Manuel de sécurité de la gamme SV2

FICHE TECHNIQUE DU PRODUIT

INTRODUCTION

Le présent document contient des renseignements de sécurité pour les vannes et accessoires de la gamme SV2.

Autres publications connexes :

- 32-00029, Guide d'utilisation de la gamme SV2
- 32-00031, Guide d'utilisation des outils HMI/PC

Protection physique de l'appareil

⚠ REMARQUE SUR LA CYBERSÉCURITÉ

Les produits de la gamme SV2 contiennent des pièces électroniques et des logiciels. L'installateur/la direction de l'usine doit s'assurer qu'aucune personne non autorisée n'accède à la vanne et à l'interface de programmation pour modifier les paramètres (le cas échéant).

Tout accès non autorisé visant à changer l'interface de câblage de la vanne, remplacer des pièces et changer le matériel ou le logiciel de l'appareil ne devrait pas être permis. Tout manquement à cet égard pose un risque à la sécurité.

Une étiquette inviolable a été placée à l'intérieur du boîtier électrique de la vanne pour indiquer s'il a été ouvert. L'étiquette est située entre l'ensemble de pièces électroniques principal de la vanne et le boîtier électrique dans lequel il se trouve.

REMARQUE : Puisque l'ensemble de pièces électroniques principal de la vanne est remplaçable sur site, ce sceau doit être brisé pour le remplacer.

Les vannes de la gamme SV2 offrent diverses mesures de sécurité qui empêchent leur utilisation non autorisée à distance. Cependant, il ne faut pas oublier que la sécurité physique est absolument essentielle pour éviter de nombreuses menaces locales.

Lorsque vous installez un appareil, sélectionnez toujours un endroit dont l'accès est limité ou même interdit. Nous vous recommandons de verrouiller l'appareil dans une armoire fermée dont l'accès est limité au personnel formé et autorisé.

De plus, il est fortement conseillé de protéger physiquement le câblage de l'appareil. Un exemple de câblage correctement et incorrectement exécuté est montré à la figure 1.

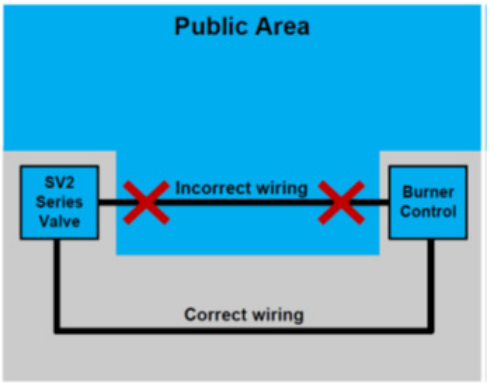


Fig. 1. Exemple de câblage correctement et incorrectement exécuté

⚠ MISE EN GARDE

Une personne non autorisée pourrait trafiquer le câblage de l'appareil si celui-ci n'est pas sécurisé, ce qui pourrait entraîner un comportement dangereux. Cette règle s'applique au câblage des produits de la gamme SV2, mais également à celui de tout équipement contrôlé.

32-00151F-02

REMARQUE : Ce produit peut contenir ou être dérivé de matériel, y compris les logiciels, de tierces parties. Le matériel d'une tierce partie peut être soumis à des licences, des avis, des restrictions et des obligations imposés par le concédant de licence. Les licences, les avis, les restrictions et les obligations, le cas échéant, se trouvent dans le matériel accompagnant le produit, dans les documents ou dans les fichiers accompagnant ce matériel d'une tierce partie, dans un fichier nommé third_party_licenses sur le média contenant le produit, ou à l'adresse http://www.honeywell.com/ps/thirdpartylicenses.

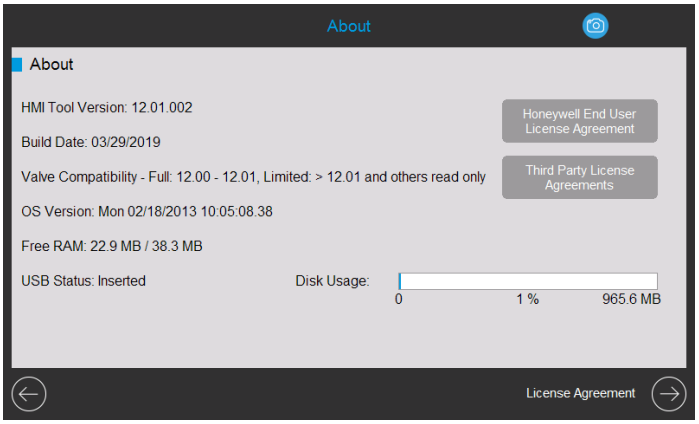


Fig. 2. À propos de la page avec les contrats de licence.

Modules accessoires de la gamme SV2

On peut ajouter des fonctionnalités évoluées aux vannes de la gamme SV2 en y raccordant des modules accessoires. Parmi ceux-ci, on retrouve le module de rapport air/carburant et le module de pression. Ces modules utilisent un câblage externe qui, s'il est trafiqué, peut limiter ou désactiver la fonctionnalité de l'appareil ou même provoquer un comportement dangereux.

