Beveiligingshandleiding voor de SV2-serie

PRODUCTSPECIFICATIEBLAD

INLEIDING

Dit document biedt beveiligingsinformatie voor kleppen en accessoires van de SV2-serie.

Overige relevante publicaties zijn:

- 32-00029, Gebruikershandleiding voor de SV2-serie
- 32-00031, Gebruikershandleiding voor HMI/PC Tool

Fysieke apparaatbeveiliging

⚠ KENNISGEVING

CYBERBEVEILIGING

Producten van de SV2-serie bevatten elektronica en software. De monteur of het faciliteitsbeheer moet zorg dragen om te beveiligen tegen ongeautoriseerde toegang tot de klep en de programmeringsinterface voor parameteraanpassing (indien van toepassing).

Ongeautoriseerde toegang om de bekabelingsinterface van de klep te wijzigen, onderdelen te vervangen of hardware of software van het apparaat te wijzigen moet worden verboden. Doet u dit niet, dan is dit mogelijk een beveiligingsrisico.

Er is binnen in de elektrische behuizing van de klep een sabotagelabel geplaatst om aan te geven of het is geopend. Het label bevindt zich tussen de hoofdelektronica en de elektrische behuizing waarin dit zich bevindt.

OPMERKING: De hoofdelektronica van de klep kan worden vervangen. Hiervoor moet het label worden gebroken.

De kleppen van de SV2-serie zijn ontworpen met verschillende beveiligingsfuncties om te voorkomen dat ze op afstand worden misbruikt. Fysieke beveiliging blijft echter absoluut essentieel om veel lokale bedreigingen te voorkomen.

Kies bij het installeren van het apparaat altijd een fysieke locatie met beperkte toegang. Het is aan te raden dat u het apparaat in een afgesloten kast installeert, waar alleen goedgekeurd en getraind personeel toegang tot heeft.

Het wordt ook aangeraden om alle bekabeling van het apparaat fysiek te beveiligen. U kunt in afbeelding 1 een voorbeeld zien van correcte en incorrecte bekabeling.

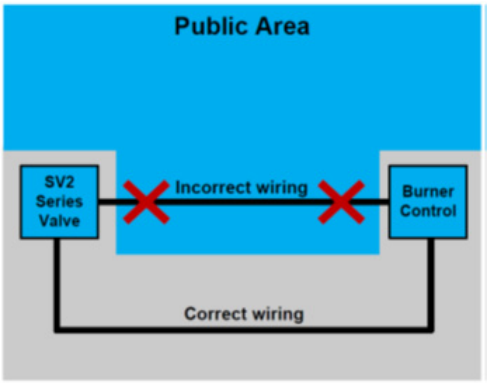


Fig. 1. Voorbeelden van correcte en incorrecte bekabeling

⚠ VOORZICHTIG

Wanneer de bekabeling niet wordt beveiligd, kan een onbevoegd persoon de bekabeling van het apparaat saboteren, wat kan leiden tot gevaarlijk gedrag. Deze regel is van toepassing op de specifieke bekabeling van producten in de SV2-serie, maar ook op eventuele andere aangestuurde apparatuur.

32-00151D-02

LET OP: Dit product bevat mogelijk of is mogelijk afgeleid van materialen, waaronder software, van derden. Materialen van derden kunnen onderworpen zijn aan licenties, kennisgevingen, beperkingen en verplichtingen opgelegd door de licentiegever. De licenties, kennisgevingen, beperkingen en verplichtingen, indien aanwezig, zijn te vinden in de materialen bij het product, in de documenten of bestanden bij deze materialen van derden, in een bestand met de naam third_party_licenses op de media die het product bevatten, of op http://www.honeywell.com/ps/thirdpartylicenses.

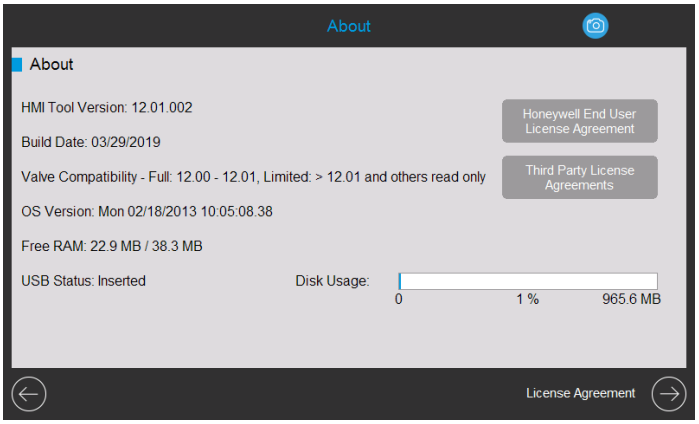


Fig. 2. Informatiepagina met licentieovereenkomsten.

Accessoiremodules voor de SV2-serie

De kleppen in de SV2-serie ondersteunen het aansluiten van accessoiremodules waarmee geavanceerde functionaliteit wordt aangeboden. Er is onder andere een brandstof-/luchtratiomodule en een drukmodule. Deze modules gebruiken externe bekabeling die, indien gesaboteerd, de functionaliteit van het apparaat op een gevaarlijke manier beïnvloeden, of het apparaat beperken of volledig uitschakelen.

