Cyber Security

Sicher automatisieren

SICHER AUTOMATISIEREN

durch SSL/TLS-Verschlüsselung

Durch die vielfältigen Varianten aller Controller der Baureihe PFC mitsamt ihren unterschiedlichen Schnittstellen sind Sie auch für zukünftige Aufgaben perfekt gerüstet – und zwar sowohl im Anlagen- und Maschinenbau als auch in der Fertigungs- und Verfahrenstechnik.

Das skalierbare I/O-System ermöglicht das Automatisieren von einzelnen Maschinen bis hin zu ganzen Anlagen. Eine große Auswahl von über 500 unterschiedlichen I/O-Modulen bietet höchste Flexibilität und Funktionsvielfalt. Ein Anpassen an neue oder geänderte Aufgaben gelingt so überaus leicht.

Schützen Sie Ihre Daten vor Hackern und anderen unerlaubten Zugriffen! Seit der Vernetzung industrieller Analgen mit dem Internet sind Steuerungssysteme anfälliger für Cyberattacken. Der Controller bietet umfangreiche Sicherheitspakete, bestehend aus SSL/TLS, SSH, VPN und einer Firewall. Durch diesen perfekten Schutz minimiert der Controller konsequent die Auswirkungen eines Angriffs auf die Maschinen und Anlagen.

Ein integrierter Passwortschutz und die gesicherte Kommunikation schützen vor Zugriffen auf Funktionen, Programminhalte und das Einschleusen von Schadsoftware.

