Manual de seguridad para la serie SV2

FICHA TÉCNICA DEL PRODUCTO

INTRODUCCIÓN

En este documento, se proporciona información de seguridad para las válvulas y los accesorios de la serie SV2.

Otras publicaciones pertinentes son las siguientes:

- 32-00029, Manual del Usuario para la serie SV2
- 32-00031, Manual del Usuario para la herramienta para HMI/PC

Protección física del dispositivo

⚠ AVISO DE SEGURIDAD CIBERNÉTICA

Los productos de la serie SV2 tienen piezas electrónicas y de software. El instalador o la gerencia de las instalaciones deben tomar recaudos para evitar el acceso no autorizado a la válvula y a la interfaz de programación para modificar parámetros (si corresponde).

No se debe permitir el acceso no autorizado para modificar la interfaz de cableado de la válvula, reemplazar piezas ni cambiar el hardware o software del dispositivo. De no cumplirse lo anterior, puede generarse un riesgo para la seguridad.

Se ha colocado una etiqueta a prueba de manipulación inviolable dentro de la carcasa eléctrica de la válvula para detectar cualquier acceso. La etiqueta se encuentra entre el ensamble electrónico principal de la válvula y la carcasa eléctrica que la contiene.

NOTA: El ensamble electrónico principal de la válvula puede reemplazarse en el sitio y, por lo tanto, se debe romper este sello para reemplazarlo.

Las válvulas de la serie SV2 están diseñadas para proporcionar varias funciones de seguridad con el fin de evitar que se haga un mal uso de ellas de manera remota. Sin embargo, es importante recordar que la seguridad física es absolutamente fundamental para evitar muchas amenazas locales.

Cuando instale un dispositivo, seleccione siempre una ubicación física con acceso limitado o incluso restringido. Se recomienda bloquear el dispositivo en un gabinete cerrado al que solo tenga acceso personal autorizado y capacitado.

Además, se recomienda mantener físicamente seguro todo el cableado del dispositivo. En la Fig. 1, se muestra un ejemplo de cableado correcto e incorrecto.

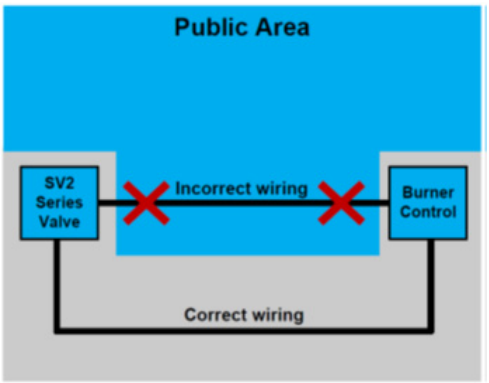


Fig. 1. Ejemplos de cableado correcto e incorrecto

⚠ PRECAUCIÓN

Cuando el cableado del dispositivo no está seguro, una persona no autorizada podría manipularlo, lo cual representa una conducta peligrosa. Esta norma se aplica al cableado específico de los productos de la serie SV2, pero también a cualquier otro equipo controlado.

32-00151S-02

NOTA: Este producto puede contener materiales (incluso software) de terceros o materiales derivados de ellos. Es posible que dichos materiales estén sujetos a licencias, avisos, restricciones y obligaciones impuestas por el licenciante. Las licencias, los avisos, las restricciones y las obligaciones, si los hubiese, se pueden encontrar en los materiales que acompañan al producto, en los documentos o archivos incluidos en dichos materiales, en un archivo llamado third_party_licenses en el medio que contiene el producto o en http://www.honeywell.com/ps/thirdpartylicenses.

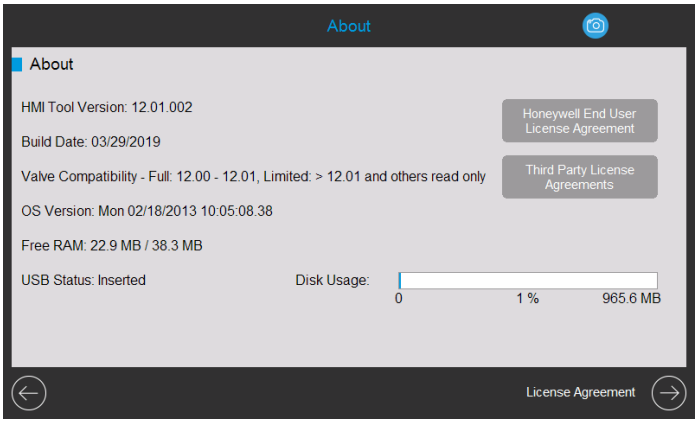


Fig. 2. Página Acerca de con los acuerdos de licencia.

Módulos accesorios de la serie SV2

Las válvulas de la serie SV2 admiten la conexión de módulos accesorios que proporcionan funcionalidad avanzada. Entre estos, se incluyen el módulo aire-combustible y el módulo de presión. Estos módulos utilizan un cableado externo; si se los manipula erróneamente, se puede afectar la funcionalidad del dispositivo de una manera peligrosa, o bien limitarla o, directamente, desactivarla.