Hoewel het misschien niet duidelijk te zien is, gebruikt de brandstof-/luchtratiomodule ook externe leidingen, die bij onbevoegde aanpassing kunnen veroorzaken dat het apparaat defect raakt.

MODBUS®-COMMUNICATIE

Voor configuratie en apparaatmonitoring van de SV2-serie, wordt Modbus-communicatie met een RS-485 BUS gebruikt. Deze communicatie vereist speciale aandacht met betrekking tot beveiliging.

Beveiligde versus onbeveiligde communicatie

Het Modbus-protocol is onbeveiligd in zijn aard en biedt geen ingebouwde beveiligingsmaatregelen. Apparaten van de SV2-serie met firmwareversie 10 en hoger ondersteunen echter Secured Modbus. Dit is een eigen uitbreiding van Honeywell op het standaardprotocol.

Beveiligde Modbus ondersteunt integriteitsvalidatie van berichten zodat deze niet kunnen worden gesaboteerd door iemand die de RS-485-doorgang gebruikt. Dit protocol beschermt de apparaatgegevens echter niet voor het aflezen door onbevoegd personeel.

Sessiebeheer

De kleppen in de SV2-serie en HMI/PC Tools ondersteunen een beveiligde sessie wanneer Secured Modbus wordt gebruikt. Dit betekent dat er een beveiligde tunnel tussen de HMI/PC-clienttoepassing en de klep van de SV2-serie tot stand wordt gebracht wanneer de gebruiker zich aanmeldt met een wachtwoord voor ofwel Monteur ofwel de OEM-toegangsniveaus. Zie afbeelding 2-4.

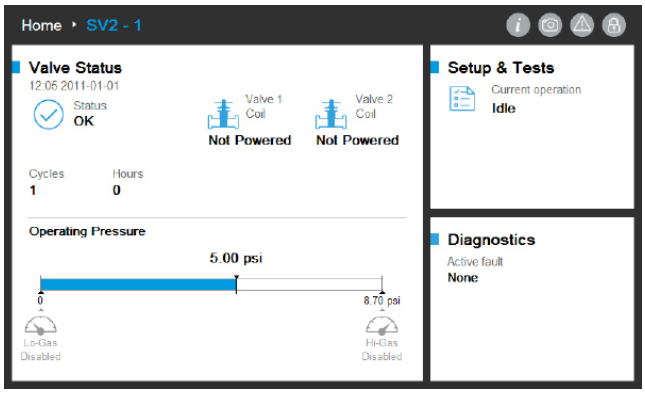


Fig. 3. Sessie is niet tot stand gebracht. De gebruiker is niet aangemeld.

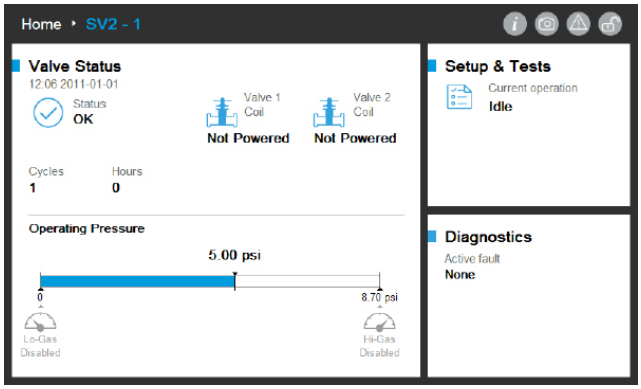


Fig. 4. Sessie is tot stand gebracht. De gebruiker is aangemeld als monteur.

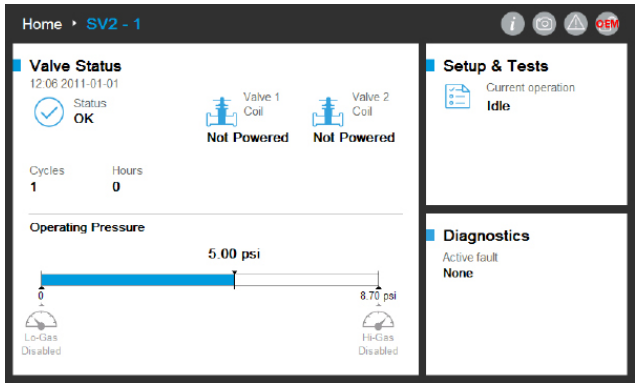


Fig. 5. Sessie is tot stand gebracht. De gebruiker is aangemeld als OEM.

Een sessie moet tot stand worden gebracht en worden gebruikt om wijzigingen in de klepconfiguratie te kunnen aanbrengen. Typische configuraties zijn bijvoorbeeld:

1. Veiligheidsverificatie van kritieke configuratiegegevens
2. Activeren van vooraf gemengde klepconfiguratie
3. Configuratie van de drukmodule
4. Beveiligingsconfiguratie (wachtwoord instellen, aanpassen van toegangsrechten)
5. Configuratie van bewijs van sluiten
6. Bewijsprocedure voor de klep
7. Eenheden (druk, volume en lekkage)
8. Algemene klepinstellingen (Modbus-adres, Baudrate)

OPMERKINGEN:

- Er kan slechts één sessie tegelijk actief zijn. Wanneer er dus één gebruiker is aangemeld, moet een andere gebruiker wachten tot de eerdere sessie is beëindigd.
- Een beveiligde sessie wordt beëindigd indien er geen beveiligde communicatie wordt ontvangen binnen 20 seconden na het laatste beveiligde bericht.
- Een beveiligde sessie wordt beëindigd door de HMI/PC Tool van de SV2-serie indien de gebruiker langer dan 10 minuten inactief is.

