Honeywell

Advanced

GUÍA DE SEGURIDAD

Exención de responsabilidad

Si bien hemos hecho todo lo posible para garantizar la exactitud de este documento, Honeywell no se hace responsable de ningún tipo de daño, incluidos, a título meramente enunciativo, daños consecuentes que puedan derivarse de la aplicación o el uso de la información aquí contenida. La información y las especificaciones aquí publicadas son actuales en la fecha de esta publicación y están sujetas a cambios sin previo aviso. Podrá encontrar las últimas especificaciones del producto en nuestro sitio web o poniéndose en contacto con nuestra oficina corporativa en Atlanta (Georgia, EE. UU.).

Para muchas comunicaciones industriales basadas en RS-485, el estado predeterminado se desactiva en el momento del envío desde la fábrica para garantizar la mejor seguridad, debido a que los buses de comunicación heredados utilizan tecnología antigua para garantizar la mejor compatibilidad y se diseñaron con protección de seguridad débil. Por lo tanto, para maximizar la protección de su sistema, Honeywell ha desactivado preventivamente los puertos de comunicación de los buses industriales heredados (en el momento del envío desde la fábrica) y el usuario deberá habilitar explícitamente las redes en la estación de cada red. Si desea habilitar estos puertos, debe ser consciente del riesgo de cualquier infracción de seguridad debida al uso de tecnología heredada. Entre ellos se incluyen los siguientes: PanelBus, C-Bus, BACnet, M-Bus, CP-IO Bus, NovarNet, el protocolo XCM-LCD, SBC S-Bus y Modbus, etc.

Desarrollo según ISA-62443

Honeywell lleva muchos años basándose en el estándar ISA 62443-4-1, así como en otros estándares similares aplicables para desarrollar de forma segura nuestros productos de tecnología para edificios. Por ejemplo, los productos para edificios de Honeywell también usan ISA/IEC 62443-4-2 como referencia para los requisitos de seguridad técnica de los componentes y utilizamos ISA/IEC 62443-3-3 para sistemas completos. Por lo tanto, para los integradores y clientes que deseen utilizar tecnologías de edificios, la conformidad de Honeywell con la familia de estándares ISA/IEC 62443 puede proporcionar un alto nivel de confianza en que nuestros productos no solo afirmen ser ciberseguros, sino que lo sean, porque se han diseñado, probado y validado para ofrecer ciberseguridad desde el principio.

En Honeywell desarrollamos nuestros productos de conformidad con ISA/IEC 62443-4-1, y hemos sido evaluados y auditados por terceros al respecto.

Introducción y público destinatario

Por la presente, Honeywell declara expresamente que sus controladores no cuentan con protección inherente contra ciberataques desde Internet y que su uso previsto se restringe a redes privadas. No obstante, las redes privadas también pueden ser objeto de ciberataques lanzados por personas con conocimientos y capacidades de IT, por lo que requieren protección. Por lo tanto, se aconseja a los clientes adoptar directrices de prácticas recomendadas de instalación y seguridad para los productos basados en IP de Advanced Plant Controller con vistas a mitigar el riesgo que plantean este tipo de ataques.

En las siguientes directrices se describen las prácticas recomendadas generales de seguridad para los productos basados en IP de Advanced Plant Controller. Se enumeran en orden de creciente mitigación.

Los requisitos exactos de cada instalación deben evaluarse caso por caso. La inmensa mayoría de las instalaciones que implementen todos los niveles de mitigación que se describen aquí cumplirán con creces los requeridos para la seguridad satisfactoria del sistema. Con la incorporación de los elementos a 1 a 5 (en relación con las redes de área local), Consulte *«Recomendación sobre las redes de área local (LAN)» en la página 18.* responderá en términos generales a los requisitos de la mayor parte de las instalaciones de red de control de automatización.

Este manual contiene información para guiar al personal de un distribuidor de Honeywell sobre cómo instalar y configurar de forma segura un Advanced Plant Controller, un HMI y módulos de E/S. La información relacionada con la seguridad sobre el funcionamiento, la función de copia de seguridad y restauración USB, y la instalación del archivo CleanDist del controlador puede encontrarse en la Guía de instrucciones de instalación y puesta en servicio (31-00584).

NOTA:

Lea detenidamente y comprenda todos los manuales de instalación, configuración y funcionamiento relevantes, y asegúrese de obtener con regularidad las últimas versiones.

.

Tabla 1 Información sobre el producto

Producto	Número de producto	Descripción
Plant Controller	N-ADV-134-H	Niagara Advanced Controller con cuatro puertos Ethernet, un puerto para el HMI y 4 puertos RS485 4
	N-ADV-133-H	Niagara Advanced Controller con cuatro puertos Ethernet, un puerto para el HMI y 3 puertos RS485 3
	N-ADV-112-H	Niagara Advanced Controller con cuatro puertos Ethernet, un puerto para el HMI y 2 puertos RS485 2
HMI	HMI-DN	HMI con montaje sobre carril DIN
	HMI-WL	Montaje en puerta/pared
Módulo de E/S	IO-16UIO-S-S	Módulo de E/S 16UIO sin HOA, comunicaciones de serie y terminales roscados
	IOD-16UIO-S-S	Módulo de E/S 16UIO con pantalla HOA, comunicaciones de serie y terminalesroscados
	IO-16UI-S-S	Módulo de E/S 16UI, comunicaciones de serie y terminales roscados
	IO-16DI-S-S	Módulo de E/S 16DI, comunicaciones de serie y terminales roscados
	IO-8DOR-S-S	Módulo de E/S 8DO sin HOA, relés de C/O, comunicaciones de serie y terminales roscados
	IOD-8DOR-S-S	Módulo de E/S 8DO con pantalla HOA, relés de C/O, comunicaciones de serie y terminales roscados
	IO-16UIO-S-P	Módulo de E/S 16UIO con pantalla HOA, comunicaciones de serie y terminales a presión
	IO-16UI-S-P	Módulo de E/S 16UIO, comunicaciones de serie y terminales a presión
	IO-16DI-S-P	Módulo de E/S 16DI, comunicaciones de serie y terminales a presión
	IO-8DOR-S-P	Módulo de E/S 8DO sin HOA, relés de C/O, comunicaciones de serie y terminales a presión
	IOD-8DOR-S-P	Módulo de E/S 8DO con pantalla HOA, relés de C/O, comunicaciones de serie y terminales a presión

1. ¿POR QUÉ PROTEGER SUS ADVANCED CONTROLLERS?

- Proteja los sistemas de planta de sus clientes contra cambios no autorizados en sus puntos operativos establecidos, anulaciones y programas de tiempo.
- Impida el acceso a los detalles de las cuentas de usuario, p. ej., nombres de usuario, contraseñas, direcciones de correo electrónico, números SMS (móviles), etc.
- Impida el acceso a datos sensibles desde el punto de vista comercial: por ejemplo, métricas de consumo de energía, soluciones de estrategia de control especializadas, etc.
- Impida el acceso no autorizado al controlador, ordenadores y redes que alojen software de BMS y dispositivos de control.
- Mantenga la integridad de los datos y proporcione rendición de cuentas.

2. DESCRIPCIÓN GENERAL DEL SISTEMA

La descripción general de la instalación típica del sistema.

