

SIMPLE NETWORK SECURITY FOR YOUR MACHINES WITH ZONES AND CONDUITS

Carsten Bokholt
Managing Director
Helmholz GmbH & Co. KG

FACTS AND FIGURES – HELMHOLZ GMBH & CO. KG



- Founded in 1988
- Located near Erlangen, Bavaria
- 80 employees at company headquarters
- Local suppliers (EMS), local production
- Global partnerships
- >35% export share
- More than 8,000,000 applications worldwide with Helmholz products



HELMHOLZ: INDUSTRIAL COMMUNICATION FOR AUTOMATION



CYBERSECURITY IN OT

- EU Cyber Resilience Act (CRA) → products with digital elements
- NIS 2 cybersecurity guideline ("Network & Information Systems") → IT
- IEC 62443 – Security in industrial communication and automation
- Other standards related to security:
 - Machinery Directive regulation 2023/1230
 - UNR 155/156 “automotive communication”
 - ISO/TR 22100-4 “machinery”
 - IEC/TR 60601-4-5 „medical devices“
 - ISO/IEC 27000 “IT security”
 - sector-specific regulations
 - IEC 61508 “Functional Safety”



IEC 62443 NORMATIVE STRUCTURE

IEC 62443 <i>Industrial communication networks – Network and system security</i>							
General		Policies & Procedures	System	Component / Product			
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS Security Program Ratings	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers				
		2-5	Implementation guidance for IACS asset owners				

IACS = "Industrial automation and control system"
 OT = "Operational technology"
 IT = "Information technology"