Wachtwoord-/sleutelbeheer

Een wachtwoord is een zin of tekenreeks die aan de volgende regels moet voldoen:

- Ten minste twaalf tekens lang
- Ten minste één hoofdletter en één kleine letter
- Ten minste één cijfer
- Geen speciale tekens

De kleppen van de SV2-serie worden verzonden met standaardwachtwoorden ingesteld voor OEM en Monteur. Deze wachtwoorden moeten worden gewijzigd voordat u de klep kunt gebruiken in een toepassing zonder observering door gebruikers.

Indien u vergeet het wachtwoord te wijzigen, wordt u blijvend uitgesloten wanneer de beveiligde sessie wordt beëindigd. Dit is een beveiligingsmaatregel die voorkomt dat u een klep in onbeveiligde modus gebruikt (zonder geschikte wachtwoordconfiguratie). Zie afbeelding 5-8.

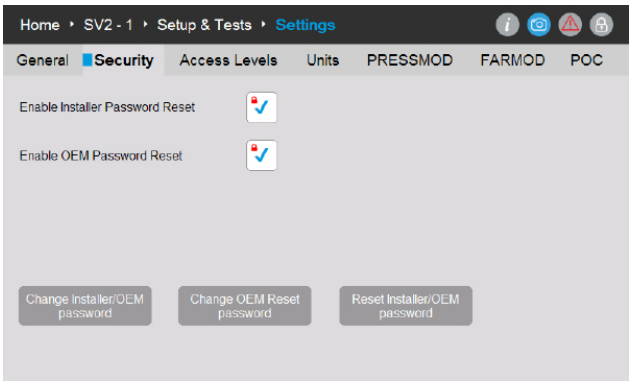


Fig. 6. Wachtwoorden voor OEM, OEM herstellen en Monteur kunnen worden gewijzigd op de beveiligingspagina.

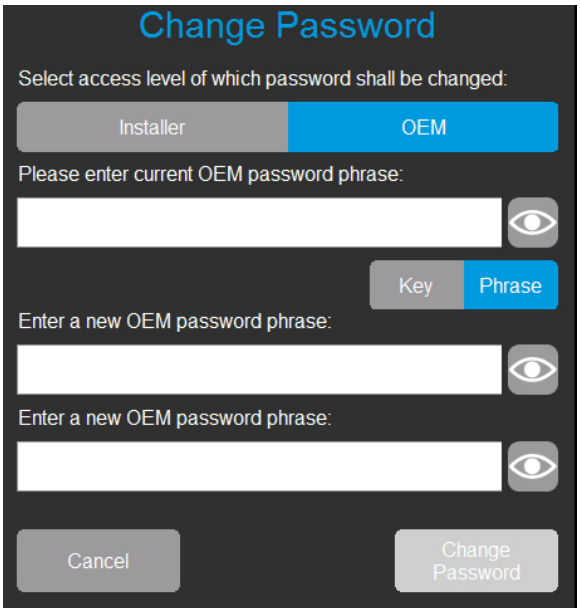


Fig. 7. Gebruiker aangemeld als OEM kan het wachtwoord voor Monteur of OEM wijzigen. Gebruiker voert het huidige OEM-wachtwoord in en het nieuwe wachtwoord twee keer in.

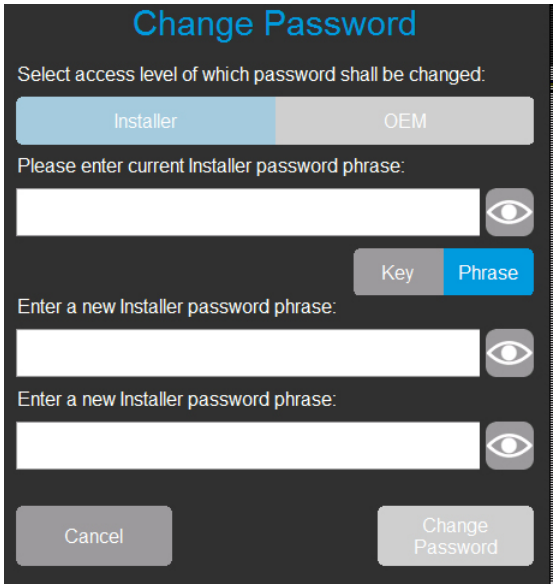


Fig. 8. Gebruiker aangemeld als Monteur kan alleen het wachtwoord voor Monteur wijzigen. Gebruiker voert het huidige Monteur-wachtwoord in en het nieuwe wachtwoord twee keer in.

