Sicherheitshandbuch für die Serie SV2

PRODUKTDATENBLATT

EINLEITUNG

Dieses Dokument bietet Sicherheitsinformationen für die Ventile der SV2-Serie und Zubehör.

Weitere anwendbare Publikationen sind folgende:

- 32-00029, Sicherheitshandbuch der SV2-Serie
- 32-00031, Tool-Benutzerhandbuch der HMI/PC-Serie

Physischer geräteschutz

⚠ HINWEIS ZUR CYBERSICHERHEIT

Produkte der SV2-Serie enthalten Elektronik und Software. Monteur/Facility Management muss unautorisierten Zugang zum Ventil und zur Programmieroberfläche verhindern, da sonst ggf. Parameter verändert werden könnten.

Unautorisierter Zugang zur Veränderung der Ventil-Verdrahtungsschnittstelle, zum Austausch von Teilen, zur Veränderung der Gerätehardware oder -software darf nicht geduldet werden. Eine Unterlassung dessen kann ein Sicherheitsrisiko darstellen.

Ein fälschungssicheres Etikett wurde im Elektrikgehäuse des Ventils platziert und gibt an, ob ein Zugang erfolgte. Das Etikett befindet sich zwischen der Hauptelektronik des Ventils und dem Elektrikgehäuse, in dem diese sich befindet.

HINWEIS: Die Hauptelektronik des Ventils kann vor Ort ausgetauscht werden. Dafür muss jedoch das Siegel gebrochen werden.

Die Serie-SV2-Ventile sollen unterschiedliche Sicherheits-Funktionen bieten und dadurch jegliche falsche Verwendung verhindern. Es ist jedoch wichtig, sich daran zu erinnern, dass die physische Sicherheit absolut essentiell ist, um viele örtliche Gefahren zu verhindern.

Wählen Sie beim Installieren eines Gerätes immer einen physischen Ort mit limitiertem oder sogar beschränktem Zugang. Es wird empfohlen, das Gerät in einem abgeschlossenen Raum zu verwahren, zu dem approbiertes und geschultes Personal Zugang hat.

Auch wird es streng empfohlen, die gesamte Verkabelung des Gerätes physisch sicher zu verwahren. In Abb. 1 sieht man Beispiele für korrekte und nicht korrekte Verdrahtung.

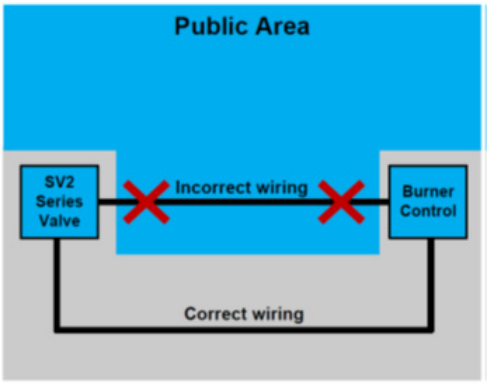


Fig. 1. Beispiele für korrekte und nicht korrekte Verdrahtung

⚠ VORSICHT

Falls die Verdrahtung entsichert wird, könnte eine unautorisierte Person die Verdrahtung des Gerätes fälschen, was Gefahr bedeutet. Die Regelung gilt für die spezifische Verdrahtung der SV2-Serien-Produkte, aber sie gilt auch für jedes andere kontrollierte Gerät.

32-00151G-02

HINWEIS: Dieses Produkt kann Materialien, einschließlich Software, von Dritten enthalten oder von diesen abgeleitet sein. Die Materialien von Drittanbietern können Lizenzen, Hinweisen, Einschränkungen und Verpflichtungen unterliegen, die durch den Lizenzgeber festgesetzt werden. Die Lizenzen, Hinweise, Einschränkungen und Verpflichtungen, sofern zutreffend, finden Sie in den Begleitmaterialien zum Produkt, in den Dokumenten oder Dateien, die diesen Materialien von Drittanbietern beiliegen, in einer Datei mit dem Namen third_party_ licenses auf den Medien, die das Produkt enthalten, oder unter http://www.honeywell.com/ps/thirdpartylicenses.

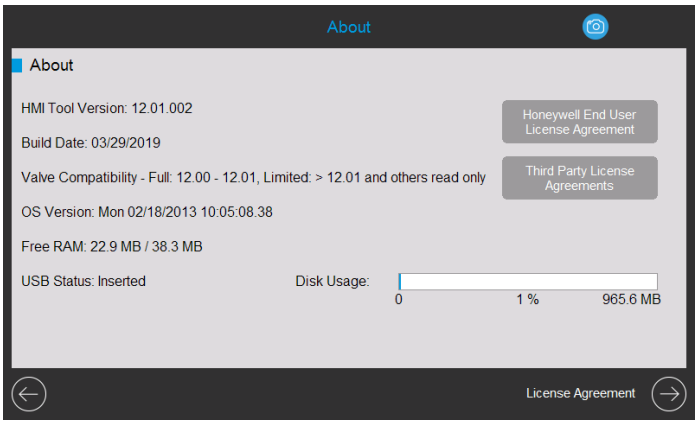


Fig. 2. Infoseite mit Lizenzvereinbarungen.

