Cyber Security

Automate Securely

AUTOMATE SECURELY

Using SSL/TLS Encryption

Due to the multiple variants of all controllers in the PFC Series and their various interfaces, you are also perfectly equipped for future tasks – both in systems and mechanical engineering and in manufacturing and process technologies.

The scaleable I/O system enables automation from the level of individual machines to entire systems. A large selection from over 500 different I/O modules offers the highest degree of flexibility and functionality. Adapting to new or changed tasks can be achieved easily.

Protect your data from hackers and any other unauthorized access! Since the networking of industrial systems with the Internet, control systems are more vulnerable to cyber attacks. The controller offers comprehensive security packages consisting of SSL/TLS, SSH, VPN, and a firewall. Due to this high level of protection, the controller thus minimizes the effects of an attack on machines and systems.

Integrated password protection and secured communication protect against access to functions, programming contents, and the introduction of malware.

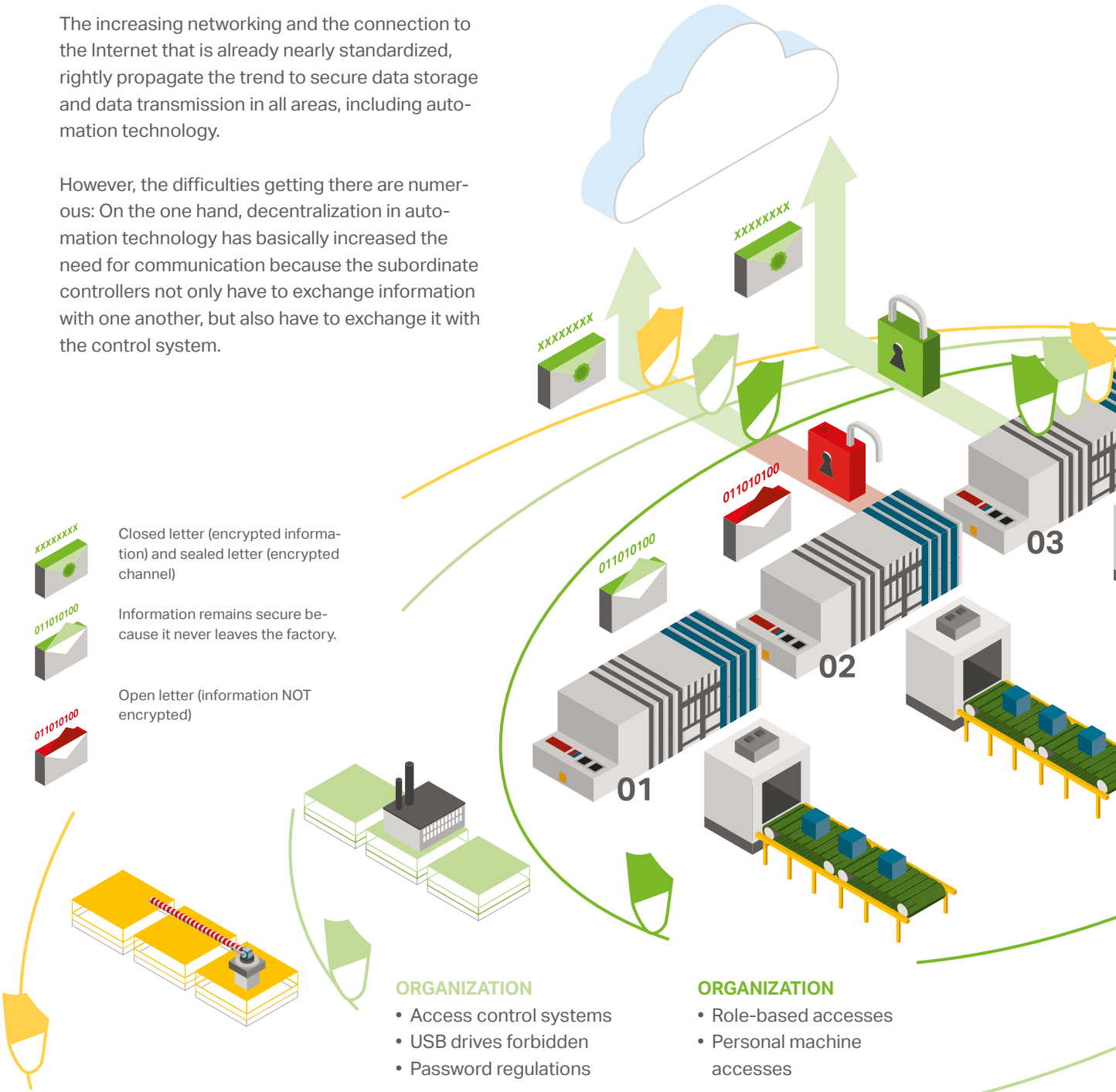
CYBER SECURITY

Integration and IT Security

Many Fieldbuses, Minimal Security

The increasing networking and the connection to the Internet that is already nearly standardized, rightly propagate the trend to secure data storage and data transmission in all areas, including automation technology.

However, the difficulties getting there are numerous: On the one hand, decentralization in automation technology has basically increased the need for communication because the subordinate controllers not only have to exchange information with one another, but also have to exchange it with the control system.



ORGANIZATION
- Turnstile or similar
- Facility identification
- Fence/wall

IT
- Router
- Firewall

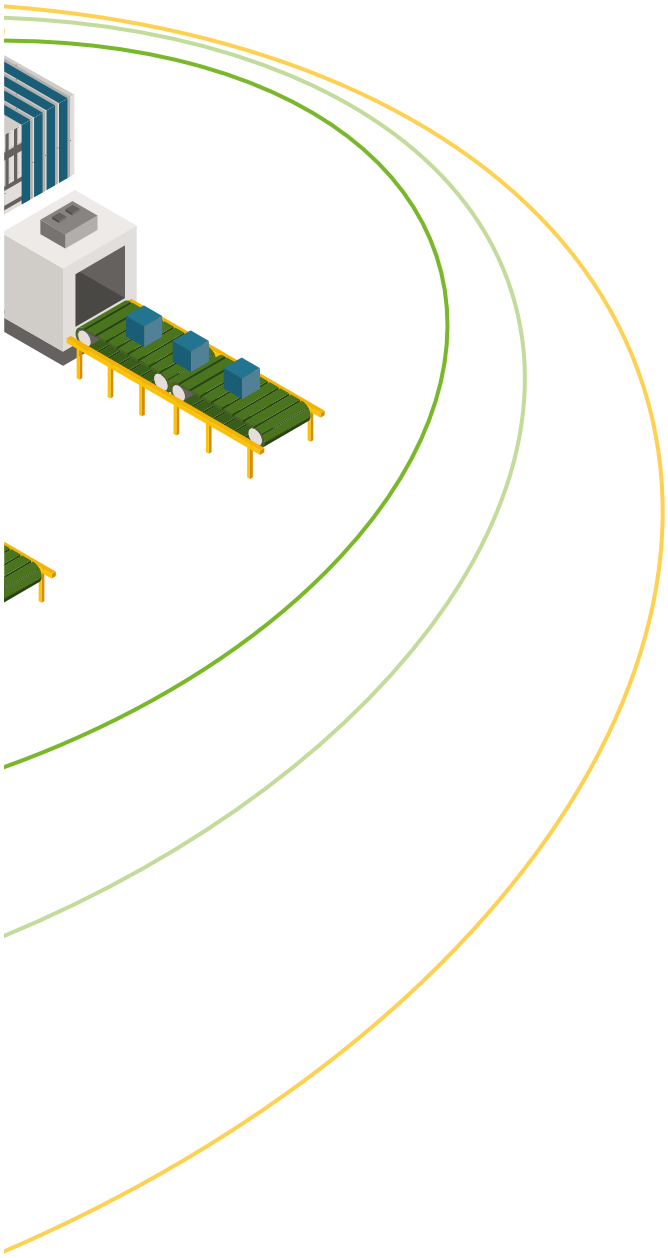
ORGANIZATION
- Access control systems
- USB drives forbidden
- Password regulations