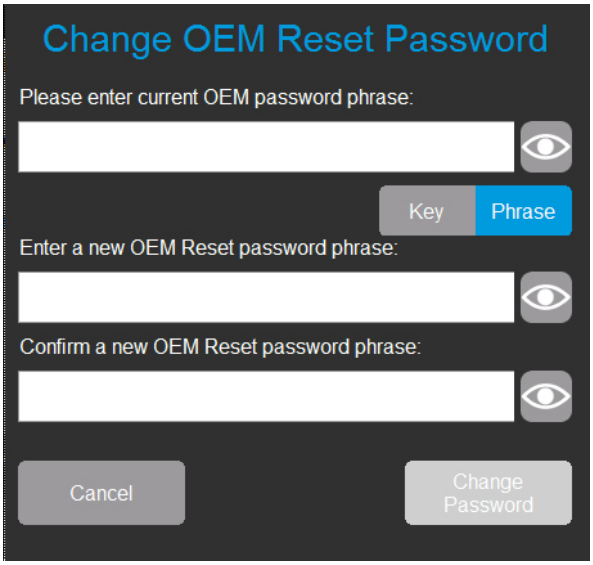


Fig. 9. Gebruiker aangemeld als OEM kan ook het wachtwoord voor OEM herstellen wijzigen. Gebruiker voert het huidige OEM-wachtwoord in en het nieuwe OEM-herstelwachtwoord twee keer in.

Wachtwoord opnieuw instellen

Indien de hoofdwachtwoorden voor Monteur en/of OEM verloren raken, kunt u het wachtwoord herstellen indien de herstelmechanismen door de OEM zijn ingeschakeld. Zie afbeelding 5. Het herstelmechanisme verschilt voor Monteur en OEM. Let op, het wisselen van de stroom naar de klep of de gebruikersinterface overschrijft deze methode niet.

Het wachtwoordherstelmechanisme stelt de geschikte gebruiker in staat om de huidige wachtwoorden terug te zetten naar de standaard fabriekswaarden van Honeywell. Zodra de wachtwoorden zijn hersteld, kan de gebruiker zich aanmelden en nieuwe wachtwoorden toewijzen.

Na het herstellen naar de standaardwaarde, indien de hoofdwachtwoorden voor OEM, Monteur en het OEM-herstelwachtwoord niet zijn ingesteld op een nieuw niet-standaard wachtwoord zal de klep zich in vergrendelde status bevinden en is deze niet operationeel tenzij de OEM-gebruiker is aangemeld. De betreffende wachtwoorden moeten worden geconfigureerd om de foutcode(s) te wissen.

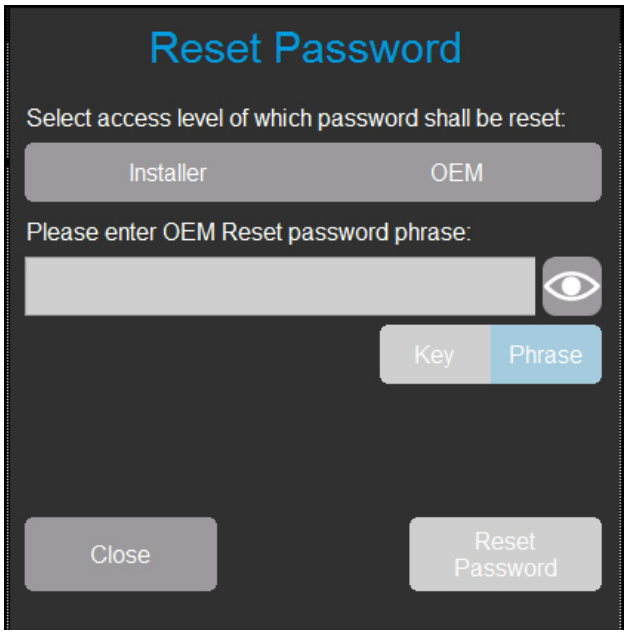


Fig. 10. Gebruiker selecteert het toegangsniveau van het wachtwoord dat moet worden hersteld. Gebruiker voert een geldig herstelwachtwoord in.

De wachtwoordherstelfunctie is standaard voor zowel de Monteur als de OEM uitgeschakeld en moet worden ingeschakeld bij initiële configuratie van elk apparaat door de OEM of de originele eigenaar, zoals aangegeven in afbeelding 5.

OPMERKINGEN:

- **De OEM kan kiezen om de OEM-wachtwoordherstelfunctie in of uit te schakelen. Zie afbeelding 5.**
  - **Indien het is ingeschakeld en het OEM-hoofdwachtwoord raakt verloren, dan kan de OEM de wachtwoorden herstellen naar de standaard fabriekswaarden van Honeywell en nieuwe wachtwoorden toewijzen.**
  - **Indien het is uitgeschakeld en het OEM-hoofdwachtwoord raakt verloren, kan de OEM het wachtwoord niet herstellen en is deze effectief uitgesloten van het aanpassen van de klep op OEM-niveau.**
  - **Indien het hoofdwachtwoord op Monteurniveau bekend is, kan de OEM toegang verkrijgen tot de klep door dit te gebruiken en de parameters aanpassen waar de Monteur toegang tot heeft gekregen.**
  - **Om weer op OEM-niveau te kunnen aanpassen, moeten de hoofdelectronica van de klep worden vervangen en moet de klep volledig opnieuw worden geprogrammeerd, zowel op OEM- als op Monteurniveau.**

Wachtwoordbeveiliging

Om te voorkomen dat een sessiewachtwoord door willekeurige pogingen wordt geraden, worden alle wachtwoorden beveiligd met een mechanisme dat forcering detecteert. Dit mechanisme schakelt het aanmelden tijdelijk uit voor de getroffen account en klep. Het apparaat moet ofwel van stroom worden gewisseld of de persoon die zich wil aanmelden moet ten minste één minuut wachten voor de volgende poging.

