Honeywell

Advanced

GUIDE DE SÉCURITÉ

Pourquoi sécuriser vos Advanced Controllers ? 5

Vue d'ensemble du système 6

- Internet/intranet/réseau d'entreprise 7
- Réseau BAS 7
- Pare-feu BAS 7
- Station de travail Niagara 4 7
- Commutateur Ethernet 7
- Advanced Plant Controller 7
- MMI 7
- Module E/S 7

Planification et sécurité des réseaux 8

- Réseau Ethernet 8
- Serveur Web 8
- Réseau IP BACnet 8
- MS/TP (licences NC) 8
- USB 8
- RS485 (y compris les licences Modbus) 8
- Réseau IP Modbus (licences INT) 8

Système de sécurité Advanced Controller, MMI et module E/S 9

- Sécurité lorsqu'elle n'est pas configurée 9
- Protection contre les appareils non autorisés 9
  - Code de vérification du compte 9
- Comptes système 9
  - Compte des systèmes d'ingénierie 9
    - Rôle ingénierie 10
    - Rôle administrateur 10
  - Compte système d'appareil 10
  - Création d'un compte système 10
- Gestion synchronisée des comptes 10
- Modification d'une clé réseau Advanced Controller 11
- Sécurité locale 11
- Accès à des pages Web 11
  - Accès initial 11
  - Utilisateurs connectés 12
- Récupération du mot de passe 12

Sécurisation du système d'exploitation Niagara 12

® Marque déposée aux États-Unis
Copyright © 2023 Honeywell Inc. • Tous droits réservés

Bonnes pratiques générales 12
Paramétrage de pare-feu 12
Version du système d'exploitation 12
Antivirus 12
Protection contre les intrusions 13
Règlement général sur la protection des données (RGPD) 13
Communication sécurisée 14
Relations client/serveur 14
Certificats 15
Certificats auto-signés 15
Convention d'affectation de noms 15
Magasins de certificats 16
Chiffrement 16
Vue d'ensemble du tableau de bord de sécurité 16
Planification et installation 17
Installation et configuration recommandées 17
BACnet uniquement 17
BACnet et Niagara 18
Recommandation relative aux réseaux locaux (LAN) 18
Documentation 19
Documenter les appareils physiques et les configurations, y compris les informations clés relatives à la sécurité 19
Documenter les systèmes externes, en particulier l'interaction entre l'Advanced Plant Controller et ses systèmes connexes 19
Contrôle d'accès et sécurité physique 20
Sécuriser physiquement l'Advanced Plant Controller, le MMI et les modules E/S 20
Autocollant sur le panneau d'accès ou le boîtier de l'automate 20
Séparer et protéger les réseaux 20
Sécurisation de l'Advanced Controller, du MMI et du module E/S 21
Identifiants du compte système d'administrateur fournis à l'utilisateur du site 21
Développement d'un programme de sécurité 21
Considérations physiques et environnementales 21
Mises à jour de sécurité et packs de maintenance 21
Utilisateurs et mots de passe 21
Utilisateurs 21
Mots de passe 22
Configuration d'un Advanced Plant Controller 23
Créer et gérer des configurations de base 23

Modifier les mots de passe par défaut 23
Autres considérations 23
Contrat de mise à jour 23
Configuration du réseau informatique 23
Configuration du pare-feu BAS 24
Configuration de l'authentification 25
Procédure 25
Livraison du système 25
Installation du logiciel de sauvegarde USB et du fichier CleanDist 25
Mise hors service du système 25
Sécurité des produits Advanced basés sur Niagara 26
Liste de contrôle de sécurité de l'installation 27

Clause de non-responsabilité

Malgré nos efforts déployés pour assurer l'exactitude de ce document, Honeywell n'est pas responsable des dommages de quelque nature que ce soit, y compris, sans s'y limiter, les dommages consécutifs découlant de l'application ou de l'utilisation des informations contenues dans ce document. Les informations et spécifications publiées ici sont à jour à la date de cette publication et sont sujettes à changement sans préavis. Les dernières spécifications de produits peuvent être trouvées sur notre site Web ou en contactant notre siège social à Atlanta, en Géorgie (États-Unis).

Pour de nombreuses communications industrielles basées sur RS-485, l'état par défaut est désactivé au moment de l'expédition départ usine afin de garantir la meilleure sécurité, d'une part car ces bus de communication hérités utilisent la technologie héritée pour la meilleure compatibilité et d'autre part car ils ont été conçus avec une protection de sécurité faible. Ainsi, pour maximiser la protection de votre système, Honeywell a désactivé de manière proactive les ports de communication des bus industriels hérités (au moment de l'expédition départ usine), et l'utilisateur doit activer explicitement les réseaux dans la station de chaque réseau. Si vous souhaitez activer ces ports, vous devez être conscient du risque de toute violation de la sécurité apportée par l'utilisation de la technologie héritée. Ceux-ci incluent, mais sans s'y limiter : Panel-bus, C-Bus, BACnet, M-Bus, CP-IO Bus, NovarNet, protocole XCM-LCD, SBC S-Bus et Modbus, etc.

Développement vers ISA-62443

Honeywell s'appuie sur la norme ISA 62443-4-1 depuis de nombreuses années et sur les normes complémentaires applicables pour développer nos produits de technologie du bâtiment en toute sécurité. Par exemple, les produits de bâtiments de Honeywell utilisent également ISA/CEI 62443-4-2 comme base pour les exigences de sécurité technique dans les composants, et nous utilisons ISA/CEI 62443-3-3 pour les systèmes complets. Ainsi, pour les intégrateurs et les clients qui choisissent les technologies du bâtiment, l'adhésion de Honeywell à la famille de normes ISA/CEI 62443 peut fournir un niveau élevé de confiance que nos produits ne prétendent pas seulement être cyber-résilients : ils ont dès le départ été conçus, testés et validés pour la cyber-résilience.

Honeywell développe nos produits selon la norme ISA/CEI 62443-4-1 et nous avons été évalués par une tierce partie et audités par rapport à cette norme.

Introduction et public visé

Honeywell déclare expressément par la présente que ses automates ne possèdent pas de protection intrinsèque contre les cyberattaques provenant d'Internet et sont donc destinés uniquement à être utilisés dans des réseaux privés. Cependant, même des réseaux privés peuvent toujours faire l'objet de cyberattaques malveillantes par des informaticiens qualifiés et équipés, et nécessitent donc une protection. Les clients doivent donc adopter les directives relatives aux meilleures pratiques d'installation et de sécurité pour les produits Advanced Plant Controller basés sur IP afin d'atténuer le risque posé par de telles attaques.

Les instructions suivantes décrivent les meilleures pratiques générales de sécurité pour les produits Advanced Plant Controllerbasés sur IP. Elles sont énumérées par ordre croissant d'atténuation.

Les besoins exacts de chaque site doivent être évalués au cas par cas. La grande majorité des installations mettant en œuvre tous les niveaux d'atténuation décrits ici dépasseront de loin ce qui est requis pour une sécurité satisfaisante du système. Intégrant les points 1 à 5 (relatifs aux réseaux locaux), Voir *"Recommandation relative aux réseaux locaux (LAN)" en page 18.* répondra généralement aux exigences de la plupart des installations de réseaux de contrôle d'automatisation.

Ce manuel contient des informations pour guider le personnel d'un concessionnaire Honeywell sur la façon d'installer et de configurer en toute sécurité un Advanced Plant Controller, des modules MMI et E/S. Vous trouverez des informations relatives à la sécurité sur le fonctionnement, la sauvegarde et la restauration USB et l'installation du fichier CleanDist de l'automate dans les instructions d'installation et le guide de mise en service (31-00584).

REMARQUE :

Veuillez prendre le temps de lire et de comprendre tous les manuels d'installation, de configuration et d'utilisation pertinents et assurez-vous d'obtenir régulièrement les dernières versions

.

Tableau 1 Informations sur le produit

Produit	Numéro de produit	Description
Automate d'installation	N-ADV-134-H	Niagara Advanced Controller avec quatre ports réseaux, port pour MMI et 4 ports RS485
	N-ADV-133-H	Niagara Advanced Controller avec quatre ports Ethernet, port pour MMI et 3 ports RS485
	N-ADV-112-H	Niagara Advanced Controller avec deux ports réseaux, port pour MMI et 2 ports RS485
MMI	HMI-DN	MMI avec montage sur rail DIN
	HMI-WL	Montage sur porte/mur
Module E/S	IO-16UIO-S-S	Module E/S 16UIO sans HOA, communications série, bornes à vis
	IOD-16UIO-S-S	Module E/S 16UIO avec écran HOA, communications série, vis Bornes
	IO-16UI-S-S	Module E/S 16UI, communications série, bornes à vis
	IO-16DI-S-S	Module E/S 16DI, communications série, bornes à vis
	IO-8DOR-S-S	Module E/S 8DO sans HOA, relais C/O, communications série, bornes à vis
	IOD-8DOR-S-S	Module E/S 8DO avec écran HOA, relais C/O, communications série, bornes à vis
	IO-16UIO-S-P	Module E/S 16UIO avec écran HOA, communications série, bornes push
	IO-16UI-S-P	Module E/S 16UIO, communications série, bornes push
	IO-16DI-S-P	Module E/S 16DI, communications série, bornes push
	IO-8DOR-S-P	Module E/S 8DO sans HOA, relais C/O, communications série, bornes push
	IOD-8DOR-S-P	Module E/S 8DO avec écran HOA, relais C/O, communications série, bornes push

1. POURQUOI SÉCURISER VOS ADVANCED CONTROLLERS ?

- Protégez les systèmes d'installations de vos clients contre les modifications non autorisées des points de consigne d'exploitation, des dérogations et des planifications.
- Empêcher l'accès aux détails du compte utilisateur : par exemple, noms d'utilisateur, mots de passe, adresses e-mail, numéros SMS (mobiles), etc.
- Prévenir l'accès aux données commercialement sensibles : Par exemple : mesures de consommation d'énergie, solutions de stratégie de contrôle spécialisées, etc.
- Empêcher l'accès non autorisé à l'automate, aux ordinateurs et aux réseaux hébergeant le logiciel BMS et les dispositifs de contrôle.
- Maintenir l'intégrité des données et assurer la responsabilisation.

