Cybersecurity
Automate Securely

AUTOMATE SECURELY

With PFC100 and PFC200 Series Controllers

In addition to the scalability and flexibility of the I/O system and the standardized MQTT protocol for easy connection to different cloud solutions, the PFC100 and PFC200 Series also offer comprehensive security functionalities to protect your systems against cybersecurity attacks.

A password protection integrated directly on the controller and secured communication protect against access to functions, programming contents, and the introduction of malware.

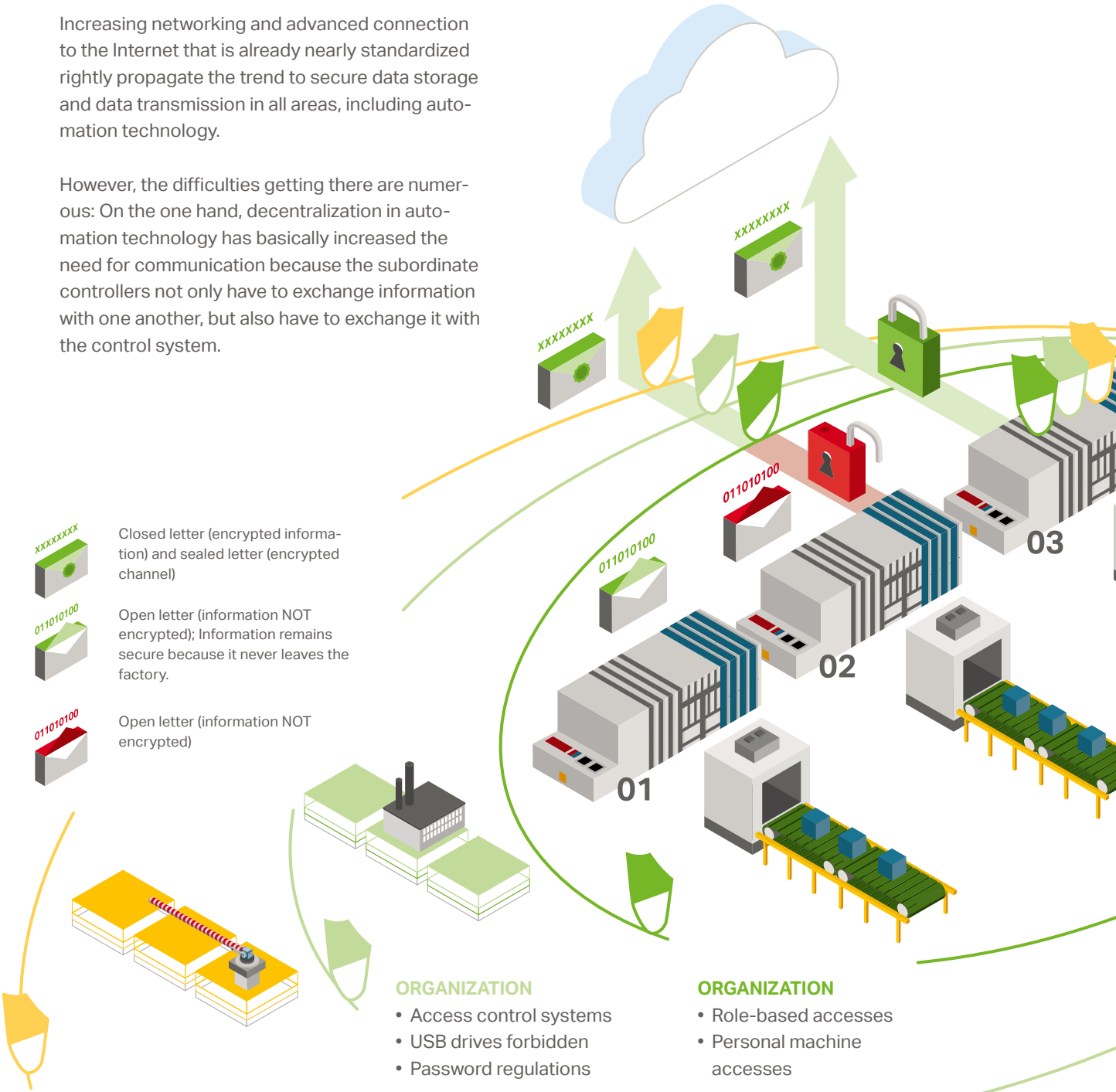
CYBERSECURITY

Integration and IT Security

Many Fieldbuses, Minimal Security

Increasing networking and advanced 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.



xxxxxxxx Closed letter (encrypted information) and sealed letter (encrypted channel)