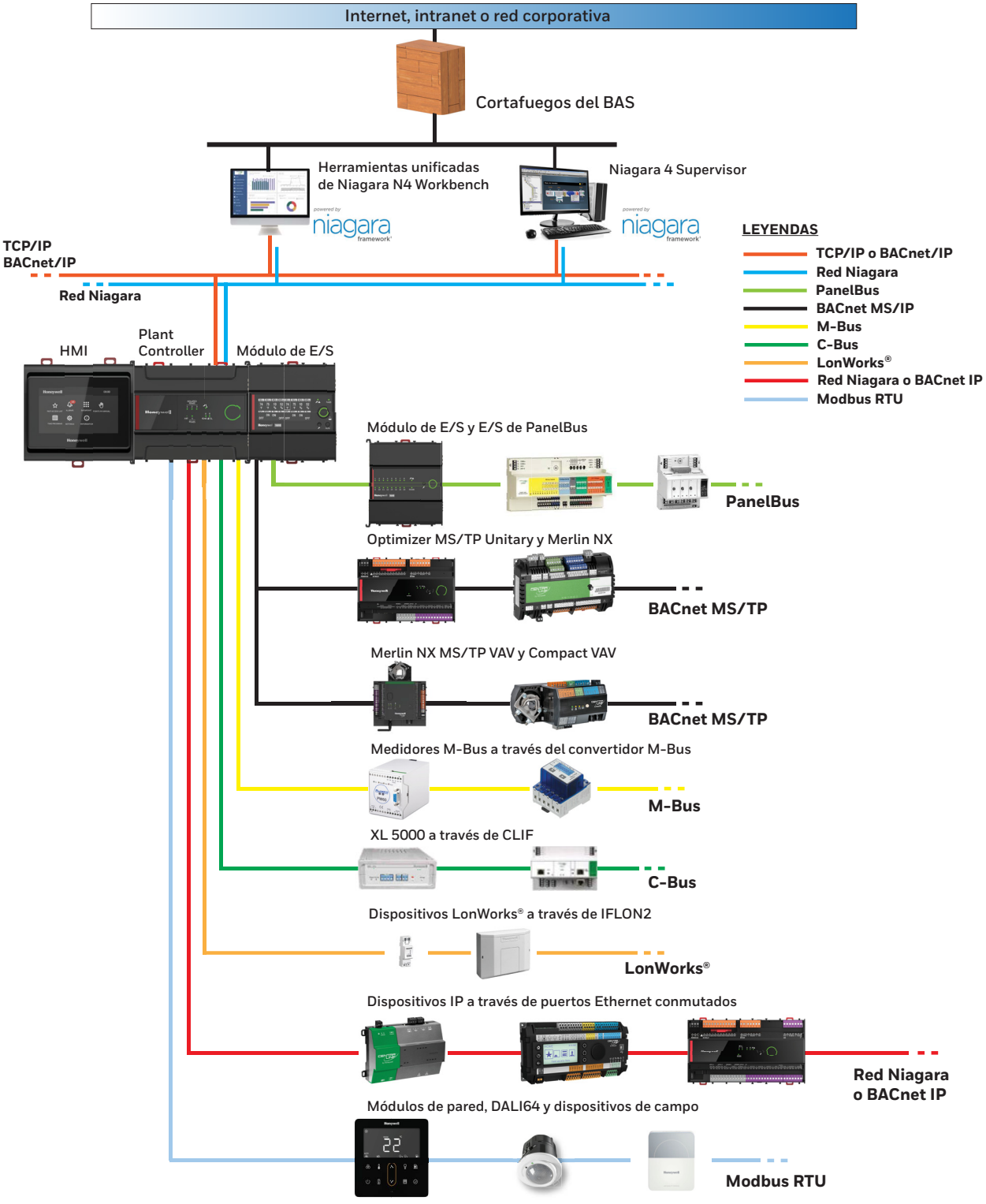

Fig. 1 Descripción general del sistema

2. 1 Internet, intranet o red corporativa

Esta es una representación de red simplificada y lógica de todas las redes fuera del ámbito del sistema de automatización de los edificios (BAS). Puede proporcionar acceso a las interfaces de gestión del BAS (p. ej., la interfaz de usuario web de la estación de trabajo principal de Niagara), pero debe proporcionar acceso a Internet, de forma que los ordenadores Niagara puedan comprobar si existen actualizaciones del sistema operativo y del antivirus, y descargarlas, a menos que se haya facilitado otro medio para hacerlo.

2. 2 Red del BAS

Esta red se utiliza únicamente para protocolos del BAS, que constan de BACnet/IP, BACnet/Ethernet y cualquier protocolo que pueda utilizar los Niagara Integration Services en un Advanced Plant Controller. Esta red no debe ser la misma que Internet, intranet o la red corporativa.

2. 3 Cortafuegos del BAS

Para proporcionar separación y protección adicionales para el BAS, se debe utilizar un cortafuegos entre Internet, la intranet o la red corporativa y cualquier dispositivo del BAS que se conecte, como la estación de trabajo principal de Niagara, estaciones de trabajo de Niagara y Advanced Plant Controller. El cortafuegos limita el acceso al BAS únicamente a los ordenadores autorizados y puede ayudar a reducir el riesgo de ataques, como un ataque de denegación de servicio.

2. 4 Niagara 4 workstation

La estación de trabajo principal de Niagara es un ordenador que se ejecuta con software de Niagara. Requiere dos conexiones de red, una para conectar con la interfaz de usuario web de administración a través de un navegador web (por lo general, en Internet, la intranet o la red corporativa) y otra para conectar con la red del BAS.

2. 5 Conmutador Ethernet

Un conmutador Ethernet crea redes y utiliza varios puertos para establecer la comunicación entre dispositivos en la LAN. Los conmutadores Ethernet difieren de los enrutadores, que conectan redes y solo utilizan un único puerto LAN y WAN. Una infraestructura corporativa totalmente cableada e inalámbrica proporciona conectividad por cable y WI-FI para conectividad inalámbrica.

2. 6 Advanced Plant Controller

El Advanced Plant Controller es un controlador global que se conecta a una red Ethernet, BACnet IP y aloja segmentos de red MS/TP. MS/TP es una conexión de bajo ancho de banda que se utiliza para conectar controladores y sensores.

2. 7 HMI

El HMI se conecta y recibe alimentación de los Advanced Plant Controllers de Niagara. Estos dispositivos incorporan una pantalla táctil capacitiva que permite utilizar los dedos y proporciona al operador funciones para ver, acceder y resolver problemas de puntos del controlador, módulos de E/S y otros equipos conectados.

2. 8 Módulo de E/S

Los módulos de E/S se pueden conectar al controlador con conexiones de tipo touch flake (alimentación y comunicaciones) o los módulos de E/S se pueden conectar a un adaptador de cableado que se suministrará con alimentación y se conectará a una de las interfaces RS485 del controlador. Los módulos de E/S se pueden programar mediante la herramienta de ingeniería existente, como la herramienta ComfortPoint Open Studio y Niagara 4 Workbench.

3. PLANIFICACIÓN Y SEGURIDAD DE RED

3. 1 Red Ethernet

Se recomienda que la red Ethernet utilizada por el sistema BMS esté separada de la red normal de la oficina.

Ejemplo:

Mediante un espacio de aire o una red privada virtual. Se debe restringir el acceso físico a la infraestructura de red Ethernet. También debe asegurarse de que la instalación cumple la política de IT de su empresa.

Los Advanced Controllers no deben conectarse directamente a Internet.

3. 2 Servidor web

El Advanced Controller proporciona servidores web tanto HTTP como HTTPS. Si no se requiere un servidor web, se recomienda desactivar ambos servidores web.

3. 3 Red BACnet IP

Debido a la naturaleza insegura del protocolo BACnet, el Advanced Controller, el HMI y los módulos de E/S que utilizan BACnet no deben conectarse a Internet bajo ninguna circunstancia. El sistema de seguridad del Advanced Controller no ofrece protección contra los accesos de escritura de BACnet. Se debe restringir el acceso físico a la infraestructura de red BACnet IP. Si no se necesitan comunicaciones BACnet IP, el módulo de red (BACnet IP) del Advanced Controller deberá desactivarse estableciendo el parámetro «Disable Module» en «1».

Si se necesitan comunicaciones BACnet, se recomienda encarecidamente no activar los servicios BACnet Backup/Restore, Reinitialize Device y BACnet Writable. Sin embargo, esto significará que la estrategia creada no es compatible con BTL (Consulte *«Seguridad local» en la página 11.*).

3. 4 MS/TP (licencias NC)

Se debe restringir el acceso físico a la infraestructura de red MS/TP. Si no se necesita la red MS/TP, el módulo de red (BACnet MSTP) del Advanced Controller deberá desactivarse estableciendo el parámetro «Disable Module» en «1».

Bus de E/S (licencias CAN)
Se debe restringir el acceso físico al bus de E/S.

3. 5 USB

Se debe restringir el acceso físico al puerto de ingeniería local USB del Advanced Controller.

3. 6 RS485 (incluidas licencias Modbus)

Se debe restringir el acceso físico al puerto RS485 del controlador. Si no se necesita ningún módulo de red conectado al puerto, no se deberá incluir en la estrategia.

3. 7 Red IP Modbus (licencias INT)

Debido a la naturaleza insegura del protocolo Modbus, los Advanced Controllers que utilizan Modbus IP no deben conectarse a Internet bajo ninguna circunstancia. Se debe restringir el acceso físico a la infraestructura de red Modbus IP. Si no se necesitan comunicaciones Modbus IP, no se deberá incluir el módulo de red (Modbus IP) del Advanced Controller en la estrategia.

4. SISTEMA DE SEGURIDAD DEL ADVANCED CONTROLLER, EL HMI Y EL MÓDULO DE E/S

La seguridad de los Advanced Controllers cumple el estándar ISA 62433-3-3 SL 3 y proporciona arranques seguros, una red autenticada y cifrada, cifrado en reposo y gestión sincronizada de cuentas.

Para obtener acceso a productos de Advanced Controller o realizar cualquiera de las tareas anteriores, se debe proporcionar un nombre de usuario y una contraseña válidos para una cuenta del sistema de ingeniería o una cuenta del sistema de dispositivos.

4. 1 Seguridad cuando no está configurado

Para interactuar con un Advanced Controller, un HMI y módulos de E/S, se deben proporcionar credenciales válidas. El controlador se suministra de fábrica sin ninguna credencial (cuentas del sistema o módulos del usuario) para garantizar que estará protegido contra accesos no autorizados cuando se encienda por primera vez. La primera vez que se realiza un intento de conectar con un vCNC en uno de los productos Advanced en la red Niagara, se debe crear una cuenta del sistema de ingeniería con función de administrador.

