di verifica account, con tutti gli Advanced Controller nella stessa rete Niagara. Ciò consente:

- Singolo accesso alla rete
- Ridotti costi di configurazione e manutenzione dell’accesso attraverso il sito, senza compromettere la sicurezza

Tutti gli Advanced Controller nella stessa rete presentano gli stessi account di sistema.

Quando un Advanced Controller senza account di sistema si connette alla rete Ethernet e viene configurato con la chiave di rete e la porta UDP per la rete Niagara, si unisce a quest’ultima rete e ottiene automaticamente gli account di sistema dagli altri controller che ne fanno parte.

Esempio:

se un Advanced Controller senza account di sistema viene aggiunto al sistema menzionato sopra e viene configurato con la chiave di rete (112233) e la porta UDP della rete Niagara, si unisce a tale rete e ottiene gli account di sistema (utente 1, 2 e 3) dagli altri Advanced Controller nella rete.

Al termine della sincronizzazione, è possibile connettersi a un eventuale vCNC, visualizzare pagine Web e accedere a qualsiasi Advanced Controller nella rete Niagara utilizzando qualunque account di sistema.

Se gli account di sistema vengono modificati, ad es. si aggiunge, elimina o modifica un account, tali modifiche vengono sincronizzate automaticamente attraverso tutti gli Advanced Controller nella rete Niagara.

Esempio:

se ci sono cinque Advanced Controller e gli account di sistema nel controller (1) vengono modificati rimuovendo l'utente 2, rinominando l'utente 3 come utente 3a e aggiungendo l'utente 4, le modifiche vengono sincronizzate con i controller (2), (3), (4) e (5).

NOTE:
Se durante la sincronizzazione emerge un conflitto, la modifica più recente ha la priorità.

4. 5 Modifica della chiave di rete di un Advanced Controller

Quando si modifica la chiave di rete di un Advanced Controller, tutti gli account di sistema vengono eliminati e il controller rimosso dalla sua attuale rete Niagara. Per modificare la chiave di rete è necessario essere autorizzati da un account di sistema con ruolo di ingegnerizzazione o amministratore valido.

Una volta effettuata la modifica, il controller si unisce a una rete Niagara utilizzando la chiave di rete, se ne esiste una, e ottiene gli account di sistema dall'Advanced Controller nella nuova rete Niagara, a condizione che abbia la stessa porta UDP.

4. 6 Sicurezza locale

La sicurezza locale utilizza utenti locali (moduli utente) per consentire l'accesso alle pagine Web degli Advanced Controller, o a un display connesso localmente, e controllare le informazioni visibili o i valori che si possono regolare.

Per accedere e apportare modifiche è necessario fornire un nome utente e una password validi per un utente locale. Dal livello del codice PIN di un utente dipendono i parametri che questi può visualizzare e regolare.

NOTE:
Gli utenti locali NON sono sincronizzati con altri Advanced Controller nella rete Niagara.

4. 7 Accesso a pagine Web

L'accesso alle pagine Web di un Advanced Controller è protetto dal sistema di sicurezza di tale dispositivo. Quando si accede al server Web del controller viene visualizzata una pagina Web che fornisce informazioni di base e consente il login di un utente - Vedere *"Accesso iniziale" a pag. 11.*

Gli utenti che eseguono il login vengono gestiti come utenti connessi - Vedere *"Utenti connessi" a pag. 12.* e gli utenti che accedono alle pagine Web senza eseguire il login possono connettersi come descritto in *"Accesso iniziale" a pag. 11*.

4. 7. 1 Accesso iniziale

Al primo accesso al server Web del controller la pagina "Welcome" (Benvenuto) visualizzata e l'accesso consentito dipendono dall'attuale configurazione di sicurezza del controller stesso:

- Non vi sono account di sistema di ingegnerizzazione né moduli utente (impostazione di fabbrica)
  Si apre la pagina "Welcome" (Benvenuto), che offre accesso completo alle pagine Web del controller e la capacità di apportare modifiche.

NOTE:
Poiché non vi sono account di sistema di ingegnerizzazione o moduli utente il login non è possibile.

- Account di sistema di ingegnerizzazione ma nessun modulo utente
  Si apre la pagina "Welcome" (Benvenuto) e il controller permette di accedere solo a "Sensor" (Sensore), "Digital Input" (Ingresso digitale), "Knob" (Manopola), "Switch", "Driver", "Schedule" (Pianificazione), "Time Schedule" (Pianificazione oraria), "Time" (Ora), "Plot modules" (Moduli plot), "Alarm Log" (Registro allarmi) e "Graphics" (Grafici) ma non consente modifiche.

NOTE:
Sarà possibile eseguire il login tramite gli account di sistema di ingegnerizzazione.

- Account di sistema di ingegnerizzazione e moduli utente
  La visualizzazione e l'accesso iniziali sono controllati dai moduli utente. Se esiste un modulo utente denominato "Guest" (Ospite) senza password, quando ci si connette alle pagine Web dell'Advanced Controller senza eseguire il login il controller fornisce i diritti di accesso (impostazioni predefinite di livello utente, pagina home e visualizzazione) specificati dal modulo utente "Guest" (Ospite).

  Per impostazione predefinita, il modulo utente "Guest" (Ospite) fornisce accesso esclusivamente alla pagina "Welcome" (Benvenuto) dell'Advanced Controller e ha il livello utente "0". Ciò significa che un utente che si connette al controller senza eseguire il login potrà visualizzare soltanto la pagina "Welcome" (Benvenuto). Per un accesso più ampio, l'utente "Guest" (Ospite) può essere configurato allo stesso modo di qualsiasi altro modulo utente di tipo 0.

NOTE:
Il workbench Niagara impedisce che all'utente "Guest" (Ospite) vengano forniti una password, un codice PIN o un livello utente superiore a "0". Tuttavia, consente di configurare impostazioni predefinite relative alla pagina home e alla visualizzazione.

Si consiglia fortemente di lasciare l'utente "Guest" (Ospite) con la configurazione predefinita (livello utente "0" e nessun diritto di visualizzazione).

Se non esiste un modulo utente denominato "Guest" (Ospite) o se tale modulo è stato configurato con una password, si apre la pagina "Welcome" (Benvenuto) e il controller permette di accedere solo a "Sensor" (Sensore), "Digital Input" (Ingresso digitale), "Knob" (Manopola), "Switch", "Driver", "Schedule" (Pianificazione), "Time Schedule" (Pianificazione oraria), "Time" (Ora), "Plot modules" (Moduli plot), "Alarm Log" (Registro allarmi) e "Graphics" (Grafici) ma non consente modifiche.