Bien que cela puisse ne pas être évident, le module de rapport air/carburant utilise également une tuyauterie externe qui, si elle est modifiée sans autorisation, peut endommager l'appareil.

COMMUNICATION MODBUS®

On utilise la communication Modbus avec le bus RS-485 pour configurer et assurer la surveillance des appareils de la gamme SV2. En matière de sécurité, on doit porter une attention particulière à cette communication.

Communications sécurisées/communications non sécurisées

Par sa nature, le protocole Modbus n'est pas sécurisé et n'intègre aucune méthode de sécurité. Cependant, les appareils de la gamme SV2 exécutant le micrologiciel version 10 ou plus prennent en charge la fonction Secured Modbus, une extension du protocole standard exclusive à Honeywell.

Secured Modbus prend en charge la validation de l'intégrité des messages de manière à empêcher qu'une personne puisse les trafiquer en accédant à la conduite RS-485. Ce protocole n'empêche toutefois pas une personne non autorisée de lire les données de l'appareil.

Gestion de session

Les vannes de la gamme SV2 et les outils HMI et PC prennent en charge les sessions sécurisées avec Secured Modbus. Cela signifie que lorsque l'utilisateur se connecte par mot de passe avec un compte Installateur ou Fabricant d'origine, un tunnel sécurisé est établi entre l'application HMI ou PC clients et la vanne de la gamme SV2. Consultez les figures 2 à 4.

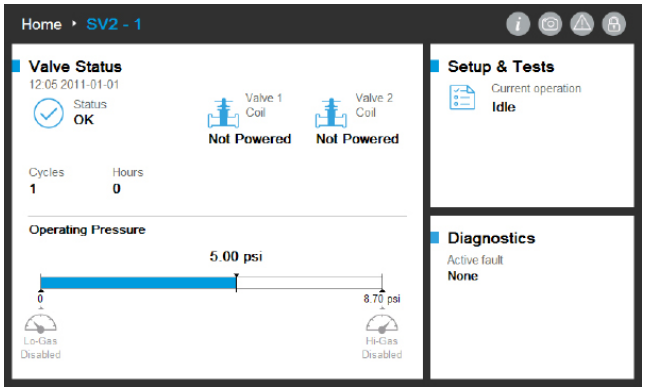


Fig. 3. Session non établie. L'utilisateur n'est pas connecté.

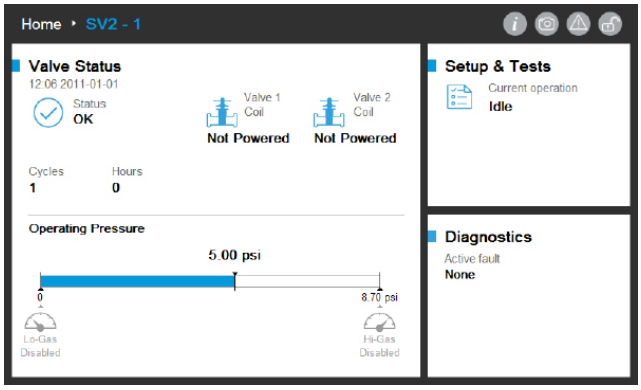


Fig. 4. Session établie. L'utilisateur est connecté en tant qu'installateur.

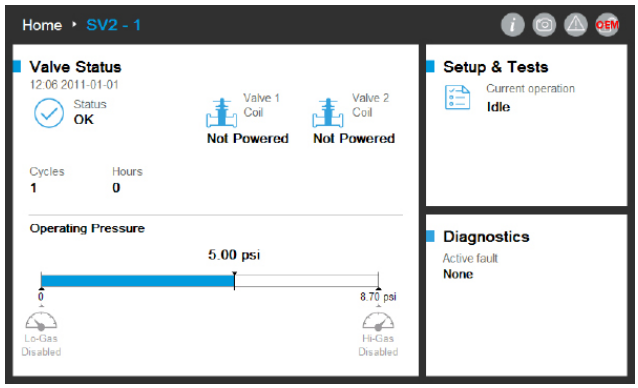


Fig. 5. Session établie. L'utilisateur est connecté en tant que fabricant d'origine.

Une session doit être établie pour apporter des modifications à la configuration de la vanne. Par exemple, les configurations habituelles sont :

1. Vérification de sécurité des données de configuration essentielles
2. Mise en service de la configuration du prémélange de la vanne
3. Configuration du module de pression
4. Configuration de la sécurité (configuration du mot de passe, modification des privilèges d'accès)
5. Configuration de la preuve de fermeture
6. Séquence de contrôle d'étanchéité
7. Unités (pression, volume et fuite)
8. Paramètres généraux de la vanne (adresse Modbus, débit de transmission)

REMARQUES :

- Une seule session peut être active à la fois. Autrement dit, lorsqu'un utilisateur est connecté, le prochain utilisateur doit attendre la fermeture de la session en cours.
- Si aucune communication sécurisée n'est reçue 20 secondes après la transmission du dernier message sécurisé, la session sécurisée est fermée.
- L'outil HMI ou PC de la gamme SV2 ferme la session sécurisée si l'utilisateur est inactif depuis 10 minutes.