Zubehörmodule der SV2-Serie

Die Ventile der SV2-Serie unterstützen die Verbindung der Zubehörmodule, welche fortgeschrittene Funktionalität bieten. Diese beinhalten das Kraftstoff-/Luftverhältnis-Modul und das Druck-Modul. Diese Module benötigen eine externe Verdrahtung und wenn diese einmal gefälscht wurde, könnten sie auf gefährliche Art und Weise die Funktionalität des Gerätes beeinflussen, beeinträchtigen oder diese komplett außer Kraft setzen.

Obwohl es nicht offensichtlich scheinen mag, benötigt auch das Kraftstoff-/Luftverhältnis-Modul eine externe Verdrahtung, welche im Falle einer unautorisierten Modifikation einen Geräteausfall verursachen könnte.

MODBUS®-KOMMUNIKATION

Für die Konfiguration der SV2-Serie und die Geräteüberwachung wird die Modbus-Kommunikation unter Anwendung eines RS-485 BUS verwendet. Diese Kommunikation erfordert eine spezielle Vorsicht, wenn es um Sicherheit geht.

Sichere vs. unsichere Kommunikation

Das Modbus-Protokoll ist von Natur aus unsicher und bietet keine eigenen Sicherheitsmittel; die SV2-Serie mit der Firmware-Version 10 und später unterstützt einen gesicherten Modbus, welches eine proprietäre Erweiterung des Standardprotokolls von Honeywell darstellt.

Der gesicherte Modbus unterstützt die Integritätsvalidierung von Nachrichten, sodass diese von niemandem gefälscht werden können, der sich Zugang zum Rohrkabel des RS-485 verschafft. Dieses Protokoll schützt jedoch die Gerätedaten nicht davor, dass diese von unautorisiertem Personal gelesen werden.

Session-Management

Die Ventile der SV2-Serie und HMI/PC-Tools unterstützen eine gesicherte Session bei der Verwendung von Modbus. Dies bedeutet, dass, wenn der Benutzer sich mit einem Passwort entweder in der Installer- oder in der OEM-Zugangsebene einloggt, zwischen der Benutzer-HMI/PC-Kundenapplikation und dem Ventil der SV2-Serie ein gesicherter Tunnel hergestellt wird. Weitere Informationen finden Sie in den Abbildungen. 2-4.

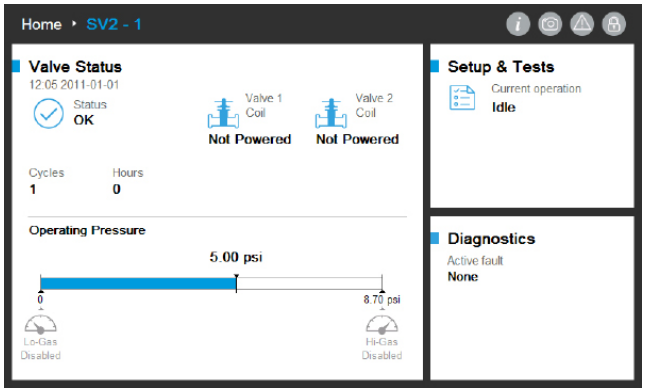


Fig. 3. Session wurde nicht hergestellt. Der Benutzer ist nicht eingeloggt.

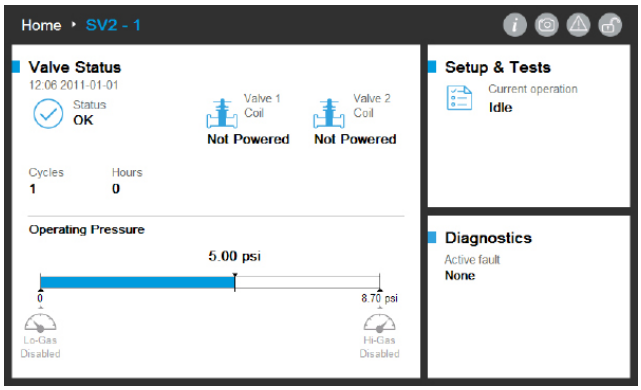


Fig. 4. Session wurde hergestellt. Der Benutzer ist als Installer eingeloggt.

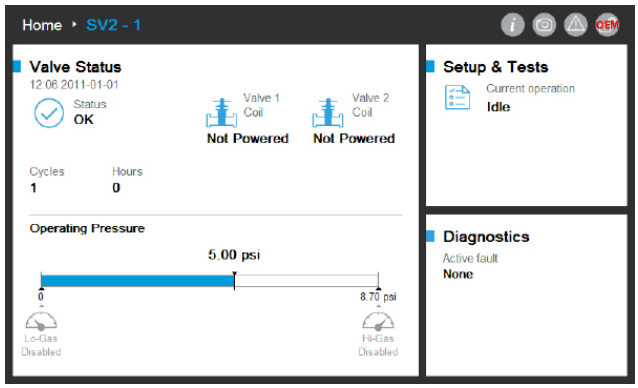


Fig. 5. Session wurde hergestellt. Der Benutzer ist als OEM eingeloggt.

