Manuale sulla sicurezza Serie SV2

FOGLIO DATI DEL PRODOTTO

INTRODUZIONE

Il presente documento offre le informazioni sulla sicurezza relative alle valvole e agli accessori Serie SV2.

Altre pubblicazioni applicabili:

- 32-00029, Manuale dell'utente Serie SV2
- 32-00031, Manuale dell'utente Strumento PC/IUM

Protezione del dispositivo fisico

⚠ AVVISO SULLA SICUREZZA INFORMATICA

I prodotti Serie SV2 contengono componenti elettronici e software. L'installatore o il gestore della struttura deve prestare attenzione al fine di prevenire l'accesso non autorizzato alla valvola e all'interfaccia di programmazione per la modifica dei parametri (se applicabile).

Non deve essere consentito l'accesso non autorizzato per modificare l'interfaccia del cablaggio della valvola, sostituire parti, modificare l'hardware o il software del dispositivo. L'inosservanza di tale misura può comportare un rischio per la sicurezza.

Un'etichetta anti-manomissione è stata collocata all'interno dell'unità elettrica della valvola per indicare se si è verificato l'accesso. L'etichetta è posizionata tra il gruppo elettronico principale della valvola e l'armadio elettrico in cui è inserito.

NOTA: il gruppo elettronico principale della valvola può essere sostituito sul campo, quindi è necessario rompere il sigillo per sostituirlo.

Le valvole Serie SV2 sono ideate per fornire varie funzionalità di sicurezza avanzate per evitarne l'uso improprio da remoto. Ad ogni modo, è importante ricordare che la sicurezza fisica è assolutamente fondamentale per evitare numerose minacce locali.

Nell'installazione di un dispositivo, selezionare sempre un luogo fisico con accesso limitato o addirittura circoscritto. È consigliabile conservare il dispositivo in un armadio chiuso con accesso consentito esclusivamente al personale approvato e formato.

In aggiunta, è vivamente consigliato di mantenere fisicamente sicuro tutto il cablaggio del dispositivo. Gli esempi del cablaggio corretto e scorretto sono mostrati in Fig.1.

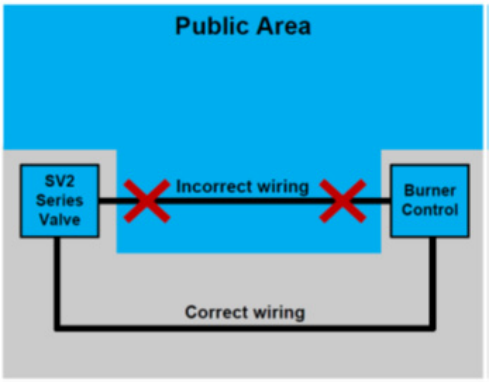


Fig. 1. Esempi di cablaggio corretto e scorretto

⚠ ATTENZIONE

Quando il cablaggio non è sicuro, un soggetto non autorizzato potrebbe manomettere il cablaggio del dispositivo, generando un comportamento pericoloso. Questa norma si applica al cablaggio specifico dei prodotti Serie SV2, tuttavia si applica anche ad altre apparecchiature controllate.

32-00151I-02

NOTA: questo prodotto può contenere o essere derivato da materiali di terze parti, compresi i software. I materiali di terze parti possono essere soggetti a licenze, avvisi, restrizioni e obblighi imposti dal Licenziante. Le licenze, le notifiche, le restrizioni e gli obblighi, se presenti, posso essere ritrovati nei materiali che accompagnano il prodotto, nei documenti o nei file che accompagnano tali materiali di terze parti, in un file denominato third_party_licenses sui supporti contenenti il prodotto o all'indirizzo http://www.honeywell.com/ps/thirdpartylicenses.

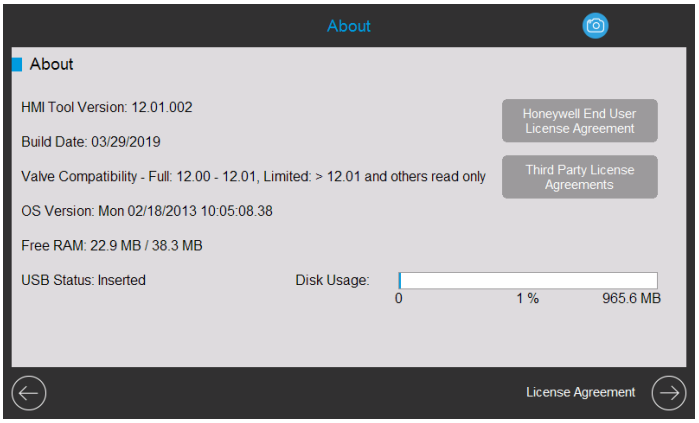


Fig. 2. Informazioni sulla pagina con i contratti di licenza.