Gestion de clés/mots de passe

Un mot de passe correspond à une phrase ou à une chaîne de caractères qui doit répondre aux critères suivants :

- Contenir au moins 12 caractères
- Contenir au moins une majuscule et une minuscule
- Contenir au moins un chiffre
- Ne contenir aucun caractère spécial

Les vannes de la gamme SV2 sont livrées avec des mots de passe de fabricant d'origine et d'installateur par défaut. Vous devez modifier ces mots de passe avant de pouvoir utiliser ces vannes dans un système sans observation de l'utilisateur.

Si vous oubliez de modifier le mot de passe par défaut, la vanne sera verrouillée après la session sécurisée. Il s'agit d'une mesure de sécurité empêchant d'utiliser une vanne en mode non sécurisé (sans mot de passe correctement configuré). Consultez les figures 5 à 8.

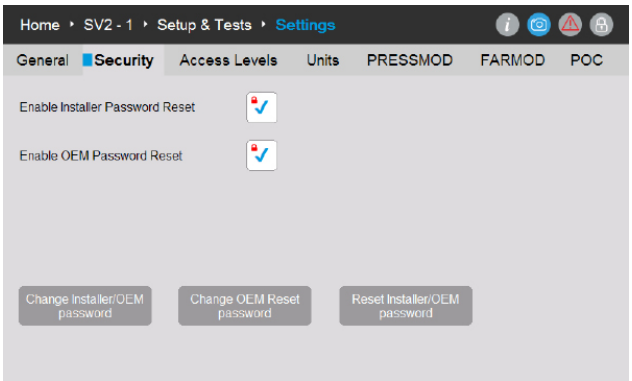


Fig. 6. **On peut modifier les mots de passe des comptes Fabricant d'origine, Réinitialisation fabricant d'origine et Installateur depuis la page Sécurité.**

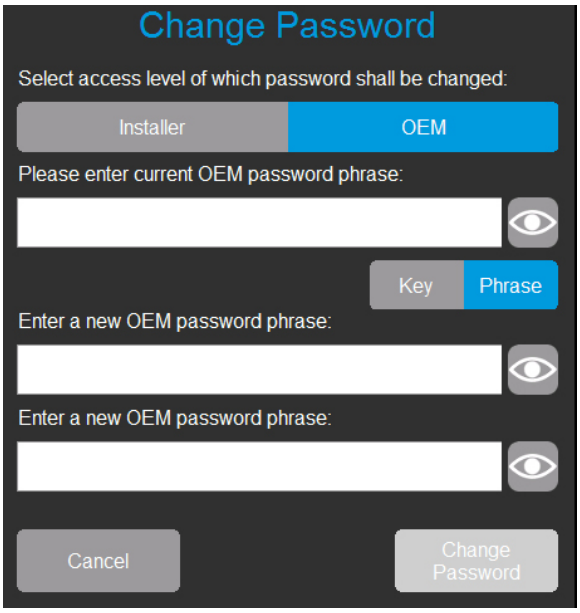


Fig. 7. **Un utilisateur connecté en tant que fabricant d'origine peut modifier les mots de passe des comptes Fabricant d'origine et Installateur. L'utilisateur entre le mot de passe actuel du compte Fabricant d'origine et entre deux fois le nouveau mot de passe.**

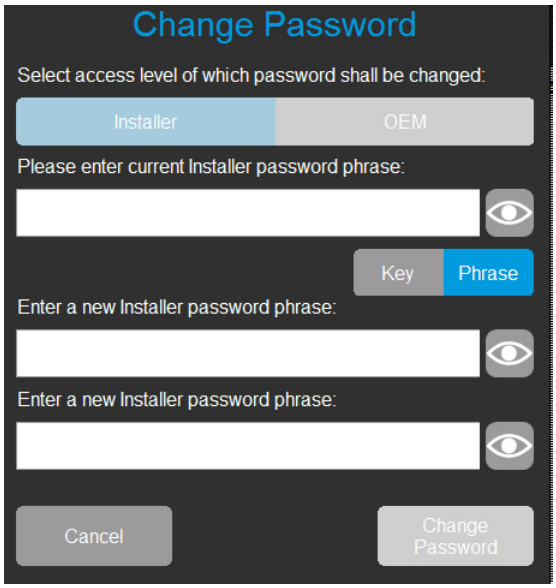


Fig. 8. Un utilisateur connecté en tant qu'installateur peut seulement modifier le mot de passe du compte Installateur. L'utilisateur entre le mot de passe actuel du compte Installateur et entre deux fois le nouveau mot de passe.