Eine Session muss hergestellt und verwendet werden, um irgendwelche Veränderungen an der Konfiguration des Ventils vornehmen zu können. Typische Konfigurationen sind zum Beispiel folgende:

1. Sicherheitsüberprüfung von kritischen Konfigurationsdaten
2. Abnahmetest der Premix-Ventilkonfiguration
3. Konfiguration des Druckmoduls
4. Sicherheitskonfiguration (Passwort-Setup, Zugang zu Privilegien-Modifikation)
5. Konfiguration des Sicherheitsverschlusses
6. Prüfsequenz des Ventils
7. Einheiten (Druck, Volumen und Undichtigkeit)
8. Allgemeine Ventil-Einstellungen (Modbus Addresse, Baud-Rate)

ANMERKUNGEN:

- Es kann jeweils nur eine Session zur selben Zeit aktiv sein. In anderen Worten, falls ein Benutzer eingeloggt ist, muss ein anderer warten, bis die vorherige Session beendet ist.
- Eine gesicherte Session ist beendet, wenn innerhalb von 20 Sekunden nach der letzten sicheren Nachricht keine sichere Kommunikation mehr erhalten wurde.
- Eine gesicherte Session wird durch ein HMI/PC-Tool der SV2-Serie beendet, wenn der Benutzer mehr als 10 Minuten lang inaktiv ist.

Passwort/Key Management

Ein Passwort ist ein Satz oder eine Zeichenfolge, welche den folgenden Regeln entsprechen muss:

- Mindestens zwölf Zeichen lang
- Mindestens ein Groß- und ein Kleinbuchstabe
- Mindestens eine Zahl
- Keine Sonderzeichen

Die Ventile der SV2-Serie werden mit vorkonfigurierten standardmäßigen OEM und Installer-Passwörtern verschickt. Diese Passwörter müssen geändert werden, bevor das Ventil in einer Applikation ohne Nutzerbeobachtung verwendet werden kann.

Wenn man vergisst, das standardmäßige Passwort zu ändern, wird das eine permanente Sperre hervorrufen, sobald die gesicherte Session beendet wurde. Das ist eine

Sicherheitsmaßnahme, um eine Anwendung des Ventils in einem ungesicherten Modus zu verhindern (ohne korrekte Passwortkonfiguration). Weitere Informationen finden Sie in den Abbildungen. 5-8.

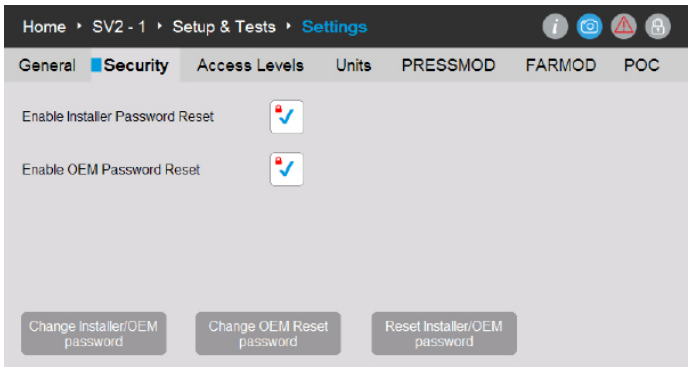


Fig. 6. OEM, OEM-Reset und Installer-Passwörter können auf der Sicherheitsseite geändert werden.

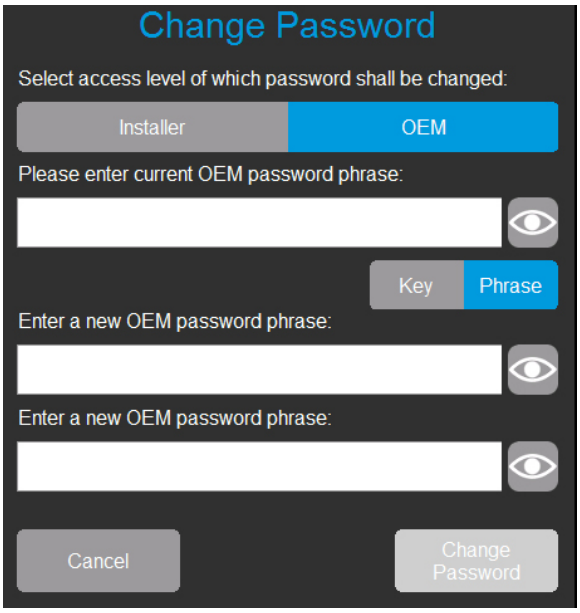


Fig. 7. Ein Benutzer, der als OEM eingeloggt ist, kann das Installer- oder OEM-Passwort ändern. Der Benutzer gibt das gegenwärtige OEM-Passwort und zweimal das neue Passwort ein.

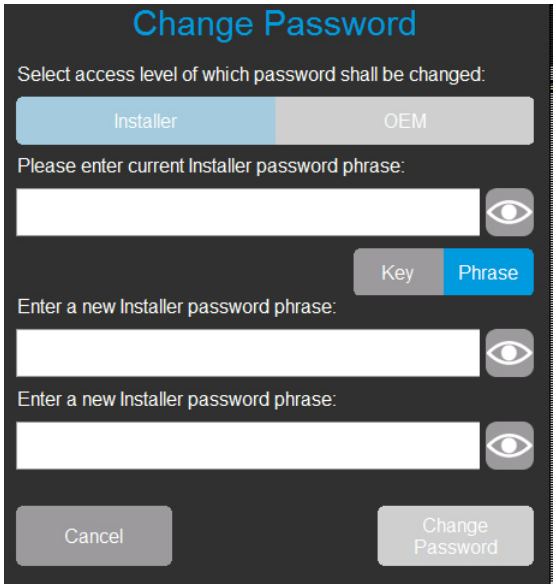


Fig. 8. Ein Benutzer, der als Installer eingeloggt ist, kann nur das Installer-Passwort ändern. Der Benutzer gibt das gegenwärtige Installer-Passwort und zweimal das neue Passwort ein.