Indien dit voorkomt, worden de fouten weergegeven op de diagnosepagina van de HMI/PC Tool. Er zijn vier mogelijke foutcodes die bij deze gebeurtenis horen:

- Account Monteur tijdelijk uitgeschakeld
- Account OEM tijdelijk uitgeschakeld
- Wachtwoordherstelfunctie Monteur tijdelijk uitgeschakeld
- Wachtwoordherstelfunctie OEM tijdelijk uitgeschakeld

Beste werkwijzen

Het wordt aanbevolen om altijd sterke, moeilijk te raden wachtwoorden te gebruiken. Raadpleeg het onderdeel Wachtwoord-/sleutelbeheer eerder in dit document.

Accountbeheer

Er worden twee gebruikersaccounts geïmplementeerd in de kleppen van de SV2-serie. Deze accounts zijn:

1. Monteur
2. OEM

Het account Monteur is ondergeschikt aan het account OEM. Met andere woorden: alle functies die de Monteur kan gebruiken, kunnen door de OEM worden beheerd.

Daarentegen kunnen alle functies die de OEM kan gebruiken, alleen door de OEM worden gebruikt.

Gebruikersaccounts kunnen niet worden verwijderd of toegevoegd en het beoogde gebruik is als volgt:

1. Het account OEM wordt gebruikt om kritieke klepfuncties te configureren zoals configuratie van de drukmodule, de brandstof-/luchtmodule, de brandstof-/luchtontsteking en de basis brandstof-/luchtcurves.
2. Het account Monteur wordt gebruikt om de minder kritieke functies te configureren zoals functionele beperkingen of toepassingsspecifieke variabelen.

Toegangsbeheer

Toegangsrechten zijn standaard configureerbaar voor elke kritieke functie. Het standaard gebruikersniveau voor alle beveiligingsfuncties is op Monteur geconfigureerd en moet naar het OEM-gebruikersniveau worden verhoogd op basis van de specifieke toepassing. Configuratie kan worden uitgevoerd met de Honeywell HMI Tool of PC Tool, zoals aangegeven in afbeelding 11:

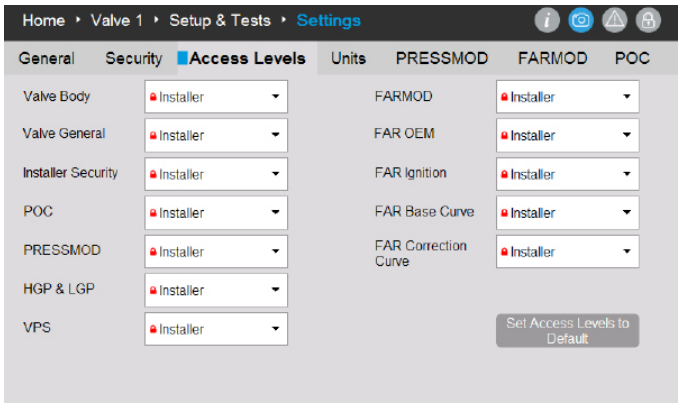


Fig. 11. Pagina toegangsniveaus. Elke configuratiegroep kan worden ingesteld op Monteur, OEM of Alleen lezen.

Externe verbindingsbeveiliging versus fysieke beveiliging

Om externe verbinding via communicatie beveiligd te houden, is het belangrijk om de volgende items te overwegen, die voornamelijk van toepassing zijn op initiële apparaatconfiguratie:

- Wanneer het apparaat fysiek toegankelijk is voor een potentiële aanvaller, kan het herstelwachtwoord voor de Monteur worden verkregen door de aanvaller door dit af te lezen van de sticker achterop de hoofdelektronicadoos van de klep voor later gebruik.
- Wanneer een sessie tot stand wordt gebracht met het standaard wachtwoord van de klep, kunt u dit nooit als beveiligd beschouwen. Het wordt aanbevolen dat u de initiële wachtwoorden voor de accounts OEM en Monteur opnieuw instelt terwijl er geen andere apparaten zijn verbonden met het RS-485-netwerk waarmee de klep is verbonden.

HMI EN PC TOOLS

Als u de kleppen van de SV2-serie en de tools van de gebruikersinterface beveiligd wilt houden, is het essentieel dat u betrouwbare en beveiligde gebruikerstoegang hiervoor aanbiedt. Daarom moeten er verschillende beveiligingsmaatregelen worden getroffen met de PC Tool en de HMI Tool, zoals hieronder beschreven.