NOTE:
Sarà possibile eseguire il login tramite gli account di sistema di ingegnerizzazione.e qualsiasi modulo utente esistente.

4. 7. 2 Utenti connessi

Per eseguire il login in una pagina Web dell'Advanced Controller, è necessario inserire un nome utente e una password corrispondenti a un account di sistema di ingegnerizzazione o a un modulo utente di tipo 0 dell'Advanced Controller.

4. 8 Recupero della password

Se un utente ha dimenticato la password, può recuperarla tramite il workbench Niagara. Per informazioni dettagliate sulla procedura di recupero tramite Niagara di una password dimenticata, vedere la Guida utente del workbench Niagara.

5. PROTEZIONE DEL SISTEMA OPERATIVO NIAGARA

5. 0. 1 Best practice generali

Per proteggere il sistema operativo, attenersi a best practice generali simili alle seguenti:

- Salvaschermo protetto da password
- Software di crittografia dell'unità

5. 0. 2 Impostazione del firewall

Il sistema operativo deve essere configurato in modo da utilizzare un firewall che venga aggiornato automaticamente. La configurazione deve impedire l'accesso (IN/OUT) per tutte le porte, tranne quelle a cui è necessario accedere. NON lasciare aperte le porte inutilizzate.

5. 0. 3 Versione del sistema operativo

È NECESSARIO assicurarsi che in tutti i dispositivi che eseguono applicazioni Niagara o che sono connessi alla stessa rete IP siano installati gli aggiornamenti più recenti del sistema operativo. È opportuno assicurarsi che gli aggiornamenti automatici di Windows rimangano attivi e vengano installati puntualmente.

5. 0. 4 Protezione antivirus

È NECESSARIO assicurarsi che in tutti i computer che eseguono applicazioni Niagara o che sono connessi alla stessa rete IP sia in funzione un software di protezione antivirus con definizioni di virus aggiornate.

5. 0. 5 Protezione dalle intrusioni

Si consiglia di utilizzare un sistema di rilevamento intrusioni (IDS), prodotto da un fornitore affidabile di soluzioni di sicurezza, su tutti i computer che eseguono applicazioni Niagara. Attenersi a best practice per i prodotti scelti, nonché ai criteri informatici aziendali, dove viene effettuata l'installazione.

Molti IDS e prodotti firewall offrono una soluzione completa per la registrazione di tutto il traffico in ingresso e in uscita dal computer, che permette agli utenti di registrare qualsiasi attività al livello minimo.

6. REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR)

Il Regolamento generale sulla protezione dei dati (UE) 2016/679 (GDPR) è una normativa UE sulla protezione e la riservatezza dei dati valida per tutti i singoli cittadini dell'Unione Europea (UE) e dello Spazio Economico Europeo (SEE). Riguarda anche il trasferimento dei dati personali all'esterno delle aree della UE e del SEE. Il GDPR comprende le disposizioni e i requisiti correlati al trattamento dei dati personali delle persone (interessati) all'interno del SEE e si applica a qualsiasi organizzazione creata nel SEE (indipendentemente dalla sua sede e dalla cittadinanza degli interessati) o che tratti informazioni personali di interessati all'interno del SEE.

Ai sensi del GDPR, i dati personali comprendono qualsiasi informazione utilizzabile per identificare un individuo. Ciò comprende, senza limitazione:

- nomi utente,
- password,
- numeri di telefono,
- indirizzi e-mail,
- indirizzi di lavoro o residenziali.

Qualsiasi informazione del genere inserita nell'Advanced Controller, in HMI o nel modulo I/O viene crittografata e memorizzata nei prodotti Advanced presso la sede di un cliente. Honeywell non è coinvolta nella memorizzazione e/o nel trattamento dei dati personali nel prodotti Honeywell Advanced.

La responsabilità della conformità ai requisiti del GDPR spetta interamente all'integratore del sistema o all'amministratore del sistema che, pertanto, deve assicurare l'implementazione di sistemi tecnici e organizzativi adeguati per:

- ottenere il consenso esplicito da ciascun interessato per la memorizzazione, l'utilizzo e/o il trattamento dei dati personali,
- consentire alle persone di avere accesso ai propri dati personali al fine di verificarne l'accuratezza,
- permettere alle persone di ritirare il proprio consenso in qualunque momento e di imporre che i propri dati personali vengano cancellati in modo permanente,
- mantenere costantemente la sicurezza e l'integrità della memorizzazione e dell'accesso ai dati,
- segnalare qualsiasi violazione della sicurezza dei dati (che possa compromettere la privacy dell'utente) alle autorità competenti entro 72 ore dal verificarsi della violazione.

7. COMUNICAZIONI SICURE

Un'infrastruttura a chiave pubblica (PKI) supporta la distribuzione e l'identificazione delle chiavi di crittografia pubbliche utilizzate per proteggere lo scambio di dati nelle reti, come su Internet. Una PKI verifica l'identità dell'interlocutore e codifica l'effettiva trasmissione dati. La verifica dell'identità fornisce la sicurezza con "non ripudio" dell'identità del server. La crittografia garantisce riservatezza durante la trasmissione nella rete. Il requisito dei moduli con codice firmato assicura che solo il codice previsto venga eseguito nel sistema.

Per predisporre reti sicure con PKI, Niagara supporta il protocollo TLS (Transport Layer Security), versioni 1.0, 1.1 e 1.2. TLS sostituisce il predecessore, il protocollo SSL (Secure Sockets Layer).

Ogni installazione Niagara crea automaticamente un certificato predefinito, che permette la crittografia immediata della connessione. Tuttavia, questi certificati generano avvisi nel browser e nel workbench e solitamente non sono adatti per gli utenti finali. La creazione e la firma di certificati digitali personalizzati consentono un utilizzo ottimale di TLS nel browser e supportano sia la crittografia che l'autenticazione del server.

Oltre alla sicurezza delle comunicazioni, ogni modulo di codice informatico eseguito nel sistema è protetto con una firma digitale. Anche gli oggetti di programma aggiunti richiedono la firma o non vengono eseguiti.

Tuttavia per proteggere i dati memorizzati su un dispositivo di archiviazione non è sufficiente verificare il server, crittografare la trasmissione e garantire che venga eseguito solo il codice firmato. È necessario limitare anche l'accesso fisico ai computer e ai controller che gestiscono il modello di edificio, configurare l'autenticazione degli utenti ricorrendo a password complesse e proteggere i componenti controllando le autorizzazioni.