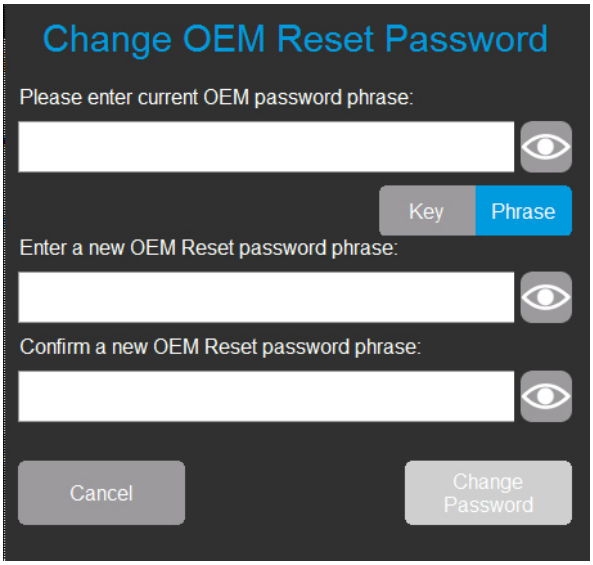


Fig. 9. Ein Benutzer, der als OEM eingeloggt ist, kann auch das OEM-Reset-Passwort ändern. Der Benutzer gibt das gegenwärtige OEM-Passwort und zweimal das neue OEM-Reset-Passwort ein.

Passwort-Reset

Sollten die Hauptzugangs-Passwörter des Installers und/oder des OEM verloren worden sein, ist ein Passwort-Reset möglich, wenn die Reset-Mechanismen vom OEM aktiviert wurden. Weitere Informationen finden Sie in Abb. 5. Der Reset-Mechanismus wird zwischen Installer und OEM variieren. Beachten Sie, dass eine Betätigung des Ventils oder der Benutzeroberfläche diese Vorgehensweise nicht aufhebt.

Der Passwort-Reset-Mechanismus ermöglicht dem richtigen Benutzer nur, das gegenwärtige Passwort/die gegenwärtigen Passwörter auf den standardmäßigen Wert/die standardmäßigen Werte der Honeywell Fabrik zurückzusetzen. Wenn das Passwort/die Passwörter zurückgesetzt wurden, kann der Benutzer sich einloggen und ein neues Passwort/neue Passwörter vergeben.

Wenn die OEM- und Installer-Hauptpasswörter und das OEM-Reset-Passwort nach dem Zurücksetzen auf den Standardwert nicht auf den neuen nicht-standardmäßigen Wert gesetzt wurden, wird das Ventil gesperrt und nicht betriebsbereit sein, bis der OEM-Benutzer angemeldet ist. Das anwendbare Passwort/die anwendbaren Passwörter müssen konfiguriert werden, um den Fehlercode/die Fehlercodes zu löschen.

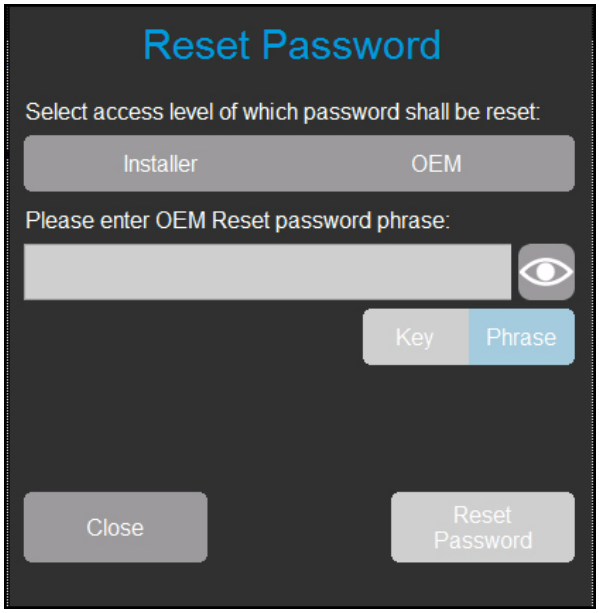


Fig. 10. Ein nicht eingeloggter Benutzer möchte die Zugangsebene des Passwortes zurücksetzen. Der Benutzer gibt einen gültigen Reset-Passwortsatz ein.

Standardmäßig wird die Passwort-Reset-Funktion für den Installer und den OEM deaktiviert und muss nach anfänglicher Konfiguration von jedem Gerät durch den OEM oder den ursprünglichen Besitzer wie in Abb. 5 freigegeben werden.

ANMERKUNGEN:

- **Der OEM kann auswählen, ob er die Passwort-Reset-Funktion aktiviert oder deaktiviert. Weitere Informationen finden Sie in Abb. 5.**
  - **Falls sie aktiviert ist und das OEM-Hauptzugangs-Passwort verloren wurde, kann der OEM die Passwörter auf die standardmäßigen Honeywell Fabrikswerte zurücksetzen und neue Passwörter vergeben**
  - **Falls sie deaktiviert wurde und das OEM-Passwort verloren wurde, kann der OEM das Passwort nicht zurücksetzen und das Ventil auf OEM-Ebene nicht bearbeiten.**
  - **Falls das Hauptpasswort auf Installer-Ebene bekannt ist, kann der OEM damit auf das Ventil zugreifen und die Parameter bearbeiten, auf die der Installer zugreifen kann.**
  - **Um ein Editieren auf OEM-Ebene wieder zu ermöglichen, müsste sowohl auf OEM- als auch auf Installer-Ebene die Elektronik des Ventils ausgetauscht und das Ventil komplett neu programmiert werden.**

Passwortschutz

Um die Möglichkeit zu verhindern, dass ein Session-Passwort durch zufällige Versuche erraten wird, sind alle Passwörter durch einen Brute-Force-Erkennungsmechanismus geschützt. Dieser Mechanismus deaktiviert zwischenzeitlich das Einloggen in das betroffene Konto und Ventil. Die Geräte müssen entweder mit Strom versorgt sein, oder die Person, welche sich einloggen möchte, muss mindestens eine Minute vor dem neuen Versuch warten.