HMI-beveiliging

Een losstaande HMI van de SV2-serie moet altijd fysiek worden beveiligd; dezelfde aanbevelingen voor fysieke beveiliging als voor de klep van de SV2-serie zijn van toepassing. Raadpleeg het onderdeel Fysieke apparaatbeveiliging eerder in dit document.

Beveiliging van PC Tool

De PC Tool is ontworpen om te werken op computers met Microsoft® Windows-besturingssystemen. Wanneer u een computer aansluit op een klep van de SV2-serie, zijn eventuele problemen met PC-beveiliging een beveiligingsrisico voor de klep. Daarom wordt het altijd aangeraden om de onderstaande beveiligingsrichtlijnen te volgen:

1. Gebruik altijd een besturingssysteem dat wordt ondersteund door Microsoft.
2. Zorg dat het systeem is bijgewerkt met de meest recente beveiligingsupdates.
3. Zorg dat er altijd antivirussoftware en een firewall is geïnstalleerd en dat deze zijn bijgewerkt.
4. Gebruik de whitelisting-functionaliteit die in het besturingssysteem van de PC is ingeschakeld.
5. Gebruik nooit toepassingen van een onbetrouwbare bron of illegale kopieën van toepassingen.
6. Zorg dat USB-sticks of andere accessoires die aan de PC zijn verbonden van een betrouwbare bron zijn, en geen schadelijke hardware of software bevatten (bijvoorbeeld key loggers, geheugenscanners enz.).
7. Schakel alle onnodige diensten, poorten en gebruikersaccounts op de PC uit, om externe aanvallen te voorkomen.

Een installatiebestand of binair bestand van de toepassing wordt ondertekend met een Honeywell-sleutel om te bevestigen dat het installatieprogramma van PC Tool/de PC Tool-toepassing van een geverifieerde bron komt. Hoewel de ondertekening een goed beveiligingsniveau biedt, wordt het altijd aangeraden om alleen het installatieprogramma van PC Tool/de PC Tool-toepassing te gebruiken die direct door Honeywell wordt aangeboden, of door een geautoriseerde OEM/monteur van Honeywell.

Checklist beveiliging van PC Tool

Als u deze toepassing veilig wilt gebruiken, dient u te controleren of u aan het volgende voldoet:

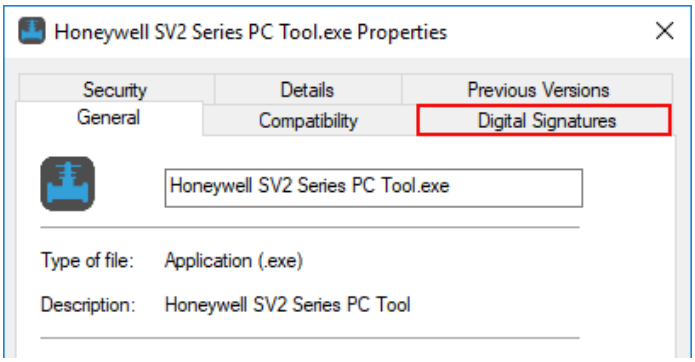
1. U gebruikt alleen een vertrouwde, ondertekende toepassing (zie het onderdeel Oorsprongverificatie van toepassing)
2. Gebruik indien mogelijk het whitelisten van toepassingen (zie het onderdeel Toepassingen whitelisten)
3. U gebruikt antivirusbescherming samen met een correct geconfigureerde firewall indien de PC is verbonden met het internet.
4. Zorg dat de PC waarop u de toepassing uitvoert, is beveiligd met een wachtwoord zodat onbevoegd personeel deze niet kan gebruiken.
5. Zorg dat fysieke toegang tot uw systeem door onbevoegd personeel is uitgesloten of beperkt (PC -> RS485 -> Modbus -> Klep van de SV2-serie).
6. PC Tool moet automatisch worden geïnstalleerd in de standaardmap van Microsoft Windows: ‘Program Files’. Deze installatielocatie is vooraf geselecteerd in het installatieprogramma van PC Tool. Als een andere installatielocatie wordt geselecteerd, moet de gebruiker de beveiligingsmachtigingen (bijv. voor beheerder) configureren om te zorgen dat de installatie van PC Tool niet wordt gesaboteerd door onbevoegd personeel.

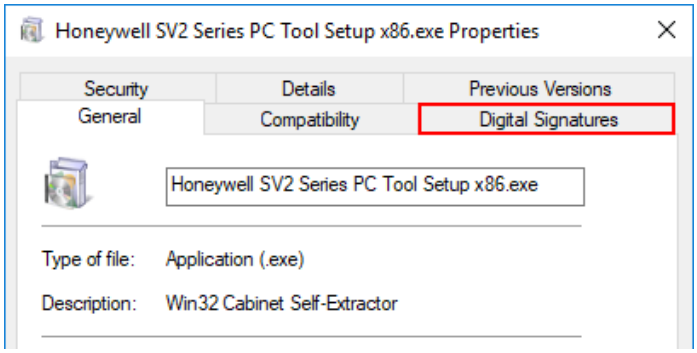
Oorsprongverificatie van de installatieprogramma/de toepassing PC Tool

Het installatieprogramma/de toepassing wordt voorzien van een digitale handtekening. Deze handtekening wordt gecontroleerd nadat er een nieuwe versie van het installatieprogramma/de toepassing is gedownload, of indien de oorsprong van het installatieprogramma/de toepassing in twijfel wordt getrokken.