2. VUE D'ENSEMBLE DU SYSTÈME

Vue d'ensemble de l'installation type du système.

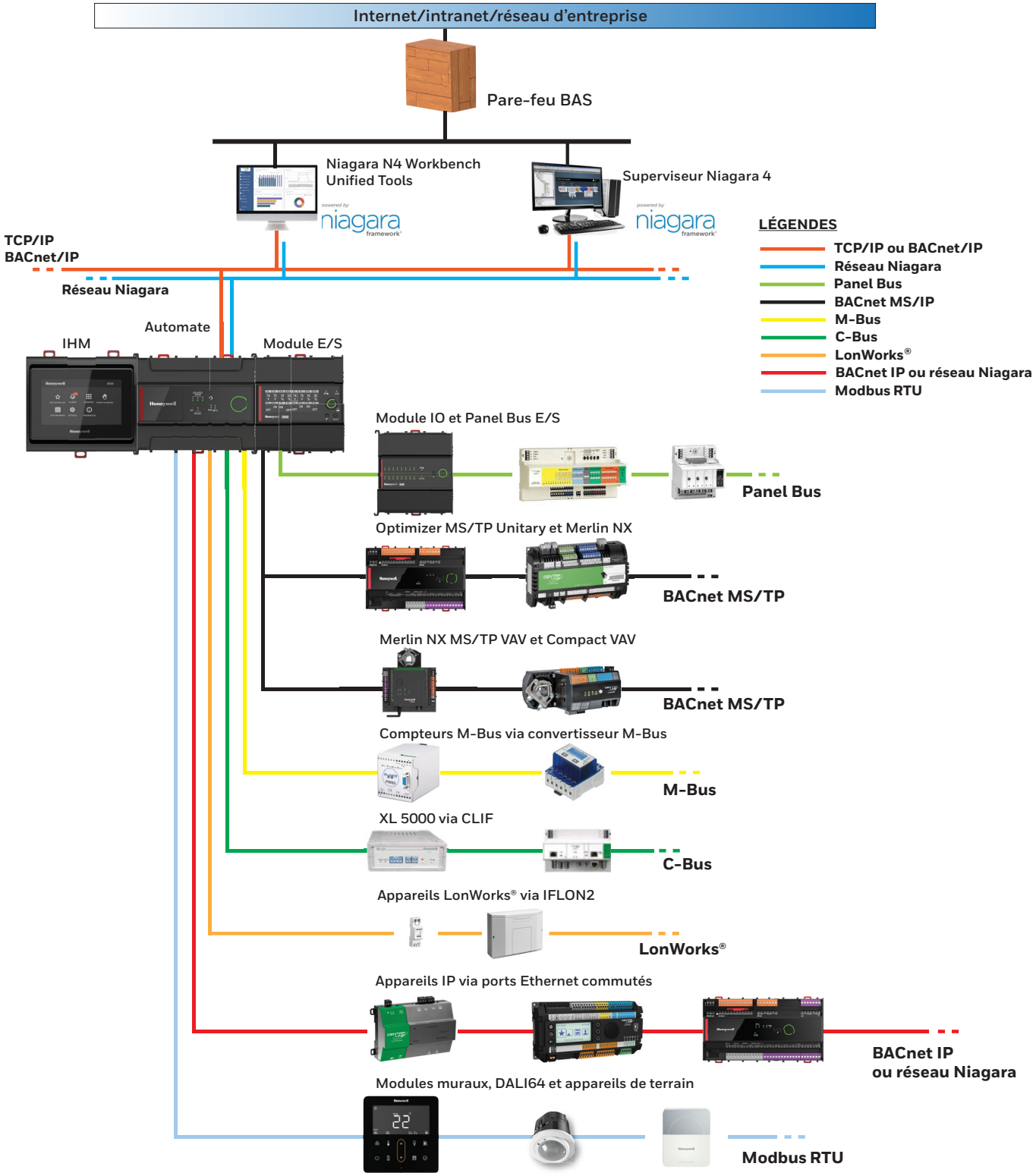

Fig. 1 Vue d'ensemble du système

2. 1 Internet/intranet/réseau d'entreprise

Il s'agit d'une représentation réseau simplifiée et logique de tous les réseaux en dehors de la portée du système d'automatisation des bâtiments (BAS). Il peut fournir un accès aux interfaces de gestion BAS (par exemple, l'interface utilisateur Web du poste de travail principal Niagara) mais doit fournir un accès à Internet pour que les ordinateurs Niagarapuissent rechercher et télécharger des mises à jour du système d'exploitation et des antivirus, à moins qu'un autre moyen de le faire ne soit fourni.

2. 2 Réseau BAS

Ce réseau est utilisé uniquement pour les protocoles BAS, qui se composent de BACnet/IP, BACnet/Ethernet et de tous les protocoles que les services d'intégration Niagara sur un Advanced Plant Controller peuvent utiliser. Ce réseau ne doit pas être le même réseau que le réseau Internet/intranet/entreprise.

2. 3 Pare-feu BAS

Pour fournir une séparation et une protection supplémentaires au BAS, un pare-feu doit être utilisé entre Internet/intranet/réseau d'entreprise et tout appareil BAS qui s'y connecte, tel que le poste de travail primaire Niagara, les stations de travail Niagara et l'Advanced Plant Controller.
Ce pare-feu limite l'accès au BAS aux seuls ordinateurs autorisés et peut contribuer à réduire le risque d'attaques, telles qu'une attaque par déni de service.

2. 4 Station de travail Niagara 4

Le poste de travail principal Niagara est un ordinateur exécutant le logiciel Niagara. Il nécessite deux connexions réseau : une pour se connecter à l'interface utilisateur Web de gestion via un navigateur Web (généralement sur le réseau Internet/intranet/entreprise) et une autre pour se connecter au réseau BAS.

2. 5 Commutateur Ethernet

Un commutateur Ethernet crée des réseaux et utilise plusieurs ports pour assurer la communication entre les appareils du réseau local. Les commutateurs Ethernet diffèrent des routeurs, qui connectent des réseaux et n'utilisent qu'un seul port LAN et WAN. Une infrastructure sans fil entièrement câblée et d'entreprise fournit une connectivité filaire et Wi-Fi pour une connectivité sans fil.

2. 6 Advanced Plant Controller

L'Advanced Plant Controller est un automate global qui se connecte à un réseau Ethernet, à BACnet IP et à des segments de réseau MS/TP hôtes. MS/TP est une connexion à faible bande passante utilisée pour connecter des automates et des capteurs.

2. 7 MMI

Le MMI est connecté et reçoit son alimentation depuis les Advanced Plant Controllers Niagara. Ces appareils sont construits avec un écran tactile capacitif prenant en charge une sélection au doigt nu et fournit à l'opérateur des fonctions pour visualiser les points d'automate, les modules E/S et autres équipements connectés, y accéder et les dépanner.

2. 8 Module E/S

Les modules E/S peuvent se connecter à l'automate à l'aide des connexions Touch Flake (alimentation et communications) ou les modules E/S peuvent se connecter à un adaptateur de câblage qui sera alimenté par l'une des interfaces RS485 de l'automate et y seront connectés. Les modules E/S sont programmables à l'aide de l'outil d'ingénierie existant tel que l'outil ComfortPoint Open Studio et Niagara 4 Workbench.

3. PLANIFICATION ET SÉCURITÉ DES RÉSEAUX

3. 1 Réseau Ethernet

Il est recommandé de séparer le réseau Ethernet utilisé par le système BMS du réseau bureautique normal.

Exemple :

Utilisation d'un air gap ou d'un réseau privé virtuel. L'accès physique à l'infrastructure du réseau Ethernet doit être restreint. Vous devez aussi vous assurer que l'installation est conforme à la politique informatique de votre entreprise.

Les Advanced Controllers ne doivent pas être connectés directement à Internet.

3. 2 Serveur Web

L'Advanced Controller fournit des serveurs Web HTTP et HTTPS. Si aucun serveur Web n'est requis, il est recommandé de désactiver les deux serveurs Web.

3. 3 Réseau IP BACnet

En raison de la nature non sécurisée du protocole BACnet, l'Advanced Controller, le MMI et les modules E/S qui utilisent BACnet ne doivent en aucun cas être connectés à Internet. Le système de sécurité Advanced Controller ne protège pas contre les écritures BACnet. L'accès physique à l'infrastructure du réseau BACnet IP doit être restreint. Si les communications IP BACnet ne sont pas requises, le module réseau Advanced Controller (BACnet IP) doit être désactivé en définissant le paramètre 'Disable Module' sur '1'.

Si des communications BACnet sont requises, il est fortement recommandé de ne pas activer les services BACnet Backup/ Restore, Reinitialize Device et BACnet Writable. Cependant, cela signifie que la stratégie créée n'est pas conforme à la norme BTL - Voir *"Sécurité locale" en page 11*.

3. 4 MS/TP (licences NC)

L'accès physique à l'infrastructure du réseau MS/TP doit être restreint. Si le réseau MS/TP n'est pas requis, le module réseau Advanced Controller (BACnet MSTP) doit être désactivé en définissant le paramètre 'Disable Module' sur '1'.

IO Bus (licences CAN)
L'accès physique au Bus E/S doit être restreint.