Falls dies passiert, werden auf der HMI/PC-Tool Diagnostikseite Fehlermeldungen erscheinen. Es gibt vier mögliche Fehlercodes, welche damit assoziiert werden:

- Installer-Konto temporär deaktiviert
- OEM-Konto temporär deaktiviert
- Passwort-Reset-Funktion für Installer temporär deaktiviert
- Passwort-Reset-Funktion für OEM temporär deaktiviert

Best Practices

Es wird empfohlen, immer starke, schwer zu erratende Passwörter zu verwenden. Bitte entnehmen Sie Informationen aus dem vorherigen Abschnitt bezüglich Passwort / Key Management dieses Dokuments.

Konto-Management

Es gibt zwei Benutzerkonten, die in den Ventilen der SV2-Serie ausgeführt werden. Diese Konten sind folgende:

1. Installer
2. OEM

Das Installer-Konto gilt als dem OEM-Konto untergeordnet. In anderen Worten können alle dem Installer zugängliche Funktionen durch den OEM kontrolliert werden.

Im Gegensatz dazu können dem OEM zugängliche Funktionen nur vom OEM verwendet werden.

Benutzerkonten können nicht entfernt oder hinzugefügt werden und ihr vorgesehener Zweck ist folgender:

1. Das OEM-Konto wird verwendet, Das OEM-Konto wird verwendet, um kritische Ventilfunktionen zu konfigurieren, wie beispielsweise die Konfiguration des Druckmoduls und des Kraftstoff-/Luftverhältnis-Moduls, die Krafstoff-/Luftzündung und die Kraftstoff-/Luftbasiskurven.
2. Das Installer-Konto wird verwendet, um weniger kritische Funktionen wie die funktionalen Limits oder spezifische Applikationsvariablen zu konfigurieren.

Zugangs-Management

Standardmäßig sind Zugangsprivilegien für jede kritische Funktion konfigurierbar. Die Standard-Benutzer-Ebene für alle Sicherheitsfunktionen ist auf Installer konfiguriert und sollte auf die OEM Benutzer-Ebene, welche auf Applikationsdetails basiert, gehoben werden. Die Konfiguration kann unter Verwendung des Honeywell HMI-Tools oder des PC-Tools wie in Abb. 11 durchgeführt werden:

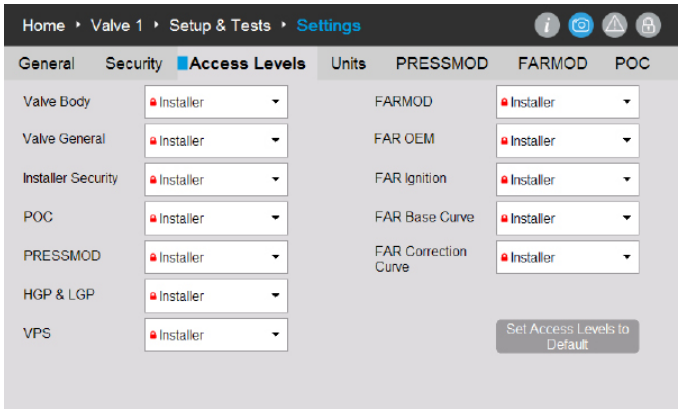


Fig. 11. SeitefürdieZugangsebene.JedeKonfigurationsgruppekönnteaufInstaller,OEM oder Read-Only gesetzt werden.

Fernverbindungs-Sicherheit vs. physische Sicherheit

Um die Fernverbindung über die Kommunikation abzusichern, ist es wichtig, die folgenden Punkte zu beachten, welche hauptsächlich für die anfängliche Gerätekonfiguration gelten:

- Falls das Gerät einem potentiellen Angreifer physisch zugänglich ist, kann der Angreifer das Installer-Reset-Passwort erhalten, indem er es auf dem Sticker auf der Hinterseite der Hauptelektronik des Ventils abliest und so kann es später verwendet werden.
- Falls eine Session unter Anwendung des Standard-Passworts im Ventil hergestellt wird, kann es nie als sicher betrachtet werden. Es wird empfohlen, dass die anfänglichen Passwörter für die OEM- und Installer-Konten nur dann gesetzt werden, wenn kein anderes Gerät auf das RS-485 Netzwerk geschaltet ist, mit welchem auch das Ventil verbunden ist.

HMI- UND PC-TOOLS

Um die Ventile der SV2-Serie und die Benutzeroberflächen-Tools abzusichern, ist es essentiell, verlässliche und sichere Benutzerzugänge zu diesen zu bieten. Aus diesem Grund sollten, wie unten beschrieben, einige Sicherheitsmaßnahmen mit dem PC-Tool und HMI-Tool verwendet werden.