4. 2 Protección contra dispositivos no autorizados

Se utiliza una clave única (clave de red) para garantizar que solo los dispositivos autorizados pueden unirse a la red Niagara. Todos los controladores que vayan a formar una red Niagara deberán tener la misma clave de red y el mismo puerto UDP. Estos elementos se configuran utilizando la herramienta IP durante el proceso de configuración inicial.

Ejemplo:

Si cuatro Advanced Plant Controllers tienen la misma clave de red (112233) y un quinto tiene una clave de red diferente (222). Cuando se conectan a la misma red Ethernet, los cuatro controladores con la misma clave de red se unen para formar una única red. Sin embargo, el quinto controlador no podrá unirse a la red porque tiene una clave de red diferente (222).

De forma similar, si el quinto controlador es nuevo (enviado de fábrica) y se añade a la red Ethernet, no podrá conectarse a la red Niagara debido a que no tiene una clave de red.

4. 2. 1 Código de verificación de cuenta

Cuando se añade una cuenta del sistema de administrador a uno de los controladores de la red, el controlador al que se ha añadido la cuenta del sistema genera automáticamente un código de verificación de cuenta. Este código se sincroniza con el resto de controladores con la misma clave de red y el mismo puerto UDP en la red Ethernet.

Una vez generado el código de verificación de cuenta, TODOS los controladores de la red DEBEN tener el mismo código de verificación de cuenta, así como la misma clave de red y el mismo puerto UDP.

Ejemplo:

Si hay cinco controladores, todos los Advanced Controllers tienen la misma clave de red. Cuatro tienen el mismo código de verificación de cuenta (AVC) y, por lo tanto, forman una red. El quinto tiene un código de verificación de cuenta diferente y, aunque tiene la misma clave de red, no puede unirse a los otros controladores.

4. 3 Cuentas del sistema

Las cuentas del sistema permiten a las personas y a los dispositivos interactuar con el Advanced Controller. El acceso otorgado dependerá del tipo de cuenta y de la función.

Hay dos tipos de cuentas del sistema:

1. Cuenta del sistema de ingeniería
2. Cuenta del sistema de dispositivos

4. 3. 1 Cuenta del sistema de ingeniería

Las cuentas del sistema de ingeniería se destinan al uso por parte de ingenieros. Cada cuenta del sistema de ingeniería tiene un nombre de cuenta y una contraseña que deberán suministrarse cuando el controlador los solicite. Si se proporcionan un nombre de usuario y una contraseña válidos, el controlador concederá acceso.

Se debe crear una cuenta del sistema de ingeniería diferente para cada persona. Las cuentas del sistema de ingeniería pueden establecerse para una de dos funciones:

- Función de ingeniería
- Función de administrador

Función de ingeniería
La función de ingeniería proporciona el acceso necesario para diseñar el sistema Advanced, crear o gestionar cuentas del sistema de dispositivos y para gestionar los detalles de la cuenta del usuario (dirección de correo electrónico, contraseña, etc.).

Función de administrador
La función de administrador proporciona el mismo acceso a la función de ingeniería, más la capacidad de gestionar todas las cuentas del sistema de ingeniería y de dispositivos.

4. 3. 2 Cuenta del sistema de dispositivos

El objetivo de las cuentas del sistema de dispositivos es permitir a dispositivos como Niagara conectarse a la red para obtener la información requerida y realizar cambios. Se recomienda crear una cuenta del sistema de dispositivos separada para cada dispositivo que vaya a acceder a la red. Tiene una función de «Supervisor».

IMPORTANTE:
Importante: Se debe configurar el propio sistema de seguridad del supervisor para restringir los derechos de acceso de cada usuario supervisor.

4. 3. 3 Creación de la cuenta del sistema

Se deberá crear una cuenta del sistema de ingeniería con la función de administrador la primera vez que se intente conectar con un vCNC en la red Niagara. A continuación, esta cuenta se sincronizará con los otros controladores de la red Niagara.

- Consulte *«Gestión sincronizada de cuentas» en la página 10.* Se pueden crear las cuentas adicionales necesarias mediante Niagara Workbench.

NOTA:
La primera vez que se cree una cuenta del sistema de ingeniería en un controlador, se generará automáticamente un código de verificación de cuenta y se sincronizará con los otros controladores de la red Ethernet con la misma clave de red y el mismo puerto UDP. Cuando un controlador tiene un código de verificación de cuenta, solo puede unirse a una red con controladores que tienen el mismo código de verificación de cuenta (Consulte *«Código de verificación de cuenta» en la página 9.*).

4. 4 Gestión sincronizada de cuentas

La gestión sincronizada de cuentas sincroniza de forma fácil y segura las cuentas del sistema, incluido el código de verificación de cuenta, con todos los Advanced Controllers de la misma red Niagara. Esto permite:

- Utilizar el inicio de sesión único en la red
- Reducir la sobrecarga de configurar y mantener el acceso a la instalación sin reducir la seguridad

Todos los Advanced Controllers de la misma red tendrán las mismas cuentas del sistema.

Cuando un Advanced Controller sin ninguna cuenta del sistema se conecta a la red Ethernet y se configura con la clave de red y el puerto UDP para la red Niagara, se unirá a la red y obtendrá automáticamente sus cuentas del sistema de los otros controladores de la red Niagara.

Ejemplo:

Si se añade al sistema anterior un Advanced Controller sin ninguna cuenta del sistema y se le otorga la clave de red para la red Niagara (112233) y el puerto UDP, se unirá a la red y obtendrá sus cuentas del sistema (Usuario 1, Usuario 2 y Usuario 3) de los otros Advanced Controllers de la red Niagara.

Una vez completada la sincronización, será posible conectar con cualquier vCNCs, visualizar páginas web e iniciar sesión en cualquier Advanced Controller de la red Niagara mediante cualquiera de las cuentas del sistema.

Si se realizan cambios en las cuentas del sistema, es decir, si se añade, elimina o edita una cuenta, estos cambios se sincronizarán automáticamente en todos los Advanced Controllers de la red Niagara.

Ejemplo:

Si hay cinco Advanced Controllers y las cuentas del sistema de un controlador (1) se editan para eliminar el Usuario 2, cambiar el nombre del Usuario 3 a Usuario 3a y se añade el Usuario 4, los cambios se sincronizarán con el Controlador (2), Controlador (3), Controlador (4) y Controlador (5).

NOTA:
Si durante el proceso de sincronización se descubre un conflicto, tendrá prioridad el último cambio.

4. 5 Cambio de una clave de red del Advanced Controller

Cuando se cambie una clave de red del Advanced Controller, se eliminarán todas las cuentas del sistema y se retirarán de su red Niagara actual. El cambio de la clave de red debe ser autorizado por una cuenta válida del sistema de administrador o de ingeniería.

Una vez realizado el cambio, se unirá a una red Niagara mediante la nueva clave de red, si ya existe una, y obtendrá las cuentas del sistema del Advanced Controller de la nueva red Niagara, siempre y cuando tenga el mismo puerto UDP.

4. 6 Seguridad local

La seguridad local utiliza usuarios locales (módulos de usuario) para permitir el acceso a las páginas web de Advanced Controllers o a una pantalla conectada localmente y para controlar la información que resulta visible o los valores que se pueden ajustar.

Para obtener acceso y realizar cambios se deben proporcionar un nombre de usuario y una contraseña válidos para un usuario local. El nivel de PIN del usuario determina qué parámetros puede ver y ajustar un usuario.

NOTA:
Los usuarios locales NO están sincronizados con otros Advanced Controllers de la red Niagara.

4. 7 Acceso a páginas web

El acceso a las páginas web del controlador está protegido por el sistema de seguridad del Advanced Controller. Cuando se accede al servidor web del controlador, se muestra una página web que proporciona información básica y permite a un usuario iniciar sesión (Consulte *«Acceso inicial» en la página 11*.).

Los usuarios que inicien sesión serán tratados como usuarios con sesión iniciada (Consulte *«Usuarios que han iniciado sesión» en la página 12*.) y los usuarios que accedan a las páginas web sin iniciar sesión recibirán el acceso descrito en *«Acceso inicial» en la página 11*.

4. 7. 1 Acceso inicial

Cuando se accede por primera vez al servidor web del controlador, aparece la página de bienvenida y el acceso otorgado dependerá de la configuración de seguridad actual del controlador:

- Ninguna cuenta del sistema de ingeniería y ningún módulo de usuario (valor predeterminado de fábrica)
  Se muestra la página de bienvenida y se otorgará acceso completo a las páginas web del controlador, así como la capacidad de realizar cambios.

NOTA:
Dado que no hay cuentas del sistema de ingeniería ni módulos de usuario, no será posible iniciar sesión.

- Cuentas del sistema de ingeniería, pero ningún módulo de usuario
  Se muestra la página de bienvenida, y el controlador concederá acceso únicamente a Sensor, Digital Input, Knob, Switch, Driver, Schedule, Time Schedule, Time, módulos Plot, Alarm Log y Graphics, y no permitirá realizar cambios.