Aunque quizás no sea evidente, para el módulo aire-combustible también se utiliza tubería externa que, en caso de que ocurriera una modificación no autorizada, podría provocar la falla del dispositivo.

COMUNICACIÓN MODBUS®

Para la configuración de la serie SV2 y el monitoreo del dispositivo, se usa una comunicación Modbus que utiliza el bus RS-485. Se necesita prestar especial atención a esta comunicación en lo que se refiere a la seguridad.

Comunicación segura frente a comunicación insegura

El protocolo Modbus, por su naturaleza, es inseguro y no proporciona medidas propias de seguridad; sin embargo, la serie SV2 con versión del firmware 10 y superior es compatible con Secured Modbus, que es una extensión del protocolo estándar propiedad de Honeywell.

Secured Modbus admite la validación de integridad de los mensajes, por lo cual nadie que acceda al conductor del RS-485 puede manipularlos. No obstante, este protocolo no protege los datos del dispositivo contra la lectura por parte de personal no autorizado.

Administración de sesión

Las válvulas de la serie SV2 y las herramientas para interfaz hombre-máquina (Human-Machine Interface, HMI) o para computadora personal (Personal Computer, PC) admiten una sesión segura cuando se utiliza Secured Modbus. Esto significa que, cuando el usuario inicia sesión con una contraseña para los niveles de acceso de Instalador o Fabricante de equipo original (Original Equipment Manufacturer, OEM), se establece un canal seguro entre la aplicación cliente HMI/PC del usuario y la válvula de la serie SV2. Consulte las Fig. 2-4.

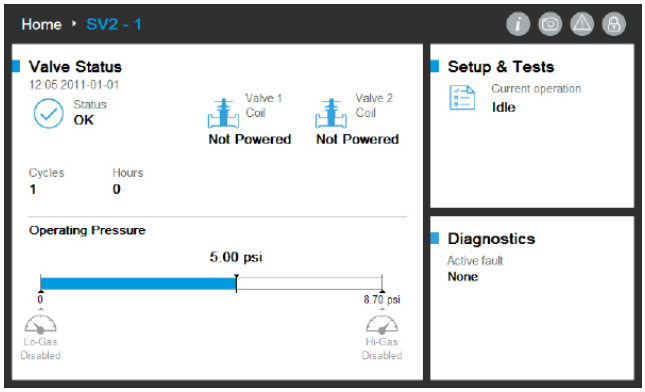


Fig. 3. Sesión no establecida. El usuario no inició sesión.

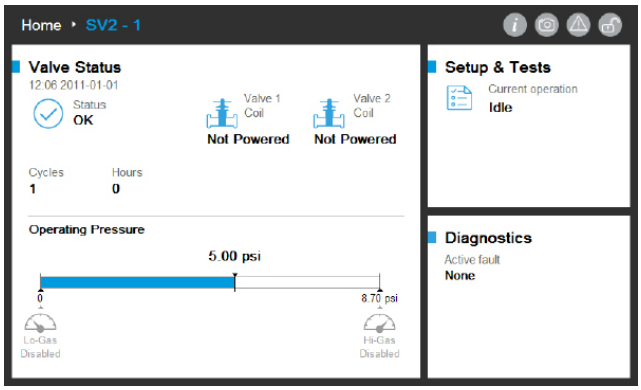


Fig. 4. Sesión establecida. El usuario inició sesión como Instalador.

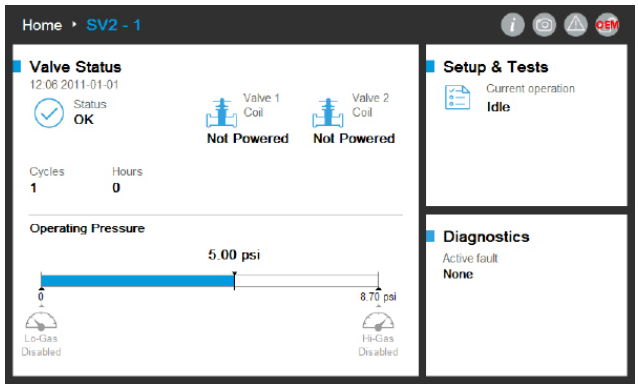


Fig. 5. Sesión establecida. El usuario inició sesión como OEM.