3. 5 USB

L'accès physique au port d'ingénierie local USB Advanced Controller doit être restreint.

3. 6 RS485 (y compris les licences Modbus)

L'accès physique au port RS485 de l'automate doit être restreint. Si cela n'est pas nécessaire, les modules réseau connectés au port ne doivent pas être inclus dans la stratégie.

3. 7 Réseau IP Modbus (licences INT)

En raison de la nature non sécurisée du protocole Modbus, les Advanced Controllers qui prennent en charge Modbus IP ne doivent en aucun cas être connectés à Internet. L'accès physique à l'infrastructure du réseau IP Modbus doit être restreint. Si les communications IP Modbus ne sont pas requises, le module réseau de l'Advanced Controller (Modbus IP) ne devrait pas être inclus dans la stratégie.

4. SYSTÈME DE SÉCURITÉ ADVANCED CONTROLLER, MMI ET MODULE E/S

La sécurité des Advanced Controllers est conforme à la norme ISA 62433-3-3 SL 3 et fournit un démarrage sécurisé, un réseau authentifié et chiffré, un chiffrement au repos et une gestion de compte synchronisée.

Pour accéder aux produits Advanced Controller ou effectuer l'une des tâches ci-dessus, un nom d'utilisateur et un mot de passe valides pour un compte de système d'ingénierie ou un compte de système d'appareil doivent être fournis.

4. 1 Sécurité lorsqu'elle n'est pas configurée

Pour interagir avec un Advanced Controller, un MMI et des modules E/S, des informations d'identification valides doivent être fournies. L'automate est fourni départ usine sans aucun identifiant (comptes système ou modules utilisateur), ce qui garantit sa protection contre tout accès non autorisé lors de sa première mise sous tension. Un compte système d'ingénierie avec le rôle d'administrateur doit être créé la première fois qu'une tentative de connexion à un vCNC est effectuée dans l'un des produits Advanced sur le réseau Niagara.

4. 2 Protection contre les appareils non autorisés

Une clé unique (clé réseau) est utilisée pour s'assurer que seuls les appareils autorisés peuvent rejoindre le réseau Niagara. Tous les automates qui doivent former un réseau Niagara doivent avoir la même clé réseau et le même port UDP. Ceux-ci sont configurés à l'aide d'IP Tool lors du processus de configuration initial.

Exemple :

Si quatre Advanced Plant Controllers ont la même clé réseau (112233), et un cinquième a une clé réseau différente (222). Lorsqu'ils sont connectés au même réseau Ethernet, les quatre automates avec la même clé réseau se rejoignent pour former un seul réseau, mais le cinquième automate ne pourra pas rejoindre le réseau car il a une clé réseau différente, c'est-à-dire (222).

De même, si le cinquième automate est neuf (tel qu'expédié depuis l'usine) et est ajouté au réseau Ethernet, il ne pourra pas se connecter au réseau Niagara car il n'a pas de clé réseau.

4. 2. 1 Code de vérification du compte

Lorsqu'un compte système d'administrateur est ajouté à l'un des automates du réseau, un code de vérification de compte est automatiquement généré par l'automate auquel le compte système a été ajouté. Ce code est synchronisé avec tous les autres automates avec la même clé réseau et le même port UDP sur le réseau Ethernet.

Une fois qu'un code de vérification de compte a été généré, TOUS les automates du réseau DOIVENT avoir le même code de vérification de compte ainsi que la même clé réseau et le même port UDP.

Exemple :

S'il y a cinq automates, tous les Advanced Controllers ont la même clé réseau. Quatre ont le même code de vérification de compte (AVC) et forment donc un réseau. Le cinquième a un code de vérification de compte différent et même s'il a la même clé réseau, il ne peut pas se joindre aux autres automates.

4. 3 Comptes système

Les comptes système permettent aux personnes et aux appareils d'interagir avec l'Advanced Controller. L'accès accordé dépend du type de compte et du rôle.

Il existe deux types de comptes système :

1. Compte des systèmes d'ingénierie
2. Compte système d'appareil

4. 3. 1 Compte des systèmes d'ingénierie

Les comptes des systèmes d'ingénierie sont destinés à être utilisés par des ingénieurs. Chaque compte système d'ingénierie a un nom de compte et un mot de passe qui doivent être fournis à la demande de l'automate. Si un nom d'utilisateur et un mot de passe valides sont fournis, l'automate accordera l'accès.

Un compte système d'ingénierie distinct doit être créé pour chaque personne. Les comptes de systèmes d'ingénierie peuvent être définis sur l'un des deux rôles suivants :

- Rôle ingénierie
- Rôle administrateur

Rôle ingénierie
Le rôle ingénierie fournit l'accès nécessaire à l'ingénierie de l'Advanced System, à la création/gestion des comptes système de l'appareil et à la gestion des détails du compte de l'utilisateur (adresse e-mail, mot de passe, etc.).

Rôle administrateur
Le rôle administrateur fournit le même accès que le rôle Ingénierie et la possibilité de gérer tous les comptes d'ingénierie et de système d'appareil.

4. 3. 2 Compte système d'appareil

Les comptes système d'appareils sont destinés à permettre aux appareils tels que Niagara de se connecter au réseau pour obtenir les informations requises et apporter des modifications. Il est recommandé de créer un compte système d'appareil distinct pour chaque appareil devant accéder au réseau. Ils ont un rôle de « superviseur ».

IMPORTANT :
Remarque importante : Le système de sécurité du superviseur doit être configuré pour restreindre les droits d'accès de chaque utilisateur superviseur.

4. 3. 3 Création d'un compte système

Un compte système d'ingénierie avec rôle d'administrateur doit être créé la première fois qu'une tentative de connexion à un vCNC est effectuée sur le réseau Niagara. Ce compte est ensuite synchronisé avec les autres automates du réseau Niagara

- Voir *"Gestion synchronisée des comptes" en page 10.* Des comptes supplémentaires peuvent être créés si nécessaire à l'aide de Niagara workbench.

REMARQUE :
La première fois qu'un compte système d'ingénierie est créé dans un automate, un code de vérification de compte est automatiquement généré et synchronisé avec les autres automates du réseau Ethernet avec la même clé réseau et le même port UDP. Lorsqu'un automate dispose d'un code de vérification de compte, il ne peut rejoindre un réseau qu'avec des automates qui ont le même code de vérification de compte - Voir *"Code de vérification du compte" en page 9.*

4. 4 Gestion synchronisée des comptes

La gestion synchronisée des comptes synchronise facilement et en toute sécurité les comptes système, y compris le code de vérification de compte, avec tous les Advanced Controllers sur le même réseau Niagara. Cela permet :

- Connexion unique pour le réseau
- Réduction des frais généraux liés à la configuration et à la maintenance de l'accès sur l'ensemble du site sans réduire la sécurité

Tous les Advanced Controllers du même réseau auront les mêmes comptes système.

Lorsqu'un Advanced Controller sans aucun compte système est connecté au réseau Ethernet et configuré avec la clé réseau et le port UDP pour le réseau Niagara, il rejoint le réseau et obtient automatiquement ses comptes système des autres automates du réseau Niagara.

Exemple :

si un Advanced Controller sans comptes système est ajouté au système ci-dessus et reçoit la clé réseau pour le réseau Niagara (112233) et le port UDP, il se joindra au réseau et obtiendra ses comptes système (utilisateur 1, utilisateur 2, utilisateur 3) auprès des autres Advanced Controllers sur le réseau Niagara.

Une fois la synchronisation terminée, il sera possible de se connecter à n'importe quel vCNC, d'afficher des pages Web et de se connecter à n'importe quel Advanced Controller sur le réseau Niagara en utilisant l'un des comptes système.

Si des modifications sont apportées aux comptes système, c'est-à-dire qu'un compte est ajouté, supprimé ou modifié, ces modifications seront automatiquement synchronisées dans tous les Advanced Controllers du réseau Niagara.

Exemple :

S'il y a cinq Advanced Controllers, les comptes système dans l'automate (1) sont modifiés pour supprimer l'utilisateur 2, renommez l'utilisateur 3 en utilisateur 3a et l'utilisateur 4 est ajouté, les modifications seront synchronisées avec l'automate (2), l'automate (3), l'automate (4) et l'automate (5).

REMARQUE :
Si un conflit est découvert au cours de la synchronisation, la dernière modification est prioritaire.

4. 5 Modification d'une clé réseau Advanced Controller

Lorsqu'une clé réseau Advanced Controller est modifiée, tous ses comptes système sont supprimés et elle est retirée de son réseau Niagara actuel. La modification de la clé réseau doit être autorisée par un compte système « ingénieur » ou « administrateur » valide.

Une fois la modification effectuée, il rejoindra un réseau Niagara à l'aide de la nouvelle clé réseau, le cas échéant, et obtiendra des comptes système de l'Advanced Controller sur le nouveau réseau Niagara à condition qu'il dispose du même port UDP.

4. 6 Sécurité locale

La sécurité locale utilise des utilisateurs locaux (modules utilisateur) pour permettre l'accès aux pages Web des Advanced Controllers ou à un affichage connecté localement et pour contrôler les informations visibles ou les valeurs pouvant être ajustées.

Pour obtenir un accès et apporter des modifications, il faut fournir un nom d'utilisateur et un mot de passe valides pour un utilisateur local. Le niveau de code PIN confidentiel de l'utilisateur détermine les paramètres qu'un utilisateur peut voir et ajuster.

REMARQUE :
Les utilisateurs locaux NE SONT PAS synchronisés avec d'autres Advanced Controllers sur le réseau Niagara.