Niagara supporta e utilizza comunicazioni sicure e codice firmato per impostazione predefinita. Non occorre acquistare licenze aggiuntive.

La sicurezza rappresenta una preoccupazione costante nel tempo. Benché gli argomenti sulle comunicazioni sicure offrano numerose informazioni preziose, sono previste modifiche e aggiornamenti in futuro.

Le comunicazioni sicure vengono illustrate di seguito. Per informazioni dettagliate fare riferimento alla Guida sulla sicurezza della stazione Niagara.

- Relazioni client/server
- Certificati
- Archivi di certificati
- Struttura delle cartelle CSR
- Impostazione di certificati
- "Certificate Wizard" (Procedura guidata certificati)
- Firma di certificati multipli
- Configurazione di comunicazioni sicure con la piattaforma
- Configurazione di comunicazioni sicure con la stazione
- Abilitazione di client e configurazione della porta corretta
- Installazione di una copia della stazione in un'altra piattaforma
- Protezione delle e-mail
- Risoluzione dei problemi per comunicazioni sicure

7. 1 Relazioni client/server

Le relazioni client/server identificano le connessioni che richiedono protezione. Le relazioni client/server del workbench variano a seconda di come si configura e si utilizza un sistema. Il workbench funge sempre da client. Una piattaforma funge sempre da server. Una stazione può fungere da client e da server.

I protocolli di sistema che gestiscono le comunicazioni sono:

- Le connessioni della piattaforma dal workbench (client) al controller o al daemon della piattaforma PC Saia PCD Supervisor (server) utilizzano Niagarad. Una connessione della piattaforma sicura è denominata anche platformtls. Una platformtls si abilita tramite la vista "Platform Administration" (Amministrazione piattaforma).
- Le connessioni della stazione locale (Saia PCD Supervisor e piattaforma) utilizzano Foxs. Queste connessioni si abilitano nel FoxService di una stazione ["Config" > "Services" (Servizi) > "FoxService"].
- Le connessioni del browser si basano su Https, nonché Foxs se si utilizza Web Launcher con un WbWebProfile. Queste connessioni si abilitano utilizzando il WebService della stazione ["Config" > "Services" (Servizi) > "WebService"].
- Connessioni del client al server e-mail della stazione, se applicabile. La protezione delle e-mail si abilita utilizzando l'EmailService della stazione ["Config" > "Services" (Servizi) > "EmailService"].

8. CERTIFICATI

Un certificato è un documento elettronico che utilizza una firma digitale per associare una chiave pubblica a una persona o un'organizzazione. I certificati possono essere utili per una varietà di scopi, a seconda di come se ne configura la proprietà "Key Usage" (Utilizzo della chiave). Il loro fine principale in questo sistema è verificare l'identità di un server, in modo da stabilire comunicazioni attendibili. Per informazioni dettagliate, fare riferimento alla Guida sulla sicurezza della stazione Niagara - Certificato.

Niagara supporta questi tipi di certificati.

- Un certificato emesso da un'autorità di certificazione (**CA** , Certificate Authority) è un documento autofirmato che appartiene a una CA. Questa può essere una terza parte o un'azienda che funge da propria CA.
- Un **certificato CA radice** è un certificato CA firmato la cui chiave privata viene utilizzata per firmare altri certificati, creando un albero di certificati attendibile. Con la sua chiave privata, un certificato CA radice può essere esportato, memorizzato in un archivio su una chiavetta USB e recuperato solo quando è necessario firmare certificati. La chiave privata di un certificato CA radice richiede di creare una password per l'esportazione e di fornire tale password quando viene utilizzata per firmare altri certificati.
- Un **certificato intermedio** è un certificato CA firmato da un certificato CA radice utilizzato per firmare certificati del server o altri certificati CA intermedi. L'uso di certificati intermedi determina l'isolamento di un gruppo di certificati del server.
- Un **certificato del server** rappresenta il lato server di una connessione sicura. Benché sia possibile impostare un certificato separato per ciascun protocollo (Foxs, Https, Webs) e configurare una piattaforma e una stazione (come server) con certificati del server separati, per semplicità la maggior parte dei sistemi utilizza lo stesso certificato del server.
- Un **certificato di firma del codice** viene utilizzato per firmare oggetti e moduli di programma. Gli integratori di sistemi ricorrono a questo certificato per impedire l'introduzione di codice nocivo quando personalizzano il framework.

8. 1 Certificati autofirmati

Un certificato autofirmato viene firmato per impostazione predefinita utilizzando la propria chiave privata, anziché quella di un certificato CA (autorità di certificazione) radice.

Il sistema supporta due tipi di certificati autofirmati:

- Un **certificato CA radice** è implicitamente attendibile, poiché non esiste alcuna autorità superiore all'autorità di certificazione (CA) che possiede tale certificato. Per questo motivo le CA, il cui compito è approvare i certificati di altre persone, proteggono con cura i propri certificati CA e le proprie chiavi private. Analogamente, se l'azienda funge da CA, è essenziale proteggere con cura il certificato CA radice utilizzato per firmare altri certificati.
- Un **certificato autofirmato predefinito**: La prima volta che si avvia un'istanza del workbench, di una piattaforma o di una stazione dopo l'installazione (messa in servizio), il sistema crea un certificato del server autofirmato predefinito con l'alias di tridium.

NOTE:

È importante non esportare tale certificato e importarlo in un archivio qualsiasi di un'altra piattaforma o stazione. Benché ciò sia possibile, farlo ridurrebbe la sicurezza e aumenterebbe la vulnerabilità.

Per ridurre al minimo il rischio di un attacco man-in-the-middle quando si utilizzano certificati autofirmati, tutte le piattaforme devono essere contenute in una rete privata sicura, offline e senza accesso pubblico da Internet.

⚠ CAUTION

Per utilizzare certificati autofirmati, prima di accedere per la prima volta alla piattaforma o alla stazione dal workbench, assicurarsi che il computer e la piattaforma in uso non si trovino in una rete aziendale o su Internet. Dopo la disconnessione, collegare il computer direttamente alla piattaforma, aprire quest'ultima dal workbench e approvarne il certificato autofirmato. Solo a questo punto si dovrebbe connettere nuovamente la piattaforma a una rete aziendale.

8. 2 Convenzione di denominazione

Gli archivi **User Key Store** (Archivio delle chiavi utente), **User Trust Store** (Archivio attendibilità dell'utente) e **System Trust Store** (Archivio attendibilità del sistema) formano il nucleo della configurazione. I certificati si somigliano molto e i vari certificati autofirmati predefiniti condividono gli stessi nomi.