HMI-Sicherheit

Jedes einzelne HMI der SV2-Serie sollte immer physisch sicher aufbewahrt werden; dieselben physischen Sicherheitsempfehlungen gelten wie für die Ventile der SV2-Serie. Entnehmen Sie weitere Informationen dem vorherigen Abschnitt bezüglich physischem Geräteschutz dieses Dokuments.

PC-Tool-Sicherheit

Das PC-Tool ist für die Verwendung auf Computern mit Microsoft® Windows-Betriebssystem vorgesehen. Wenn man einen Computer an ein Ventil der SV2-Serie anschließt, könnten jegliche zutreffende PC-Sicherheitsprobleme ein Sicherheitsrisiko für das Ventil darstellen. Aus diesem Grund wird es immer empfohlen, die Sicherheitspraktiken zu beachten, wie folgt:

1. Verwenden Sie immer ein Betriebssystem, das mit Microsoft kompatibel ist.
2. Halten Sie Ihr System immer mittels der neuesten Sicherheits-Patches auf dem neuesten Stand.
3. Installieren Sie eine Antivirus-Software und eine Firewall und halten Sie diese auf dem neuesten Stand.
4. Verwenden Sie die Whitelisting-Funktion, welche im Betriebssystem des PCs aktiviert ist.
5. Verwenden Sie nie Applikationen aus unverlässlichen Quellen oder geknackte Applikationen.
6. Stellen Sie sicher, dass USB-Sticks oder jegliches weitere Zubehör, das an den PC angeschlossen wird, aus einer verlässlichen Quelle stammen und keine schädliche Hardware oder Software enthalten (z.B. Key Logger, Speicher-Scanner, etc).
7. Deaktivieren Sie alle unnötigen Dienste, Anschlüsse und Benutzerkonten auf dem PC, um ferngesteuerte Angriffe zu verhindern.

Eine Installer-Datei oder Binärdatei zur Applikation ist durch einen Honeywell-Schlüssel signiert, zur Gewissheit, dass der Installer/die Applikation des PC-Tools aus einer verifizierten Quelle stammt. Obwohl jedoch die Signatur einen guten Sicherheitsgrad bietet, wird immer empfohlen, nur denjenigen Installer bzw. diejenige Applikation des PC-Tools zu verwenden, welche direkt von Honeywell oder einem autorisierten Honeywell OEM/Installer stammt.

PC-Tool-Sicherheitscheckliste

Um diese Applikation sicher zu verwenden, achten Sie bitte darauf, dass Sie Folgendes einhalten:

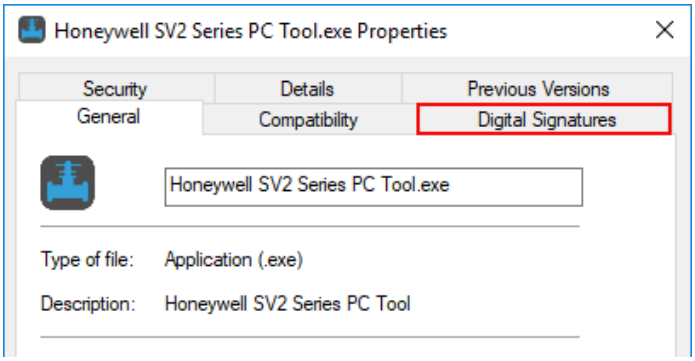
1. Verwenden Sie nur eine zuverlässige, vorzeichenbehaftete Applikation (siehe Abschnitt bezüglich Ursprungsverifikation für Applikationen)
2. Falls es Ihnen möglich ist, verwenden Sie Whitelisting von Applikationen (siehe Abschnitt bezüglich dem Whitelisting von Applikationen)
3. Verwenden Sie einen Antivirus-Schutz mit einer korrekt konfigurierten Firewall, wenn der PC ans Internet angeschlossen ist.
4. Stellen Sie sicher, dass der PC, auf welchen Sie die Applikationen laden, einen Passwortschutz aufweist, sodass unautorisiertes Personal diese nicht verwenden können.
5. Stellen Sie sicher, dass der physische Zugang zu Ihrem System durch unautorisiertes Personal eliminiert oder limitiert wird (PC -> RS485 -> Modbus -> Ventil der SV2-Serie).
6. Das PC-Tool sollte automatisch im Microsoft Windows-Standardordner „Programme“ installiert werden. Dieser Installationsort ist im Installationsprogramm des PC-Tools voreingestellt. Bei Auswahl eines anderen Installationsorts muss der Benutzer die Sicherheitsberechtigungen (z. B. für den Administrator) konfigurieren, um sicherzustellen, dass die Installation des PC-Tools nicht von unbefugtem Personal manipuliert wird.

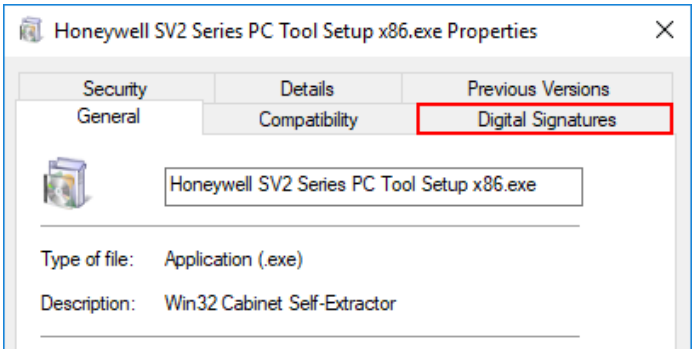
Ursprungsverifikation für die PC-Tool-Installer/Anwendung

Der Installer/Die Applikation ist mit einer digitalen Signatur versehen. Diese Signatur wird nach dem Herunterladen der neuen Version des Installers/der Applikation geprüft, oder es wird, falls jeglicher Verdacht besteht, die Herkunft des ursprünglichen Installers/der ursprünglichen Applikation geprüft.