4. 7 Accès à des pages Web

L'accès à des pages Web de l'automate est protégé par le système de sécurité de l'Advanced Controller. Lors de l'accès au serveur Web de l'automate, une page Web s'affiche qui fournit des informations de base et permet à un utilisateur de se connecter - Voir *"Accès initial" en page 11.*

Les utilisateurs qui se connectent seront traités comme des utilisateurs connectés - Voir *"Utilisateurs connectés" en page 12.* et les utilisateurs accédant à des pages Web sans se connecter recevront un accès conformément à la description dans *"Accès initial" en page 11*.

4. 7. 1 Accès initial

Lors du premier accès au serveur Web de l'automate, la page d'accueil affichée et l'accès accordé dépendent de la configuration de sécurité actuelle de l'automate :

- Aucun compte système d'ingénierie et aucun module utilisateur (paramètres d'usine par défaut)
  La page de bienvenue 'Welcome' s'affiche et un accès complet aux pages Web de l'automate et la possibilité d'apporter des modifications seront donnés.

REMARQUE :
Comme il n'existe pas de comptes système d'ingénierie ou de modules utilisateur, il ne sera pas possible de se connecter.

- Comptes de système d'ingénierie et aucun module utilisateur
  La page de bienvenue 'Welcome' s'affiche et l'automate ne donnera accès qu'au capteur, à l'entrée numérique, au bouton, au commutateur, au pilote, à la planification, à l'heure, aux modules de traçage, au journal d'alarmes et aux graphiques et n'autorisera pas les modifications.

REMARQUE :
Il sera possible de se connecter en utilisant les comptes du système d'ingénierie.

- Comptes des systèmes d'ingénierie et modules utilisateur
  L'affichage initial et l'accès sont contrôlés par les modules d'utilisateur. S'il existe un module d'utilisateur appelé 'Guest' (invité) sans mot de passe lorsque les pages Web de l'Advanced Controller sont consultées sans connexion, l'automate donnera les droits d'accès (niveau utilisateur, page d'accueil et valeurs par défaut) spécifiés par le module d'utilisateur 'Guest'.

  Par défaut, le module d'utilisateur invité 'Guest' ne donne accès qu'à la page 'Welcome' de l'Advanced Controller et a un niveau utilisateur de '0'. Cela signifie qu'un utilisateur accédant à l'automate sans se connecter ne pourra afficher que la page 'Welcome'. Afin de donner plus d'accès, l'utilisateur invité 'Guest' peut être configuré de la même manière que n'importe quel autre module d'utilisateur de type 0.

REMARQUE :
Le Niagara workbench empêche l'utilisateur invité 'Guest' de recevoir un mot de passe, un code PIN ou un niveau utilisateur supérieur à '0'. Il permet de configurer une page d'accueil et des valeurs d'affichage par défaut.

Il est fortement recommandé que l'utilisateur invité conserve la configuration par défaut (niveau utilisateur '0' et aucun droit d'affichage).

S'il n'existe pas de module d'utilisateur appelé 'Guest' ou s'il a été configuré avec un mot de passe, la page de bienvenue 'Welcome' s'affiche et l'automate ne donnera accès qu'au capteur, à l'entrée numérique, au bouton, au commutateur, au pilote, à la planification, à l'heure, aux modules de traçage, au journal d'alarmes et aux graphiques et n'autorisera pas les modifications.

REMARQUE :
Il sera possible de se connecter à l'aide des comptes système « ingénierie » et de tous les modules d'utilisateur existants.

4. 7. 2 Utilisateurs connectés

Pour ouvrir une session dans une page Web de l'Advanced Controller, il faut entrer un nom d'utilisateur et un mot de passe correspondant à l'un des comptes système « ingénierie » de l'Advanced Controller ou à l'un des modules d'utilisateur de type 0.

4. 8 Récupération du mot de passe

Si un utilisateur a oublié son mot de passe, il peut être récupéré en utilisant le Niagara workbench. Pour plus de détails sur la récupération d'un mot de passe oublié à l'aide de Niagara, consultez le guide de l'utilisateur Niagara workbench.

5. SÉCURISATION DU SYSTÈME D'EXPLOITATION NIAGARA

5. 0. 1 Bonnes pratiques générales

Suivez les bonnes pratiques générales pour sécuriser le système d'exploitation, telles que :

- Économiseur d'écran protégé par mot de passe
- Logiciel de chiffrement de disque

5. 0. 2 Paramétrage de pare-feu

Le système d'exploitation doit être configuré pour utiliser un pare-feu automatiquement mis à jour. La configuration doit empêcher l'accès (IN/OUT) pour tous les ports, sauf ceux pour lesquels un accès est requis ; NE LAISSEZ PAS les ports inutilisés ouverts.

5. 0. 3 Version du système d'exploitation

Vous DEVEZ vous assurer que les dernières mises à jour du système d'exploitation sont installées sur tout appareil exécutant des applications Niagara ou connecté au même réseau IP. Il est indiqué de s'assurer que les mises à jour Windows sont laissées en mode automatique et qu'elles sont installées en temps opportun.

5. 0. 4 Antivirus

Vous DEVEZ vous assurer que tous les ordinateurs exécutant les applications Niagara ou connectés au même réseau IP exécutent un logiciel de protection antivirus et que les définitions de virus sont tenues à jour.

5. 0. 5 Protection contre les intrusions

Il est recommandé d'utiliser un système de détection d'intrusion (IDS) d'un fournisseur de produits de sécurité réputé sur tout ordinateur exécutant l'application Niagara. Suivez les meilleures pratiques pour les produits choisis ainsi que toute stratégie informatique d'entreprise où l'installation est effectuée.

De nombreux produits IDS et pare-feu offrent une solution complète pour enregistrer la totalité du trafic entrant et sortant de l'ordinateur, offrant aux utilisateurs la possibilité d'enregistrer toutes les activités au niveau le plus bas.

6. RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Le règlement général sur la protection des données (UE) 2016/679 (RGPD) est un règlement de l'UE sur la protection des données et de la vie privée pour tous les citoyens de l'Union européenne (UE) et de l'Espace économique européen (EEE). Il traite également du transfert de données à caractère personnel en dehors des zones de l'UE et de l'EEE. Le RGPD contient des dispositions et des exigences relatives au traitement des données à caractère personnel des personnes (personnes concernées) au sein de l'EEE et s'applique à toute entreprise établie dans l'EEE (indépendamment de son emplacement et de la citoyenneté des personnes concernées) ou qui traite les informations à caractère personnel des personnes concernées au sein de l'EEE.

Selon les termes du RGPD, les données à caractère personnel comprennent toute information pouvant être utilisée pour identifier un individu. Cela inclut les éléments suivants (mais sans s'y limiter) :

- noms d'utilisateur,
- mots de passe,
- numéros de téléphone,
- adresses e-mail,
- adresses professionnelles ou résidentielles.

Toute information de ce type saisie dans l'Advanced Controller, le MMI et le module E/S est chiffrée et stockée sur les produits Advanced dans les locaux du client. Honeywell n'a aucune implication dans le stockage et/ou le traitement des données à caractère personnel dans les produits Advanced de Honeywell.

La responsabilité de la conformité aux exigences du RGPD incombe entièrement à l'intégrateur système ou à l'administrateur système et, à ce titre, il doit s'assurer que des systèmes techniques et organisationnels adéquats sont en place pour :

- obtenir le consentement explicite de chaque personne concernée pour que les données à caractère personnel soient stockées, utilisées et/ou traitées,
- permettre aux personnes d'avoir accès à leurs données à caractère personnel afin d'en vérifier l'exactitude,
- permettre aux personnes de retirer leur consentement à tout moment et de faire effacer définitivement leurs données à caractère personnel,
- maintenir à tout moment la sécurité et l'intégrité du stockage et de l'accès aux données,
- signaler toute violation de la sécurité des données (susceptible d'affecter la vie privée de l'utilisateur) à l'autorité compétente dans les 72 heures suivant la violation.

7. COMMUNICATION SÉCURISÉE

Une infrastructure à clé publique (PKI) prend en charge la distribution et l'identification des clés de chiffrement publiques utilisées pour protéger l'échange de données sur les réseaux, tels qu'Internet. La PKI vérifie l'identité de l'autre partie et encode la transmission réelle des données. La vérification de l'identité fournit une assurance non répudiée de l'identité du serveur. Le chiffrement assure la confidentialité pendant la transmission réseau. L'exigence de modules de code signés garantit que seul le code attendu s'exécute dans le système.

Pour fournir des réseaux sécurisés à l'aide de PKI, Niagara prend en charge le protocole TLS (Transport Layer Security), versions 1.0, 1.1 et 1.2. TLS remplace son prédécesseur, SSL (Secure Sockets Layer).

Chaque installation Niagara crée automatiquement un certificat par défaut, ce qui permet de chiffrer immédiatement la connexion. Cependant, ces certificats génèrent des avertissements dans le navigateur et Workbench et ne conviennent généralement pas aux utilisateurs finaux. La création et la signature de certificats numériques personnalisés permettent une utilisation transparente de TLS dans le navigateur et fournissent à la fois le chiffrement et l'authentification du serveur.

Au-delà de la sécurité des communications, chaque module de code informatique qui s'exécute dans le système est protégé par une signature numérique. Les objets de programme ajoutés nécessitent cette signature, sans quoi ils ne s'exécutent pas.

La vérification du serveur, le chiffrement de la transmission et la garantie que seul le code signé s'exécute ne sécurisent pas les données stockées sur un appareil de stockage. Vous devez toujours restreindre l'accès physique aux ordinateurs et aux automates qui gèrent votre modèle de bâtiment, configurer l'authentification des utilisateurs avec des mots de passe forts et sécuriser les composants en contrôlant les autorisations.

Niagara prend en charge et utilise la communication sécurisée et le code signé par défaut. Vous n'avez pas besoin d'acheter une licence supplémentaire.