Se debe establecer y usar una sesión para poder modificar la configuración de la válvula. Por ejemplo, las configuraciones habituales son las siguientes:

1. Verificación de seguridad de datos de configuración clave
2. Ejecución de la configuración de la válvula premezcla
3. Configuración del módulo de presión
4. Configuración de seguridad (establecimiento de contraseña, modificación de privilegios de acceso)
5. Configuración de la prueba de cierre
6. Secuencia de prueba de la válvula
7. Unidades (Presión, Volumen y Fuga)
8. Configuración general de la válvula (dirección Modbus, velocidad en baudios)

NOTAS:

- Solo puede haber una sesión activa cada vez. En otras palabras, cuando un usuario inicia sesión, cualquier otro usuario debe esperar hasta que la sesión anterior finalice.
- Una sesión segura se finaliza si no se recibe una comunicación segura dentro de los 20 segundos posteriores al último mensaje seguro.
- La herramienta para HMI/PC de la serie SV2 finaliza una sesión segura si el usuario está inactivo durante más de 10 minutos.

Administración de contraseñas/claves

Una contraseña es una frase o conjunto de caracteres y debe incluir lo siguiente:

- Al menos doce caracteres
- Al menos una mayúscula y una minúscula
- Al menos un número
- Ningún carácter especial

Las válvulas de la serie SV2 se envían con contraseñas para OEM e Instalador predeterminadas configuradas previamente. Estas contraseñas se deben cambiar antes de que se pueda usar la válvula en una aplicación sin observación por parte del usuario.

Si no se modifica la contraseña predeterminada, se produce un bloqueo continuo cuando finaliza la sesión segura. Se trata de una medida de seguridad que evita utilizar la válvula en modo no seguro (sin una configuración adecuada de contraseña). Consulte las Fig. 5-8.

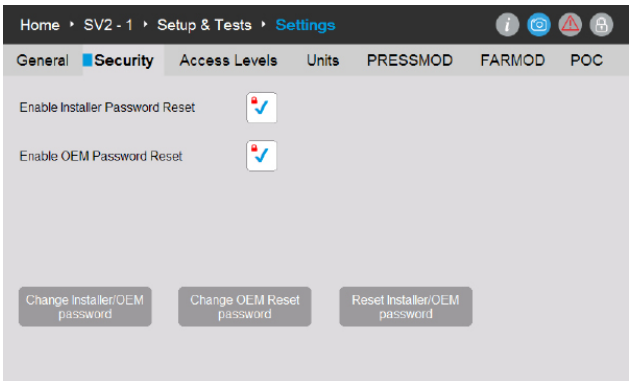


Fig. 6. Las contraseñas de OEM, así como el restablecimiento de OEM e Instalador, se pueden cambiar en la página "Security" (Seguridad).

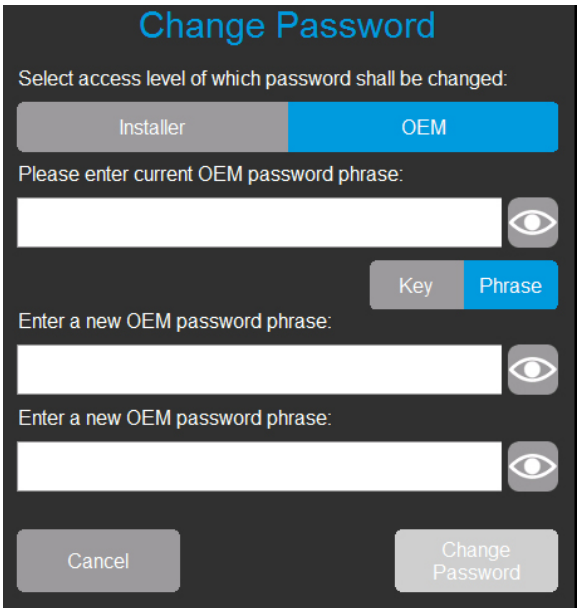


Fig. 7. El usuario que inició sesión como OEM puede modificar la contraseña de OEM o Instalador. El usuario ingresa la contraseña de OEM actual y la nueva contraseña dos veces.

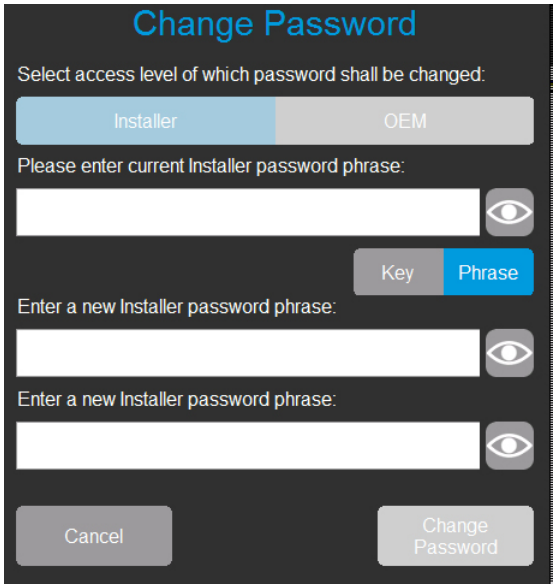


Fig. 8. El usuario que inició sesión como Instalador solo puede modificar la contraseña de Instalador. El usuario ingresa la contraseña de Instalador actual y la nueva contraseña dos veces.