8. 3 Archivi di certificati

Le gestione dei certificati si basa su quattro archivi: **User Key Store** (Archivio delle chiavi utente), **System Trust Store** (Archivio attendibilità del sistema), **User Trust Store** (Archivio attendibilità dell'utente) e l'elenco **Allowed Hosts** (Host consentiti).

Lo **User Key Store** (Archivio attendibilità dell'utente) è associato al lato server della relazione client-server. Questo archivio conserva certificati, ciascuno con le proprie chiavi, privata e pubblica. Inoltre questo archivio contiene il certificato autofirmato creato inizialmente quando è stato avviato il workbench o è stata eseguita la piattaforma per la prima volta.

Gli archivi **User Trust Store** (Archivio attendibilità dell'utente) e **System Trust Store** (Archivio attendibilità del sistema) sono associati al lato client della relazione client-server. Il "System Trust Store" (Archivio attendibilità del sistema) viene fornito già popolato con i certificati pubblici standard: certificati CA radice emessi da note autorità di certificazione quali VeriSign, Thawte e Digicert. Lo **User Trust Store** (Archivio attendibilità dell'utente) comprende i certificati CA radice e intermedi per le aziende che fungono da proprie autorità di certificazione.

L'elenco **Allowed Hosts** (Host consentiti) contiene i certificati del server che sono stati ugualmente approvati per l'uso, anche se per loro non esistono certificati CA radice attendibili nel **System Trust Store** (Archivio attendibilità del sistema) o nello **User Trust Store** (Archivio attendibilità dell'utente). Ciò include i server il cui nome host non è identico al nome comune nel certificato del server. L'utente approva l'uso di questi certificati caso per caso. Anche se le comunicazioni sono sicure, è preferibile utilizzare certificati del server firmati.

8. 4 Crittografia

La crittografia è il processo di codifica della trasmissione dati in modo che le informazioni non siano leggibili da terze parti inaffidabili. TLS utilizza la crittografia per trasmettere dati fra client e server. Benché sia possibile stabilire una connessione non crittografata utilizzando solo i protocolli Fox o Http, si consiglia fortemente di non scegliere tale opzione. Senza la crittografia, le comunicazioni sono potenzialmente vulnerabili agli attacchi. Accettare sempre le connessioni Foxs o Https predefinite.

9. PANORAMICA DELLA DASHBOARD DI SICUREZZA

In Niagara 4.u5 e versioni successive, la funzione "Security Dashboard" (Dashboard di sicurezza) fornisce (per l'amministratore e altri utenti autorizzati) una vista dall'alto della configurazione di sicurezza della stazione. Ciò consente di monitorare agevolmente la configurazione di sicurezza in molti servizi della stazione e identificare le eventuali vulnerabilità.

⚠ CAUTION

La vista "Security Dashboard" (Dashboard di sicurezza) potrebbe non visualizzare ogni possibile impostazione di sicurezza e non deve essere considerata una garanzia di una configurazione totalmente sicura. In particolare, i moduli di terze parti possono avere impostazioni di sicurezza non rilevabili dalla dashboard.

La vista "Security Dashboard" (Dashboard di sicurezza) è la vista principale nel "SecurityService" (Servizio di sicurezza) della stazione. La vista segnala punti deboli della sicurezza quali impostazioni inadeguate della complessità della password, certificati scaduti, autofirmati o non validi, protocolli di trasporto non crittografati, ecc., indicando così le aree dove la configurazione dovrebbe essere più sicura. Altri dati riferiti sono: stato di salute del sistema, numero di account attivi, account inattivi, numero di account con autorizzazioni da super-utente, ecc. Se desiderato, l'attributo "system" (sistema) nella funzionalità della licenza "securityDashboard" (Dashboard di sicurezza) può essere impostato su "true" (vero) per abilitare la vista di sistema della stazione che fornisce dettagli relativi alla sicurezza di ciascuna stazione subordinata nella rete Niagara.

"Security Dashboard" (Dashboard di sicurezza) è la vista principale per i servizi di sicurezza. Per informazioni dettagliate sulla vista, fare riferimento a "nss-SecurityDashboardView" nella Guida sulla sicurezza della stazione Niagara.

10. PIANIFICAZIONE E INSTALLAZIONE

Questa sezione comprende informazioni utili per pianificare ed eseguire l'installazione di un Advanced Plant Controller.

10. 1 Installazione e configurazione consigliate

La sezione sottostante illustra due configurazioni di installazione consigliate.

- Solo BACnet
- BACnet e Niagara

10. 1. 1 Solo BACnet

Quando l'Advanced Plant Controller viene utilizzato unicamente per le comunicazioni BACnet, connettere solo Ethernet 1 alla rete BAS dove sarà in esecuzione BACnet (BACnet/IP o BACnet/Ethernet)

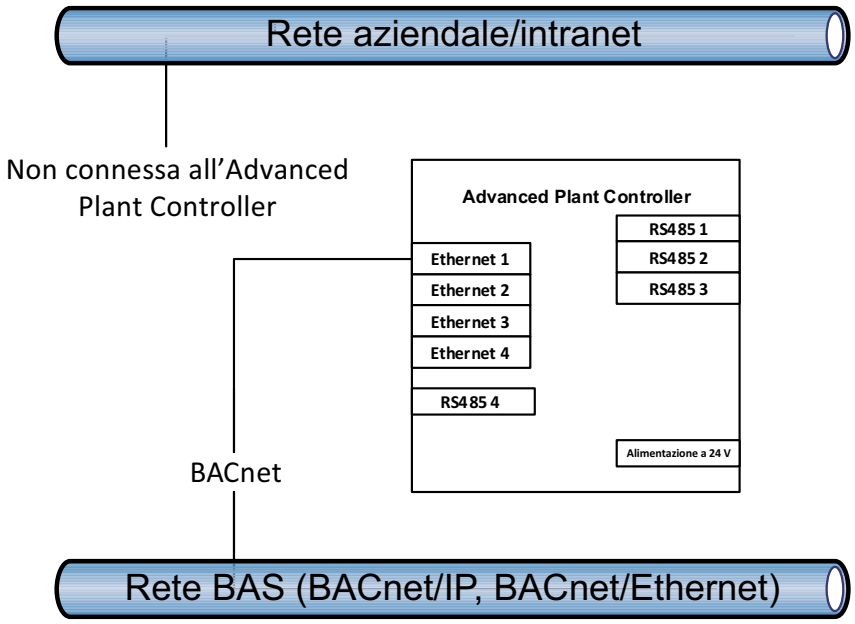

Fig. 2 Connessione BACnet

10. 1. 2 BACnet e Niagara

Quando Niagara viene utilizzato nell'Advanced Plant Controller,può essere configurato per fornire servizi, come ad esempio servizi Web o Niagara FOXS, alla rete aziendale / Internet / intranet. In tal caso, connettere Ethernet 2 alla rete aziendale / Internet / intranet tramite il firewall BAS per fornire servizi a tale rete.