Moduli degli accessori Serie SV2

Le valvole Serie SV2 supportano la connessione ai moduli degli accessori fornendo funzionalità avanzate. Questi includono il Modulo rapporto aria/combustibile e il Modulo pressione. I suddetti moduli si avvalgono del cablaggio esterno, il quale se manomesso, potrebbe influire sulla funzionalità del dispositivo in modo pericoloso, limitarlo o disabilitarlo completamente.

Benché possa non essere così ovvio, il Modulo rapporto carburante/aria impiega anche una tubazione esterna, la quale in caso di modifica non autorizzata, potrebbe comportare un malfunzionamento del dispositivo.

COMUNICAZIONE MODBUS®

Per la configurazione e il monitoraggio del dispositivo Serie SV2, è utilizzata la comunicazione Modbus che impiega il bus RS-485. La suddetta comunicazione necessita di particolare attenzione per quanto attiene alla sicurezza.

Comunicazione sicura e non sicura a confronto

Il protocollo Modbus è di natura non sicuro e non offre mezzi nativi per la sicurezza. Ciononostante, la Serie SV2 che esegue la versione 10 e successive del firmware supporta il Modbus sicuro, ovvero un'estensione proprietaria di Honeywell del protocollo standard.

Il Modbus sicuro supporta la convalida dell'integrità dei messaggi, affinché non possano essere compromessi da alcun soggetto che accede al canale RS-485. Tuttavia, il protocollo non protegge i dati del dispositivo dalla lettura da parte di personale non autorizzato.

Gestione delle sessioni

Le valvole Serie SV2 e gli Strumenti IUM/PC supportano una sessione sicura quando il Modbus sicuro è impiegato. Ciò significa che quando un utente accede con una password per i livelli di accesso Installatore o OEM, è stabilito un tunnel sicuro tra l'applicazione client IUM/PC dell'utente e la valvola Serie SV2. Consultare Fig. 2-4.

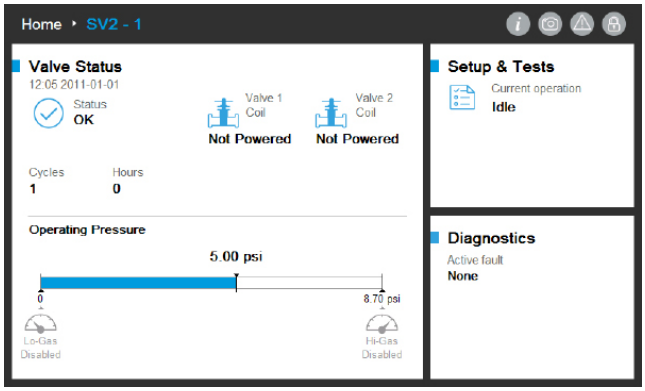


Fig. 3. Sessione non stabilita. Utente non connesso.

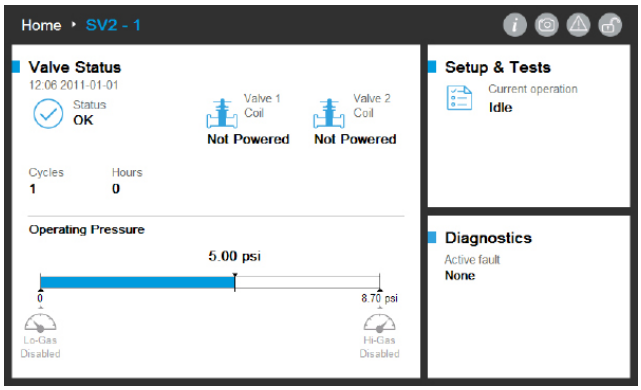


Fig. 4. Sessione stabilita. Utente connesso come Installatore.

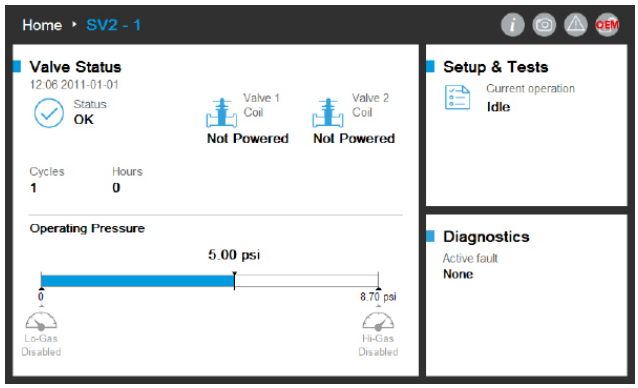


Fig. 5. Sessione stabilita. Utente connesso come OEM.