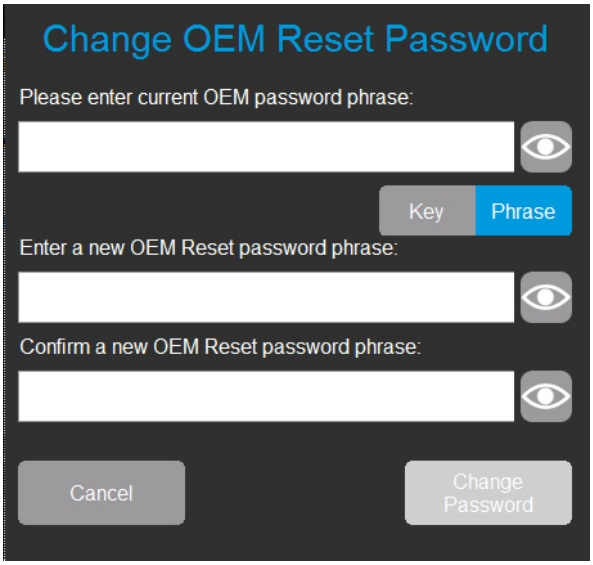


Fig. 9. El usuario que inició sesión como OEM también puede modificar la contraseña de restablecimiento de OEM. El usuario ingresa la contraseña de OEM actual y la nueva contraseña de restablecimiento de OEM dos veces.

Restablecimiento de contraseñas

Si se perdieran las contraseñas del nivel de acceso principal de Instalador u OEM, es posible restablecer la contraseña siempre que el OEM haya activado los mecanismos de restablecimiento. Consulte la Fig. 5. El mecanismo de restablecimiento variará según los niveles de Instalador y OEM. Tenga en cuenta que desconectar la energía de la válvula o de la interfaz de usuario no hará que se saltee esta metodología.

El mecanismo de restablecimiento de contraseña simplemente permite que el usuario correspondiente restablezca la contraseña actual a los valores predeterminados de fábrica de Honeywell. Cuando se restablece la contraseña, el usuario puede iniciar sesión y asignar una contraseña nueva.

Después de restablecer el valor predeterminado, si las contraseñas restablecidas de OEM + Instalador principal y OEM no se establecen en los nuevos valores no predeterminados, la válvula entrará en estado de bloqueo y no será operativa a menos que el usuario OEM inicie sesión. Se debe configurar la contraseña correspondiente para poder borrar los códigos de falla.

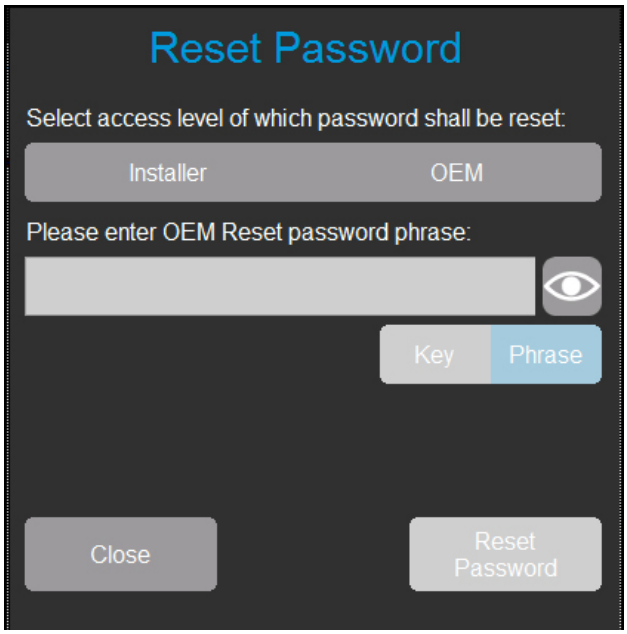


Fig. 10. El usuario invitado selecciona el nivel de acceso de la contraseña que se restablecerá. El usuario ingresa la frase válida para el restablecimiento de la contraseña.

De manera predeterminada, la función de restablecimiento de contraseña del Instalador y del OEM está desactivada y el OEM o el propietario original deben activarla en la configuración inicial de cada dispositivo, como se indica en la Fig. 5.

NOTAS:

- **El OEM puede elegir activar o desactivar la función de restablecimiento de contraseña del OEM. Consulte la Fig. 5.**
  - **Si la función está activada y se pierde la contraseña del OEM principal, el OEM puede restablecer las contraseñas a los valores predeterminados de fábrica de Honeywell y volver a asignar contraseñas nuevas.**
  - **Si la función está desactivada y se pierde la contraseña del OEM principal, el OEM no podrá restablecerla ni tendrá ningún tipo de acceso para editar la válvula a nivel del OEM.**
  - **Si se conoce la contraseña principal del nivel de Instalador, el OEM puede acceder a la válvula usando esa contraseña y, luego, editar los parámetros para los que se le ha otorgado acceso de Instalador.**
  - **Para que sea nuevamente posible la edición a nivel del OEM, se deberá reemplazar la electrónica principal de la válvula y se deberá reprogramar a niveles de OEM y de Instalador.**

Protección de contraseñas

Para evitar que se adivine la contraseña de la sesión mediante intentos aleatorios, todas las contraseñas están protegidas por un mecanismo de detección de violencia. Con este mecanismo, se deshabilita temporalmente el inicio de sesión de la cuenta y la válvula afectadas. Se debe reiniciar el ciclo de los dispositivos o la persona que inicia sesión deberá esperar al menos un minuto antes del siguiente intento.