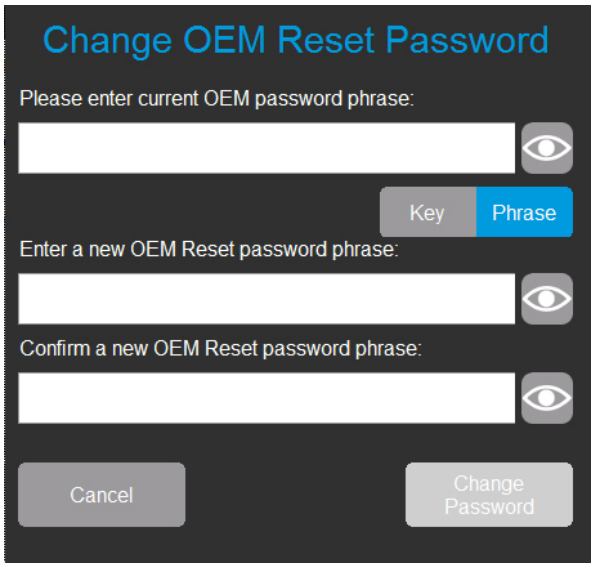


Fig. 9. Un utilisateur connecté en tant que fabricant d'origine peut également modifier le mot de passe Réinitialisation fabricant d'origine. L'utilisateur entre le mot de passe actuel du compte Fabricant d'origine et entre deux fois le nouveau mot de passe Réinitialisation fabricant d'origine.

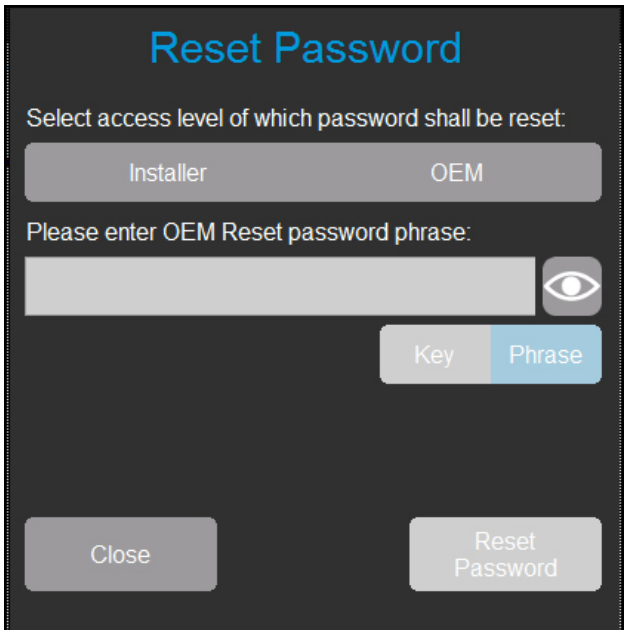


Fig. 10. L'utilisateur non connecté choisit le niveau d'accès du mot de passe à réinitialiser. L'utilisateur entre le mot de passe de réinitialisation.

Réinitialiser le mot de passe

Si vous perdez les mots de passe Installateur ou Fabricant d'origine, vous pouvez toujours les réinitialiser si cette option a été activée par le fabricant d'origine. Consultez la fig. 5. La méthode de réinitialisation varie selon qu'il s'agit d'un mot de passe de compte Installateur ou Fabricant d'origine. Prenez note que vous ne pouvez pas contourner cette méthode en effectuant un cycle de la vanne ou en coupant l'alimentation de l'interface utilisateur.

La procédure de réinitialisation de mot de passe permet simplement à un utilisateur autorisé de réinitialiser le ou les mots de passe actuels aux valeurs d'usine Honeywell par défaut. Lorsque les mots de passe sont réinitialisés, l'utilisateur peut ensuite se connecter et en définir de nouveaux.

Après la réinitialisation aux valeurs par défaut, les mots de passe des comptes Fabricant d'origine, Installateur et Réinitialisation fabricant d'origine ne sont pas réglés à de nouvelles valeurs personnalisées. La soupape sera verrouillée et ne pourra être utilisée si l'utilisateur Fabricant d'origine n'est pas connecté. Vous devez configurer les mots de passe pertinents pour pouvoir supprimer les codes d'anomalie.

Par défaut, la fonction de réinitialisation de mot de passe des comptes Installateur et Fabricant d'origine est désactivée. Le fabricant d'origine ou le propriétaire de l'appareil doit l'activer lors de la configuration initiale de chaque appareil, comme cela est indiqué à la figure 5.

REMARQUES :

- **Le fabricant d'origine peut choisir d'activer ou de désactiver la fonction de réinitialisation du mot de passe du compte Fabricant d'origine. Consultez la figure 5.**
  - **Si cette fonction est activée et que vous perdez le mot de passe du compte Fabricant d'origine, le fabricant d'origine peut réinitialiser les mots de passe aux valeurs d'usine Honeywell par défaut et en configurer de nouveaux.**
  - **Si elle est désactivée et que vous perdez le mot de passe principal du compte Fabricant d'origine, le fabricant d'origine ne pourra pas réinitialiser le mot de passe et ne pourra plus modifier la vanne au niveau du fabricant d'origine.**
  - **Si le mot de passe principal du compte Installateur est connu, le fabricant d'origine peut accéder à la vanne pour l'utiliser et pour modifier les paramètres auxquels l'installateur avait accès.**
  - **Pour réactiver les modifications au niveau du compte Fabricant d'origine, il faudrait remplacer les composants électroniques principaux de la vanne et reprogrammer la vanne au niveau des comptes Fabricant d'origine et Installateur.**

Protection des mots de passe

Pour éviter le risque qu'un mot de passe de session puisse être découvert à la suite de tentatives aléatoires, tous les mots de passe sont protégés par un mécanisme de détection d'attaques en force. Ce mécanisme désactive temporairement la connexion du compte visé et de la vanne. Vous devez effectuer un cycle de mise hors tension/mise sous tension des appareils. La personne qui tente de se connecter peut également attendre une minute avant d'effectuer une nouvelle tentative.