La sécurité est une préoccupation constante. Bien que vous trouviez beaucoup d'informations précieuses dans les rubriques de communication sécurisée, attendez-vous à des mises à jour et des changements futurs.

Vous trouverez ci-dessous les communications sécurisées. Pour plus de détails, référez-vous au Guide de sécurité de la station Niagara.

- Relations client/serveur
- Certificats
- Magasins de certificats
- Structure des dossiers CSR
- Configuration du certificat
- Assistant Certificat
- Signature de plusieurs certificats
- Configuration de la communication sécurisée sur la plateforme
- Configuration de la communication sécurisée de la station
- Activation des clients et configuration pour le port correct
- Installation d'une copie de station sur une autre plateforme
- Sécurisation des e-mails
- Résolution des problèmes de communication sécurisée

7. 1 Relations client/serveur

Les relations client/serveur identifient les connexions qui nécessitent une protection.Les relations client/serveur Workbench varient en fonction de la façon dont vous configurez et utilisez un système. Workbench est toujours un client. Une plateforme est toujours un serveur. Une station peut être un client et un serveur.

Les protocoles système qui gèrent les communications sont les suivants :

- Les connexions de plateforme depuis Workbench (client) à l'automate ou au démon de plateforme PC superviseur (serveur) utilisent Niagara. Une connexion sécurisée à une plateforme est parfois appelée platformtls. Vous activez platformtls à l'aide de la vue d'administration de plateforme.
- Les connexions des stations locales (superviseur et plateforme) utilisent Foxs. Vous activez ces connexions dans le FoxService d'une station (Config > Services > FoxService).
- Les connexions de navigateur utilisent Https, ainsi que Foxs si vous utilisez Web Launcher avec un WbWebProfile. Vous activez ces connexions à l'aide du WebService de la station (Config > Services > WebService).
- Connexions client au serveur de courriel de la station, le cas échéant. Vous activez la messagerie sécurisée à l'aide de l'EmailService de la station (Config > Services > EmailService).

8. CERTIFICATS

Un certificat est un document électronique qui utilise une signature numérique pour lier une clé publique à une personne ou une organisation. Les certificats peuvent servir à diverses fins selon la façon dont vous configurez la propriété « usage clé» du certificat. Leur objectif principal dans ce système est de vérifier l'identité d'un serveur afin que la communication puisse être digne de confiance. Pour plus de détails, veuillez consulter le Guide de sécurité de la station Niagara - Certificat.

Niagara prend en charge les types de certificats suivants :

- Un certificat **CA** (Autorité de certification) est un certificat auto-signé qui appartient à une autorité de certification. Il peut s'agir d'un tiers ou d'une société agissant en tant que sa propre autorité de certification.
- Un **certificat d'autorité de certification racine** est un certificat d'autorité de certification auto-signé dont la clé privée est utilisée pour signer d'autres certificats, créant une arborescence de certificats approuvés. Avec sa clé privée, un certificat d'autorité de certification racine peut être exporté, stocké sur une clé USB dans un coffre-fort et sorti uniquement lorsque les certificats doivent être signés. La clé privée d'un certificat d'autorité de certification racine nécessite la création d'un mot de passe lors de l'exportation et la fourniture du même mot de passe lorsque vous l'utilisez pour signer d'autres certificats.
- Un **certificat intermédiaire** est un certificat d'autorité de certification signé par un certificat délivré par une autorité de certification racine qui est utilisé pour signer des certificats de serveur ou d'autres certificats d'autorité de certification intermédiaires. L'utilisation de certificats intermédiaires isole un groupe de certificats de serveur.
- Un **certificat de serveur** représente le côté serveur d'une connexion sécurisée. Bien que vous puissiez configurer un certificat distinct pour chaque protocole (Foxs, Https, Webs). Bien que vous puissiez configurer une plateforme et une station (en tant que serveur) avec des certificats de serveur distincts, pour plus de simplicité, la plupart des systèmes utilisent généralement le même certificat de serveur.
- Un **certificat de signature de code** est un certificat utilisé pour signer des objets de programme et des modules. Les intégrateurs systèmes utilisent ce certificat pour empêcher l'introduction de code malveillant lorsqu'ils personnalisent l'infrastructure.

8. 1 Certificats auto-signés

Un certificat auto-signé est un certificat signé par défaut à l'aide de sa propre clé privée plutôt que par la clé privée d'un certificat d'autorité de certification (CA) racine.

Le système prend en charge deux types de certificats auto-signés :

- Un **certificat d'autorité de certification racine** est implicitement approuvé car il n'existe pas d'autorité supérieure à l'autorité de certification (CA) à être propriétaire de ce certificat. Pour cette raison, les autorités de certification, dont l'activité consiste à approuver les certificats d'autres personnes, protègent étroitement leurs certificats d'autorité de certification racine et leurs clés privées. De même, si votre société fait office de sa propre autorité de certification, vous devez protéger étroitement le certificat d'autorité de certification racine que vous utilisez pour signer d'autres certificats.
- Un **certificat par défaut**, **auto-signé** : La première fois que vous démarrez une instance de Workbench, une plateforme ou une station après l'installation (mise en service), le système crée un certificat de serveur auto-signé par défaut avec l'alias de tridium.

REMARQUE :

N'exportez pas ce certificat et importez-le dans un magasin d'une autre plateforme ou station. Bien que cela soit possible, cela diminue la sécurité et augmente la vulnérabilité.

Pour minimiser le risque d'attaque de l'intercepteur lors de l'utilisation de certificats auto-signés, toutes vos plateformes doivent être contenues dans un réseau privé sécurisé, hors ligne et sans accès public depuis Internet.

⚠ ATTENTION

Pour utiliser des certificats auto-signés, avant d'accéder à la plateforme ou à la station à partir de Workbench pour la première fois, assurez-vous que votre ordinateur et la plateforme ne sont pas sur un réseau d'entreprise ou sur Internet. Une fois déconnecté, connectez l'ordinateur directement à la plateforme, ouvrez la plateforme à partir de Workbench et approuvez son certificat auto-signé. Ce n'est qu'alors que vous devez reconnecter la plateforme à un réseau d'entreprise.

8. 2 Convention d'affectation de noms

Le **magasin de clés de l'utilisateur**, le **magasin de confiance de l'utilisateur**, et le **magasin de confiance du système** forment le cœur de la configuration. Les certificats se ressemblent beaucoup et les différents certificats auto-signés par défaut portent le même nom.

8. 3 Magasins de certificats

La gestion de certificats utilise quatre magasins pour gérer les certificats : un **magasin de clés de l'utilisateur**, un **magasin de confiance du système**, un **magasin de confiance de l'utilisateur** et une liste des **hôtes autorisés**.

Le **magasin de clés de l'utilisateur** est associé au côté serveur de la relation client-serveur. Ce magasin contient des certificats, chacun avec ses clés publiques et privées. En outre, ce magasin contient le certificat auto-signé initialement créé lorsque vous avez lancé Workbench ou démarré la plateforme pour la première fois.

Les **magasins de confiance de l'utilisateur** et les **magasins de confiance du système** sont associés au côté client de la relation client-serveur. Le magasin de confiance du système est prérempli avec des certificats publics standard : certificats d'autorité de certification racines provenant d'autorités de certification bien connues, telles que VeriSign, Thawte et Digicert. Le **magasin de confiance de l'utilisateur** contient des certificats d'autorité de certification racine et intermédiaires pour les sociétés qui servent de propre autorité de certification.

La liste **Hôtes autorisés** contient un ou plusieurs certificat de serveur pour lesquels il n'existe aucun certificat racine approuvé dans le **magasin de confiance du système** ou **le magasin de confiance de l'utilisateur**, mais les certificat de serveur ont quand même été approuvés pour l'utilisation. Cela inclut les serveurs pour lesquels le nom d'hôte du serveur n'est pas le même que le nom commun dans le certificat de serveur. Vous approuvez l'utilisation de ces certificats sur une base individuelle. Bien que la communication soit sécurisée, il est préférable d'utiliser des certificats de serveur signés.

8. 4 Chiffrement

Le cryptage est le processus de codage de la transmission de données afin qu'elles ne puissent pas être lues par des tiers non approuvés. TLS utilise le chiffrement pour transmettre des données entre le client et le serveur. Bien qu'il soit possible d'établir une connexion non chiffrée en utilisant uniquement les protocoles fox ou http, nous vous encourageons fortement à ne pas poursuivre cette option. Sans chiffrement, vos communications sont potentiellement sujettes à une attaque. Acceptez toujours les connexions Foxs ou Https par défaut.

9. VUE D'ENSEMBLE DU TABLEAU DE BORD DE SÉCURITÉ

Dans Niagara 4.u5 et versions ultérieures, la fonctionnalité de tableau de bord de sécurité (Security Dashboard) fournit (pour les administrateurs et autres utilisateurs autorisés) une vue d'ensemble de la configuration de sécurité de votre station. Cela vous permet de surveiller facilement la configuration de sécurité dans de nombreux services de la station et d'identifier les faiblesses de configuration de sécurité sur la station.

⚠ ATTENTION

La vue de tableau de bord de sécurité peut ne pas afficher tous les paramètres de sécurité possibles et ne doit pas être considérée comme une garantie que tout est configuré de manière sûre. En particulier, les modules tiers peuvent avoir des paramètres de sécurité qui ne s'enregistrent pas dans le tableau de bord.

La vue de tableau de bord de sécurité est la vue principale du SecurityService de la station. La vue vous avertit des faiblesses de sécurité telles que les mauvais paramètres de mot de passe fort ; certificats expirés, auto-signés ou non valides ; protocoles de transport non chiffrés, etc., indiquant des zones où la configuration devrait être plus sécurisée. Les autres données rapportées incluent : l'intégrité du système, le nombre de comptes actifs, les comptes inactifs, le nombre de comptes avec des autorisations de super-utilisateur, etc. En option, l'attribut « system » de la fonctionnalité de licence « securityDashboard » peut être défini sur « true » pour activer la vue système de la station fournissant des détails de sécurité pour chaque station subordonnée dans NiagaraNetwork.