Si esto ocurre, se anunciarán las fallas en la página “HMI/PC Tool Diagnostics” (Diagnóstico de herramienta para HMI/PC). Hay cuatro códigos de falla posibles relacionados con esta situación:

- Cuenta de Instalador temporalmente desactivada
- Cuenta de OEM temporalmente desactivada
- Función de restablecimiento de contraseña de Instalador temporalmente desactivada
- Función de restablecimiento de contraseña de OEM temporalmente desactivada

Mejores prácticas

Se recomienda usar siempre contraseñas fuertes difíciles de adivinar. Consulte la sección Administración de contraseñas/claves más arriba en este documento.

Administración de cuentas

Existen dos cuentas de usuario implementadas en las válvulas de la serie SV2 y son las siguientes:

1. Instalador
2. OEM

La cuenta de Instalador se considera dependiente de la cuenta de OEM. En otras palabras, el OEM puede controlar todas las funciones accesibles para el Instalador.

En contraposición, solo el OEM puede usar las funciones accesibles para el OEM.

Las cuentas de usuario no se pueden eliminar ni agregar. Su propósito es el siguiente:

1. La cuenta de OEM se usa para configurar las funciones clave de la válvula, como la configuración del módulo de presión, del módulo aire-combustible, el encendido aire-combustible y las curvaturas de base aire-combustible.
2. La cuenta de Instalador se usa para configurar funciones secundarias, como límites funcionales o variables específicas de la aplicación.

Administración de accesos

De manera predeterminada, para cada función clave se pueden configurar privilegios de acceso. El nivel de usuario predeterminado para todas las funciones de seguridad se configura en Instalador y se debe modificar al nivel de usuario OEM según las especificidades de la aplicación. La configuración se puede llevar a cabo con la herramienta para HMI/PC de Honeywell, como se indica en la Fig. 11:

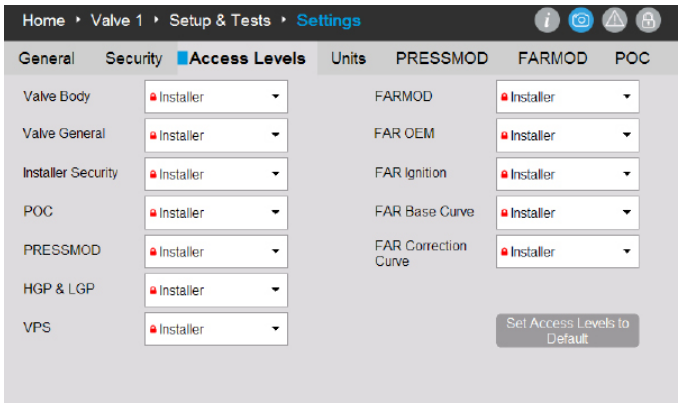


Fig. 11. Página “Access Levels” (Niveles de acceso). Cada grupo de configuración se puede establecer en Instalador, OEM o Solo lectura.

Seguridad de conexión remota frente a seguridad física

Para mantener segura la conexión remota a través del módulo de comunicación, es importante considerar los siguientes elementos que corresponden, principalmente, a la configuración inicial del dispositivo:

- Si el dispositivo es físicamente accesible a un atacante potencial, este puede obtener la contraseña de restablecimiento del Instalador al leerla en la etiqueta adhesiva ubicada en la parte posterior del ensamble principal de la válvula y, luego, puede usarla.
- Si se establece una sesión utilizando la contraseña predeterminada en la válvula, nunca se puede considerar segura. Se recomienda que las contraseñas iniciales de las cuentas de OEM e Instalador se establezcan cuando no haya otros dispositivos presentes en la red del RS-485 donde esté conectada la válvula.

HERRAMIENTAS PARA HMI O PC

Para mantener seguras las válvulas de la serie SV2 y las herramientas para interfaz de usuario, es fundamental otorgar un acceso de usuario confiable y seguro. Por este motivo, se deben tomar varias medidas de seguridad con la herramienta para PC y la herramienta para HMI, como se describe a continuación.

Seguridad de la HMI

Toda HMI independiente de la serie SV2 debe estar siempre físicamente segura. Se aplican las mismas recomendaciones de seguridad física que para la válvula de la serie SV2. Consulte la sección Protección física del dispositivo más arriba en este documento.