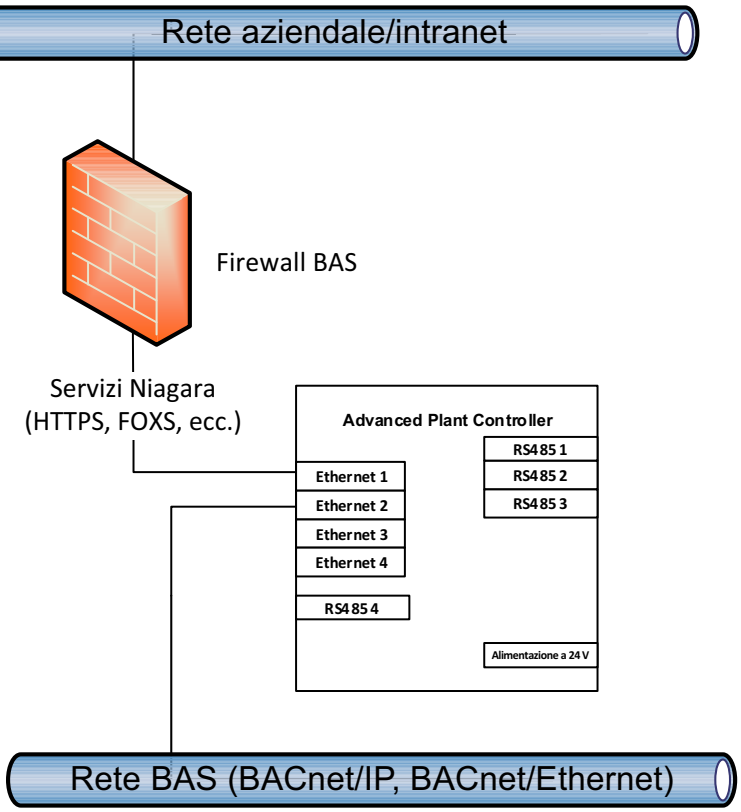

Fig. 3 Connessioni BACnet e Niagara

10. 2 Consiglio sulle reti locali (Local Area Network, LAN)

Accertarsi che il sistema utilizzi criteri password appropriati per l'accesso degli utenti a tutti i servizi. Questa linea guida comprende, senza limitazione:

1. L'utilizzo di password complesse.
2. Una durata ciclo consigliata per le password.
3. Nomi utente e password univoci per ogni utente del sistema.
4. Regole sulla divulgazione delle password.
5. Se è necessario l'accesso remoto ai sistemi di controllo edifici informatizzati, utilizzare la tecnologia VPN (Virtual Private Network) per ridurre il rischio dell'intercettazione dei dati e per proteggere i dispositivi di controllo dal posizionamento diretto in Internet.

11. DOCUMENTAZIONE

La documentazione è essenziale per acquisire le informazioni di progettazione e configurazione necessarie per mantenere un sistema sicuro.

11. 1 Documentare dispositivi fisici e configurazioni, compresi i dati chiave correlati alla sicurezza

Tutta la documentazione sui dispositivi e le configurazioni deve includere informazioni correlate alla sicurezza al fine di stabilire e mantenere i controlli di sicurezza appropriati. Ad esempio, se si modificano i servizi o le porte predefiniti nell'Advanced Plant Controller, è opportuno documentare chiaramente tali cambiamenti, in modo che sia possibile ripristinare le impostazioni in un secondo tempo.

11. 2 Documentare sistemi esterni, in particolare l'interazione fra l'Advanced Plant Controller e i sistemi correlati

BAS normalmente richiede o utilizza sistemi esterni per funzionalità quali l'infrastruttura di rete esistente, l'accesso VPN, gli host delle macchine virtuali e i firewall. Se BAS impone di configurare questi sistemi in un certo modo a scopo di sicurezza, come nel caso di un firewall che consente o rifiuta determinate porte o una rete che permette di accedere a sistemi specifici, è essenziale documentare tali informazioni. Se, a un certo momento, fosse necessario ripristinare questi sistemi, **ad esempio** a causa di un guasto delle apparecchiature o di modifiche da apportare a sistemi esterni, come **ad esempio** per potenziare un firewall, il fatto di aver documentato queste informazioni aiuterà a recuperare il livello di sicurezza precedente.

12. CONTROLLO DELL'ACCESSO E SICUREZZA FISICA

Il controllo dell'accesso consiste nel permettere e limitare l'accesso a dispositivi o funzioni esclusivamente a utenti autorizzati.

12. 1 Proteggere fisicamente l'Advanced Plant Controller, HMI e il modulo I/O

È necessario prevenire l'accesso non autorizzato alle apparecchiature di rete utilizzate insieme ai sistemi forniti da Honeywell. In qualsiasi sistema prevenire l'accesso fisico alla rete e alle apparecchiature riduce il rischio di interferenza da parte di utenti non autorizzati. Le best practice per la protezione delle installazioni informatiche prevedono che i server, i pannelli di interconnessione e le apparecchiature IT siano protetti in ambienti dotati di serrature. L'apparecchiatura Honeywell deve essere installata all'interno di armadi con serratura, posizionati a loro volta nei locali protetti di un impianto.

12. 2 Adesivi sul pannello di accesso o l'alloggiamento del controller

Applicare un adesivo a prova di manomissione sul pannello di accesso o l'alloggiamento dell'Advanced Plant Controller, di HMI o del modulo I/O.

Se un cliente richiede ulteriori garanzie che nessuno interferisca con l'accesso fisico di protezione di un Advanced Plant Controller, una HMI e un modulo I/O, installare un sigillo o un adesivo a prova di manomissione sul punto di accesso.