End customer / Operator /
 Asset owner

Machine builder /
 Solution provider

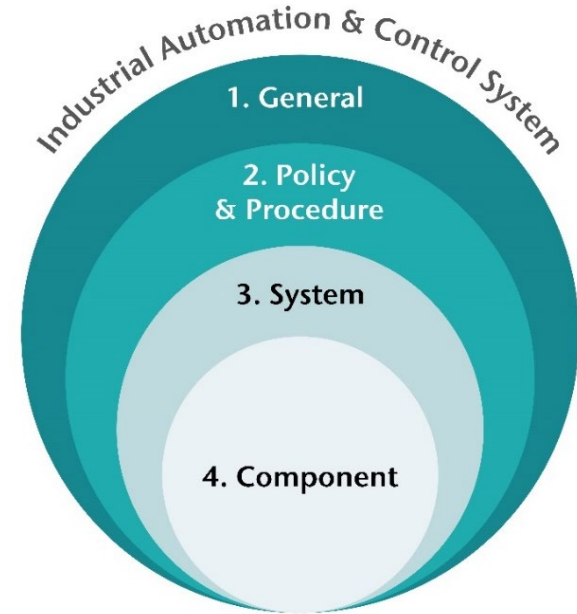
Product manufacturer



IEC 62443 CONCEPTS

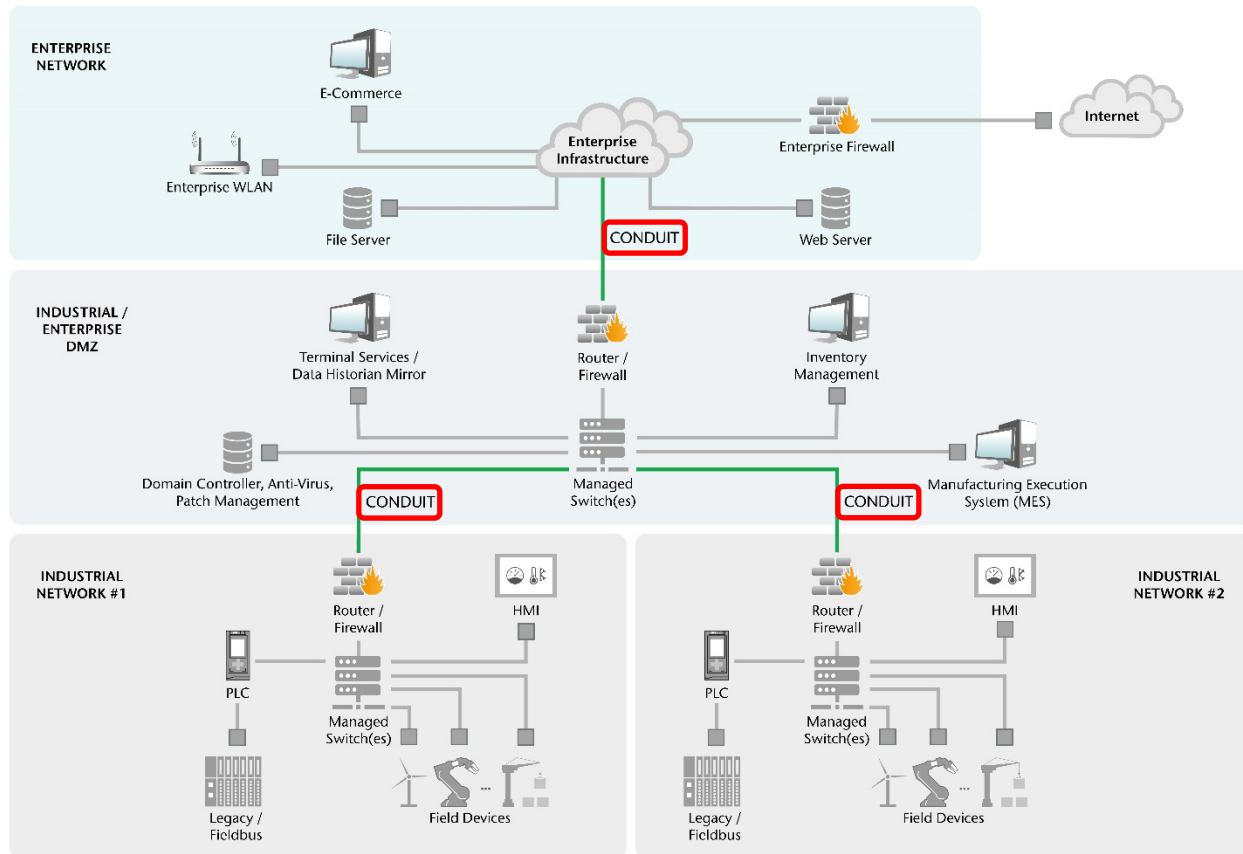
- Defense in depth

- Security methods:
 - Security by Design
 - Security by Default
 - Secure configuration / hardening guides
 - Secure HR handling and training
 - Secure development process
 - Secure development system (DevSecOps)
 - Security incident and patch management