Si cela se produit, des anomalies seront affichées sur la page de diagnostic de l'outil HMI ou PC. Quatre codes d'anomalie sont possibles pour un tel cas :

- Compte Installateur temporairement désactivé
- Compte Fabricant d'origine temporairement désactivé
- Fonction de réinitialisation du compte Installateur temporairement désactivée
- Fonction de réinitialisation du compte Fabricant d'origine temporairement désactivée

Pratiques exemplaires

Il est recommandé de toujours utiliser des mots de passe robustes et difficiles à deviner. Veuillez vous reporter à la section Gestion de clés/mots de passe plus haut dans le présent document.

Gestion des comptes

Les vannes de la gamme SV2 comprennent deux comptes d'utilisateur :

1. Installateur
2. Fabricant d'origine

Le compte Installateur est assujetti au compte Fabricant d'origine. Dit autrement, toutes les fonctions auxquelles a accès le compte Installateur peuvent être contrôlées par le compte Fabricant d'origine.

En revanche, seul le fabricant d'origine peut utiliser les fonctions auxquelles il a accès.

On ne peut pas ajouter ou supprimer les comptes d'utilisateur. Leurs fonctions sont :

1. Le compte Fabricant d'origine est utilisé pour configurer les fonctions essentielles de la vanne, comme la configuration des modules de pression, de rapport air/carburant et d'allumage air/carburant ainsi que les courbes de base air/carburant.
2. Le compte Installateur est utilisé pour configurer des fonctions moins essentielles, comme les limites fonctionnelles ou les variables propres à l'utilisation.

Gestion de l'accès

Par défaut, il est possible de configurer les privilèges d'accès pour chaque fonction essentielle. Le niveau par défaut de l'accès aux fonctions de sécurité par l'utilisateur est configuré pour le compte Installateur et devrait être modifié au compte Fabricant d'origine selon les particularités de l'utilisation. Vous pouvez utiliser l'outil HMI ou PC d'Honeywell pour effectuer la configuration, comme cela est montré à la figure 11 :

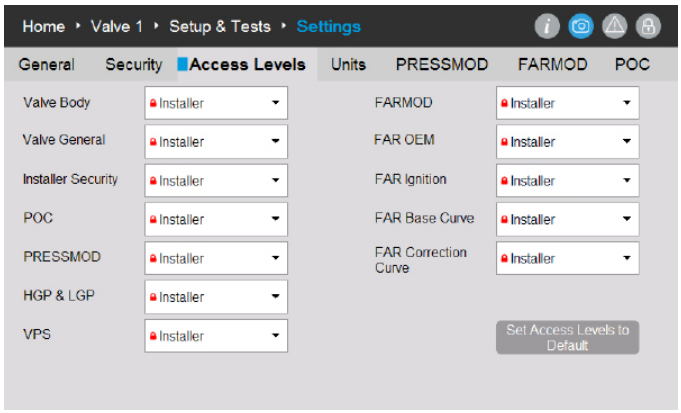


Fig. 11. Page de niveaux d'accès Chaque groupe de configuration peut être réglé à Installateur, Fabricant d'origine ou Lecture seule.

Sécurité contre les connexions à distance et sécurité physique

Pour assurer la sécurité des communications contre une connexion à distance, il est important de tenir compte des éléments suivants, qui s'appliquent principalement à la configuration initiale de l'appareil :

- Lorsqu'un attaquant potentiel a physiquement accès à l'appareil, il peut obtenir le mot de passe de réinitialisation du compte Installateur depuis l'étiquette au dos de l'ensemble électronique principal de la vanne et l'utiliser ultérieurement.
- Lorsqu'une connexion à la vanne est établie au moyen du mot de passe par défaut, cette connexion ne peut pas être considérée comme étant sécurisée. Il est recommandé de configurer les mots de passe initiaux des comptes Installateur et Fabricant d'origine sans qu'aucun autre appareil soit présent sur le réseau RS-485 sur lequel est connectée la vanne.

OUTILS HMI ET PC

Pour assurer la sécurité des vannes de la gamme SV2 et des outils d'interface, il est essentiel d'en fournir un accès fiable et sécurisé. C'est pour cette raison que l'on doit adopter plusieurs mesures de sécurité avec les outils PC et HMI, comme cela est décrit ci-dessous.

Sécurité de l'outil HMI

Tout appareil HMI autonome de la gamme SV2 doit toujours être protégé physiquement; les mêmes recommandations de sécurité physique s'appliquent aux vannes de la gamme SV2. Veuillez vous reporter à la section Protection physique de l'appareil plus haut dans le présent document.