È necessario stabilire e utilizzare una sessione per essere in grado di apportare modifiche alla configurazione della valvola. Ad esempio, le configurazioni tipiche sono:

1. Verifica della sicurezza dei dati di configurazione critici
2. Messa in funzione della configurazione della valvola premix
3. Configurazione del modulo pressione
4. Configurazione della sicurezza (impostazione password, modifica dei privilegi di accesso)
5. Prova della configurazione di chiusura
6. Sequenza di verifica della valvola
7. Unità (pressione, volume e perdite)
8. Impostazionigeneralidellavalvola(indirizzoModbus,velocità baud)

NOTE:

- Può essere attiva un'unica sessione alla volta. In altre parole, quando un utente è connesso, un altro deve attendere fino a che la sessione precedente sia terminata.
- Una sessione sicura si ritiene terminata quando non viene ricevuta alcuna comunicazione sicura entro i 20 secondi dopo la ricezione dell'ultimo messaggio sicuro.
- Una sessione sicura è terminata dallo Strumento IUM/PC Serie SV2 se l'utente non è più attivo da oltre di 10 minuti.

Gestione password/chiave

Una password è una frase o una stringa di caratteri che necessita di soddisfare le seguenti norme:

- Contenere almeno dodici caratteri
- Almeno un carattere maiuscolo e un carattere minuscolo
- Contenere almeno un numero
- Nessun carattere speciale

Le valvole Serie SV2 vengono fornite con le password predefinite OEM e Installatore preconfigurate. Prima che la valvola possa essere utilizzata in un'applicazione senza l'osservazione dell'utente è necessario modificare le suddette password.

Dimenticare di cambiare la password predefinita ha come risultato il blocco persistente quando la sessione sicura è terminata. Si tratta di una misura di sicurezza che evita l'impiego della valvola in modalità non sicura (senza un'adeguata configurazione della password). Consultare Fig. 5-8.

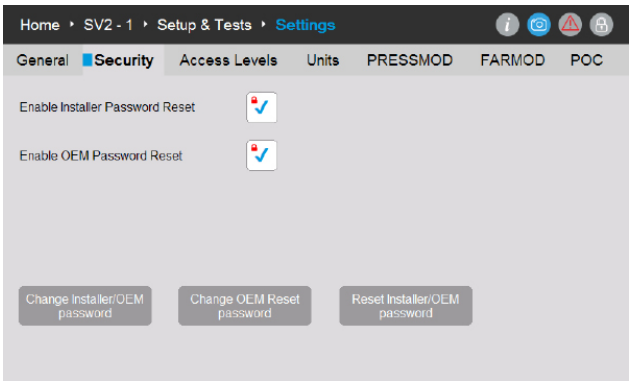


Fig. 6. Alla pagina Sicurezza, è possibile modificare OEM, Reset OEM e password Installatore.

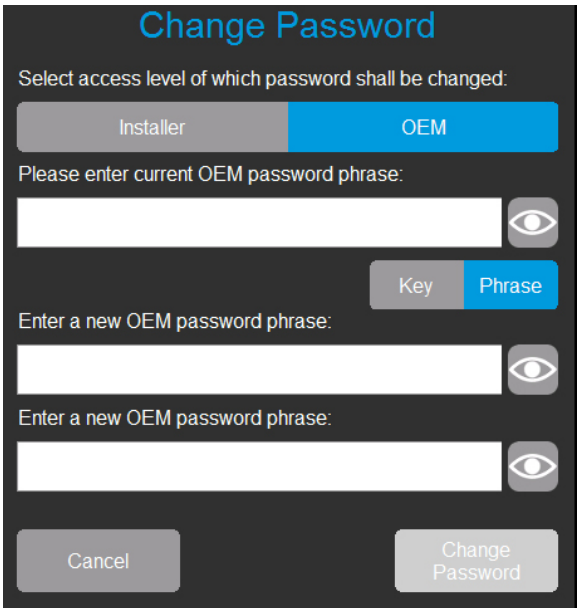


Fig. 7. L'utente connesso come OEM può modificare le password Installatore o OEM. L'utente immette la password OEM corrente e la nuova password due volte.

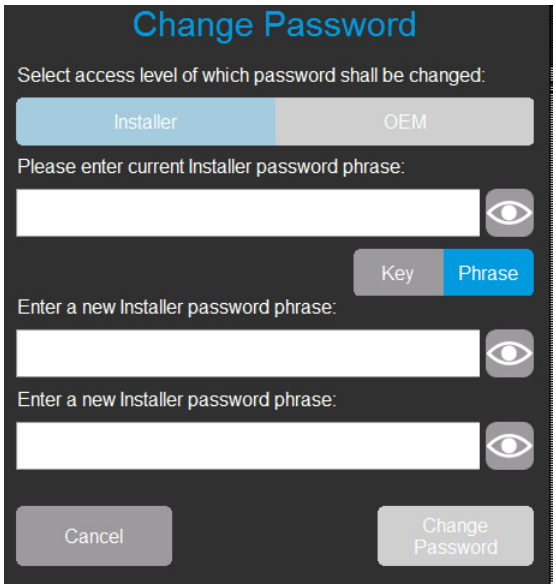


Fig. 8. L'utenteconnessocomeInstallatorepuòmodificaresololapassword Installatore. L'utente immette la password Installatore corrente e la nuova password per due volte.