IEC 62443 ZONES AND CONDUITS

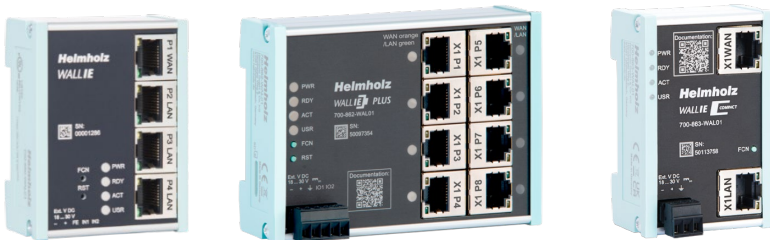
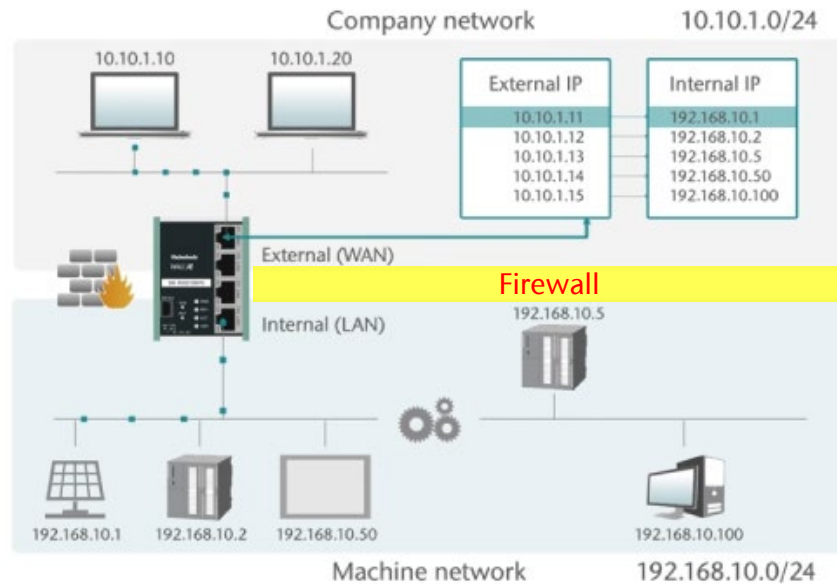
- Classical approach: one network with managed switches using VLAN
- Conduit: Restrict communication between zones of trust
- Router
- Firewalls
- Gateways



MACHINE FIREWALL AS A CONDUIT



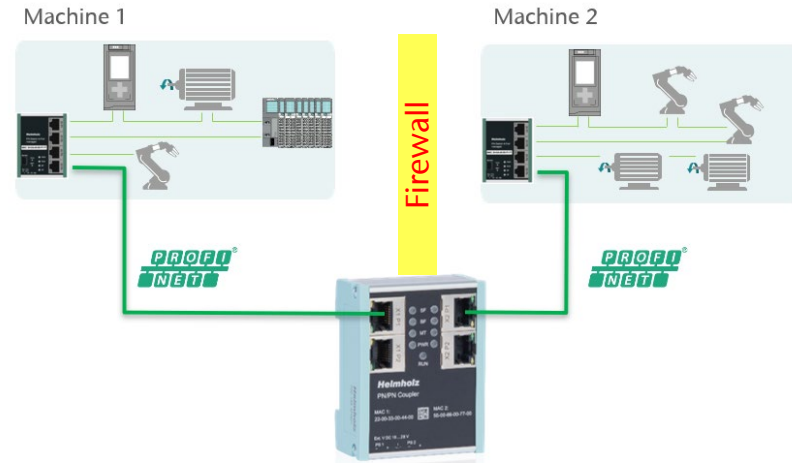
- Access is only granted for listed devices
- Limited access in both directions
- NAT
- Packet filter: IPv4 address, Ports, Protocol
- MAC-address black- / white-listing



GATEWAYS/COUPLER AS CONDUITS



- Simple IO data exchange between machines
- No Ethernet or TCP/IP traffic between machines
- No influence on Machine performance
- Available for most automation protocols