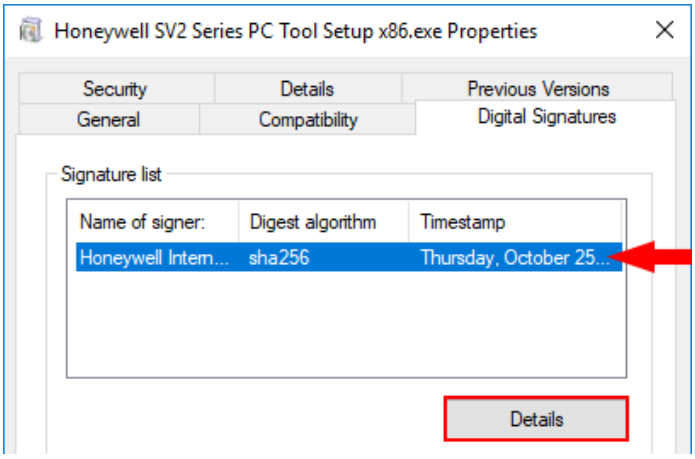
Die Signatur kann geprüft werden, indem man die folgenden Schritte beachtet:

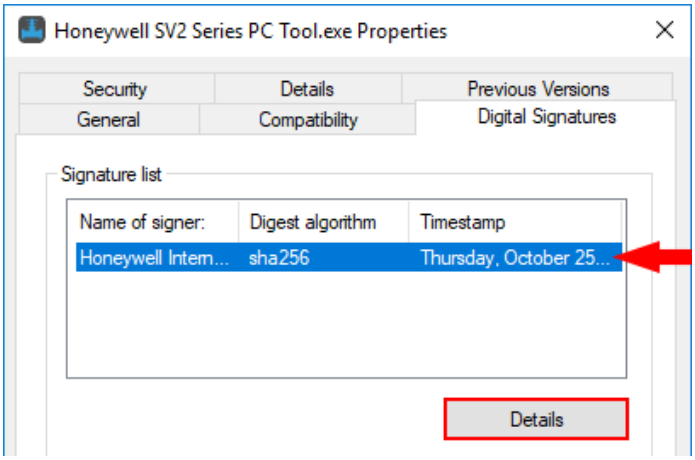
1. Klicken Sie mit der rechten Maustaste auf “Honeywell SV2 Series PC Tool Setup x86.exe” / “Honeywell SV2 Series PC Tool Setup x64.exe” und klicken Sie auf “Properties”
2. Entnehmen Sie Inhalte unter “usb_root.zip”, klicken Sie auf “app. exe” mit der rechten Maustaste und klicken Sie auf “Properties”.
3. Klicken Sie im Eigenschaften-Fenster auf “Digital Signatures”. Falls es diese Registerkarte nicht gibt, gehen Sie zu Schritt 5).



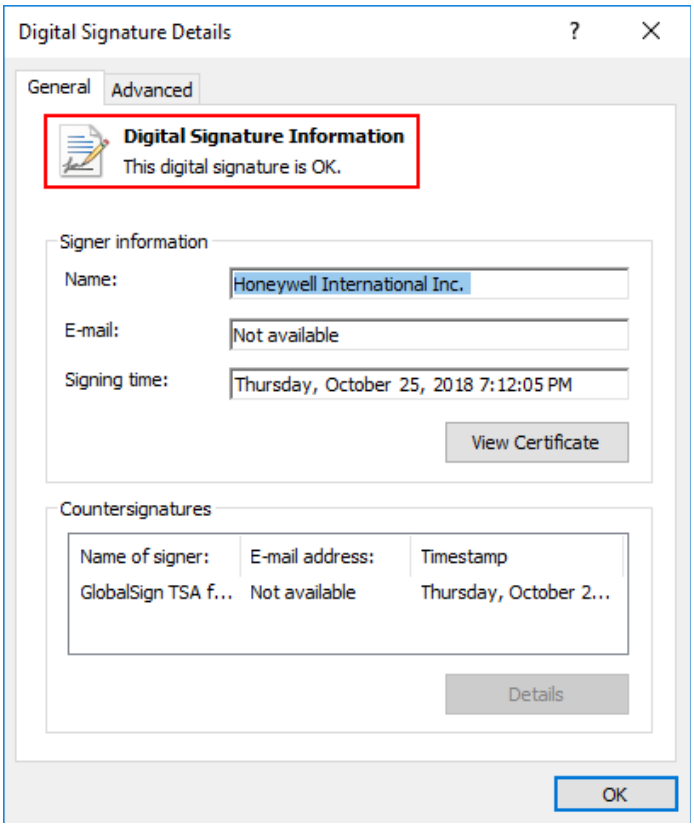


4. Auf der Registerkarte “Digital Signatures” sollte der einzige Punkt in der “Signature list” “Honeywell International Inc.” sein. Klicken Sie auf diesen Punkt und klicken Sie auf “Details”.