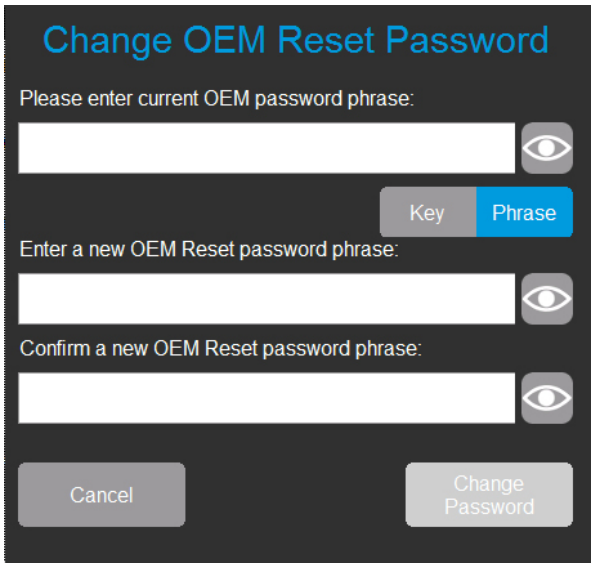


Fig. 9. L'utente connesso come OEM può modificare anche le password di reset OEM. L'utente immette la password OEM corrente e la nuova password di reset OEM per due volte.

Reset della password

Nel caso in cui le password di livello di accesso principale relative a Installatore e/o OEM venissero smarrite, è possibile il reset della password se i meccanismi di reset sono stati abilitati dall'OEM. Vedere Fig. 5 Il meccanismo di reset varierà tra i livelli Installatore e OEM. Nota: spegnere e riaccendere la valvola o l'interfaccia utente non escluderà questa metodologia.

Il meccanismo di reset della password consente semplicemente all'utente appropriato di ripristinare una o più password correnti al valore o ai valori predefiniti di fabbrica di Honeywell. Una volta eseguito il reset di una o più password, l'utente può connettersi e assegnare una o più password nuove.

A seguito del reset al valore predefinito, se le password principali di OEM + Installatore e quelle di reset di OEM non sono impostate a nuovi valori non predefiniti, la valvola entrerà in stato di blocco e non sarà operativa, a meno che l'utente OEM sia connesso. Al fine di annullare uno o più codici di errore, è necessario configurare la o le password applicabili.

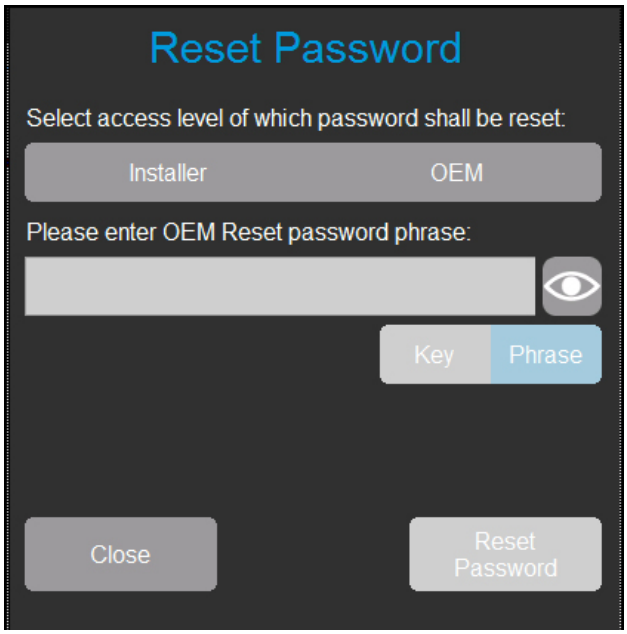


Fig. 10. L'utente non connesso seleziona il Livello di accesso della password di cui eseguire il reset. L'utente immette una frase password di reset.

Per impostazione predefinita, la funzionalità di reset della password per l'Installatore e l'OEM è disabilitata ed è necessario abilitarla nella configurazione iniziale di ciascun dispositivo dall'OEM o dal proprietario originario, come indicato in Fig. 5.

NOTE:

- **L'OEM può scegliere se abilitare o disabilitare la funzione di reset della password OEM. Vedere la Fig. 5.**
  - **Se è abilitata e la password OEM principale viene smarrita, l'OEM può eseguire il reset delle password alle impostazioni di fabbrica predefinite di Honeywell e riassegnare nuove password.**
  - **Se è disabilitata e la password OEM principale è smarrita, l'OEM non sarà in grado di effettuare il reset della password e sarà concretamente bloccata la modifica della valvola a livello di OEM.**
  - **Se si conosce la password principale del livello Installatore, l'OEM può accedere alla valvola servendosi della password e modificare i parametri ai quali ha autorizzato l'accesso Installatore.**
  - **Al fine di rendere di nuovo possibile la modifica del livello OEM, è necessario sostituire l'elettronica principale della valvola e riprogrammare completamente la valvola in entrambi i livelli OEM e Installatore.**

Protezione della password

Per evitare la possibilità che una password di sessione venga indovinata tramite tentativi casuali, tutte le password sono protette da un meccanismo in grado di rilevare attacchi di forza bruta. Il suddetto meccanismo disabilita temporaneamente la connessione all'account e alla valvola interessati. È necessario che il dispositivo sia spento e riacceso oppure che il soggetto connesso attenda almeno un minuto prima del tentativo successivo.