Sécurité de l'outil PC

L'outil PC est conçu pour fonctionner sur des ordinateurs munis d'un système d'exploitation Microsoft® Windows. Lors de la connexion entre un ordinateur et une vanne de la gamme SV2, tout problème de sécurité du PC en question peut poser un risque à la sécurité de la vanne. C'est pour cette raison qu'il est recommandé de suivre les pratiques de sécurité décrites ci-dessous :

1. Toujours utiliser un système d'exploitation pris en charge par Microsoft.
2. Toujours veiller à ce que les derniers correctifs soient installés sur le système.
3. Toujours utiliser un antivirus et un pare-feu à jour.
4. Utiliser la fonction de liste blanche du système d'exploitation du PC.
5. Ne jamais utiliser une application piratée ou provenant d'une source non fiable.
6. S'assurer que les lecteurs USB ou tout autre accessoire branché au PC proviennent de sources fiables et ne contiennent aucun matériel ou logiciel dangereux (p. ex., un capteur de frappes, un enregistreur de mémoire, etc.).
7. Désactiver tous les services, ports et comptes d'utilisateur non nécessaires du PC pour éviter une attaque à distance.

Un fichier d'installation ou un fichier binaire d'application est signé par une clé Honeywell pour confirmer que l'application ou le programme d'installation de l'outil PC provient d'une source vérifiée. Toutefois, même si la signature offre un bon niveau de protection, il est tout de même recommandé de n'utiliser que le programme d'installation ou l'application de l'outil PC fourni directement par Honeywell ou par un fabricant d'origine ou un installateur autorisé par Honeywell.

Liste de vérification de sécurité de l'outil PC

Pour utiliser cette application en toute sécurité, veuillez vous assurer de respecter les critères suivants :

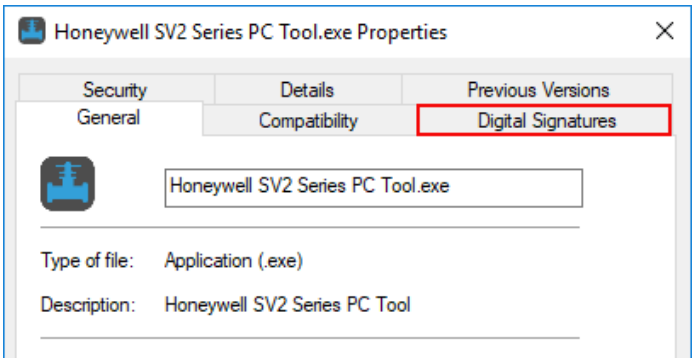
1. Vous utilisez uniquement une application signée de confiance (consultez la section Vérification de l'origine de l'application).
2. Si possible, ajoutez les applications à la liste blanche (consultez la section Ajouter les applications à la liste blanche).
3. Si l'ordinateur est connecté à Internet, vous utilisez un antivirus et un pare-feu correctement configurés.
4. Assurez-vous que l'ordinateur sur lequel vous exécutez l'application dispose d'une protection par mot de passe pour éviter toute utilisation par du personnel non autorisé.
5. Assurez-vous que l'accès physique au système par du personnel non autorisé est restreint ou limité (PC -> RS485 -> Modbus -> vanne de la gamme SV2).
6. L'outil PC doit être installé automatiquement dans le dossier standard « fichiers de programme » de Microsoft Windows. Cet emplacement d'installation est pré-sélectionné dans l'installateur de l'outil PC. Si un emplacement d'installation différent est sélectionné, l'utilisateur doit configurer les autorisations de sécurité (p. ex., à l'administrateur) pour s'assurer que l'installation de l'outil PC ne sera pas trafiquée par du personnel non autorisé.

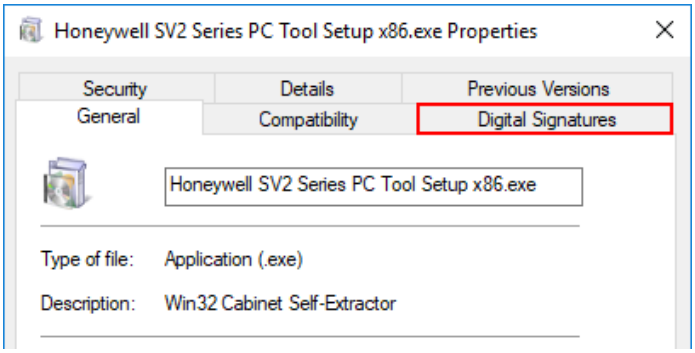
Vérification de l'origine de l'outil PC installateur/utilisation

L'application ou le programme d'installation est fourni avec une signature numérique. Vous devez vérifier cette signature lorsque vous téléchargez une nouvelle version de l'application ou du programme d'installation ou lorsque vous avez des doutes quant à l'origine de celle-ci ou de celui-ci.