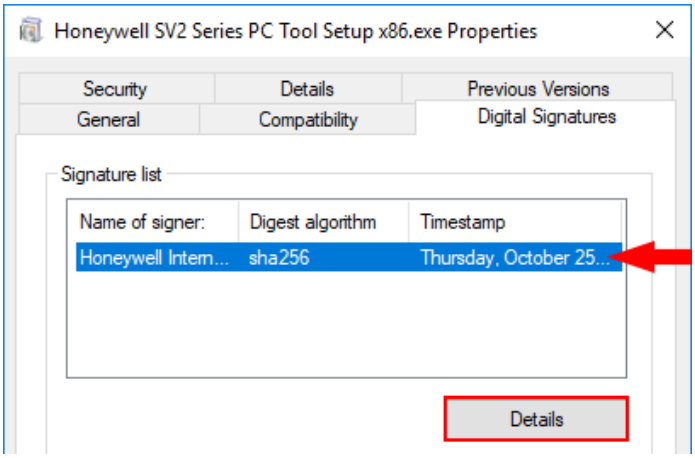
De handtekening kan worden gecontroleerd met de volgende stappen:

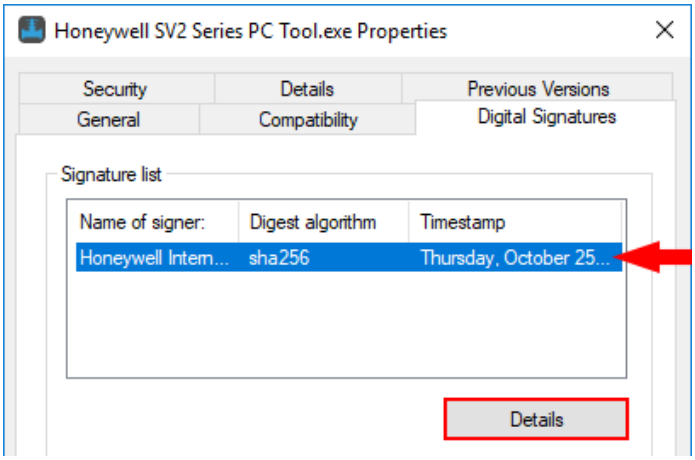
1. Klik op “Honeywell SV2 Series PC Tool Setup x86.exe” / “Honeywell SV2 Series PC Tool Setup x64.exe” met de rechtermuisknop en klik op Eigenschappen
2. Pak de inhoud van “usb_root.zip” uit, klik met de rechtermuisknop op “app. exe” en klik op Eigenschappen.
3. Klik in het venster Eigenschappen op Digitale handtekeningen. Indien dit tabblad niet aanwezig is, gaat u naar stap 5.



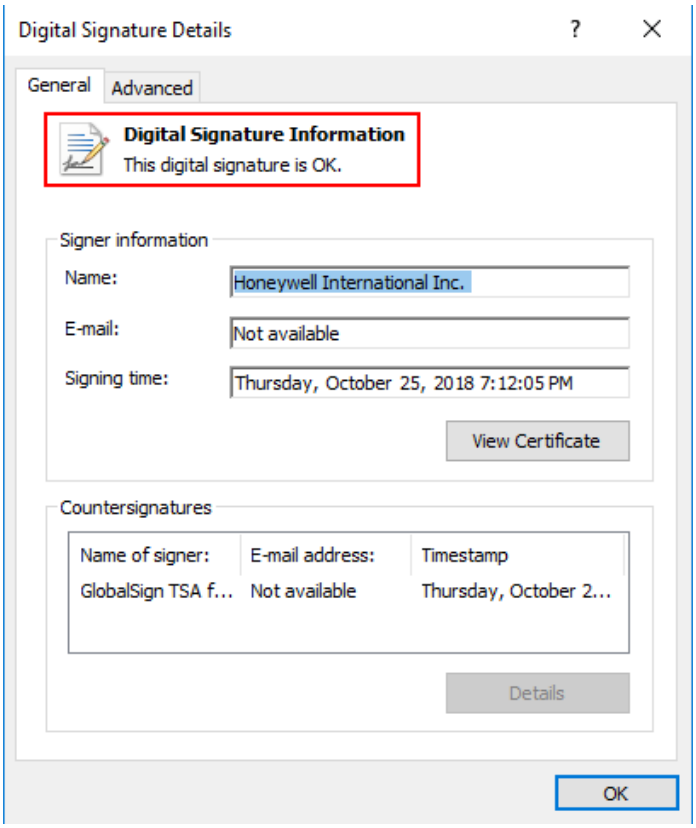


4. In het tabblad Digitale handtekeningen dient het enige item in de lijst met handtekeningen Honeywell International Inc. te heten. Klik op het item en klik op de knop Details.