Se ciò si verifica, gli errori saranno annunciati nella pagina Diagnostica Strumento IUM/PC. A questo evento sono associati quattro possibili codici di errore:

- Account Installatore temporaneamente disabilitato
- Account OEM temporaneamente disabilitato
- Funzionalità di reset della password Installatore temporaneamente disabilitata
- Funzionalità di reset della password OEM temporaneamente disabilitata

Best practice

È consigliabile utilizzare sempre password sicure e difficili da indovinare. Fare riferimento alla sezione Gestione password/chiave presentata in precedenza nel presente documento.

Gestione account

Vi sono due account utente implementati nelle valvole Serie SV2. I suddetti account sono:

1. Installatore
2. OEM

L'account Installatore è considerato sussidiario dell'account OEM. In altre parole, tutte le funzionalità accessibili dall'Installatore possono essere controllate dall'OEM.

Di contro, le funzionalità accessibili dall'OEM possono essere utilizzate esclusivamente da quest'ultimo.

Gli account utente possono essere rimossi o aggiunti e il loro scopo previsto è il seguente:

1. L'account OEM è impiegato per configurare le funzionalità critiche della valvola, quale la configurazione di Modulo pressione, Modulo combustibile/aria, Accensione combustibile/aria e Curve di base combustibile/aria.
2. L'account Installatore è impiegato per configurare funzionalità meno critiche, quali i limiti funzionali o le variabili specifiche dell'applicazione.

Gestione accessi

Per impostazione predefinita, i privilegi di accesso sono configurabili per ogni funzionalità critica. Il livello utente predefinito per tutte le funzionalità di sicurezza è configurato per l'Installatore e deve essere innalzato a livello utente OEM sulla base delle specifiche dell'applicazione. È possibile eseguire la configurazione avvalendosi dello Strumento IUM o Strumento PC di Honeywell, come da indicazione in Fig. 11:

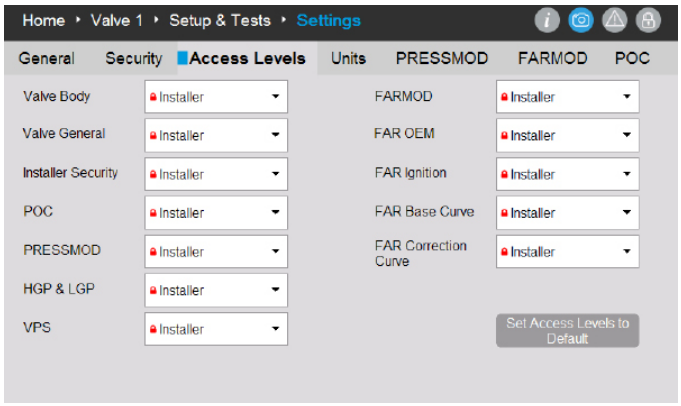


Fig. 11. Pagina livelli di accesso. Ogni gruppo di configurazione può essere impostato come Installatore, OEM oppure Sola lettura.

Sicurezza della connessione fisica da remoto e sicurezza fisica a confronto

Al fine di mantenere protetta la connessione attraverso la comunicazione, è importante considerare i seguenti elementi che si applicano principalmente alla configurazione iniziale del dispositivo:

- Quando il dispositivo è fisicamente accessibile da un potenziale aggressore, quest'ultimo può ottenere la password di reset Installatore leggendola sull'adesivo sulla parte posteriore del gruppo elettronico principale della valvola e in seguito utilizzata.
- Quando è stabilita una connessione impiegando la password predefinita nella valvola, non può mai essere considerata come sicura. È consigliabile impostare le password iniziali per gli account OEM e Installatore quando nessun altro dispositivo è presente sulla rete RS-485 a cui la valvola è connessa.

STRUMENTI IUM E PC

Per mantenere protetti valvole e strumenti dell'interfaccia utente della Serie SV2 è necessario fornire loro un accesso utente affidabile e sicuro. Per tale ragione, dovrebbero essere impiegate numerose misure di sicurezza con lo Strumento PC e lo Strumento IUM, come di seguito descritto.

Sicurezza IUM

Le IUM Serie SV2 indipendenti devono sempre essere mantenute fisicamente protette; le medesime raccomandazioni di sicurezza fisica si applicano alle IUM per quanto attiene alla valvola Serie SV2. Fare riferimento alla sezione Protezione fisica del dispositivo presentata in precedenza nel presente documento.