Le tableau de bord de sécurité est la vue principale des services de sécurité. Pour plus de détails sur la vue, reportez-vous à « nss-SecurityDashboardView » dans le Guide de sécurité de la station Niagara.

10. PLANIFICATION ET INSTALLATION

Cette section contient des informations sur la planification et l'exécution d'une installation d'Advanced Plant Controller.

10. 1 Installation et configuration recommandées

La section suivante illustre deux configurations d'installation recommandées.

- BACnet uniquement
- BACnet et Niagara

10. 1. 1 BACnet uniquement

Lorsque l'Advanced Plant Controller n'est utilisé que pour les communications BACnet, connectez uniquement Ethernet 1 au réseau BAS où BACnet (BACnet/IP ou BACnet/Ethernet) sera exécuté.

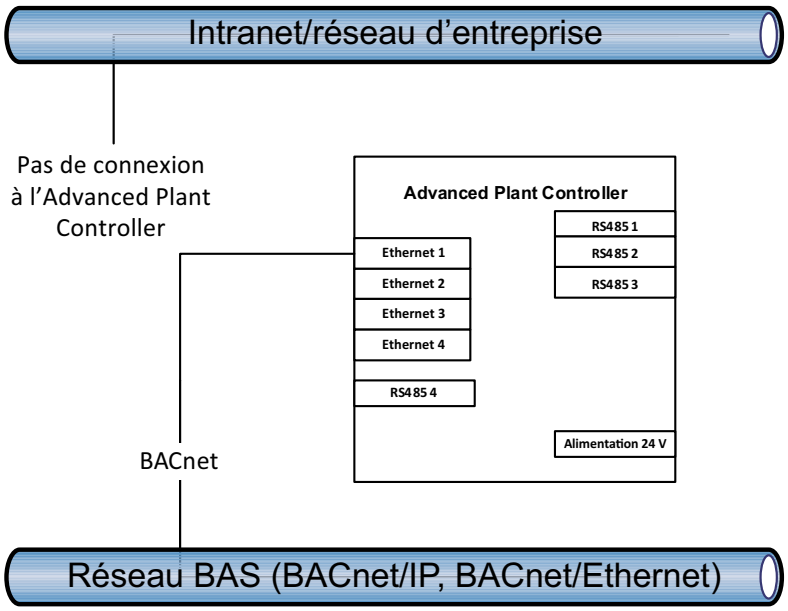

Fig. 2 Connexion BACnet

10. 1. 2 BACnet et Niagara

Lorsque Niagara est utilisé sur l'Advanced Plant Controller, il peut être configuré pour fournir des services, tels que des services Web ou Niagara FOXS, au réseau Internet/intranet/d'entreprise. Si tel est le cas, connectez Ethernet 2 au réseau Internet/intranet/d'entreprise via le pare-feu BAS pour fournir des services à ce réseau.

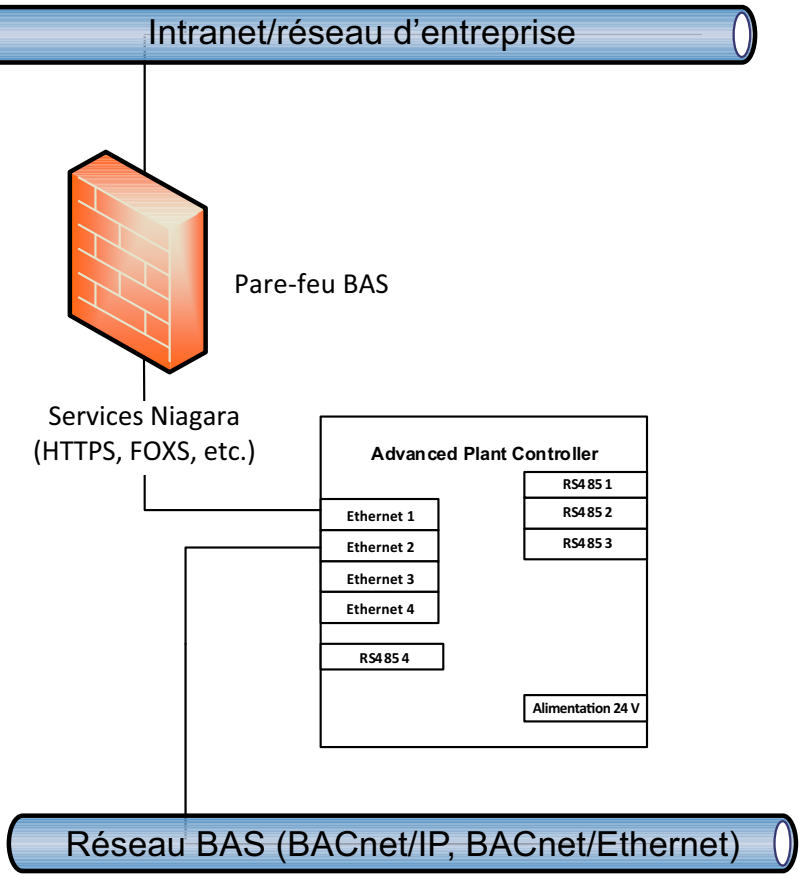

Fig. 3 Connexions BACnet et Niagara

10. 2 Recommandation relative aux réseaux locaux (LAN)

Assurez-vous que les systèmes fonctionnent selon une stratégie de mot de passe appropriée pour l'accès des utilisateurs à tous les services. Cette ligne directrice comprendrait, sans toutefois s'y limiter :

1. L'utilisation de mots de passe forts.
2. Une durée de cycle recommandée du mot de passe.
3. Des identifiants et mots de passe uniques pour chaque utilisateur du système.
4. Des règles de divulgation des mots de passe.
5. Si l'accès à distance aux systèmes de contrôle des bâtiments basés sur les TI est nécessaire, utilisez la technologie VPN (Virtual Private Network) pour réduire le risque d'interception des données et protéger les appareils de contrôle contre le placement direct sur Internet.

11. DOCUMENTATION

La documentation est essentielle pour saisir les informations de conception et de configuration nécessaires au maintien d'un système sécurisé.

11. 1 Documenter les appareils physiques et les configurations, y compris les informations clés relatives à la sécurité

Toute la documentation sur les appareils et les configurations doit inclure des informations relatives à la sécurité pour établir et maintenir les contrôles de sécurité prévus. Par exemple, si des modifications sont apportées aux services ou aux ports par défaut sur l'Advanced Plant Controller, documentez-les clairement afin que les paramètres puissent être restaurés ultérieurement.

11. 2 Documenter les systèmes externes, en particulier l'interaction entre l'Advanced Plant Controller et ses systèmes connexes

Le BAS nécessite ou utilise généralement des systèmes externes pour des raisons fonctionnelles, telles que l'infrastructure réseau existante, l'accès VPN, les hôtes de machines virtuelles et les pare-feu. Si le système BAS exige que ces systèmes soient configurés d'une certaine manière pour la sécurité, par exemple avec un pare-feu autorisant ou interdisant certains ports ou un réseau autorisant l'accès à certains systèmes, vous devez documenter ces informations. Si ces systèmes doivent être restaurés ultérieurement, **par exemple** : suite à une panne d'équipement, ou si des systèmes externes doivent subir des modifications, **par exemple :** mise à niveau d'un pare-feu, alors le fait d'avoir documenté ces informations, vous aidera à restaurer le niveau de sécurité précédent.

12. CONTRÔLE D'ACCÈS ET SÉCURITÉ PHYSIQUE

Le contrôle d'accès consiste à spécifier et à limiter l'accès aux appareils ou aux fonctions aux utilisateurs autorisés uniquement.

12. 1 Sécuriser physiquement l'Advanced Plant Controller, le MMI et les modules E/S

Empêcher l'accès non autorisé à l'équipement réseau utilisé conjointement avec les systèmes fournis par Honeywell. Quel que soit le système, évitez tout accès physique au réseau et aux équipement afin de réduire le risque d'interférences non autorisées. Les bonnes pratiques de sécurité concernant les installations informatiques demandent que les salles de serveurs, panneaux de brassage et équipements informatiques soient installés dans des locaux fermés à clé. L'équipement Honeywell doit être installé dans des armoires de contrôle verrouillées, elles-mêmes situées dans des locaux techniques sécurisés.

12. 2 Autocollant sur le panneau d'accès ou le boîtier de l'automate

Apposez un autocollant d'inviolabilité sur l'Advanced Plant Controller, le MMI et le panneau d'accès ou boîtier du module E/S

Si un client a besoin d'une assurance supplémentaire que l'accès physique protégeant un Advanced Plant Controller, un MMI et un module E/S n'a pas subi d'intrusion, installez un scellé ou un autocollant d'inviolabilité sur le point d'accès.

12. 3 Séparer et protéger les réseaux

1. Utilisez un pare-feu entre le réseau Internet/intranet/d'entreprise et le BAS.
2. Utilisez un réseau physique dédié distinct (fils séparés) ou un réseau virtuel (VLAN) pour la communication BACnet. Il doit s'agir d'un réseau distinct du réseau Internet/intranet/d'entreprise.
3. Ne connectez pas EN2 sur l'Advanced Plant Controller à un réseau, sauf si vous avez besoin de services Niagara (plateforme, station et/ou serveur Web).
   Si vous avez besoin de connecter EN2 au réseau Internet/intranet/d'entreprise , vous devez ensuite utiliser un pare-feu BAS externe entre l'Advanced Plant Controller et le réseau Internet/intranet/d'entreprise.