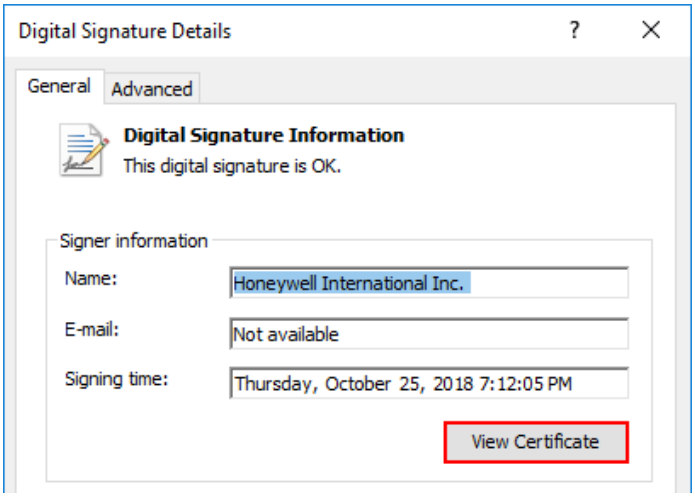




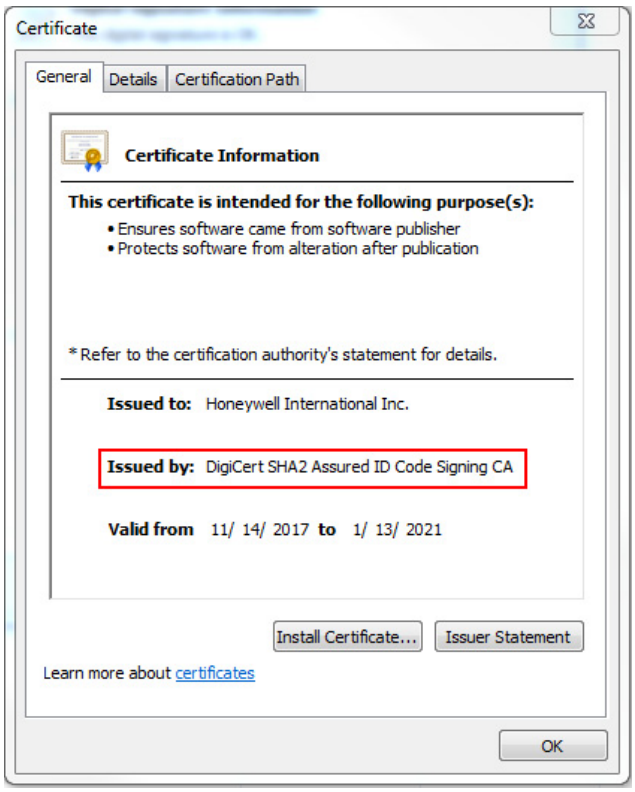
5. In het venster Details digitale handtekening controleert u de gegevens van de digitale handtekening. Hierin moet staan “Deze digitale handtekening is OK.“



6. Indien de handtekening niet OK is, of zelfs niet aanwezig is (er is in stap 2 geen tabblad voor digitale handtekeningen), is de toepassing niet vertrouwd en dient u deze te verwijderen. Een nieuwe, schone kopie kan worden gedownload van de originele bron.
7. U kunt daarnaast ook klikken op de knop Certificaat weergeven, indien u de gegevens van het certificaat wilt controleren.



8. De regel “Uitgegeven door“ in de gegevens van het certificaat moet “DigiCert“ bevatten. Dit is de naam van de certificaatprovider.



Toepassingen whitelisten

Met whitelisten kan de beheerder een lijst instellen van gewenste toepassingen. Toepassingen die niet in deze lijst staan mogen niet worden uitgevoerd. Wanneer u whitelisting instelt, is dit een sterke verbetering van uw beveiliging en minimaliseert dit het risico dat er onbedoelde software op uw apparaat wordt uitgevoerd. Whitelisting is beschikbaar als een ingebouwde tool in Windows-besturingssystemen (Windows 7, Windows 8) of kan worden uitgevoerd door software van derden.

Crashrapport

Wanneer HMI of PC Tool onverwacht vastloopt, wordt een crashrapport gemaakt. De crashrapporten van PC Tool bevinden zich in C:\Users\<gebruiker>\Documents\Honeywell\SV2 Series PC Tool\Crash reports\. Het crashrapport van HMI Tool is toegankelijk via de pagina Home/Display Setup/About. Raadpleeg afb. 1. Het crashrapport bevat de volgende informatie:

- Versie en configuratie van PC Tool
- Versie van Microsoft Windows
- Versie van Microsoft .NET Framework
- Uitzondering- en stacktracering
- Lijst met beschikbare COM-poorten
- Volledige klepconfiguratie

Meer informatie over dit product en de volledige productlijn van de SV2-serie kunt u vinden in de gebruikershandleiding voor de SV2-serie op onze website op https://combustion.honeywell.com/sv2

Voor meer informatie

Onder producten in de Honeywell Thermal Solutions-reeks vallen onder andere Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder en Maxon. Voor meer informatie over onze producten gaat u naar ThermalSolutions.honeywell.com of neemt u contact op met uw Honeywell Sales Engineer.

Honeywell Process Solutions

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

ThermalSolutions.honeywell.com

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