Sicurezza Strumento PC

Lo Strumento PC è progettato per essere eseguito sui computer dotati di sistemi operativi Microsoft® Windows. Quando si connette un computer a una valvola Serie SV2, le problematiche di sicurezza del PC applicabili possono costituire un rischio per la sicurezza della valvola. Per tale ragione, è sempre consigliabile attenersi alle pratiche di sicurezza di seguito delineate:

1. Impiegare sempre un sistema operativo supportato da Microsoft.
2. Tenere sempre il sistema aggiornato con le patch di sicurezza più recenti.
3. Disporre sempre di software antivirus e di un firewall installato e aggiornato.
4. Utilizzare le funzionalità nella withelist abilitate nel sistema operativo del PC.
5. Non utilizzare applicazioni provenienti da fonti non affidabili o a cui è stata applicata una crack.
6. Assicurarsi che le unità USB o altri accessori connessi al PC provengano da una fonte affidabile e non contengano hardware o software dannosi (ad es., keylogger, scanner di memoria, ecc.).
7. Disabilitare tutti i servizi, le porte e gli account utente non necessari nel PC per evitare un attacco da remoto.

Un file di installazione o un file binario di un'applicazione è firmato mediante una chiave Honeywell per fornire la garanzia che l'installazione/applicazione dello Strumento PC provenga da una fonte verificata. Ciononostante, malgrado la firma offra un buon livello di sicurezza, è consigliabile utilizzare sempre unicamente l'installazione/applicazione dello Strumento PC fornita direttamente da Honeywell o da un OEM/Installatore autorizzato Honeywell.

Lista di controllo della sicurezza Strumento PC

Al fine di utilizzare con sicurezza la suddetta applicazione, assicurarsi di soddisfare le seguenti condizioni:

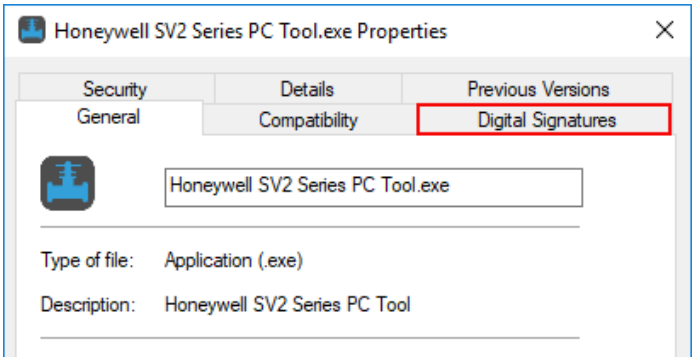
1. Utilizzare solo un'applicazione affidabile e firmata (consultare la sezione Verifica dell'origine dell'applicazione)
2. Se possibile, servirsi della whitelist delle applicazioni (consultare la sezione Applicazioni in whitelist)
3. Utilizzare una protezione antivirus insieme a un firewall adeguatamente configurato se il PC è connesso a Internet.
4. Assicurarsi che il PC sul quale si esegue l'applicazione sia dotato di protezione mediante password affinché il personale non autorizzato non possa impiegarlo.
5. Assicurarsi che l'accesso fisico al sistema da parte del personale autorizzato sia eliminato o limitato (PC -> RS485 -> Modbus -> Valvola Serie SV2).
6. 6.Strumento PC deve essere installato automaticamente nella cartella standard di Microsoft Windows "Programmi". Questo percorso di installazione è stato pre-selezionato nel programma di installazione dell'utilità PC. Se si seleziona una posizione di installazione diversa, l'utente deve configurare le autorizzazioni di sicurezza (ad esempio, l'amministratore) per assicurarsi che l'installazione di Strumento PC non venga manomessa da personale non autorizzato.

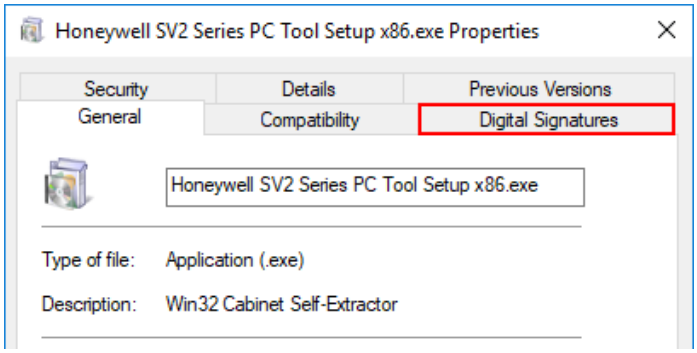
Verifica dell'origine dell'installatore/ applicazione Strumento PC

L'installazione/applicazione è fornita con una firma digitale. La firma sarà controllata a seguito del download di una nuova versione dell'installazione/applicazione o in caso di sospetti sull'origine dell'installazione/applicazione.

