



AUTOMAZIONE IN SICUREZZA

Utilizzo della crittografia SSL / TLS

Grazie alle molteplici varianti di tutti i controller della serie PFC WAGO e delle loro diverse interfacce, si è perfettamente pronti per nuove attività future, sia nei sistemi e nell'ingegneria meccanica, sia nelle tecnologie di produzione e di processo.

Il sistema I/O modulare consente l'automazione dal livello di singole macchine a interi sistemi. Un'ampia selezione fra oltre 500 diversi moduli I/O offre il massimo grado di flessibilità e funzionalità. E' facile quindi l'adattamento a compiti nuovi o a modifiche di quelli esistenti.

Proteggi i tuoi dati dagli hacker e da qualsiasi altro accesso non autorizzato! Da quanto il collegamento in rete di sistemi industriali si effettua via Internet, i sistemi di controllo sono più vulnerabili agli attacchi informatici. Il controller offre pacchetti di sicurezza completi composti da SSL / TLS, SSH, VPN e un firewall. Grazie a questo alto livello di protezione, il controller minimizza gli effetti di un eventuale attacco su macchine e sistemi.

Protezione integrata delle password e comunicazione protetta difendono dall'accesso alle funzioni, ai contenuti di programmazione e dall'introduzione di malware.



CYBER SECURITY

Integrazione e sicurezza IT

Molti Bus di campo, Minima Sicurezza

Il crescente networking e la connessione a Internet ormai standardizzata, aumentando i rischi e quindi la tendenza a proteggere l'archiviazione dei dati e la trasmissione di questi in tutte le aree, inclusa la tecnologia di automazione. Tuttavia, le difficoltà per arrivarci sono numerose: da un lato, il decentramento nella tecnologia dell'automazione ha notevolmente aumentato la necessità di comunicazione, perché i controllori subordinati non devono solo scambiare informazioni tra loro, ma devono anche scambiarli con il sistema di controllo.

D'altra parte, nel corso degli anni, in questo campo e nell'automazione, sono stati stabiliti i più diversi sistemi bus con i quali i dati possono essere trasmessi in modo deterministico, ma questi non includono alcun concetto di sicurezza. Mentre la sicurezza funzionale è stata un problema per molto tempo, la sicurezza informatica ha un ruolo trascurabile in molti settori della tecnologia di automazione.

Alte prestazioni, Massima Sicurezza

WAGO ha risposto a queste esigenze per i componenti di automazione con i controllori PFC100 e PFC200. Linux® è la base per l'implementazione di tecnologie crittografate tramite TLS 1.2. Una connessione IPsec o OpenVPN può essere implementata direttamente dal PLC tramite il quale i dati vengono inviati crittografati. Inoltre, un firewall standard protegge il PFC100 da accessi non autorizzati. Gli utenti hanno quindi la possibilità di aggiornare i controllori in base ai requisiti indicati nel white paper BDEW (Federal Association of Energy and Water Industries) e nel catalogo di sicurezza BSI-IT (Federal Office for Information Security).

Entrambi i controller PFC100 e PFC200 supportano tutti i protocolli della famiglia TCP/IP: DHCP, DNS, SNMP, FTP, Telnet, http e Modbus TCP / UDP. Al fine di garantire la sicurezza e l'integrità delle informazioni durante l'accesso al Web e il trasferimento dei dati, i metodi di crittografia SSH e SSL/TLS sono integrati come standard per stabilire connessioni HTTPS e FTPS sicure.

Entrambe le generazioni di controller possono essere configurate tramite il server Web integrato attraverso una Web-Based Management (Gestione via Web), l'ambiente di runtime e! RUNTIME (CODESYS 3) e l'ambiente di programmazione CODESYS (IEC 61131-3).

VANTAGGI:

- **Funzioni di diagnostica complete**
- **Alta sicurezza**
- **Integrazione semplice**
- **Comunicazione senza interruzioni**

Nello sviluppo originale dei protocolli fieldbus, che al momento sono ampiamente utilizzati, l'attenzione si è concentrata sull'alta affidabilità, velocità e affidabilità funzionale assicurando la disponibilità e l'utilizzo di sistemi embedded a risorse ridotte.

Di regola, i bus di campo non forniscono autenticazione e trasmettono i dati utilizzando caratteri in chiaro. Questi sistemi però, progettati per il comfort e l'affidabilità operativa, spesso presentano punti deboli e quindi facile accesso per gli attacchi esterni.

Siamo in grado di prevenire queste carenze di sicurezza utilizzando i seguenti protocolli:

- SSH/SFTP, FTPS und HTTPS
- Firewall con Mac-Filter
- OpenVPN e IPsec
- TLS 1.2
- SNMPv3

Protocolli Standard IT:

SNMP

- SNMP versione 1, 2, 3
- Accesso alle variabili SNMP
- Invio di blocchi tramite librerie PLC

MySQL/MSSQL

- Accesso al database con istruzioni SQL

HTTP

- Scambio di dati con server Web remoti tramite librerie PLC, ad es. PHP, ASP.NET

HTTPS, TLS / SSL V 1.2

- Proteggi la trasmissione dei dati con certificati

SMTP, FTP, SFTP, FTPS, NTP

- Scambio di posta, trasferimento dati e sincronizzazione temporale

SSH, Firewall, VPN, IPsec Standard

WAGO – I VANTAGGI IN BREVE:

- **IPSec (Internet Protocol Security) e una connessione OpenVPN per l'invio di dati crittografati direttamente dal controller**
- **Implementazione di tecnologie crittografate basate su Linux® tramite TLS 1.2 (Transport Layer Security)**
- **Firewall integrato standard per la protezione da attacchi indesiderati dalla rete**

Wago Elettronica Srl a Socio Unico

Soggetta all'attività di direzione e coordinamento di Wago Auslandsbeteiligungs GmbH

Via Parini, 1 - 40033 Casalecchio di Reno (BO) - Italy

Nr. R.I. e Cod.Fisc.: 04288700372 - P.IVA: 01770461208

phone: +39 051 6132112

fax: +39 051 6132888

info-ita@wago.com - www.wago.it

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.