CAN Newsletter Online

CONTROLLER FAMILY

IT security from Cloud to controller

Wago's PFC100 and PFC200 controllers not only encrypt data via onboard SSL/TLS 1.2 security protocols, but also transmit data to higher-level systems via VPN tunnel. CANopen is available as an interface.

The PFC200 controller series (Photo: Wago)

Internet of Things (IoT) applications demand reliable automation technology that emphasizes IT security. Ultimately, production data are a valuable asset that must be well protected. Wago focused on this need while developing the PFC100 and PFC200 controllers. They are characterized by a cross-platform real-time Linux system, which is available as an open-source operating system that can be scaled, updated, and supports tools such as Rsync. This makes them suitable for use as secure gateways.

The factory-installed Linux foundation not only supports essential security protocols, it also ensures that these will be constantly refined thanks to the Linux community. Wago's controllers are not merely simple PLCs capable of transmitting data to the Cloud. Rather, they are Linux computers, which also happen to support Codesys PLC Runtime. An additional advantage are their various interfaces and fieldbuses, such as CANopen, Profibus DP, Devicenet, and Modbus-TCP, which can be utilized independent of the manufacturer.

All members of the PFC200 series are also designed to implement the security requirements according to ISO 27000 – depending on the application and the risk analysis. They provide onboard VPN functionality based on the Strong Swan package and the OpenVPN package, which is a secure communications solution for Linux operating systems. In addition, the data in the PFC200 controller can be encoded using SSL/TLS 1.2 (Secure Sockets Layer/Transport Layer Security) encryption. A VPN tunnel is then established directly via IPsec or OpenVPN, transfers data to the Cloud, and can do so wirelessly if desired.

While IPsec encrypts at the operating system level or layer 3, OpenVPN ensures data integrity on the application layer (layer 5). This results in communication connections between the controllers and network access points that cannot be bugged or manipulated by third parties. An upstream VPN router is no longer required. While communicating with a PFC200, an encrypted LAN/WAN connection can be established, and the contents of those interchanges can only be understood by the two endpoints. Connections are established only after successful authentication. An encryption method with a pre-shared key is used, in which the keys must be known to both parties prior to communication. This method has the advantage of being easy to implement, says the company. Alternatively, an x.509 certificate is provided, which is a method wherein a public key infrastructure generates digital certificates.

The controller can be used as a scalable node, which can be retrofitted into pre-existing automation systems without involving the actual automation process – data is collected in parallel and can be transmitted to the Cloud, for example via MQTT or OPC UA. Internal production use of the data is also possible via linkage to the manufacturing execution system (MES). System operators have the opportunity to maintain an overview of their production facilities due to the Cloud capability. Complex processes can be recorded, as well as mapped, and visualized via smartphones or tablets. Relevant areas can be filtered according to depth of detail by using a graduated hierarchy, which simplifies the localization of potential error functions.

cw