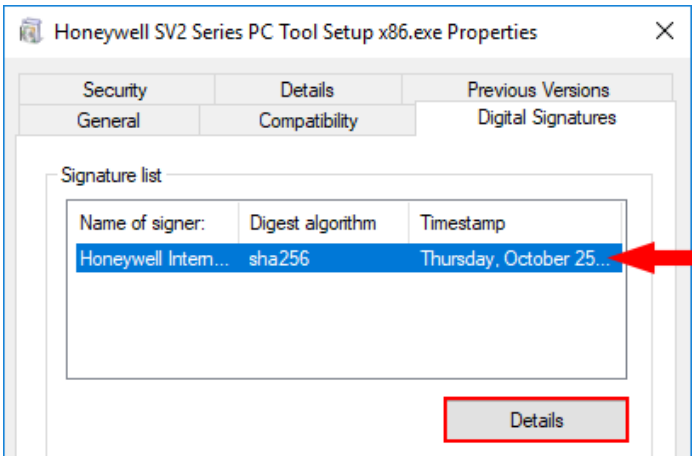
La firma può essere verificata seguendo questi passaggi:

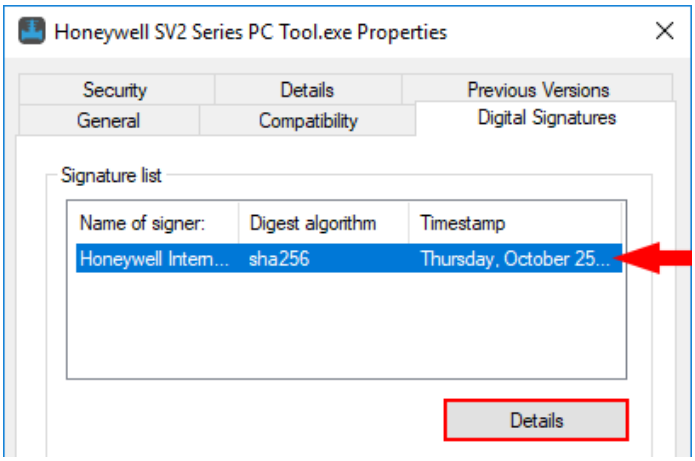
1. Fare clic con il pulsante destro del mouse su "Honeywell SV2 Series PC Tool Setup x86.exe" / "Honeywell SV2 Series PC Tool Setup x64.exe" e quindi su "Proprietà".
2. Estrarre i contenuti di "usb_root.zip" e fare clic con il pulsante destro del mouse su "app.exe" e quindi su "Proprietà".
3. Nella finestra "Proprietà" fare clic su "Firme digitali". Se la scheda non è presente passare al passaggio 5).



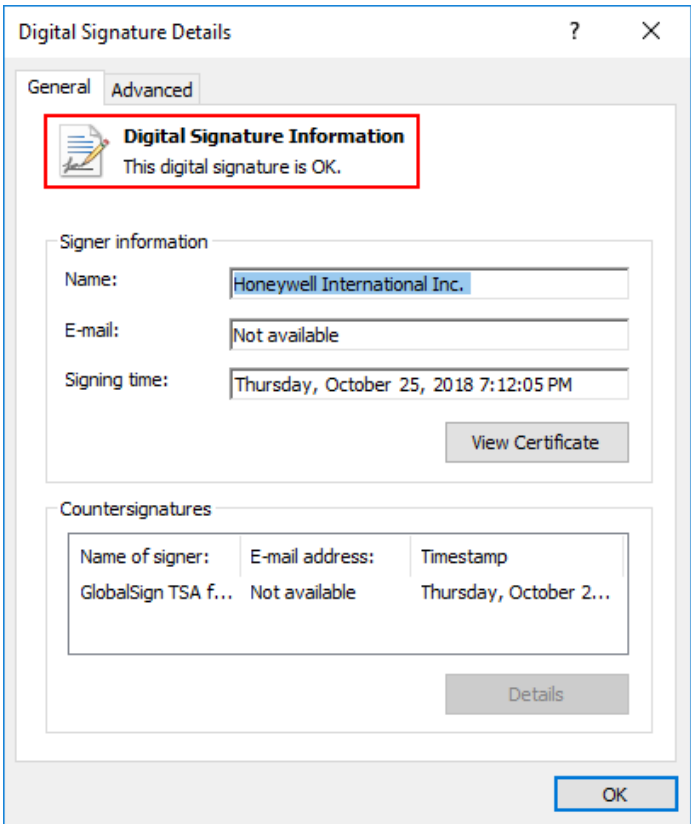


4. Nella scheda “Firme digitali”, l’unica voce in “Elenco firme” deve essere denominata “Honeywell International Inc.”. Fare clic sulla voce e quindi sul pulsante “Dettagli”.