NOTA:
Será posible iniciar sesión utilizando cuentas del sistema de ingeniería.

- Cuentas del sistema de ingeniería y módulos de usuario
  Los módulos de usuario controlan la pantalla inicial y el acceso. Si hay un módulo de usuario denominado «Guest» sin una contraseña cuando se accede a las páginas web del Advanced Controller sin iniciar sesión, el controlador otorgará los derechos de acceso (nivel de usuario, página Home y vistas predeterminadas) especificados en el módulo de usuario «Guest».

  De manera predeterminada, el módulo de usuario «Guest» solo proporciona acceso a la página de bienvenida de Advanced y tiene un nivel de usuario de «0». Esto significa que un usuario que acceda al controlador sin iniciar sesión solo será capaz de ver la página de bienvenida. Para otorgar más acceso, el usuario «Guest» puede configurarse de la misma forma que cualquier otro módulo de usuario Tipo 0.

NOTA:
Niagara Workbench impide que el usuario «Guest» reciba una contraseña, un PIN o un nivel de usuario superior a «0». Permite configurar una página Home y las vistas predeterminadas.

Se recomienda encarecidamente dejar al usuario Guest con la configuración predeterminada (nivel de usuario de «0» y sin derechos de visualización).

Si no existe ningún módulo de usuario denominado «Guest» o se ha configurado con una contraseña, se mostrará la página de bienvenida y el controlador concederá acceso únicamente a Sensor, Digital Input, Knob, Switch, Driver, Schedule, Time Schedule, Time, módulos Plot, Alarm Log y Graphics, y no permitirá realizar cambios.

NOTA:
Será posible iniciar sesión con las cuentas del sistema de ingeniería y cualquier módulo de usuario que exista.

4. 7. 2 Usuarios que han iniciado sesión

Para iniciar sesión en un página web de un Advanced Controller, se deben introducir un nombre de usuario y una contraseña que coincidan con una de las cuentas del sistema de ingeniería del Advanced Controller o con módulos de usuario de tipo 0.

4. 8 Recuperación de la contraseña

Si un usuario ha olvidado su contraseña, se podrá recuperar utilizando Niagara Workbench. Para obtener detalles sobre la recuperación de una contraseña olvidada con Niagara, consulte la Guía del usuario de Niagara Workbench.

5. PROTECCIÓN DEL SISTEMA OPERATIVO NIAGARA

5. 0. 1 Práctica recomendada general

Siga la práctica recomendada general para proteger el sistema operativo, como:

- Un salvapantallas protegido con contraseña
- Software de cifrado de unidades

5. 0. 2 Ajuste del cortafuegos

El sistema operativo se debe configurar para usar un cortafuegos que se actualice automáticamente. La configuración debe evitar el acceso (de entrada y salida) para todos los puertos salvo para aquellos que requieran acceso. NO deje ningún puerto no usado abierto.

5. 0. 3 Versión del sistema operativo

DEBE asegurarse de que cualquier dispositivo que ejecute aplicaciones Niagara o que esté conectado a la misma red IP tenga instaladas las últimas actualizaciones del sistema operativo. Es recomendable asegurarse de que las actualizaciones de Windows se dejen en modo automático y de que se instalen oportunamente.

5. 0. 4 Protección antivirus

DEBE asegurarse de que cualquier ordenador que ejecute aplicaciones Niagara o que esté conectado a la misma red IP utilice software de protección antivirus y de que las definiciones de virus estén actualizadas.

5. 0. 5 Protección contra intrusiones

Se recomienda utilizar un sistema de detección de intrusiones (IDS) de un proveedor reputado de productos de seguridad en cualquier ordenador que ejecute aplicaciones Niagara. Siga las prácticas recomendadas para los productos seleccionados, así como cualquier política corporativa de IT donde se haya realizado la instalación.

Muchos IDS y productos de cortafuegos ofrecen una solución completa para registrar todo el tráfico entrante y saliente del ordenador, y proporcionan a los usuarios la capacidad de registrar toda la actividad al nivel más bajo.

6. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

El Reglamento General de Protección de Datos (UE)2016/679 (RGPD) es un reglamento de la UE relativo a la protección de datos y la privacidad que se aplica a todos los particulares de la Unión Europea (UE) y del Espacio Económico Europeo (EEE). También aborda la transferencia de datos personales fuera de la Unión Europea (UE) y del Espacio Económico Europeo (EEE). El RGPD contiene disposiciones y requisitos relacionados con el tratamiento de datos personales de particulares (interesados) dentro del EEE y se aplica a todas las empresas establecidas en el EEE (con independencia de su ubicación y de la nacionalidad de los interesados) o que traten la información personal de los interesados dentro del EEE.

Según los términos del RGPD, los datos personales incluyen cualquier información que pueda ser utilizada para identificar a una persona. Entre ellos se incluyen los siguientes:

- nombres de usuario,
- contraseñas,
- números de teléfono,
- direcciones de correo electrónico,
- direcciones residenciales o de trabajo.

Toda esta información introducida en el Advanced Controller, el HMI y el módulo de E/S se cifra y se almacena en los productos Advanced, en las instalaciones de un cliente. Honeywell no tiene ninguna relación con el almacenamiento ni el tratamiento de datos personales dentro de los productos Advanced Honeywell.

La responsabilidad del cumplimiento de los requisitos del RGPD recae completamente en el integrador o administrador del sistema y, en este sentido, son ellos quienes deben asegurarse de que se cuenta con los sistemas técnicos y organizativos adecuados para:

- obtener el consentimiento explícito de cada interesado para almacenar, utilizar o tratar los datos personales,
- permitir que los particulares obtengan acceso a sus datos personales para verificar su precisión,
- permitir que los particulares retiren su consentimiento en cualquier momento y que se borren sus datos personales de manera permanente,
- mantener la seguridad y la integridad del almacenamiento de datos y el acceso a ellos en todo momento,
- informar de cualquier infracción de seguridad de los datos (que pueda afectar a la privacidad del usuario) a la autoridad pertinente en un plazo de 72 horas a partir del momento en que tenga lugar la infracción.

7. COMUNICACIÓN SEGURA

Una infraestructura de clave pública (PKI) admite la distribución e identificación de claves de cifrado públicas utilizadas para proteger el intercambio de datos a través de las redes, como Internet. PKI verifica la identidad de la otra parte y codifica la transmisión de datos real. La verificación de la identidad proporciona garantía de aceptación de la identidad del servidor. El cifrado proporciona confidencialidad durante la transmisión de red. Requerir módulos de código firmado garantiza que solo se utilice el código esperado en el sistema

Para proporcionar redes seguras con PKI, Niagara admite el protocolo TLS (Seguridad de la capa de transporte), versiones 1.0, 1.1 y 1.2. TLS reemplaza a su predecesor, SSL (Capa de sockets seguros).

Cada instalación de Niagara crea automáticamente un certificado predeterminado que permite cifrar la conexión inmediatamente. Sin embargo, estos certificados generan avisos en el navegador y en Workbench, y generalmente no son adecuados para los usuarios finales. Crear y firmar certificados digitales personalizados permite un uso impecable de TLS en el navegador, y proporciona cifrado y autenticación del servidor.

Además de la seguridad de la comunicación, cada módulo del código del ordenador que se ejecuta en el sistema está protegido con una firma digital. Los objetos de programa añadidos requieren esta firma o no se ejecutan.

Verificar el servidor, cifrar la transmisión y garantizar que solo se ejecute el código firmado no ofrece protección para los datos almacenados en un dispositivo de almacenamiento. Seguirá necesitando restringir el acceso físico a los ordenadores y controladores que gestionan el modelo de edificio, configurar la autenticación de los usuarios con contraseñas seguras y proteger los componentes controlando los permisos.

Niagara admite y utiliza comunicaciones seguras y códigos firmados de manera predeterminada. No es necesario adquirir una licencia adicional.

La seguridad es una preocupación constante. Aunque encontrará una gran cantidad de información valiosa en los temas dedicados a las comunicaciones seguras, espere actualizaciones y cambios futuros.

Más abajo se enumeran las comunicaciones seguras. Para obtener más detalles, consulte la Guía de seguridad de la estación Niagara.

- Relaciones cliente/servidor
- Certificados
- Almacenes de certificados
- Estructura de la carpeta CSR
- Instalación de certificados
- Asistente de certificados
- Firma de varios certificados
- Configuración de la comunicación segura entre plataformas
- Configuración de la comunicación segura entre estaciones
- Activación y configuración de clientes para el puerto correcto
- Instalación de una copia de estación en otra plataforma
- Protección del correo electrónico
- Resolución de problemas de comunicaciones seguras

7. 1 Relaciones cliente/servidor

Las relaciones cliente/servidor identifican las conexiones que requieren protección. Las relaciones cliente/servidor de Workbench varían en función de cómo se configure y se utilice un sistema. Workbench es siempre un cliente. Una plataforma es siempre un servidor. Una estación puede ser un cliente y un servidor.