PN/PN-Coupler



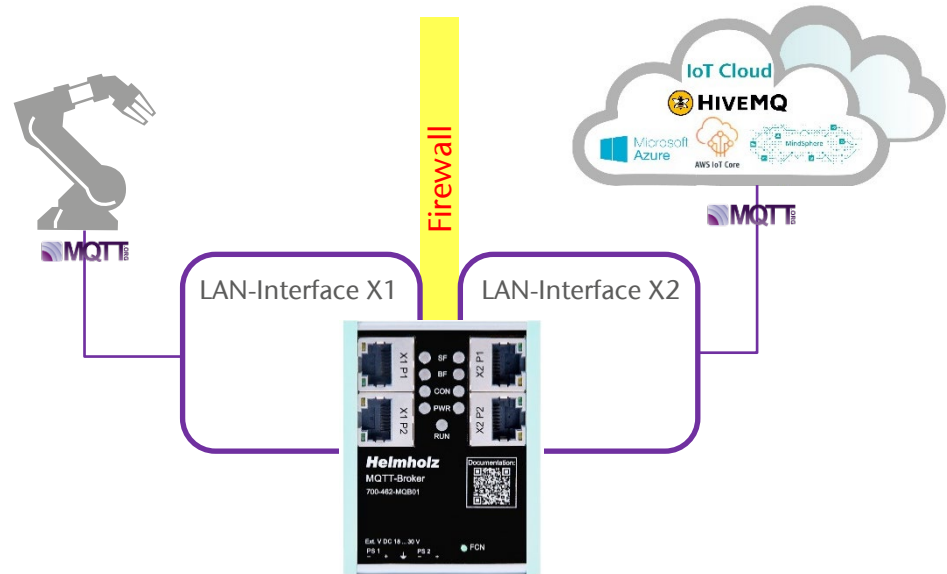
Industrial Ethernet

26 maart 2024 | De Basiliek, Veenendaal

A MQTT BROKER AS A CONDUIT

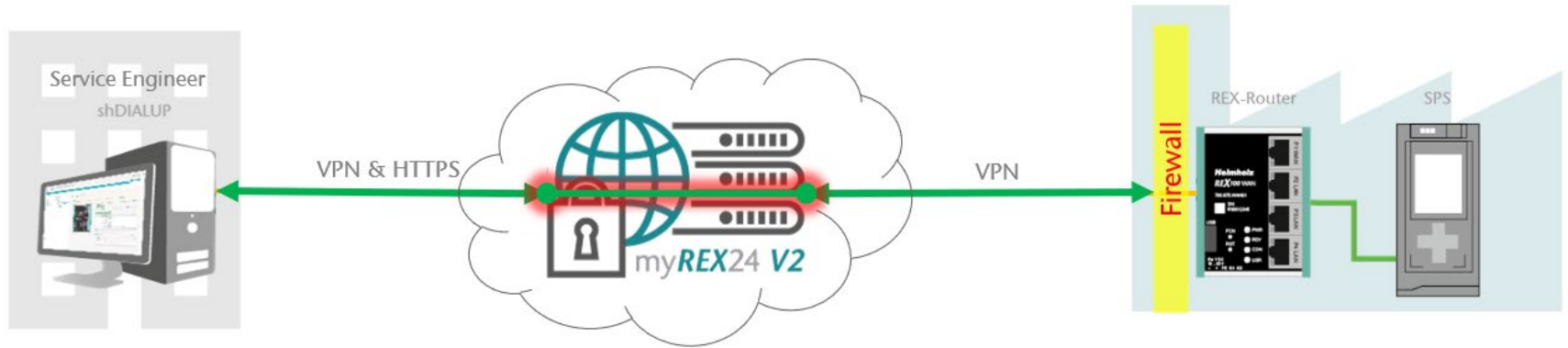


- MQTT Broker Device
- 2 separated networks (X1/X2)
- only MQTT topic content is copied between both networks
- SSL secured communication



A ROUTER AS A CONDUIT

- Remote Maintenance + IIoT
- Specialized secure routers for remote machine communication
- VPN, HTTPS, SSL secured
- Firewall & NAT



INFORMATION IS VITAL FOR SECURE OT!

- Where do I get information about security issues?
- Where do I get firmware updates?
- How can I secure my device configuration?
- Who can I ask about possible security issues in my machine/factory?



→ PSIRT - “Product Security Incident Response Team”

→ Email: psirt@helmholz.de / Webpage PSIRT

→ CERT@VDE



▪ Partners:

- TeleTrust
- BSI = Bundesamt für Sicherheit in der Informationstechnik (“Federal Office for Information Security”)





LET ´S GET SECURE!

35th anniversary
Helmholtz
COMPATIBLE WITH YOU



Industrial Ethernet
26 maart 2024 | De Basillek, Veenendaal

Helmholtz GmbH & Co. KG

Page 13 | March 2024