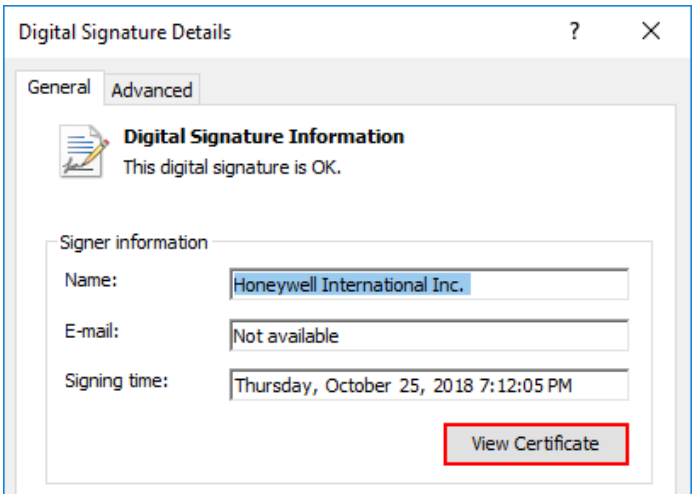


5. Nella finestra, “Dettagli firma digitale”, verificare le “Informazioni firma digitale”. Dovrebbe recare la dicitura “Questa firma digitale è accettabile”.

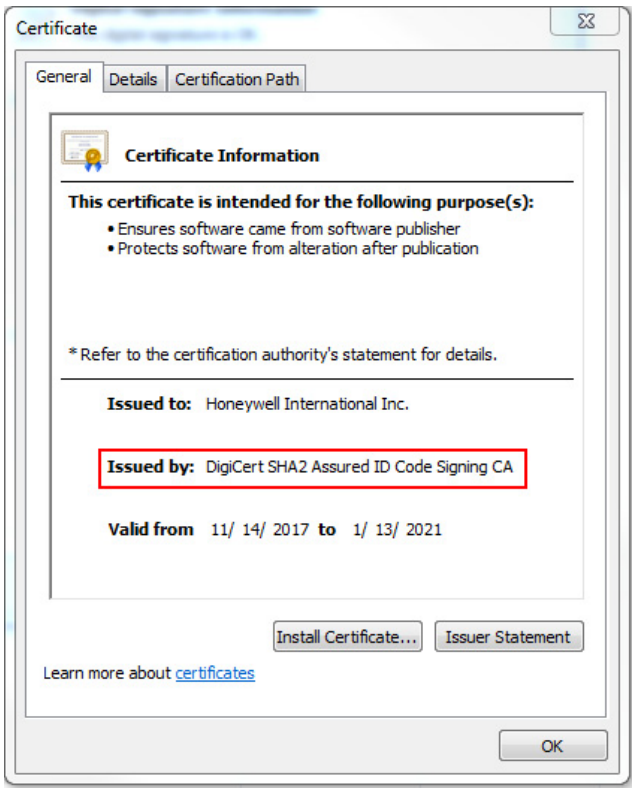


6. Qualora la firma non fosse accettabile o addirittura non presente (nel passaggio 2 nessuna scheda di firma digitale, l’applicazione non è affidabile e deve essere eliminata. Dalla fonte originale è possibile scaricare una copia nuova e “pulita”.

7. Inoltre, se si desidera verificare i dettagli del certificato, fare clic sul pulsante “Visualizza certificato”.



8. La riga “Emesso da” nel menu dettagli del certificato deve contenere “DigiCert”, ovvero il nome del provider del certificato.



Applicazioni in whitelist

La whitelist consente all’amministratore di impostare un elenco di applicazioni desiderate. Non è consentita l’esecuzione delle applicazioni non presenti nell’elenco. L’impostazione della whitelist aumenta considerevolmente la sicurezza e riduce al minimo il rischio di eseguire software non intenzionali sulla macchina. La whitelist è disponibile come pulsante integrato nei sistemi operativi Windows (Windows 7 e Windows 8) o può essere realizzata da un software di terzi.

Report di arresto anomalo del sistema

Quando lo Strumento HMI o PC si arresta in modo imprevisto, viene creato un report di arresto anomalo del sistema. I report di arresto anomalo del sistema di Strumento PC si trovano in C:\Utenti\<user>\Documenti\Honeywell\SV2 Series PC Tool\Crash reports\. Il report di arresto anomalo del sistema di Strumento HMI è accessibile dalla pagina Home/Display Setup/About. Fare riferimento alla Fig. 1. Il report di arresto anomalo del sistema contiene le seguenti informazioni:

- Versione e configurazione di Strumento PC
- Versione del sistema operativo Microsoft Windows
- Versione di Microsoft .NET Framework
- Eccezione e analisi dello stack
- Elenco delle porte COM disponibili
- Configurazione completa valvole

Per ulteriori informazioni su questo prodotto e sull'intera linea di prodotti Serie SV2, fare riferimento alla Guida per l'utente Serie SV2 disponibile sul nostro sito Web all'indirizzo https://combustion.honeywell.com/sv2

Per ulteriori informazioni

La famiglia di prodotti Honeywell Thermal Solutions comprende Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder e Maxon. Per maggiori informazioni sui nostri prodotti, visitare ThermalSolutions.honeywell.com o contattare il proprio Honeywell Sales Engineer

Honeywell Process Solutions

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

ThermalSolutions.honeywell.com

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