Los protocolos del sistema que gestionan las comunicaciones son:

- Las conexiones de plataforma desde Workbench (cliente) al controlador o al daemon de la plataforma del PC Supervisor (servidor) utilizan Niagara. Una conexión de plataforma segura se conoce a veces como platformtls. Active platformtls con ayuda de la vista Platform Administration.
- Las conexiones de una estación local (Supervisor y plataforma) utilizan Foxs. Estas conexiones se activan en el FoxService de una estación (Config > Services > FoxService).
- Las conexiones del navegador utilizan Https, así como Foxs si se utiliza Web Launcher con un WbWebProfile. Estas conexiones se activan utilizando el WebService de la estación (Config > Services > WebService).
- Conexiones de cliente al servidor de correo electrónico de la estación, si corresponde. El correo electrónico seguro se activa utilizando el EmailService de la estación (Config > Services > EmailService).

8. CERTIFICADOS

Un certificado es un documento electrónico que utiliza una firma digital para asociar una clave pública a una persona u organización. Los certificados pueden responder a todo un conjunto de propósitos en función de cómo se configure la propiedad Key Usage del certificado. El objetivo principal en este sistema es verificar la identidad de un servidor para que la comunicación sea fiable. Para obtener más detalles, consulte la Guía de seguridad de la estación Niagara - Certificado.

Niagara admite los siguientes tipos de certificados:

- Un certificado de **CA** (Autoridad de certificación) es un certificado autofirmado que pertenece a una CA. Puede tratarse de un tercero o de una empresa que funcione como su propia CA.
- Un **certificado de CA raíz** es un certificado de CA autofirmado cuya clave privada se utiliza para firmar otros certificados que crean un árbol fiable de certificados. Con su clave privada, un certificado de CA raíz puede exportarse, almacenarse en una unidad de memoria USB en un depósito y extraerse únicamente cuando hay que firmar certificados. Una clave privada de un certificado de CA raíz requiere crear una contraseña para la exportación y el aprovisionamiento de la misma contraseña cuando se usa para firmar otros certificados.
- Un **certificado intermedio** es un certificado de CA firmado por un certificado de CA raíz que se utiliza para firmar certificados de servidor y otros certificados de CA intermedios. El uso de certificados intermedios aísla un grupo de certificados de servidor.
- Un **certificado de servidor** representa el lado del servidor de una conexión segura. Aunque se puede configurar un certificado independiente para cada protocolo (Foxs, Https y Webs) y configurar una plataforma y un estación (como servidor) con certificados independientes de servidor, por motivos de simplicidad la mayoría de los sistemas utiliza el mismo certificado de servidor.
- Un **certificado de firma de código** es un certificado utilizado para firmar objetos y módulos de programa. Los integradores de sistemas utilizan este certificado para impedir la introducción de código malicioso cuando personalizan el marco de trabajo.

8. 1 Certificados autofirmados

Un certificado autofirmado es un certificado firmado de manera predeterminada con su propia clave privada en lugar de con la clave privada de un certificado de CA (Autoridad de certificación) raíz.

El sistema admite dos tipos de certificados autofirmados:

- Un **certificado de CA raíz** es implícitamente fiable porque no existe ninguna autoridad superior a la CA (Autoridad de certificación) que posee este certificado. Por este motivo, las CA cuya actividad consiste en avalar los certificados de otras personas vigilan de cerca sus certificados de CA raíz y sus claves privadas. De la misma manera, si su empresa funciona como su propio CA, deberá vigilar de cerca el certificado de CA raíz que utiliza para firmar otros certificados.
- Un **certificado autofirmado predeterminado**: la primera vez que se inicia una instancia de Workbench, una plataforma o una estación tras la instalación (puesta en servicio), el sistema crea un certificado de servidor autofirmado predeterminado con un alias de tridium.

NOTA:

No exporte este certificado ni lo importe en ningún almacén de otra plataforma o estación. Aunque es posible, hacerlo reduce la seguridad y aumenta la vulnerabilidad.

Para minimizar el riesgo de un ataque de suplantación de identidad cuando se usan certificados autofirmados, debe mantener todas sus plataformas en una red privada segura, fuera de línea y sin acceso público desde Internet.

⚠ PRECAUCIÓN

Para utilizar certificados autofirmados, antes de acceder a la plataforma o a la estación desde Workbench por primera vez, asegúrese de que su ordenador y la plataforma no se encuentran en ninguna red corporativa ni en Internet. Una vez desconectado, conecte el ordenador directamente a la plataforma, abra la plataforma en Workbench y apruebe su certificado autofirmado. Solo entonces debe reconectar la plataforma a una red corporativa.

8. 2 Convención de nomenclatura

El **User Key Store**, el **User Trust Store** y el **System Trust Store** son los elementos centrales de la configuración. Los certificados se parecen mucho y varios certificados autofirmados predeterminados tienen nombres idénticos.

8. 3 Almacenes de certificados

La gestión de certificados utiliza cuatro almacenes para gestionar certificados: un **User Key Store**, un **System Trust Store**, un **User Trust Store** y una lista **Allowed Hosts**.

El **User Key Store** está asociado con el lado del servidor de la relación cliente/servidor. Este almacén guarda los certificados, cada uno con su clave pública y privada. Además, este almacén contiene el certificado autofirmado creado inicialmente cuando se lanzó Workbench o se inició la plataforma por primera vez.

Los almacenes **User Trust Store** y **System Trust Store** están asociados con lado del cliente de la relación cliente/servidor. El System Trust Store viene preconfigurado con certificados públicos estándar: certificados de CA raíz de autoridades de certificación conocidas, como VeriSign, Thawte y Digicert. El **User Trust Store** guarda los certificados intermedios y de CA raíz de empresas que actúan como su propia autoridad de certificación.

La lista **Allowed Hosts** contiene los certificados de servidor para los que no existe certificado de CA raíz fiable en el **User Trust System** o el **User Trust Store** del cliente, pero los certificados de servidor se han aprobado para su uso de todos modos. Aquí se incluyen servidores para los que el nombre de host del servidor no es el mismo que el nombre común en el certificado de servidor. El uso de estos certificados se aprueba de manera individual. Si bien la comunicación es segura, resulta conveniente utilizar certificados de servidor firmados.

8. 4 Cifrado

El cifrado es el proceso de codificar la transmisión de datos para que no pueda ser leída por terceros que no son de confianza. TLS utiliza cifrado para transmitir datos entre el cliente y el servidor. Si bien es posible realizar una conexión no cifrada utilizando únicamente los protocolos fox o http, aconsejamos encarecidamente no utilizar esta opción. Sin cifrado, sus comunicaciones corren el peligro de sufrir un ataque. Acepte siempre las conexiones Foxs o Https predeterminadas.

9. DESCRIPCIÓN GENERAL DE SECURITY DASHBOARD

En Niagara 4.u5 y versiones posteriores, la función Security Dashboard proporciona (para administradores y otros usuarios autorizados) una vista de pájaro de la configuración de seguridad de su estación. Esta vista de pájaro le permite supervisar fácilmente la configuración de seguridad de una gran cantidad de servicios de estación e identificar cualquier debilidad de la configuración de seguridad en la estación.

⚠ PRECAUCIÓN

La vista Security Dashboard puede no mostrar todos los ajustes de seguridad posibles, y no debe considerarse como una garantía de que todo está configurado de forma segura. En concreto, los modelos de terceros pueden tener ajustes de seguridad no registrados en el panel.

La vista Security Dashboard es la vista principal del servicio de seguridad de la estación. Esta vista le avisa de debilidades de seguridad, como ajustes de seguridad deficiente de las contraseñas; certificados caducados, autofirmados o no válidos; protocolos de transporte no cifrados, etc., que indican áreas donde la configuración debe ser más segura. Otros datos recopilados incluyen: estado del sistema, número de cuentas activas, cuentas no activas, número de cuentas con permisos de superusuario, etc. Opcionalmente, el atributo «sistema» de la función de licencias «securityDashboard» puede establecerse en «true» para activar la vista del sistema de la estación que proporciona detalles de seguridad para cada estación subordinada de la red Niagara.

Security Dashboard es la vista principal de los servicios de seguridad. Para los detalles completos de la vista, consulte «nss-SecurityDashboardView» en la Guía de seguridad de la estación Niagara.

10. PLANIFICACIÓN E INSTALACIÓN

Esta sección incluye información para la planificación y la realización de una instalación del Advanced Plant Controller.

10. 1 Instalación y configuración recomendadas

La siguiente sección ilustra dos configuraciones de instalación recomendadas.

- Solo BACnet
- BACnet y Niagara

10. 1. 1 Solo BACnet

Cuando el Advanced Plant Controller solo se utiliza para comunicaciones BACnet, conecte solo Ethernet 1 a la red del BAS donde se esté ejecutando BACnet (BACnet/IP o BACnet/Ethernet).