13. SÉCURISATION DE L'ADVANCED CONTROLLER, DU MMI ET DU MODULE E/S

13. 1 Identifiants du compte système d'administrateur fournis à l'utilisateur du site

Les identifiants du compte système 'Admin' doivent être fournis au propriétaire du site pour lui permettre de gérer les comptes système.

13. 2 Développement d'un programme de sécurité

Reportez-vous aux « Meilleures pratiques générales en matière de sécurité »

13. 3 Considérations physiques et environnementales

L'Advanced Controller, le MMI et le module E/S doivent être installés dans un environnement verrouillé, par exemple situé dans un local technique sécurisé ou une armoire verrouillée.

REMARQUE :
Veillez à ce que l'emplacement soit ventilé correctement.

13. 4 Mises à jour de sécurité et packs de maintenance

Assurez-vous que l'Advanced Controller, le MMI et le module E/S exécute la dernière version du firmware.

14. UTILISATEURS ET MOTS DE PASSE

14. 1 Utilisateurs

Assurez-vous que le nombre d'utilisateurs et les niveaux d'accès fournis sont appropriés pour les activités qu'ils doivent effectuer.

- **Au niveau de l'appareil de l'automate, configurez les comptes système ou les utilisateurs dans les automates pour le client Web, le superviseur et l'accès peer-to-peer.**

  Configuration des modules utilisateur dans les Advanced Controllers, cela signifie qu'un utilisateur devra se connecter à un appareil avec des identifiants valides avant que des ajustements puissent être effectués. Assurez-vous que les droits d'accès appropriés sont attribués aux comptes système et aux utilisateurs.

- **Utiliser un compte différent pour chaque utilisateur**

  Utilisez des noms et des mots de passe uniques pour chaque utilisateur/compte sur le système, plutôt qu'un accès générique. Des personnes différentes ne devraient jamais partager le même compte. Par exemple, plutôt qu'un compte « gestionnaires » général que plusieurs gestionnaires pourraient utiliser, chaque gestionnaire devrait avoir son propre compte distinct.

Il existe de nombreuses raisons pour chaque utilisateur d'avoir son propre compte individuel :

- Si chaque personne a son propre compte, les journaux d'audit seront plus informatifs. Il sera facile de déterminer exactement quel utilisateur a fait quoi. Cela peut aider à détecter si un compte a été compromis.

REMARQUE :
Tous les produits ne disposent pas d'un système de journal d'audit, mais lorsqu'il est disponible, il ne doit pas être désactivé.

- Si un compte est supprimé ou modifié, cela ne gêne pas beaucoup de gens. Par exemple, si une personne ne doit plus avoir accès au compte, la suppression de son accès individuel est simple. S'il s'agit d'un compte partagé, les seules options sont de changer le mot de passe et d'avertir tout le monde, ou de supprimer le compte et d'avertir tout le monde. Laisser le compte tel quel n'est pas une option : l'objectif est de révoquer l'accès.
- Si chaque personne a son propre compte, il est beaucoup plus facile d'adapter les autorisations pour répondre précisément à ses besoins. Avec un compte partagé, les personnes risquent d'avoir plus d'autorisations qu'elles ne le devraient.

  - Un compte partagé signifie un mot de passe partagé. Le partage des mots de passe est une très mauvaise pratique en matière de sécurité. Cela rend beaucoup plus probable la fuite du mot de passe et rend plus difficile la mise en œuvre de certaines meilleures pratiques de mot de passe, telles que l'expiration du mot de passe.

- **Utilisation d'utilisateurs d'ingénierie uniques pour les projets**

  L'utilisation des mêmes détails de compte sur chaque projet est une pratique courante de certaines entreprises. Une fois que cela est connu, si un système est compromis, l'attaquant pourrait potentiellement avoir des informations d'identification pour accéder à de nombreux autres projets installés par la même entreprise.

- **Désactiver les comptes connus lorsque cela est possible**

  Certains produits ont des comptes par défaut. Ceux-ci doivent être configurés de sorte que le mot de passe ne soit plus le mot de passe par défaut.

- **Attribuer aux utilisateurs seulement les autorisations strictement nécessaires**

  Assurez-vous que seuls les comptes requis sont configurés sur le système avec seulement les niveaux de sécurité minimum requis, plutôt qu'un accès complet. Lors de la création d'un nouveau compte, réfléchissez à ce que la personne doit faire dans le système, puis attribuez des autorisations minimales requises pour effectuer ce travail. Par exemple, une personne qui a seulement besoin de voir des alarmes n'a pas besoin d'un accès administrateur. Accorder des autorisations qui ne sont pas requises augmente le risque d'une violation de la sécurité. L'utilisateur peut modifier par inadvertance (ou délibérément) des paramètres qu'il n'a pas à modifier.

- **Utiliser le nombre minimal possible de comptes d'administrateur système**

  N'attribuez des autorisations aux administrateurs système qu'en cas d'absolue nécessité. En permettant un accès complet à tout, ce type de compte est extrêmement puissant. L'accès au compte est réservé au seul administrateur système. Pensez également à fournir à l'administrateur système deux comptes, un pour un accès quotidien pour gérer les activités quotidiennes, et un deuxième compte d'accès de haut niveau qui n'est requis que lorsque des changements de type d'administration sont nécessaires.

14. 2 Mots de passe

Le système Niagara et les systèmes d'exploitation utilisés dans les produits Honeywell Advanced doivent utiliser des mots de passe pour authentifier les utilisateurs dans un rôle « superviseur », « affichage », « outil » ou « système d'exploitation ». La gestion correcte des mots de passe est particulièrement importante. Ne pas utiliser ce niveau de sécurité le plus initial signifiera que toute personne accédant au système via un affichage, un client Web ou un superviseur aura accès pour effectuer des ajustements. S'assurer que le système Niagara applique une stratégie de mot de passe appropriée pour l'accès des utilisateurs ; cette directive comprendrait, sans toutefois s'y limiter :

- **L'utilisation de mots de passe forts** - Utiliser des mots de passe forts. Référez-vous aux dernières normes de sécurité pour plus de détails sur ce qui fait un mot de passe fort.
- **Changement de mot de passe cyclique recommandé** - Certains produits Niagara permettent à l'administrateur système de spécifier une période après laquelle un mot de passe doit être modifié. Bien que tous les produits n'appliquent actuellement pas ce cycle de modification de mot de passe, une stratégie de site peut le recommander.
- **Règles de divulgation des mots de passe** - L'utilisateur DOIT s'assurer qu'il ne divulgue pas à autrui les détails de son nom d'utilisateur et de son mot de passe et de ne pas les écrire.

15. CONFIGURATION D'UN ADVANCED PLANT CONTROLLER

Pour la configuration d'un Advanced Plant Controller, référez-vous au Guide d'instructions d'installation et de mise en service (31-00584). Référez-vous au Guide du pilote du MMI - (31-00590) pour le MMI et au Guide du pilote de Panel Bus (31-00591) pour les modules E/S.

15. 1 Créer et gérer des configurations de base

Créez et gérez une ligne de base de configurations d'Advanced Plant Controller correctement configurées pour la sécurité. Assurez-vous que cette ligne de base inclut également les fichiers DCF et les composants Niagara. Ne validez pas les configurations non sécurisées dans la ligne de base pour éviter une future application par inadvertance. Mettez à jour toute documentation pertinente lorsque les configurations changent.

15. 2 Modifier les mots de passe par défaut

Modifiez tous les mots de passe par défaut : Mot de passe de configuration de la console, mot de passe de sauvegarde/restauration/redémarrage/contrôle et mot de passe de la plateforme Niagara. Lors de la mise en service, assurez-vous que l'appareil est protégé par un mot de passe. Veillez à ce que les niveaux utilisateurs appropriés soient affectés aux utilisateurs du site.

15. 3 Autres considérations

15. 3. 1 Contrat de mise à jour

Adoptez une politique de mise à jour adaptée à l'infrastructure installée sur le site comme un contrat de mise à jour. Cette politique doit notamment comprendre la mise à jour de la dernière version des composants suivants du système :

- Firmware des appareils pour automate, modules E/S, MMI, etc. ;
- Logiciel de supervision, tel que le logiciel Arena NX ;
- Systèmes d'exploitation d'ordinateur / serveur ;
- Infrastructure du réseau et tous les systèmes d'accès à distance.

15. 3. 2 Configuration du réseau informatique

Configurez séparément les réseaux informatiques destinés aux systèmes de contrôle domotique et le réseau informatique de l'entreprise du client. Pour cela, configurez des réseaux locaux virtuels (VLAN) au sein de l'infrastructure informatique du client ou installez une infrastructure réseau séparée par un entrefer dédiée aux systèmes de contrôle domotique.

Quand un superviseur de système centralisé sert d'interface à des automates (par exemple : Niagara) et si le système ne demande pas d'accès direct à chaque appareil du serveur Web, alors l'infrastructure réseau doit être configurée de sorte à limiter l'accès au serveur Web.

Des réseaux locaux virtuels dynamiques avec attribution d'adresses MAC peuvent fournir une protection contre des connexions non autorisées d'un appareil au système et réduire ainsi le risque associé aux informations de surveillance individuelle sur le réseau.