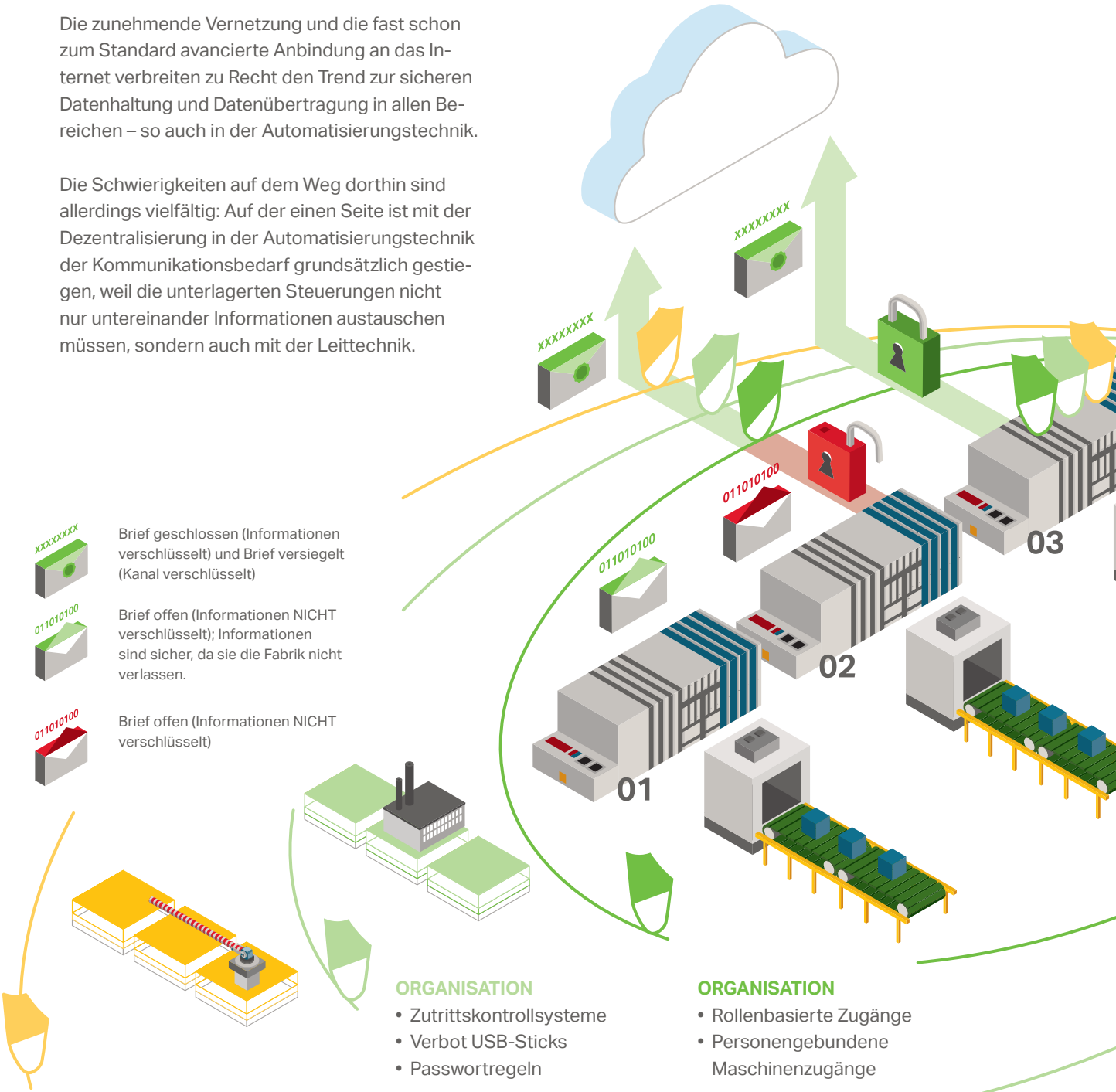
CYBER SECURITY

Integration und Sicherheit im IT-Umfeld

Viele Feldbusse, wenig Sicherheit

Die zunehmende Vernetzung und die fast schon zum Standard avancierte Anbindung an das Internet verbreiten zu Recht den Trend zur sicheren Datenhaltung und Datenübertragung in allen Bereichen – so auch in der Automatisierungstechnik.

Die Schwierigkeiten auf dem Weg dorthin sind allerdings vielfältig: Auf der einen Seite ist mit der Dezentralisierung in der Automatisierungstechnik der Kommunikationsbedarf grundsätzlich gestiegen, weil die unterlagerten Steuerungen nicht nur untereinander Informationen austauschen müssen, sondern auch mit der Leittechnik.



xxxxxxxx Brief geschlossen (Informationen verschlüsselt) und Brief versiegelt (Kanal verschlüsselt)

011010100 Brief offen (Informationen NICHT verschlüsselt); Informationen sind sicher, da sie die Fabrik nicht verlassen.

011010100 Brief offen (Informationen NICHT verschlüsselt)

ORGANISATION
- Drehkreuz o. ä.
- Werksausweis
- Zaun/Mauer

IT
- Router
- Firewall

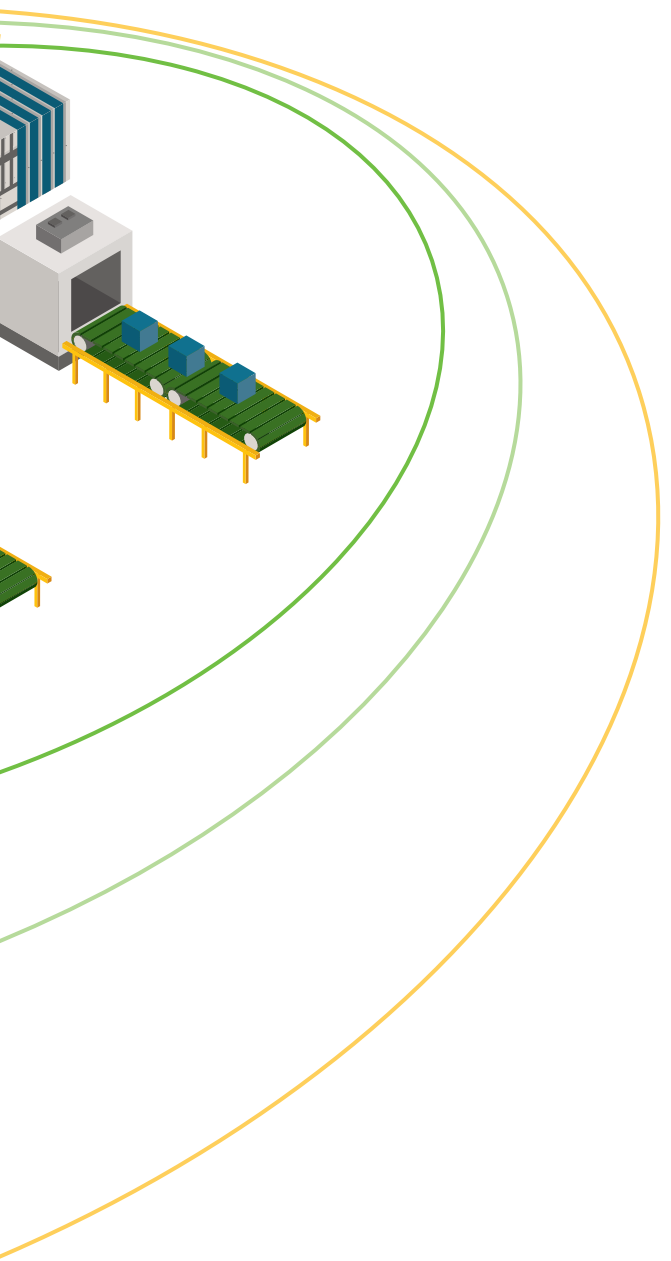
ORGANISATION
- Zutrittskontrollsysteme
- Verbot USB-Sticks
- Passwortregeln