Seguridad de la herramienta para PC

La herramienta para PC está diseñada para ejecutarse en computadoras con sistemas operativos de Microsoft® Windows. Cuando conecte una computadora a una válvula de la serie SV2, todos los problemas de seguridad relacionados con una PC pueden significar un riesgo de seguridad para la válvula. Por este motivo, siempre se recomienda implementar las siguientes prácticas de seguridad:

1. Siempre utilice un sistema operativo compatible con Microsoft.
2. Siempre mantenga actualizado el sistema con los últimos parches de seguridad.
3. Siempre tenga instalados y actualizados un software antivirus y un cortafuegos.
4. Utilice la función de listas blancas activada en el sistema operativo de la PC.
5. Nunca utilice aplicaciones de una fuente no confiable ni aplicaciones falsificadas.
6. Asegúrese de que las unidades USB y demás accesorios conectados a la PC vengan de una fuente confiable y de que no incluyan hardware ni software dañinos (por ejemplo, registradores de claves, escáneres de memoria, etc.).
7. Desactive todos los servicios, puertos y cuentas de usuario que no sean necesarios en la PC, a fin de evitar un ataque remoto.

Para brindar garantía de que la aplicación/instalador de herramienta para PC viene de una fuente verificada, un archivo binario de la aplicación o un archivo del instalador está firmado por una clave Honeywell. Sin embargo, aunque la firma proporcione un buen nivel de seguridad, siempre se recomienda usar solamente la aplicación/instalador de herramienta para PC recibida directamente de Honeywell o de un OEM/Instalador de Honeywell autorizado.

Lista de verificación de seguridad de la herramienta para PC

Para usar esta aplicación de manera segura, verifique que se cumpla lo siguiente:

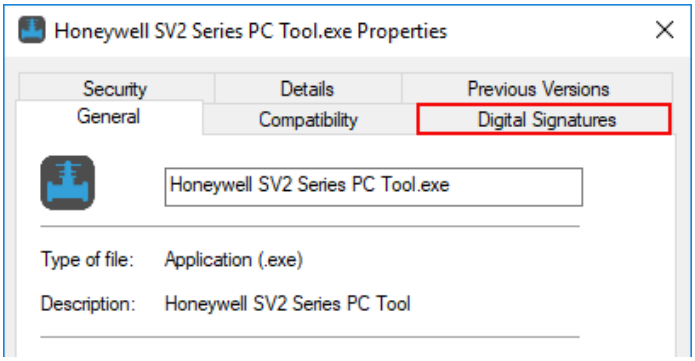
1. Utilice solamente una aplicación confiable y firmada (consulte la sección Verificación de origen de la aplicación).
2. Si es posible, use una lista blanca de aplicaciones (consulte la sección Aplicaciones para crear listas blancas).
3. Use protección antivirus junto con un cortafuegos configurado adecuadamente si la PC está conectada a Internet.
4. Asegúrese de que la PC donde se ejecute la aplicación tenga protección con contraseña para evitar el uso por parte de personal no autorizado.
5. Asegúrese de que el personal no autorizado no tenga acceso físico al sistema o de que tenga acceso limitado (PC -> RS485 -> Modbus -> Válvula de la serie SV2).
6. La herramienta para PC se debe instalar de forma automática en la carpeta predeterminada de Archivos de programa de Microsoft Windows. La ubicación para la instalación está preseleccionada en el instalador de la herramienta para PC. Si selecciona una ubicación diferente, el usuario debe configurar los permisos de seguridad (p. ej., para el administrador) para evitar que personal no autorizado manipule la instalación de la herramienta para PC.

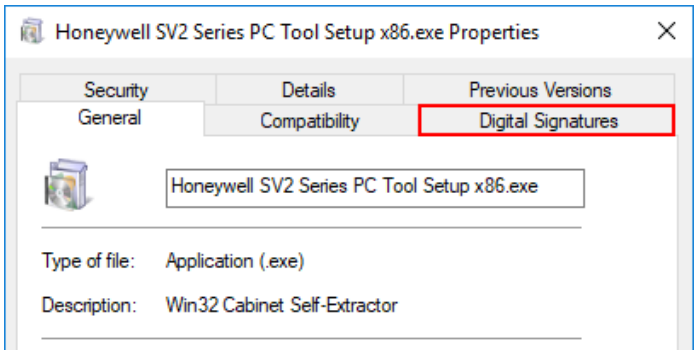
Verificación de origen de la aplicación/ instalador de herramienta para PC

La aplicación/instalador incluye una firma digital. La firma se verificará luego de descargar una nueva versión de la aplicación/instalador o si existe alguna sospecha del origen de la aplicación/instalador.