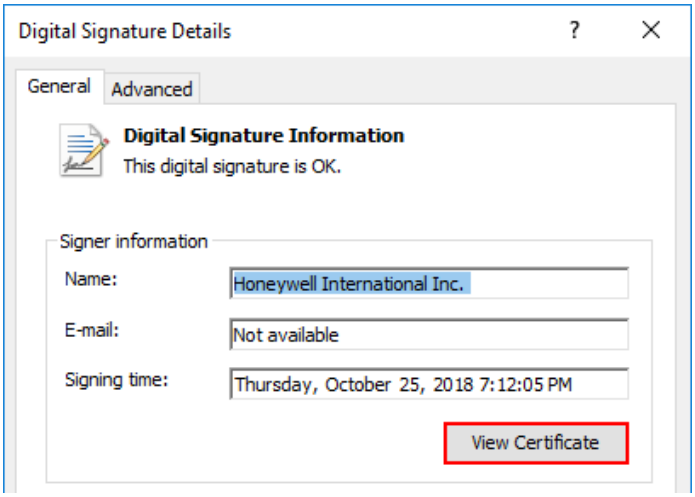




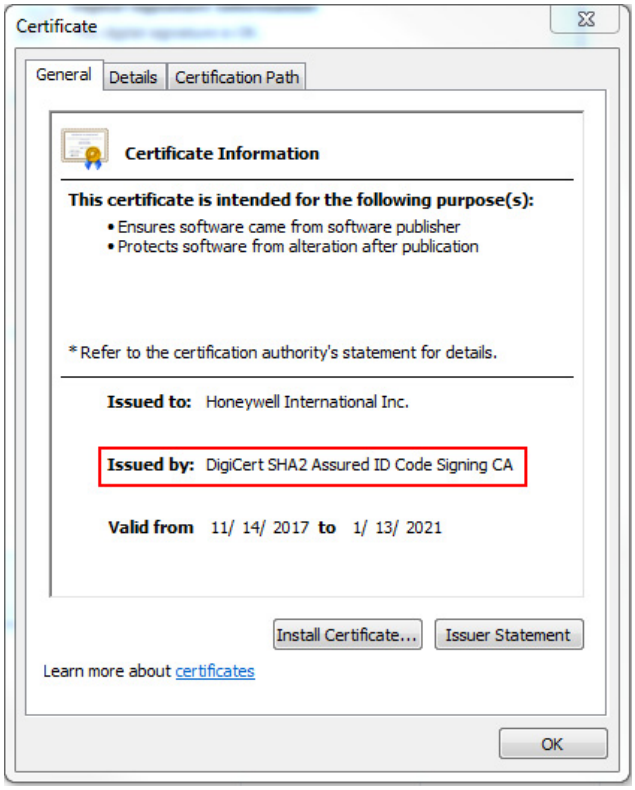
5. Prüfen Sie die “Digital Signature Information” im Fenster “Digital Signature Details”. Es sollte folgende Meldung gezeigt werden: “This digital signature is OK.”



6. Falls die Signatur nicht OK ist oder nicht einmal existiert (in Schritt 2 keine Signaturen-Registerkarte), wird der Applikation nicht vertraut und sie sollte gelöscht werden. Eine neue, saubere Kopie kann aus der ursprünglichen Quelle heruntergeladen werden.
7. Zusätzlich klicken Sie auf “View Certificate”, falls Sie die Details des Zertifikats prüfen möchten.



8. Die Zeile “Issued by” in den Details des Zertifikats muss “DigiCert” enthalten, was der Name des Providers des Zertifikats ist.



Whitelisting-Applikationen

Whitelisting ermöglicht dem Administrator, eine Liste gewünschter Applikationen aufzustellen. Applikationen, die nicht auf dieser Liste stehen, sind nicht erlaubt. Das Aufsetzen von Whitelisting erhöht Ihre Sicherheit in hohem Maße und minimiert das Risiko des Betreibens von ungewollter Software auf Ihrem Gerät. Whitelisting ist als eingebautes Tool im Windows-Betriebssystem verfügbar (Windows 7, Windows 8), oder kann von einer Drittpartei-Software ausgeführt werden.

Absturzbericht

Wenn das HMI- oder das PC-Tool unerwartet abstürzt, wird ein Absturzbericht erstellt. Die PC-Tool-Absturzberichte werden unter C:\Benutzer\<Benutzer>\Dokumente\Honeywell\SV2 Series PC Tool\Absturzberichte\ abgelegt. Der Absturzbericht des HMI-Tools kann über die Seite Home/Display Setup/ About aufgerufen werden. Siehe Abb. 1. Der Absturzbericht enthält die folgenden Informationen:

- Version und Konfiguration des PC-Tools
- Microsoft Windows-Betriebssystemversion
- Microsoft .NET Framework-Version
- Ausnahme und Stack-Trace
- Liste der verfügbaren COM-Ports
- Vollständige Ventilkonfiguration

Weitere Informationen zu diesem Produkt und der gesamten Produktlinie der SV2-Serie finden Sie im Benutzerhandbuch der SV2-Serie auf unserer Website unter https://combustion.honeywell.com/sv2

Weitere Informationen

Zur Produktfamilie Honeywell Thermal Solutions gehören Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder und Maxon. Weitere Informationen zu unseren Produkten finden Sie unter ThermalSolutions.honeywell.com oder wenden Sie sich an Ihren Honeywell-Vertriebsingenieur.

Honeywell Process Solutions

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

ThermalSolutions.honeywell.com

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