12. 3 Segregare e proteggere le reti

1. Utilizzare un firewall fra la rete aziendale / Internet / intranet e BAS.
2. Predisporre una rete fisica dedicata separata (cavi separati) o una rete virtuale (VLAN) per le comunicazioni BACnet. Tale rete deve essere separata dalla rete aziendale / Internet / intranet.
3. Non connettere EN2 sull'Advanced Plant Controller ad alcuna rete, a meno che non siano necessari i servizi Niagara (piattaforma, stazione e/o Webserver). Se occorre connettere EN2 alla rete aziendale / Internet / intranet, è necessario utilizzare un firewall BAS esterno fra l'Advanced Plant Controller e la rete aziendale / Internet / intranet.

13. PROTEZIONE DI ADVANCED CONTROLLER, HMI E MODULO I/O

13. 1 Credenziali dell'account di sistema amministratore fornite all'utente del sito

Le credenziali dell'account di sistema amministratore devono essere fornite al proprietario del sito, per consentirgli di gestire gli account di sistema.

13. 2 Sviluppo di un programma di protezione

Fare riferimento a "Best practice di sicurezza generali"

13. 3 Considerazioni di carattere fisico e ambientale

L'Advanced Controller, HMI e il modulo I/O devono essere installati all'interno di un ambiente sicuro, ad esempio nel locale protetto di un impianto o in un armadio dotato di serratura.

NOTE:
Garantire una ventilazione adeguata.

13. 4 Aggiornamenti e service pack di sicurezza

Accertarsi che l'Advanced Controller, HMI e il modulo I/O eseguano la versione del firmware più recente.

14. UTENTI E PASSWORD

14. 1 Utenti

Assicurarsi che il numero di utenti e livelli di accesso fornito sia appropriato per le attività da eseguire.

- **A livello dei controller configurare utenti o account di sistema per l'accesso peer-to-peer o come client Web o Saia PCD Supervisor.**

  Nella configurazione di moduli utente negli Advanced controller, ciò significa che un utente dovrà accedere a un dispositivo utilizzando credenziali valide prima di poter effettuare regolazioni. Assicurarsi di assegnare diritti di accesso appropriati agli utenti e agli account di sistema.

- **Utilizzare un account diverso per ogni utente**

  Scegliere nomi utente e password univoci per ogni utente / account nel sistema, anziché assegnare accessi generici. Persone diverse non dovrebbero mai condividere lo stesso account. Ad esempio, invece di un account generale dedicato ai manager e utilizzabile da molti responsabili indifferentemente, ogni manager dovrebbe avere un proprio account separato.

Vi sono svariati motivi per cui a ogni utente dovrebbe essere assegnato un account individuale:

- Se ogni persona ha un proprio account, i registri di verifica saranno più accurati. Sarà facile stabilire esattamente quale utente ha eseguito una determinata operazione. E questo può contribuire a indicare se un account è stato compromesso.

NOTE:
Non tutti i prodotti includono una funzionalità di registrazione delle verifiche, ma quando è disponibile non andrebbe disabilitata.

- La rimozione o la modifica di un account non disturba molte persone. Ad esempio, se una persona non dovrebbe più accedere, eliminare il suo accesso singolo è semplice. Se si tratta di un account condiviso, le uniche opzioni sono modificare la password e avvertire tutti o eliminare l'account e avvertire tutti. Lasciare l'account invariato non è un'opzione - l'obiettivo è revocare l'accesso.
- Se ogni persona ha un proprio account, è molto più facile impostare autorizzazioni su misura per soddisfare esattamente le sue esigenze. Un account condiviso potrebbe fornire a un gruppo di persone un numero di autorizzazioni superiore al dovuto.

- In un account condiviso, le persone condividono la stessa password. Condividere le password è una pratica di sicurezza estremamente pericolosa. Aumenta notevolmente la probabilità che la password trapeli e diventa molto più difficile implementare determinate best practice per le password, come ad esempio la definizione di una scadenza.

- **Ricorso a utenti di ingegnerizzazione unici per i progetti**

  È abbastanza comune per le aziende utilizzare gli stessi dettagli dell'account per ogni progetto. Ciò è molto pericoloso perché è sufficiente che un malintenzionato comprometta un singolo sistema per venirlo a sapere e sfruttare tali credenziali per accedere a numerosi altri progetti installati dalla stessa azienda.

- **Disattivare gli account noti quando possibile**

  Alcuni prodotti hanno account predefiniti. Questi prodotti vanno configurati in modo che la password non sia più quella predefinita.

- **Assegnare le minime autorizzazioni necessarie per gli utenti**

  Accertarsi che solo gli account richiesti siano configurati nel sistema e dotati dei livelli di sicurezza minimi indispensabili, invece dell'accesso completo. Al momento di creare un nuovo account, è importante riflettere su ciò che la persona deve svolgere nel sistema, quindi assegnare le autorizzazioni minime necessarie per tali operazioni. Ad esempio, a qualcuno che ha bisogno soltanto di vedere gli allarmi non serve l'accesso da amministratore. Fornire autorizzazioni non necessarie aumenta la possibilità di una violazione della sicurezza. L'utente potrebbe involontariamente (o intenzionalmente) modificare impostazioni che dovrebbero rimanere invariate.

- **Utilizzare il numero minimo possibile di account da amministratori del sistema**

  Assegnare autorizzazioni da amministratore solo quando è indispensabile. L'account da amministratore del sistema è estremamente potente - offre accesso completo a tutto. Solo l'effettivo amministratore del sistema dovrebbe disporre di questo account. Un'altra opzione è fornire all'amministratore del sistema due account: uno per l'accesso di routine, utile nella gestione delle attività quotidiane, e il secondo per un accesso superiore, richiesto solo quando occorre apportare modifiche amministrative.

14. 2 Password

Nel sistema Trend e nei sistemi operativi che utilizzavano prodotti Advanced Honeywell le password consentono di autenticare utenti per l'accesso a Saia PCD Supervisor, display, strumenti e sistemi operativi. Una gestione corretta delle password è fondamentale. Se questo livello di sicurezza iniziale viene trascurato, chiunque acceda al sistema tramite un display, un client Web o un Saia PCD Supervisor può apportare modifiche. Accertarsi che nel sistema Niagara l'accesso degli utenti sia conforme a criteri password appropriati come quelli elencati di seguito, a titolo esemplificativo.

- **L'utilizzo di password complesse** - si consiglia di ricorrere a password complesse. Per le caratteristiche di una password complessa, fare riferimento ai più recenti standard di sicurezza.
- **Una durata ciclo consigliata per le password** - alcuni prodotti Niagara consentono all'amministratore del sistema di specificare un periodo trascorso il quale è necessario modificare la password. Benché attualmente non tutti i prodotti applichino questo periodo di scadenza della password, un criterio configurato nel sito potrebbe consigliarlo.
- **Regole sulla divulgazione della password** - L'utente DEVE accertarsi di non condividere con altri i dettagli relativi al proprio nome utente e password, né di trascriverli.