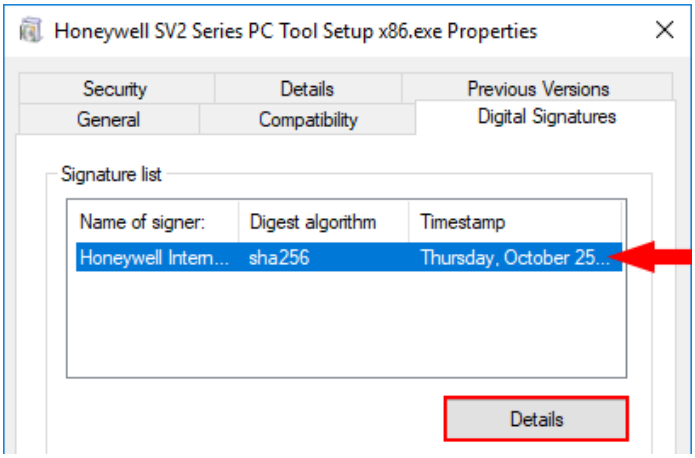
La firma se puede verificar mediante los siguientes pasos:

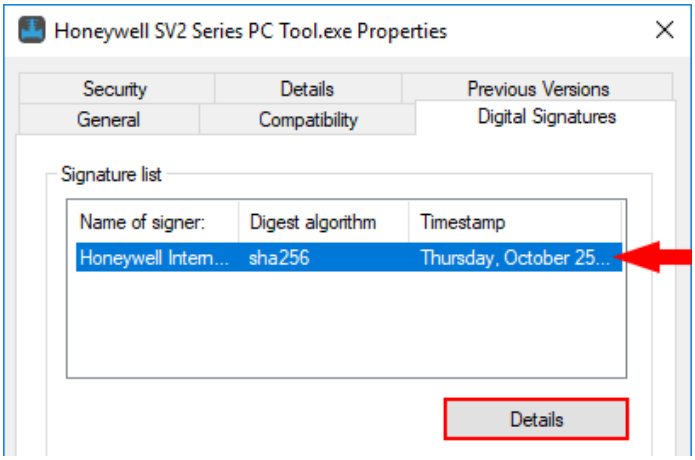
1. Haga clic en “Honeywell SV2 Series PC Tool Setup x86. exe” / “Honeywell SV2 Series PC Tool Setup x64.exe” con el botón derecho del mouse y, luego, haga clic en “Properties” (Propiedades).
2. Extraiga el contenido de “usb_root.zip” y haga clic en “app. exe” con el botón derecho del mouse; luego, haga clic en “Properties” (Propiedades).
3. En la ventana “Properties” (Propiedades), haga clic en “Digital signatures” (Firmas digitales). Si no aparece la pestaña, continúe al paso 5.



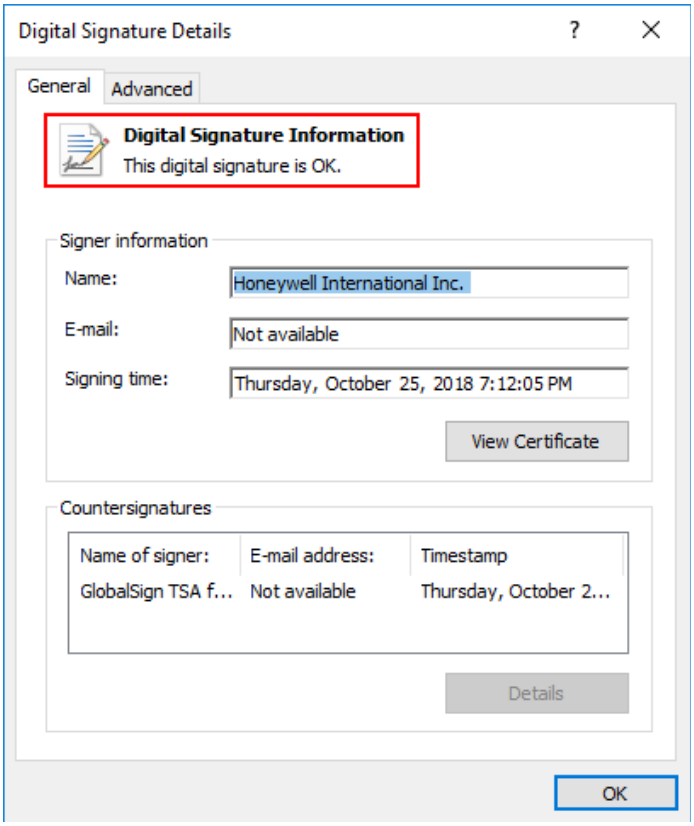


4. En la pestaña “Digital signatures” (Firmas digitales), el único elemento en “Signature list” (Lista de firmas) debe ser “Honeywell International Inc.”. Haga clic ahí y, luego, haga clic en el botón “Details” (Detalles).