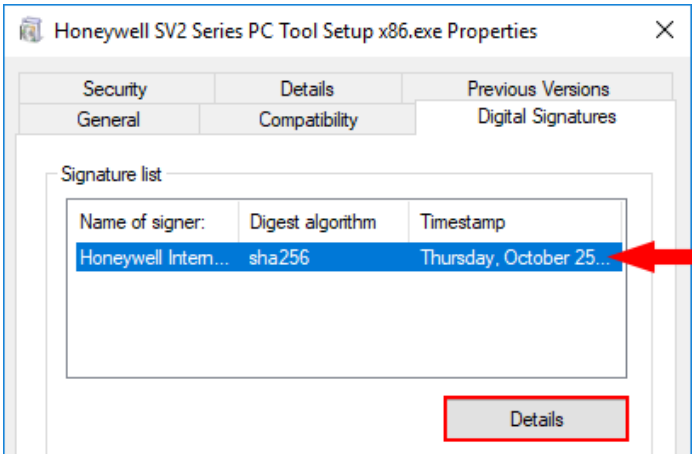
Vous pouvez suivre ces étapes pour vérifier la signature :

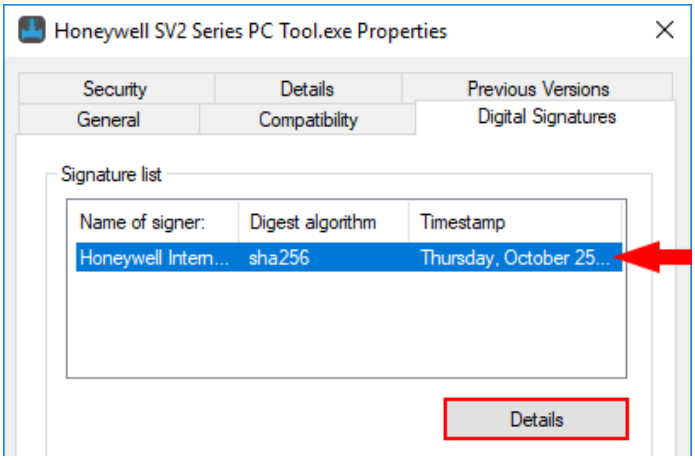
1. Avec le bouton droit de la souris, cliquez sur l'application «Honeywell SV2 Series PC Tool Setup x86.exe» / «Honeywell SV2 Series PC Tool Setup x64.exe» et cliquez sur « Propriétés ».
2. Décompressez le contenu du fichier «usb_root.zip», puis avec le bouton droit de la souris, cliquez sur l'application « app.exe » et cliquez sur « Propriétés ».
3. Dans la fenêtre des propriétés, cliquez sur « Signatures numériques ». Si cet onglet n'est pas présent, passez à l'étape 5.



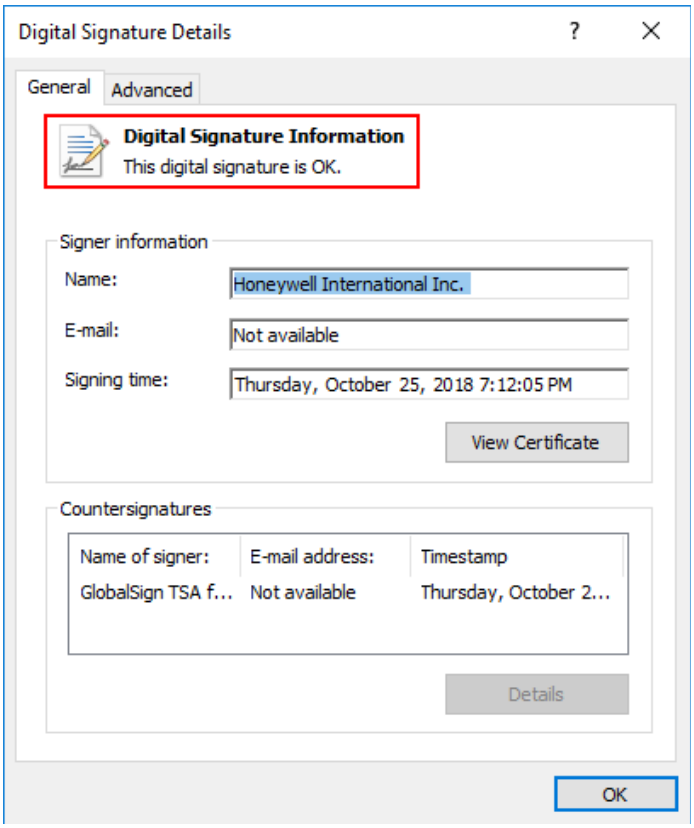


4. À l'onglet « Signatures numériques », le seul élément de la « Liste de signatures » devrait être nommé « Honeywell International Inc. ». Cliquez sur cet élément, puis cliquez sur le bouton « Détails ».