IT
- Netzsegmentierung physikalisch/VLAN
- Switches/Router/Firewall
- WLAN-, WPA-Verschlüsselung

ORGANISATION
- Rollenbasierte Zugänge
- Personengebundene Maschinenzugänge

IT
- Segmentierung mit VLANs
- Switche/Router/Firewall
- Radiusserver

Auf der anderen Seite haben sich auf der Feld- und Automatisierungsebene im Laufe der Jahre unterschiedlichste Bussysteme etabliert, mit denen die Daten zwar deterministisch übertragen werden können, die allerdings keinerlei Schutzkonzepte beinhalten.
Während also die funktionale Sicherheit beispielsweise seit langer Zeit ein Thema ist, spielt Cyber-Security in weiten Teilen der Automatisierungstechnik bis dato eine vernachlässigte Rolle.



Große Performance, hohe Sicherheit

WAGO hat mit den Controllern PFC100 und PFC200 auf diese Anforderungen an Automatisierungskomponenten reagiert.
Linux® bietet dabei die Basis, die es erlaubt, Verschlüsselungstechnologien via TLS 1.2 zu implementieren. So lässt sich direkt aus der Steuerung eine IPsec- oder OpenVPN-Verbindung realisieren, über die Daten verschlüsselt versendet werden. Eine standardmäßig integrierte Firewall schützt darüber hinaus vor unerwünschten Netzwerkzugriffen. Die Anwender haben somit die Möglichkeit, die Steuerungen entsprechend der Anforderungen gemäß BDEW-White Paper und BSI-IT-Sicherheitskatalog zu ertüchtigen.

Sowohl der Controller PFC100 als auch der PFC200 unterstützen für den Datenaustausch in einem Netzwerk alle relevanten Protokolle der TCP/IP-Familie: DHCP, DNS, SNTP, FTP, Telnet, http sowie Modbus TCP/UDP.
Um bei Webzugriffen und Datentransfers die Sicherheit und Integrität der Informationen zu gewährlisten, sind für den Aufbau sicherer HTTPS- und FTPS-Verbindungen die Verschlüsselungsmethoden SSH und SSL/TLS standardmäßig integriert.

Beide Steuerungsgenerationen lassen sich über den integrierten Webserver per Web-Based-Management, über die Laufzeitumgebung ***e!****RUNTIME* (CODESYS 3) sowie die CODESYS-Programmierumgebung gemäß IEC 61131-3 projektieren.

IHR NUTZEN:

- **Umfangreiche Diagnosefunktionen**
- **Hohe Sicherheit**
- **Einfache Integration**
- **Durchgängige Kommunikation**

ANGEMESSENER SCHUTZ

durch sichere Protokolle

Bei der ursprünglichen Entwicklung der aktuell stark verbreiteten Feldbusprotokolle lag das Augenmerk auf der hohen Zuverlässigkeit, Geschwindigkeit und Funktionssicherheit bezogen auf Lauffähigkeit und ressourcenarme Embedded-Systeme.

In der Regel bieten Feldbusse keine Authentifizierung und übertragen ihre Daten im Klartext. Diese auf Komfort und Betriebssicherheit entwickelten Systeme bieten für Angreifer von außen oft einfach zu nutzende Schwachstellen.

Durch die folgenden Protokolle schaffen wir es, diesen Sicherheitsdefiziten vorzubeugen:

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

DIE WAGO-VORTEILE AUF EINEN BLICK:

- **IPsec-(Internet Protocol Security-) und OpenVPN-Verbindung zum Versand verschlüsselter Daten direkt aus der Steuerung**
- **Implementieren von Verschlüsselungstechnologien via TLS 1.2 (Transport Layer Security) auf Basis von Linux®**
- **Standardmäßig integrierte Firewall, zum Schutz vor unerwünschten Netzwerkangriffen**

Standard-IT-Protokolle:

SNMP
- SNMP-Version 1, 2, 3
- Zugriff auf SNMP-Variablen
- Senden von Traps über SPS-Bibliotheken

MySQL / MSSQL
- Datenbankzugriffe mit SQL-Statements

HTTP
- Datenaustausch mit entfernten Webservern über SPS-Bibliotheken, z. B. PHP, ASP.NET

HTTPS, TLS/SSL V 1.2
- Sichere Datenübertragung mit Zertifikaten

SMTP, FTP, SFTP, FTPS, NTP
- Mailversand, Datentransfer und Zeitsynchronisation

SSH, Firewall, VPN, IPsec

WE INNOVATE!

0888-0133/0100-0101 - CYBER SECURITY FLYER DE - 11/2016-00 - Printed in Germany - Technische Änderungen vorbehalten

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

Zentrale	0571/ 887 - 0
Vertrieb	0571/ 887 - 222
Auftragsservice	0571/ 887 - 44 333
Fax	0571/ 887 - 844 169