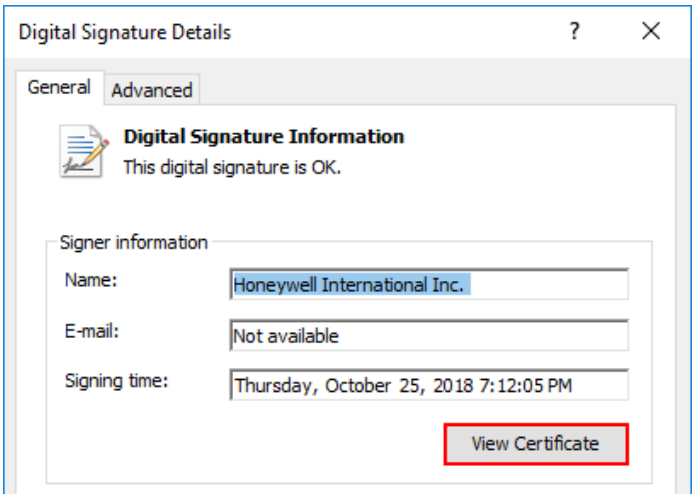




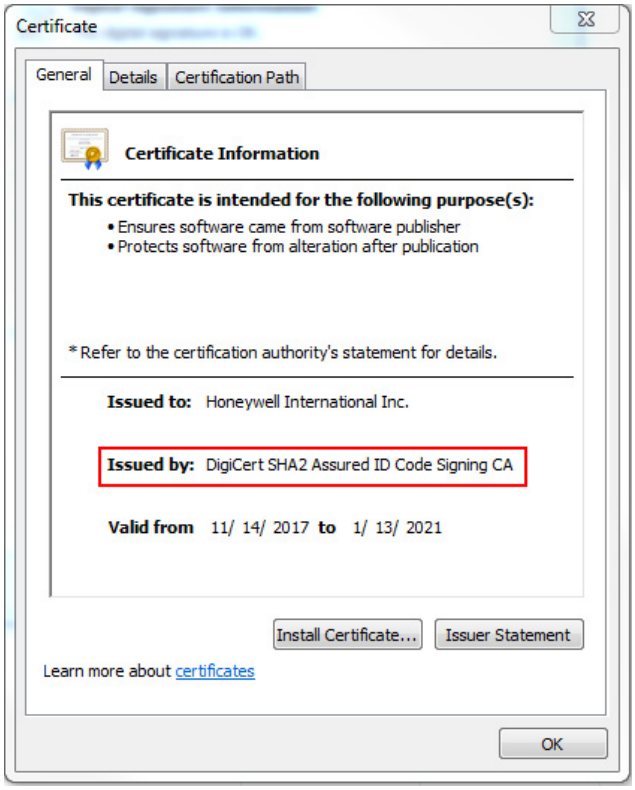
5. En la ventana “Digital Signature Details” (Detalles de la firma digital), haga clic en “Digital Signature Information” (Información de la firma digital). Debería decir “This digital signature is OK” (Esta firma digital es correcta).



6. Si la firma no es correcta o si no hay firma (cuando en el paso 2 no hay pestaña de firma digital), la aplicación no es confiable y se debe eliminar. Se puede descargar una copia nueva y limpia de la fuente original.
7. Además, si desea verificar los detalles del certificado, haga clic en el botón “View Certificate” (Ver certificado).



8. El campo “Issued by” (Publicado por) en los detalles del certificado debe presentar el texto “DigiCert”, que es el nombre del proveedor del certificado.



Aplicaciones para crear listas blancas

La creación de listas blancas permite que el administrador configure una lista de aplicaciones deseadas. No se permitirá la ejecución de aplicaciones que no estén en esta lista. Configurar listas blancas aumenta notablemente la seguridad y reduce el riesgo de ejecutar software de manera involuntaria en su máquina. La creación de listas blancas está disponible como una herramienta incorporada en los sistemas operativos de Windows (Windows 7, Windows 8). Asimismo, se pueden crear con software de terceros.

Informe de error

Cuando se produce algún error inesperado en la herramienta HMI o de PC, se elabora un informe de error. Los informes de error de la herramienta de PC se encuentran en C:\Users\<user>\Documents\Honeywell\SV2 Series PC Tool\Crash reports\. Se puede acceder a los informes de error de la herramienta HMI desde la página Home/Display Setup/About. Consulte la Fig. 1. El informe de error contiene la siguiente información:

- Versión y configuración de la herramienta de PC
- Versión del sistema operativo de Microsoft Windows
- Versión del marco de trabajo de Microsoft .NET
- Excepción y seguimiento de pila
- Lista de puertos de comunicación disponibles
- Configuración completa de la(s) válvula(s)

Para obtener más información sobre este producto y sobre toda la línea de productos de la serie SV2, consulte el manual del usuario de la serie SV2 en nuestro sitio web https://combustion.honeywell.com/sv2

Para obtener más información:
La familia de productos de Honeywell Thermal Solutions incluye Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder y Maxon. Para conocer más sobre nuestros productos, visite ThermalSolutions.honeywell.com o comuníquese con su ingeniero de Ventas de Honeywell.

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

ThermalSolutions.honeywell.com

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