15. CONFIGURAZIONE DI UN ADVANCED PLANT CONTROLLER

Per informazioni sulla configurazione di un Advanced Plant Controller, fare riferimento alla Guida di istruzioni per l'installazione e la messa in servizio (31-00584). Fare riferimento alla Guida al driver di HMI (31-00590) per HMI e alla Guida al driver di Panel Bus (31-00591) per il modulo I/O.

15. 1 Creare ed eseguire la manutenzione di configurazioni di base

Creare ed eseguire la manutenzione di una base di configurazioni dell'Advanced Plant Controller che siano state configurate in modo appropriato per la sicurezza. Accertarsi che la base includa anche i file DCF e i componenti Niagara. Non associare alla base, con il commit, configurazioni non sicure, onde evitare di applicarle involontariamente in futuro. Aggiornare la documentazione pertinente quando si modificano le configurazioni.

15. 2 Modificare le password predefinite

Modificare tutte le password predefinite: la password di configurazione della console, la password di backup / ripristino / riavvio / controllo e la password della piattaforma Niagara. Al termine della messa a in servizio, accertarsi che il dispositivo sia protetto tramite password. Accertarsi che agli utenti del sito siano assegnati livelli utente appropriati.

15. 3 Ulteriori considerazioni

15. 3. 1 Contratto sul livello di servizio

Adottare criteri di aggiornamento appropriati per l'infrastruttura installata nel sito nell'ambito di un contratto sul livello di servizio. I criteri devono includere, senza limitazione, l'aggiornamento dei seguenti componenti di sistema all'ultima versione:

- Firmware del dispositivo per controller, moduli I/O, ecc.;
- Software Saia PCD Supervisor, ad esempio Arena NX;
- Sistemi operativi di computer / server;
- Infrastruttura di rete ed eventuali sistemi di accesso remoto.

15. 3. 2 Configurazione della rete IT

Configurare reti IT separate per i sistemi di controllo automazione e per la rete informatica aziendale del cliente. Ciò è possibile configurando reti VLAN (LAN virtuali) all'interno dell'infrastruttura IT del cliente o installando un'infrastruttura di rete separata da intercapedini e dedicata ai sistemi di controllo automazione.

Se ci si interfaccia con i controller mediante un Saia PCD Supervisor di sistema centralizzato (ad esempio Niagara) e il sistema non richiede l'accesso diretto al server Web di singoli dispositivi, l'infrastruttura di rete deve essere configurata in modo da limitare l'accesso al server Web.

Assegnando gli indirizzi MAC è possibile proteggere le reti VLAN dinamiche dal collegamento non autorizzato di un dispositivo al sistema e ridurre il rischio associato a una singola informazione di monitoraggio sulla rete.

16. CONFIGURAZIONE DEL FIREWALL BAS

La tabella seguente descrive le porte di rete utilizzate in un Advanced Plant Controller. Vedere *"Panoramica del sistema" a pag. 6.* per un esempio di architettura di installazione. La tabella presenta le seguenti colonne:

- Porta predefinita e protocollo (TCP o UDP)
- Scopo della porta
- Se sia necessario o meno modificare la porta predefinita
- Se si dovrebbero consentire o meno le connessioni o il traffico in ingresso tramite il firewall BAS
- Sotto la tabella sono elencate note aggiuntive

Tabella 2 Configurazione del firewall BAS

Porta predefinita / protocollo	Scopo	Modif. imp. predef.?	Consentire attraverso il firewall BAS?	Note
80/TCP	HTTP	No	No	
443/TCP	HTTPs	No	Eventualmente, se è necessario l'accesso Web dalla rete aziendale / Internet / intranet	1
1911/TCP	Fox (versione non sicura del protocollo di applicazione Niagara)	Sì	No	
4911/TCP	Fox + SSL (versione sicura del protocollo di applicazione Niagara)	Sì	No	
3011/TCP	NiagaraD (versione non sicura del protocollo di piattaforma Niagara)	Sì	No	
5011/TCP	NiagaraD + SSL (versione sicura del protocollo di piattaforma Niagara)	Sì	No	
2601/TCP	Porta console Zebra	No	No	2
2602/TCP	Porta console RIP			2
47808/UDP	Connessione di rete BACnet/IP	Sì	No	3

NOTE:

1. Se è supportata l'interfaccia utente Web remota diretta, consentire questa porta attraverso il firewall BAS.
2. La porta viene aperta automaticamente da questo daemon e la funzionalità non può essere disabilitata. Il daemon è configurato in modo da non consentire l'accesso tramite questa porta.
3. Attenersi alle linee guida di configurazione della rete riportate in questo manuale, in modo che l'Advanced Plant Controller non debba mai trasmettere il traffico UDP attraverso il firewall BAS.

17. IMPOSTAZIONE DELL'AUTENTICAZIONE

Lo schema di autenticazione Google è un meccanismo di autenticazione a due fattori che richiede all'utente di inserire la propria password, oltre a un token monouso, per accedere a una stazione. Ciò protegge l'account di un utente anche se la sua password è compromessa.

Questo schema di autenticazione si affida a una password una-tantum temporanea (Time-based OneTime Password, TOTP) e all'app Google Authenticator sul dispositivo mobile dell'utente per generare e verificare token di autenticazione monouso. L'autenticazione di Google è temporanea, pertanto non c'è dipendenza dalle comunicazioni di rete fra il dispositivo mobile dell'utente, la stazione o i server esterni. Poiché il codice di autenticazione è temporaneo, l'orario nella stazione e quello nel telefono devono essere relativamente sincronizzati fra loro. L'app fornisce un buffer di circa 1,5 minuti per tenere conto dello sfasamento degli orari.

Requisiti preliminari: il telefono cellulare dell'utente richiede l'app Google Authentication. La procedura viene eseguita nel workbench. L'utente è incluso nel database della stazione.

17. 1 Procedura

1. Aprire il pannello "gauth" e aggiungere **GoogleAuthenticationScheme** a **Services** (Servizi) > nodo **Authenticationservice** nell'albero di navigazione.
2. Fare clic con il pulsante destro del mouse su **Userservice**, quindi fare doppio clic sull'utente nella tabella. Si apre la vista "Edit" (Modifica) per l'utente.
3. Configurare la proprietà "Authentication Scheme Name" (Nome schema di autenticazione) su **GoogleAuthenticationScheme** e fare clic su **Save** (Salva).
4. Fare clic sul pulsante accanto alla chiave segreta sotto il codice di autenticazione dell'utente e attenersi ai messaggi visualizzati.
5. Per completare la configurazione, fare clic su **Save** (Salva). In base alla vista che si sta utilizzando, può essere necessario aprire di nuovo la vista dell'utente o aggiornare dopo il salvataggio.