011010100 Open letter (information NOT encrypted); Information remains secure because it never leaves the factory.

011010100 Open letter (information NOT encrypted)

ORGANIZATION
- Security gate or similar
- Facility identification
- Fence/wall

IT
- Router
- Firewall

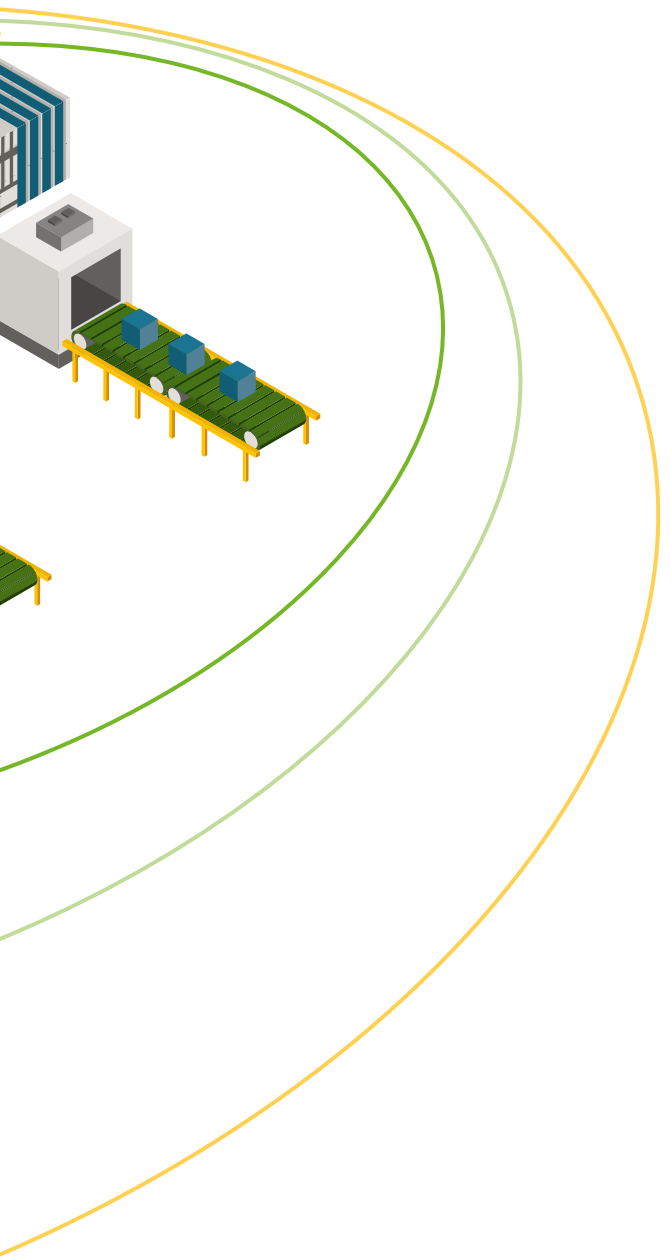
ORGANIZATION
- Access control systems
- USB drives forbidden
- Password regulations

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 at the field and automation levels, 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, cybersecurity 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 PFC100 and PFC200 Controllers.
Linux® provides the basis that allows security mechanisms (e.g., IP tables (firewall), VPN, IEEE 802.1x and SCEP) to be implemented. An IPsec or OpenVPN connection can be implemented directly from the PLC via which data are sent encrypted. In addition, a standard integrated firewall provides protection against 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 for the simple connection to a network: DHCP, DNS, SNTP, FTP, Telnet, http and Modbus TCP/UDP.
In order to ensure information security and integrity during Web access and data transfers, the TLS 1.2 encryption method is used as standard for establishing secure HTTPS and FTPS connections, and the SSH protocol is integrated as standard for establishing secure shell and SFTP connections.

Both controller generations can be configured via integrated Webserver (Web-Based Management) and WAGO's ***e!****COCKPIT* programming environment (based on CODESYS) according to IEC 61131-3.

YOUR BENEFITS:

- **VPN directly on the controller**
- **Current encryption protocols**
- **SCEP for the distribution and blocking of public certificates**
- **Network access protection through IEEE 802.1x**

DATA PROTECTION

With Secure Protocols

In parallel with increasing networking, concerns about IT security are increasing – with justification. Therefore, the machine manufacturers and operators are intensifying their efforts to transport their own machine data as securely as possible and protect it against undesired access. With the PFC100 and PFC200 Controllers, WAGO provides the solution for the increasing demands on automation components. A standard integrated firewall provides protection against unauthorized access. There is no need for encryption via external components and protection through external firewalls.

Standard IT Protocols for PFC100 and PFC200 Controllers:

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

MySQL/MSSQ
- Database accesses with SQL statements

HTTP
- Data exchange with remote Web servers via PLC libraries

HTTPS, TLS V 1.2
- Secured data transmission based on certificates

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

WAGO BENEFITS AT A GLANCE:

- **IPSec (Internet Protocol Security) and an OpenVPN connection for sending encrypted data directly from the controller**
- **Implement Linux®-based encrypted technologies via TLS 1.2 (Transport Layer Security)**
- **Standard built-in firewall to protect against unwanted network attacks**
- **IEEE 802.1x WPA Supplicant**
- **Simple Certificate Enrollment Protocol (SCEP)**

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

Headquarters	+49 571/ 887 - 0
Sales	+49 571/ 887 - 222
Orders	+49 571/ 887 - 44 333
Fax	+49 571/ 887 - 844 169

0888-0133/0101-6901 - CYBER SECURITY FLYER 1.1 US - 01/2018-00 - Printed in Germany - Subject to design changes