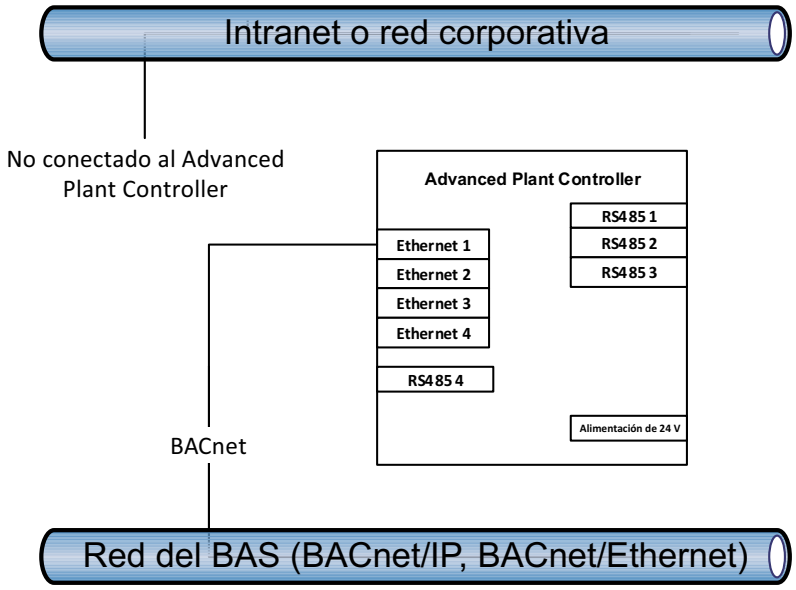

Fig. 2 Conexión BACnet

10. 1. 2 BACnet y Niagara

Cuando se utiliza Niagara en el Advanced Plant Controller, se puede configurar para proporcionar servicios, como servicios web o Niagara FOXS, a Internet, la intranet o la red corporativa. Si este es el caso, conecte Ethernet 2 a Internet, a la intranet o la red corporativa a través del cortafuegos del BAS para prestar servicios a esa red.

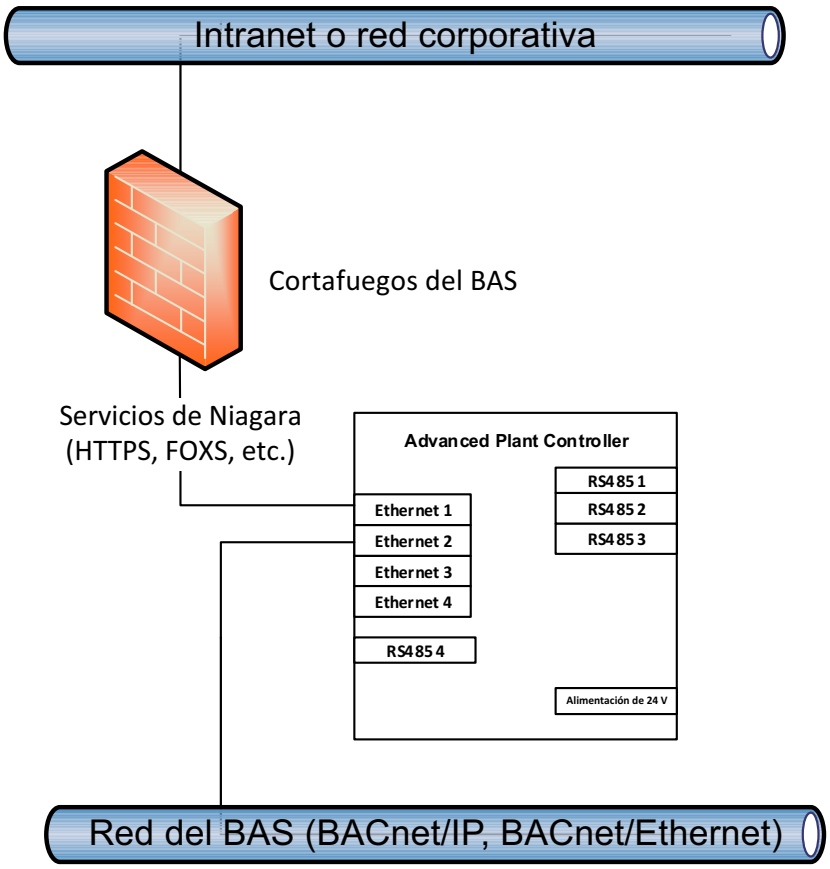

Fig. 3 Conexiones BACnet y Niagara

10. 2 Recomendación sobre las redes de área local (LAN)

Asegúrese de que los sistemas utilizan una política de contraseña adecuada para el acceso de los usuarios a todos los servicios. Esta directriz incluiría, entre otras, las siguientes recomendaciones:

1. El uso de contraseñas seguras.
2. Un tiempo de ciclo de contraseña recomendado.
3. Nombres de usuario y contraseñas únicos para cada usuario del sistema.
4. Reglas de divulgación de contraseñas.
5. Si se requiere acceso remoto a sistemas de control de edificios basado en IT, utilice tecnología VPN (Red privada virtual) para reducir el riesgo de interceptación de datos y proteger los dispositivos de control de su ubicación directa en Internet.

11. DOCUMENTACIÓN

La documentación es esencial para capturar la información de diseño y configuración requerida para mantener un sistema seguro.

11. 1 Documentación de los dispositivos físicos y las configuraciones, incluida información clave relacionada con la seguridad

Toda la documentación sobre dispositivos y configuraciones debe incluir información relacionada con la seguridad para establecer y mantener los controles de seguridad previstos. Por ejemplo, si se realizan cambios en los servicios o puertos predeterminados del Advanced Plant Controller, documéntelos claramente para que los ajustes puedan restaurarse en algún momento en el futuro.

11. 2 Documentación de los sistemas externos, especialmente la interacción entre el Advanced Plant Controller y sus sistemas relacionados

El BAS requiere o utiliza habitualmente sistemas externos para funcionar, como una infraestructura de red existente, acceso VPN, hosts de máquinas virtuales y cortafuegos. Si el BAS requiere configurar esos sistemas de una determinada forma para fines de seguridad, como un cortafuegos que permita o rechace determinados puertos o una red que permita el acceso a determinados sistemas, deberá documentar esta información. Si estos sistemas necesitan restaurarse en algún momento en el futuro, **por ejemplo,** debido al fallo de equipos o a la necesidad de realizar cambios en los sistemas externos, **por ejemplo,** actualizar un cortafuegos, documentar esta información puede ayudarle a restaurar el sistema al nivel de seguridad anterior.

12. CONTROL DE ACCESO Y SEGURIDAD FÍSICA

El control de acceso conlleva especificar y limitar el acceso a los dispositivos y funciones solo a usuarios autorizados.

12. 1 Protección física del Advanced Plant Controller, el HMI y el módulo de E/S

Impida el acceso no autorizado a los equipos de red que se utilizan en combinación con sistemas proporcionados por Honeywell. Con cualquier sistema, impedir el acceso físico a la red y a los equipos reduce el riesgo de interferencias no autorizadas. Las prácticas recomendadas de seguridad en las instalaciones de IT aconsejan utilizar salas de servidores, paneles de conexión y equipos de IT en cuartos cerrados con llave. Los equipos de Honeywell deben instalarse en armarios de control cerrados con llave y ubicados en salas protegidas.

12. 2 Adhesivo sobre el panel de acceso o el cerramiento del controlador

Coloque un adhesivo de seguridad sobre el panel de acceso o el cerramiento del Advanced Plant Controller, el HMI y el módulo de E/S

Si un cliente necesita seguridad adicional de que no se ha producido el acceso físico a un Advanced Plant Controller, un HMI y un módulo de E/S, instale un sello o adhesivo de seguridad sobre el punto de acceso.

12. 3 Segregación y protección de las redes

1. Utilice un cortafuegos entre Internet, la intranet o la red corporativa y el BAS.
2. Utilice una red física específica separada (cables separados) o una red virtual (VLAN) para la comunicación BACnet. Esta red debe estar separada de Internet, la intranet o la red corporativa.
3. No conecte EN2 en el Advanced Plant Controller a ninguna red a menos que necesite servicios Niagara (plataforma, estación o servidor web). Si necesita conectar EN2 a Internet, la intranet o la red corporativa, deberá utilizar un cortafuegos BAS externo entre el Advanced Plant Controller e Internet, la intranet o la red corporativa.

13. PROTECCIÓN DEL ADVANCED CONTROLLER, EL HMI Y EL MÓDULO DE E/S

13. 1 Credenciales de la cuenta del sistema de administrador proporcionadas a usuarios de la instalación

Deben proporcionarse las credenciales de la cuenta del sistema de administrador al titular de la instalación para permitirle gestionar las cuentas del sistema.

13. 2 Desarrollo de un programa de seguridad

Consulte la «Práctica recomendada general de seguridad»

13. 3 Consideración física y ambiental

El Advanced Controller, el HMI y el módulo de E/S deben instalarse dentro de un entorno cerrado con llave, p. ej., ubicado en una sala protegida o un armario cerrado con llave.