IT
- Physical network segmentation/VLAN
- Switches/router/firewall
- WLAN, WPA encryption

ORGANIZATION
- Role-based accesses
- Personal machine accesses

IT
- Segmentation using VLANs
- Switches/router/firewall
- Radius server

On the other hand, over the years in this field and in automation, the most diverse bus systems have been established with which the data can be transmitted deterministically, but these do not include any security concepts.
Whereas functional safety has been an issue for a long time, cyber security plays a negligible role in many areas of automation technology.



High Performance, Maximum Security

WAGO has responded to these requirements for automation components with the PFC 100 and PFC200 Controllers.
Linux® is the base for implementing encrypted technologies via TLS 1.2. An IPsec or OpenVPN connection can be implemented directly from the PLC via which data are sent encrypted. In addition, a standard firewall protects the PFC100 from unauthorized access. Users thus have the option of upgrading controllers according to the requirements stated in the BDEW (Federal Association of Energy and Water Industries) white paper and the BSI-IT (Federal Office for Information Security) security catalog.

Both the PFC100 and PFC200 Controllers support all TCP/IP family protocols: DHCP, DNS, SNTP, FTP, Telnet, http and Modbus TCP/UDP.
In order to ensure the security and integrity of the information during Web access and data transfers, the encryption methods SSH and SSL/TLS are integrated as standard for establishing secure HTTPS and FTPS connections.

Both controller generations can be configured via the integrated web server via Web-Based Management, the runtime environment ***e!***RUNTIME (CODESYS 3) and the CODESYS programming environment (IEC 61131-3).

YOUR ADVANTAGES:

- **Comprehensive diagnostics functions**
- **High security**
- **Simple integration**
- **Seamless communication**

REASONABLE PROTECTION

Using Secure Protocols

In the original development of the currently widely used fieldbus protocols, the focus was on the high reliability, speed and functional reliability with regard to running capability and low-resource embedded systems.

As a rule, fieldbuses do not provide authentication and transmit their data using plaintext. These systems, which are designed for comfort and operational reliability, often provide easy-to-use weak points for external attackers.

We are able to prevent these security deficiencies using the following protocols:

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

WAGO BENEFITS AT A GLANCE:

- **IPSec (Internet Protocol Security) and an OpenVPN connection for sending encrypted data directly from the controller**
- **Implementing Linux®-based encrypted technologies via TLS 1.2 (Transport Layer Security)**
- **Standard built-in firewall to protect against unwanted network attacks**

Standard IT Protocols:

SNMP
- SNMP version 1, 2, 3
- Access to SNMP variables
- Sending traps via PLC libraries

MySQL/MSSQL
- Database accesses with SQL statements

HTTP
- Data exchange with remote Web servers via PLC libraries, e.g., PHP, ASP.NET

HTTPS, TLS/SSL V 1.2
- Secure data transmission with certificates

SMTP, FTP, SFTP, FTPS, NTP
- Mail exchange, data transfer and time synchronization

SSH, Firewall, VPN, IPsec

WE INNOVATE!

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 · 32385 Minden
Hansastraße 27 · 32423 Minden
info@wago.com
www.wago.com

Headquarters	+49(0)571/ 887 - 0
Sales	+49(0)571/ 887 - 222
Order service	+49(0)571/ 887 - 44 333
Fax	+49(0)571/ 887 - 844 169

0888-0133/0100-6901 – CYBER SECURITY FLYER US – 11/2016-00 - Printed in Germany – Subject to design changes