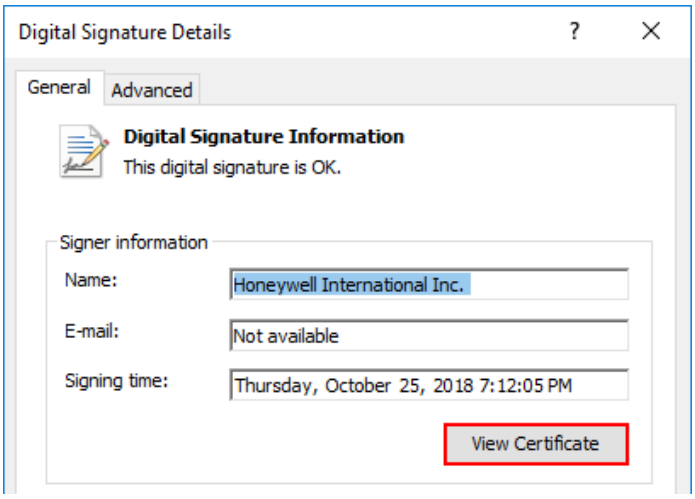




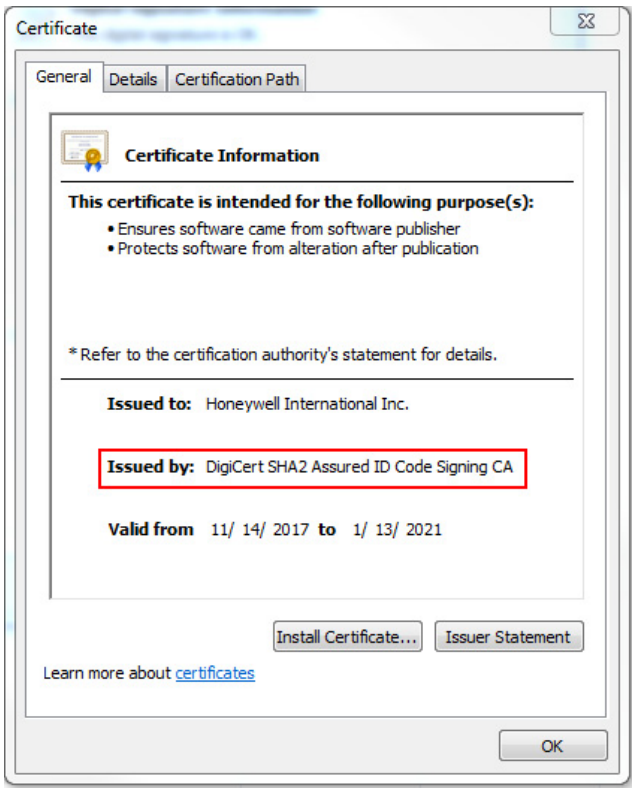
5. Dans la fenêtre « Détails de la signature numérique », vérifiez l'élément « Information sur la signature numérique ». Il devrait y être écrit « Cette signature numérique est OK ».



6. Si la signature n'est pas OK ou si elle n'est pas présente (étape 2, aucun onglet de signature numérique), il ne s'agit pas d'une application de confiance et vous devriez la supprimer. Vous pouvez télécharger une nouvelle copie propre de la source d'origine.
7. De plus, vous pouvez consulter les détails du certificat en cliquant sur le bouton « Afficher le certificat ».



8. La ligne « Publié par » dans les détails du certificat doit contenir le nom « DigiCert ». Il s'agit du nom du fournisseur du certificat.



Ajouter des applications à la liste blanche

L'ajout d'applications à la liste blanche permet à l'administrateur de définir une liste d'applications autorisées. Les applications qui ne font pas partie de cette liste ne pourront pas être exécutées. La configuration de la liste blanche augmente considérablement le niveau de sécurité et réduit les risques d'exécuter involontairement un logiciel sur votre ordinateur. L'ajout d'applications à la liste blanche est un outil intégré aux systèmes d'exploitation Windows (Windows 7, Windows 8) ou peut être fait au moyen d'une application tierce.

Rapport d'incident

Lorsque l'outil HMI ou PC tombe inopinément en panne, un rapport d'incident est créé. Les rapports d'incident de l'outil PC sont situés à C:\Users\<user>\Documents\Honeywell\SV2 Series PC Tool\Crash reports\. Le rapport d'incident de l'outil HMI est accessible à partir de Home/Display Setup/About page. Reportez-vous à la Fig. 1. Le rapport d'incident contient les informations suivantes :

- Version et configuration de l'outil PC
- Version du système d'exploitation Microsoft Windows
- Version Microsoft .NET Framework
- Exception et trace d'appels
- Liste des ports de communication disponibles
- Configuration complète des vannes

Pour obtenir plus d'information sur ce produit et sur la gamme complète de produits SV2, consultez le guide d'utilisation de la gamme SV2 sur notre site Web, à l'adresse https://combustion.honeywell.com/sv2

Pour en savoir davantage

La gamme de produits du groupe Solutions thermiques (HTS) d'Honeywell comprend les produits de Sécurité de la combustion Honeywell, de même que les produits Eclipse, Exothermics, Hauck, Kromschröder et Maxon. Pour en apprendre davantage sur nos produits, visitez le site ThermalSolutions.honeywell.com ou communiquez avec votre ingénieur commercial Honeywell.

Honeywell Process Solutions

Solutions thermiques (HTS) de Honeywell
1250, West Sam Houston Parkway
South Houston, TX 77042

ThermalSolutions.honeywell.com

32-00151F-02 Rev. 05-19
Printed in USA