NOTA:
Asegúrese de que existe una ventilación adecuada.

13. 4 Actualizaciones de seguridad y paquetes de servicio

Asegúrese de que el Advanced Controller, el HMI y el módulo de E/S ejecutan la última versión del firmware.

14. USUARIOS Y CONTRASEÑAS

14. 1 Usuarios

Asegúrese de que el número de usuarios y niveles de acceso proporcionados son adecuados para las actividades que necesitan realizar.

- **En el nivel de dispositivo de controlador configure cuentas o usuarios del sistema en controladores para el acceso al cliente web, el Supervisor y entre pares.**

  Si se configuran módulos de usuarios en los Advanced Controllers, el usuario tendrá que iniciar sesión en un dispositivo con credenciales válidas para poder realizar ajustes. Asegúrese de que se han asignado los derechos de acceso adecuados para las cuentas y los usuarios del sistema.

- **Utilice una cuenta diferente para cada usuario**

  Utilice nombres y contraseñas únicos para cada usuario/cuenta del sistema, en lugar de un acceso genérico. La misma cuenta no debe ser compartida nunca por diferentes personas. Por ejemplo, en lugar de configurar una cuenta general de tipo «managers» que podrían usar muchos managers, cada manager debe tener su propia cuenta independiente.

Existen muchas razones para que cada usuario tenga su propia cuenta individual:

- Si cada persona tiene su propia cuenta, los registros de auditoría resultarán más informativos. Será fácil determinar exactamente qué hizo cada usuario. Esto puede ayudar a detectar si una cuenta se ha visto comprometida.

NOTA:
No todos los productos tienen una función de registro de auditoría, pero no debe desactivarse cuando exista.

- Si se elimina o se modifica una cuenta, se evitarán molestias a muchas personas. Por ejemplo, si una persona debe dejar de tener acceso al sistema, eliminar su acceso individual será sencillo. Si se utiliza una cuenta compartida, las únicas opciones son cambiar la contraseña e informar a todo el mundo, o eliminar la cuenta e informar a todo el mundo. Dejar la cuenta como está no es una opción. El objetivo es revocar el acceso.
- Si cada persona tiene su propia cuenta, resulta mucho más fácil ajustar los permisos para responder con precisión a sus necesidades. Una cuenta compartida podría traducirse en la existencia de personas con más permisos de los que deberían.

  - Cuando se comparte una cuenta, se comparte una contraseña. Compartir contraseñas es una práctica absolutamente nada recomendable. Incrementa en gran medida la probabilidad de que la contraseña se filtre y dificulta la implementación de determinadas prácticas de contraseña recomendadas, como la caducidad de las contraseñas.

- **Uso de usuarios de ingeniería únicos para proyectos**

  En algunas empresas es habitual utilizar los mismos detalles de cuenta para todos los proyectos. Cuando esto es sabido y si un sistema se ve comprometido, el atacante podría estar en posesión de credenciales que le permitirían acceder a muchos otros proyectos instalados por la misma empresa.

- **Desactive las cuentas conocidas cuando sea posible**

  Algunos productos tienen cuentas predeterminadas. Estas deben configurarse de manera que la contraseña no sea la predeterminada.

- **Asigne los permisos mínimos requeridos para los usuarios**

  Asegúrese de que solo se han configurado las cuentas requeridas en el sistema con los niveles de seguridad mínimos requeridos en lugar de acceso completo. Al crear una nueva cuenta, piense en qué debe hacer la persona en el sistema y, a continuación, asigne los permisos mínimos requeridos para realizar ese trabajo. Por ejemplo, una persona que solo necesita ver alarmas no necesita acceso de administrador. Otorgar permisos que no son necesarios aumenta la probabilidad de que se produzca una filtración de seguridad. El usuario podría cambiar sin querer (o queriendo) ajustes que no se deberían cambiar.

- **Utilice el número mínimo posible de cuentas de administrador del sistema**

  Asigne solo permisos de administrador del sistema cuando sean absolutamente necesarios. Este tipo de cuenta es una cuenta muy potente, ya que permite un acceso completo a todo. Solo el administrador del sistema debe tener acceso a la cuenta. Piense también en proporcionar al administrador del sistema dos cuentas de acceso, una para el acceso diario destinado a gestionar las actividades rutinarias y una segunda de nivel superior que solo se utilizará cuando se requieran cambios de tipo administrativo.

14. 2 Contraseñas

Niagara y los sistemas operativos utilizados en los productos Advanced Honeywell deben utilizar contraseñas para autenticar usuarios en un supervisor, pantalla, herramienta o sistema operativo. Es especialmente importante gestionar las contraseñas correctamente. No aplicar este nivel tan básico de seguridad permitirá realizar ajustes a cualquier persona que acceda al sistema a través de una pantalla, cliente web o supervisor. Asegúrese de que el sistema Niagara utiliza una política de contraseñas adecuada para el acceso de usuarios. Esta directriz incluiría, entre otros, estos elementos:

- **El uso de contraseñas seguras**: se deben utilizar contraseñas seguras. Consulte los estándares de seguridad más recientes para conocer los detalles que hacen segura una contraseña.
- **Un tiempo de ciclo de contraseña recomendado**: algunos productos Niagara permiten al administrador del sistema especificar un periodo tras el que se deberá cambiar una contraseña. Aunque no todos los productos aplican actualmente este periodo de cambio de contraseña, una política del sitio puede recomendarlo.
- **Reglas de divulgación de contraseñas**: el usuario DEBE asegurarse de no divulgar detalles de su nombre de usuario y contraseña a otros, y de no anotarlos en ningún lugar.

15. CONFIGURACIÓN DE UN ADVANCED PLANT CONTROLLER

Para configurar un Advanced Plant Controller, consulte la Guía de instrucciones de instalación y puesta en servicio (31-00584). Consulte la Guía del controlador HMI (31-00590) para el HMI y la Guía del controlador de PanelBus (31-00591) para el módulo de E/S.

15. 1 Creación y mantenimiento de configuraciones de referencia

Cree y mantenga una configuración de referencia del Advanced Plant Controller para garantizar que se ha configurado correctamente en términos de seguridad. Asegúrese de que esta referencia también incluya archivos DCF y componentes de Niagara. No introduzca configuraciones inseguras en esta configuración de referencia para evitar que se apliquen involuntariamente en el futuro. Actualice cualquier documentación relevante cuando cambien las configuraciones.

15. 2 Cambio de las contraseñas predeterminadas

Cambie todas las contraseñas predeterminadas: la contraseña de configuración de la consola, la contraseña de copia de seguridad, restauración, reinicio y control, y la contraseña de la plataforma Niagara. Al completar la puesta en servicio, asegúrese de que el dispositivo esté protegido con contraseña. Asegúrese de que se han asignado los niveles de usuario adecuados para los usuarios de la instalación.

15. 3 Consideraciones adicionales

15. 3. 1 Acuerdo de nivel de servicio

Adopte una política de actualización adecuada para la infraestructura instalada en la instalación como parte de un acuerdo de nivel de servicio. Esta política debe incluir, a título meramente enunciativo, la actualización de los siguientes componentes del sistema a la última versión:

- Firmware de los dispositivos para el controlador, los módulos de E/S, el HMI, etc.;
- El software de supervisor, como el software Arena NX;
- Los sistemas operativos de los ordenadores y los servidores;
- Infraestructura de red y cualquier sistema de acceso remoto.

15. 3. 2 Configuración de redes de IT

Configure redes de IT separadas para los sistemas de control de automatización y la red de IT corporativa del cliente. Para ello, configure LAN virtuales (VLAN) dentro de la infraestructura de IT del cliente o instale una infraestructura de red aislada, independiente y específica de los sistemas de control de automatización.

Al interactuar con controladores utilizando un supervisor centralizado del sistema (por ejemplo, Niagara) y cuando el sistema no requiere acceso directo al servidor web de dispositivos individuales, la infraestructura de red se debe configurar para restringir el acceso al servidor web.

Las VLAN dinámicas que utilizan la asignación de direcciones MAC pueden ofrecer protección contra la conexión no autorizada de un dispositivo en el sistema y pueden reducir el riesgo asociado a una persona que examine la información en la red.