18. CONSEGNA DEL SISTEMA

Questa sezione contiene informazioni che occorre fornire alla consegna di BAS al proprietario del sistema.

- Documentazione che comprende informazioni relative alla sicurezza, impostazioni di configurazione, nomi utente e password di amministrazione, piani di ripristino di emergenza e procedure di backup e ripristino.
- Formazione degli utenti finali su attività di manutenzione correlate alla sicurezza.

19. BACKUP VIA USB E INSTALLAZIONE DI FILE CLEANDIST

Informazioni relative al backup via USB e all'installazione dei file CleanDist sono disponibili nella Guida di istruzioni per l'installazione e la messa in servizio - 31-00584.

20. DISMISSIONE DEL SISTEMA

I dati sensibili devono essere cancellati dalle unità che vengono ritirate dal servizio. A tale scopo si può eseguire il ripristino delle impostazioni di fabbrica. Fare riferimento a LED del pulsante / allarme Manutenzione e Installazione dei file CleanDist nella Guida di istruzioni per l'installazione e la messa in servizio - 31-00584.

NOTE:

La procedura dei file CleanDist può eseguire il ripristino delle impostazioni di fabbrica installando il file clean4.

21. SICUREZZA DEI PRODOTTI ADVANCED BASATI SU NIAGARA

Per i prodotti Honeywell Advanced basati sui framework Niagara N4 e Niagara AX (ad es. Advanced Plant Controller, HMI e modulo I/O), occorre attenersi al consiglio di Tridium sulla protezione del framework Niagara.

È possibile apportare a Niagara una serie di modifiche di configurazione, allo scopo di massimizzare la sicurezza dei prodotti Honeywell Advanced.

- Utilizzare la funzione “Password Strength” (Complessità della password)
- Abilitare la funzione “Account Lockout” (Blocco dell’account)
- Impostare una scadenza per le password
- Utilizzare “Password History” (Cronologia della password)
- Utilizzare la funzione “Password Reset” (Reimpostazione della password)
- Lasciare deselezionata la casella “Remember These Credentials” (Ricorda queste credenziali)
- Modificare la passphrase predefinita del sistema
- Utilizzare TLS per impostare la passphrase del sistema
- Scegliere una passphrase del sistema complessa
- Proteggere la passphrase del sistema
- Accertarsi che il proprietario della piattaforma conosca la passphrase del sistema
- Utilizzare un account diverso per ogni utente della piattaforma
- Utilizzare nomi account univoci per ogni progetto
- Accertarsi che il proprietario della piattaforma conosca le credenziali della piattaforma
- Utilizzare un account diverso per ogni utente della stazione
- Utilizzare account di servizio univoci per ogni progetto
- Disattivare gli account noti quando possibile
- Impostare una scadenza automatica per gli account temporanei
- Modificare le credenziali degli account di sistema
- Impedire le sessioni simultanee quando appropriato
- Configurare ruoli con autorizzazioni minime richieste
- Assegnare i ruoli minimi necessari agli utenti
- Utilizzare il numero minimo possibile di super-utenti
- Richiedere autorizzazioni da super-utente per gli oggetti di programma
- Utilizzare le autorizzazioni minime necessarie per gli account esterni
- Utilizzare uno schema di autenticazione appropriato per il tipo di account
- Rimuovere gli schemi di autorizzazione non necessari
- TLS e gestione di certificati
- Installazione di moduli
- Richiedere oggetti di programma e robot firmati
- Disabilitare SSH e SFTP
- Disabilitare i servizi non necessari
- Configurare in modo sicuro i servizi necessari
- Aggiornare Niagara 4 alla versione più recente
- Installare il prodotto in un’ubicazione sicura
- Accertarsi che le stazioni siano dietro a una VPN

Sono disponibili pubblicazioni tecniche specifiche alle quali è essenziale attenersi per garantire la massima protezione possibile del sistema. Inoltre esistono numerose opzioni, come la crittografia SSL e fasi aggiuntive, concepite per proteggere elementi quali i moduli di programma. Per informazioni dettagliate fare riferimento al sito Web di Tridium, dove sono reperibili la Guida al rafforzamento di Niagara 4 (per i prodotti basati su Niagara 4) e la Guida al rafforzamento di Niagara (per i prodotti basati su Niagara AX).

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

Honeywell Building Technologies

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

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

Honeywell

22. LISTA DI CONTROLLO DELLA SICUREZZA DELL'INSTALLAZIONE

Istanza del dispositivo Advanced Plant Controller: _____

Descrizione dell'Advanced Plant Controller: _____

Ubicazione dell'Advanced Plant Controller: _____

Installatore:_____ Data: _____

Completare le seguenti attività correlate alla sicurezza per ogni Advanced Plant Controller installato

- ☐ Installare un firewall fra l'Advanced Plant Controller e le reti esterne. Vedere *"BACnet e Niagara" a pag. 18.*
- ☐ Proteggere fisicamente l'Advanced Plant Controller. Vedere *"Proteggere fisicamente l'Advanced Plant Controller, HMI e il modulo I/O" a pag. 20.*
- ☐ Sostituire la password predefinita con una password univoca per ciascuno di questi componenti: configurazione della console, backup / ripristino / riavvio / controllo e la piattaforma Niagara. Vedere la Guida di istruzioni per l'installazione e la messa in servizio - 31-00584
- ☐ Se è necessario un server Web, configurarlo in modo che funzioni solamente tramite HTTPS. Vedere la Guida di istruzioni per l'installazione e la messa in servizio - 31-00584

Stato del server Web: disabilitato / abilitato.

Se il servizio Web è abilitato, completare quanto segue:

- ☐ Impostare "Http Enabled" (Http abilitato) = "false" (falso).
- ☐ Impostare "Https Enabled" (Https abilitato) = "true" (vero).
- ☐ Impostare "Https Only" (Solo Https) = "true" (vero).
- ☐ Configurare il firewall BAS. Vedere *"Configurazione del firewall BAS" a pag. 24.*
- ☐ Fornire tutti i dati richiesti al proprietario del sistema BAS al momento della consegna. Vedere *"Impostazione dell'autenticazione" a pag. 25.*