16. CONFIGURATION DU PARE-FEU BAS

Le tableau suivant décrit les ports réseau utilisés dans un Advanced Plant Controller. Voir Voir *"Vue d'ensemble du système" en page 6.* pour obtenir un exemple d'architecture d'installation. Le tableau comporte les colonnes suivantes :

- Port par défaut et protocole (TCP ou UDP)
- Finalité du port
- Le port par défaut doit-il être modifié ou non
- Des connexions entrantes ou le trafic doivent-ils être autorisés ou non via le pare-feu BAS
- Des notes supplémentaires sont énumérées sous le tableau

Tableau 2 Configuration du pare-feu BAS

Port/protocole par défaut	Finalité	Changer de valeur par défaut ?	Autoriser à travers le pare-feu BAS ?	Remarques
80/TCP	HTTP	Non	Non	
443/TCP	HTTPs	Non	Éventuellement, si l'accès Web à partir du réseau Internet/ intranet/d'entreprise est requis.	1
1911/TCP	Fox (version non sécurisée du protocole d'application Niagara)	Oui	Non	
4911/TCP	Fox + SSL (version sécurisée du protocole d'application Niagara)	Oui	Non	
3011/TCP	NiagaraD (version non sécurisée du protocole de plateforme Niagara)	Oui	Non	
5011/TCP	NiagaraD + SSL (version sécurisée du protocole de la plateforme Niagara)	Oui	Non	
2601/TCP	Port console Zebra	Non	Non	2
2602/TCP	Port de console RIP			2
47808/UDP	Connexion réseau BACnet/IP	Oui	Non	3

REMARQUE :

1. Si l'interface utilisateur Web distante directe est prise en charge, ce port doit être autorisé à traverser le pare-feu BAS.
2. Le port est automatiquement ouvert par ce démon et cette fonctionnalité ne peut pas être désactivée. Le démon est configuré pour n'autoriser aucune connexion via ce port.
3. Suivez les instructions de configuration réseau énoncées dans ce manuel afin que l'Advanced Plant Controller n'ait jamais besoin de transmettre le trafic UDP via le pare-feu BAS.

17. CONFIGURATION DE L'AUTHENTIFICATION

Le Google Authentication Scheme est un mécanisme d'authentification à deux facteurs qui oblige l'utilisateur à entrer son mot de passe ainsi qu'un jeton à usage unique lors de la connexion à une station. Cela protège le compte d'un utilisateur même si son mot de passe est compromis.

Ce schéma d'authentification repose sur TOTP (Time-based OneTime Password) et l'application Google Authenticator sur l'appareil mobile de l'utilisateur pour générer et vérifier les jetons d'authentification à usage unique. L'authentification Google est basée sur le temps : il n'existe donc aucune dépendance à la communication réseau entre l'appareil mobile de l'utilisateur, la station ou les serveurs externes. Étant donné que l'authentificateur est basé sur le temps, l'heure dans la station et l'heure dans le téléphone doivent rester relativement synchronisées. L'application fournit une mémoire tampon de plus ou moins 1,5 minute pour tenir compte du décalage de l'horloge.

Prérequis : Le téléphone mobile de l'utilisateur nécessite l'application Google Authentication. Vous travaillez dans Workbench. L'utilisateur existe dans la base de données de la station.

17. 1 Procédure

1. Ouvrez la palette gauth et ajoutez **GoogleAuthenticationScheme** au nœud **Services** > **Authenticationservice** dans l'arborescence de navigation.
2. Cliquez avec le bouton droit sur **UserService**, puis double-cliquez sur l'utilisateur dans le tableau. La vue d'édition de l'utilisateur s'ouvre.
3. Configurez la propriété du nom de schéma d'authentification **GoogleAuthenticationScheme** et cliquez sur **Save**.
4. Cliquez sur le bouton à côté de la clé secrète dans l'authentificateur de l'utilisateur et suivez les invites.
5. Pour terminer la configuration, cliquez sur **Save**. Selon la vue que vous utilisez, vous devrez peut-être ouvrir à nouveau l'utilisateur ou l'actualiser après l'enregistrement.

18. LIVRAISON DU SYSTÈME

Cette section contient les informations que vous devez fournir lorsque le BAS est remis au propriétaire du système.

- Documentation comprenant des informations de sécurité, des paramètres de configuration, des noms d'utilisateur et des mots de passe d'administration, des plans de sinistre et de récupération, ainsi que des procédures de sauvegarde et de restauration.
- Formation de l'utilisateur final sur les tâches de maintenance de la sécurité.

19. INSTALLATION DU LOGICIEL DE SAUVEGARDE USB ET DU FICHIER CLEANDIST

Les informations sur l'installation du logiciel de sauvegarde USB et du fichier CleanDist sont disponibles dans le Guide d'instructions d'installation et de mise en service - 31-00584.

20. MISE HORS SERVICE DU SYSTÈME

Les données sensibles doivent être effacées des unités qui sont mises hors service, ce qui peut être fait en effectuant une réinitialisation d'usine. Référez-vous à la LED du bouton de service/d'alarme et à l'installation du fichier Cleandist dans le Guide d'instructions d'installation et de mise en service - 31-00584.

REMARQUE :
La procédure de fichier Cleandist peut effectuer le réglage d'usine en installant le fichier clean4.

21. SÉCURITÉ DES PRODUITS ADVANCED BASÉS SUR NIAGARA

Pour les produits Honeywell Advanced basés sur les frameworks Niagara N4 et Niagara AX (par exemple, Advanced Plant Controller, MMI et modules E/S, vous devez suivre les conseils de Tridium sur la sécurisation du framework Niagara.

Un certain nombre de modifications de configuration peuvent être apportées à Niagara afin d'optimiser la sécurité des produits Advanced Honeywell.

- Utiliser la fonctionnalité de mot de passe fort
- Activer la fonctionnalité de verrouillage de compte
- Expiration des mots de passe
- Utiliser l'historique des mots de passe
- Utiliser la fonction de réinitialisation du mot de passe
- Laisser décochée la case « Remember These Credentials » de mémorisation des identifiants
- Modifier la phrase secrète système par défaut
- Utiliser TLS pour définir la phrase secrète système
- Choisir une phrase secrète système fort
- Protéger la phrase secrète du système
- S'assurer que le propriétaire de la plateforme connaît la phrase secrète du système
- Utiliser un compte différent pour chaque utilisateur de la plateforme
- Utiliser des noms de compte uniques pour chaque projet
- S'assurer que le propriétaire de la plateforme connaît les identifiants de la plateforme
- Utiliser un compte différent pour chaque utilisateur de la station
- Utiliser des comptes de type de service uniques pour chaque projet
- Désactiver les comptes connus lorsque cela est possible
- Configurer des comptes temporaires pour qu'ils expirent automatiquement
- Modifier les identifiants du compte de type système
- Interdire les sessions simultanées lorsque cela est possible
- Configurer des rôles avec des autorisations minimales requises
- Attribuer des rôles minimaux requis aux utilisateurs
- Utiliser le nombre minimum possible de super utilisateurs
- Exiger des autorisations de super utilisateur pour les objets programme
- Utiliser les autorisations minimales requises pour les comptes externes
- Utiliser un schéma d'authentification approprié pour le type de compte
- Supprimer les schémas d'authentification inutiles
- TLS & gestion des certificats
- Installation de module
- Exiger des objets de programme et des robots signés
- Désactiver SSH et SFTP
- Désactiver les services inutiles
- Configurer les services nécessaires de manière sûre
- Mettez à jour Niagara 4 vers la dernière version
- Installer le produit dans un emplacement sécurisé
- Assurez-vous que les stations sont derrière un VPN

Des publications techniques spécifiques sont disponibles et doivent être suivies pour s'assurer que le système est verrouillé de la manière la plus sûre possible. De nombreuses options existent telles que le cryptage SSL et des étapes supplémentaires pour protéger des éléments tels que les modules de programme ; pour plus de détails, reportez-vous au site Web de Tridium pour le Guide de renforcement Niagara 4 (pour les produits basés sur Niagara N4) et le Guide de durcissement Niagara (produits basés sur Niagara AX).

Le contenu de ce document est fourni à titre informatif uniquement. Le contenu et le produit décrits sont sujets à changement sans préavis. Honeywell ne fait aucune déclaration ou garantie concernant ce document. Honeywell ne pourra en aucun cas être tenu responsable des omissions ou des erreurs techniques ou éditoriales dans ce document, ni des dommages, directs ou accessoires, résultant de ou liés à l'utilisation de ce document. Aucune partie de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de Honeywell.

Honeywell Building Technologies

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

® Marque déposée aux États-Unis
©2023 Honeywell International Inc.
31-00594-01 Rév. 07-23

22. LISTE DE CONTRÔLE DE SÉCURITÉ DE L'INSTALLATION

Instance de l'appareil Advanced Plant Controller : _____

Description Advanced Plant Controller : _____

Emplacement Advanced Plant Controller : _____

Installateur : _____ Date :_____

Effectuez les tâches de sécurité suivantes pour chaque Advanced Plant Controller installé

- ☐ Installez un pare-feu entre l'Advanced Plant Controller et le ou les réseaux externes. Voir *"BACnet et Niagara" en page 18.*
- ☐ Sécurisez physiquement l'Advanced Plant Controller. Voir *"Sécuriser physiquement l'Advanced Plant Controller, le MMI et les modules E/S" en page 20.*
- ☐ Remplacez le mot de passe par défaut par un mot de passe unique pour chacun des éléments suivants : Configuration de la console, sauvegarde/restauration/redémarrage/contrôle et plateforme Niagara. Voir le Guide d'instructions d'installation et de mise en service - 31-00584
- ☐ Si un serveur Web est nécessaire, configurez-le pour qu'il fonctionne uniquement en mode HTTPS. Voir le Guide d'instructions d'installation et de mise en service - 31-00584

Statut du serveur Web : Désactivé / Activé.

Si le service Web est activé, procédez comme suit :

- ☐ Set Http Enabled = false.
- ☐ Set Https Enabled = true.
- ☐ Set Https Only = true.
- ☐ Configurez le pare-feu BAS. Voir *"Configuration du pare-feu BAS" en page 24.*
- ☐ Fournir toutes les données requises au propriétaire du système BAS lors de la livraison. Voir *"Configuration de l'authentification" en page 25.*