16. CONFIGURACIÓN DEL CORTAFUEGOS DEL BAS

En la siguiente tabla se describen los puertos de red utilizados en un Advanced Plant Controller. Consulte la sección Consulte *«Descripción general del sistema» en la página 6.* para obtener un ejemplo de arquitectura de instalación. La tabla tiene las siguientes columnas:

- Puerto predeterminado y el protocolo (TCP o UDP)
- Finalidad del puerto
- Si se debe cambiar o no el puerto predeterminado
- Si se deben permitir o no las conexiones o el tráfico entrantes a través del cortafuegos del BAS
- Debajo de la tabla se incluyen observaciones adicionales

Tabla 2 Configuración del cortafuegos del BAS

Puerto predeterminado/ protocolo	Finalidad	¿Cambiar predeterminado?	¿Permitir el paso a través del cortafuegos del BAS?	Observaciones
80/TCP	HTTP	No	No	
443/TCP	HTTPs	No	Posiblemente, si se requiere acceso web desde Internet, la intranet o la red corporativa.	1
1911/TCP	Fox (versión no segura del protocolo de la aplicación Niagara)	Sí	No	
4911/TCP	Fox + SSL (versión segura del protocolo de la aplicación Niagara)	Sí	No	
3011/TCP	NiagaraD (versión no segura del protocolo de la plataforma Niagara)	Sí	No	
5011/TCP	NiagaraD + SSL (versión segura del protocolo de la plataforma Niagara)	Sí	No	
2601/TCP	Puerto de la consola Zebra	No	No	2
2602/TCP	Puerto de la consola RIP			2
47808/UDP	Conexión de red BACnet IP	Sí	No	3

NOTA:

1. Si se admite la interfaz de usuario web remota directa, se deberá permitir este puerto a través del cortafuegos del BAS.
2. Este proceso abre el puerto automáticamente y esta funcionalidad no se puede desactivar. El proceso se ha configurado para no permitir ningún inicio de sesión a través de este puerto.
3. Siga las directrices de configuración de red recogidas en este manual para que el Advanced Plant Controller no necesite nunca pasar tráfico UDP a través del cortafuegos del BAS.

17. CONFIGURACIÓN DE LA AUTENTICACIÓN

El esquema de autenticación de Google es un mecanismo de autenticación de dos factores que requiere que el usuario introduzca su contraseña, además de un token de un único uso cuando inicia sesión en una estación. Este sistema protege la cuenta del usuario incluso si su contraseña se ve comprometida.

Este esquema de autenticación se basa en TOTP (contraseña de un solo uso basada en el tiempo) y la aplicación Google Authenticator instalada en el dispositivo móvil del usuario para generar y verificar tokens de autenticación de un solo uso. La autenticación de Google se basa en el tiempo, por lo que no existe dependencia de la comunicación de red entre el dispositivo móvil del usuario, la estación y los servidores externos. Como el autenticador se basa en el tiempo, la hora de la estación y la hora del teléfono deben estar relativamente sincronizadas. La aplicación proporciona un margen de 1,5 minutos más o menos para posibles desviaciones del reloj.

Requisitos previos: El teléfono móvil del usuario debe tener instalada la aplicación Google Authentication. Usted debe trabajar en Workbench. El usuario existe en la base de datos de la estación.

17. 1 Procedimiento

1. Abra la paleta gauth y añada **GoogleAuthenticationScheme** al nodo **Services** > **Authenticationservice** en el árbol Nav.
2. Haga clic con el botón secundario en **Userservice** y haga doble clic en el usuario en la tabla. Se abrirá la vista Edit para el usuario.
3. Configure la propiedad Authentication Scheme Name en **GoogleAuthenticationScheme** y haga clic en **Save**.
4. Haga clic en el botón situado junto a la clave secreta debajo del autenticador del usuario y siga las instrucciones.
5. Para completar la configuración, haga clic en **Save**. Dependiendo de la vista que esté usando, puede que necesite abrir el usuario de nuevo o actualizar tras guardar.

18. ENTREGA DEL SISTEMA

En esta sección se incluye información que se debe proporcionar cuando el BAS se entrega al titular del sistema.

- Documentación que incluye información de seguridad, ajustes de configuración, nombres de usuario de administración y contraseñas, planes de desastre y recuperación, y procedimientos de copia de seguridad y restauración.
- Formación de los usuarios finales sobre las tareas de mantenimiento de la seguridad.

19. COPIA DE SEGURIDAD USB E INSTALACIÓN DEL ARCHIVO CLEANDIST

La información de copia de seguridad USB y de la instalación del archivo CleanDist puede encontrarse en la Guía de instrucciones de instalación y puesta en servicio - 31-00584.

20. DESMANTELAMIENTO DEL SISTEMA

Los datos sensibles deben eliminarse de las unidades que se están poniendo fuera de servicio y esta tarea se puede realizar mediante un restablecimiento a los valores de fábrica. Consulte la sección Botón de servicio/LED de alarma de servicio y la sección Instalación del archivo CleanDist de la Guía de instrucciones de instalación y puesta en servicio - 31-00584.

NOTA:
El procedimiento del archivo CleanDinst puede realizar un restablecimiento a los valores de fábrica al instalar el archivo clean4.

21. SEGURIDAD DE LOS PRODUCTOS BASADOS EN ADVANCED NIAGARA

Para los productos Advanced Honeywell basados en los marcos de trabajo Niagara N4 y Niagara AX (por ejemplo, el Advanced Plant Controller, el HMI y el módulo de E/S), debe seguir los consejos de Tridium sobre la protección del marco de trabajo de Niagara.

Se pueden realizar varios cambios de configuración en Niagara para maximizar la seguridad de los productos Advanced Honeywell.

- Utilizar la función de seguridad de las contraseñas
- Activar la función de bloqueo de las cuentas
- Activar la caducidad de las contraseñas
- Utilizar el historial de contraseñas
- Utilizar la función de restablecimiento de contraseñas
- Dejar sin marcar la casilla Remember These Credentials
- Cambiar la frase de contraseña predeterminada del sistema
- Utilizar TLS para establecer la frase de contraseña del sistema
- Seleccionar una frase de contraseña del sistema segura
- Proteger la frase de contraseña del sistema
- Asegurarse de que el titular de la plataforma conoce la frase de contraseña del sistema
- Utilizar una cuenta diferente para cada usuario de la plataforma
- Utilizar nombres de cuenta únicos para cada proyecto
- Asegurarse de que el titular de la plataforma conoce las credenciales de la plataforma
- Utilizar una cuenta diferente para cada usuario de estación
- Usar cuentas de tipo de servicio único para cada proyecto
- Desactivar las cuentas conocidas cuando sea posible
- Configurar cuentas temporales para que caduquen automáticamente
- Cambiar las credenciales de las cuentas del sistema
- Rechazar las sesiones simultáneas cuando resulte adecuado
- Configurar funciones con permisos requeridos mínimos
- Asignar funciones requeridas mínimas a usuarios
- Utilizar el número mínimo posible de superusuarios
- Requerir permisos de superusuario para objetos de programa
- Utilizar los permisos requeridos mínimos para cuentas externas
- Utilizar un esquema de autenticación adecuado para el tipo de cuenta
- Eliminar los esquemas de autenticación innecesarios
- TLS y gestión de certificados
- Instalación de módulos
- Requerir robots y objetos de programa firmados
- Desactivar SSH y SFTP
- Desactivar servicios no necesarios
- Configurar de forma segura servicios necesarios
- Actualizar Niagara 4 a la última versión
- Instalar el producto en una ubicación segura
- Asegurarse de que las estaciones se encuentran tras una VPN

Existen publicaciones técnicas específicas que se deben seguir para garantizar que el sistema está bloqueado de la forma más segura posible. Existen muchas opciones, como el cifrado SSL, y pasos adicionales para proteger elementos, como módulos de programa. Para obtener más detalles, consulte el sitio web de Tridium para la Guía de mejora de la seguridad de Niagara 4 (para productos basados en Niagara N4) y la Guía de mejora de la seguridad de Niagara (productos basados en Niagara AX).

Honeywell Building Technologies

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

® Marca comercial registrada en EE. UU.
©2023 Honeywell International Inc.
31-00594-01 Rev. 07-23

22. LISTA DE COMPROBACIÓN DE SEGURIDAD DE LA INSTALACIÓN

Advanced Plant Controller Instancia de dispositivo: _____

Advanced Plant Controller Descripción: _____

Advanced Plant Controller Ubicación: _____

Instalador: _____

Complete las siguientes tareas de seguridad para cada Advanced Plant Controller instalado

- ☐ Instale un cortafuegos entre el Advanced Plant Controller y la red o redes externas. Consulte *«BACnet y Niagara» en la página 18.*
- ☐ Proteja físicamente el Advanced Plant Controller. Consulte *«Protección física del Advanced Plant Controller, el HMI y el módulo de E/S» en la página 20.*
- ☐ Cambie la contraseña predeterminada a una contraseña única para cada uno de los siguientes elementos: configuración de la consola, función de copia de seguridad, restauración, reinicio y control, y la plataforma Niagara. Consulte la Guía de instrucciones de instalación y puesta en servicio (31-00584)
- ☐ Si se necesita un servidor web, configúrelo para que funcione solo en modo HTTPS. Consulte la Guía de instrucciones de instalación y puesta en servicio (31-00584)

Estado del servidor web: activado/desactivado.

Si el servicio web está activado, haga lo siguiente:

- ☐ Configure Http Enabled = false.
- ☐ Configure Https Enabled = true.
- ☐ Configure Https Only = true.
- ☐ Configure el cortafuegos del BAS. Consulte *«Configuración del cortafuegos del BAS» en la página 24.*
- ☐ Proporcione todos los datos requeridos al titular del sistema BAS en la entrega. Consulte *«Configuración de la autenticación» en la página 25.*