WAGO’s PFC Family – IT Security up to the Controller

WAGO’s PFC100 and PFC200 Controllers not only encrypt data via onboard SSL/TLS 1.2 security protocols, but also securely transmit data to higher-level systems via VPN tunnel

Internet of Things (IoT) applications demand reliable automation technology that heavily emphasizes IT security. Ultimately, production data are a valuable asset that must be well protected. And WAGO focused heavily 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. Consequently, they can be used 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 large Linux® community. WAGO’s controllers are not merely simple PLCs capable of transmitting data to the cloud. Rather, they are fully fledged Linux® computers, which also happen to support CODESYS PLC Runtime. An additional advantage: various interfaces and fieldbuses, such as CANopen, PROFIBUS DP, DeviceNet and Modbus-TCP, can also be utilized independent of the manufacturer.

WAGO’s flexible automation solutions reliably store data error-free from the field level for use by the cloud or an MES

Security on All Levels

All members of the WAGO PFC200 family are also designed to implement the current highest security requirements according to ISO 27000 – depending on the application and the risk analysis. They provide onboard VPN functionality based on the strongSwan package and the OpenVPN package, which is a secure communications solution for Linux® operating systems. In addition, the data in the PFC200 Controller can already 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 and transfers the data to the cloud, even 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.

During communication 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 that it is easy to implement. Alternatively, a x.509 certificate is provided, which is a method in which a public key infrastructure generates digital certificates. Due to the strong security concept of the PFC200, WAGO already currently fulfills all relevant guidelines in the area of IT security and even a large

number of the requirements from the BDEW white paper for applications in the field of energy and water supply, which are part of the “critical infrastructure” (CIP).

Convincingly Flexible

The PFC200 can also 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. This is another case in which the user profits from the security features of the WAGO controllers. An 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 easily and economically 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, In this way, potential error functions can be localized more easily and earlier.