



NTT

NTT DATA

Trust. Global. Innovate.

Cybersecurity Risks in Industry 4.0 Environments

Christian Koch, Director GRC & IoT/OT

08.10.2019



**„More than 400 businesses
were targeted every day in
2016, resulting in more than
\$3 billion in losses”**

Alliance for Manufacturing Foresight, 2017

**Problem: 99 % of all OT
attacks are not detected**



NTT DATA
TRANSFORMING THE FUTURE

Securing the Transformation – Business meets IT



Compliance

Vehicles

Vehicle/Vessel
Cyber Security

Secure Communication

Secure Provisioning

OTA Software Updates

Audits/Code Reviews

ISO 27001

SOC / CERT
Infrastructure & Cloud
Application (e.g. SAP)
Big Data
Operational Support

Corporate IT

Business Transformation

Secure Authentication
Secure Mobile Apps
Access Management
Wireless Communication
Business Process Integration

IoT Devices

GDPR

Production

Risk Assessments

Security Architecture

Remote Servicing

Predictive Maintenance

Industry Protocol Security

ISA/IEC 62443

TOP Risks in OT Environments



NTT DATA
TECHNOLOGICAL VISION

- Unknown target security level
- No network visibility
- Unknown vulnerabilities and resulting risks
- Unknown remote connections for maintenance or predictive maintenance
- Malware infection via Internet and Intranet
- Malware via removable media and external hardware
- No security awareness
- No security architecture in place
- No clear network segmentation in place
- No OT governance



Global Cyber Security Services for IoT/OT



NTT DATA
THE BACKBONE EVOLVED

NTT's Global Managed Services Platform provides a single view of dynamically evolving threats in real time, by applying advanced analytics to data gathered globally from a wide variety of sources, including NTT's internet & clouds, managed security services, communities, and vendors. Managed Security Services for IoT/OT environments were launched in 2017.

External + Unique NTT Data Sources



Single holistic view



Is IT-Security based on ISO 27001 enough for IoT/OT environments?



NTT DATA
TELECOMMUNICATIONS



What is already done with ISO 2700x?

- Focus on Confidentiality (C), Integrity (I), Availability (A)
- Information security management system (ISMS)
- Classification of information, risk analysis, security concept
- Plan-Do-Check-Act approach for IT-Security

What is missing?

No dedicated focus on IoT/OT for different user groups (manufacturer, integrator, operator) especially for:

- Non standard-IT equipment in OT environments (e.g. sensors, PLCs, non IP communicating devices, ...)
- Resilience requirements
- Health and safety requirements
- Realtime communication
- Unpatchable devices and unsecure industry protocols
- Lifetime requirements of OT-environment (e.g. 10 years, 20 years, ...)

International Standards for IoT/OT Security



NTT DATA
TELECOMMUNICATIONS

- ISA/IEC 62443 (formerly ISA-99), 62264
- NIST 800 Standards
- ISO 2700x series
- ISO/SAE CD 21434 - Road Vehicles - Cybersecurity engineering
- NERC CIP (North American Electric Reliability Corp. / Critical Infrastructure Protection)
- ISO 27019 (Information security controls for the energy utility industry)
- NEI 08-09 (Nuclear Engine Institute)
- ANSI/CAN/UL 2900 Standards
- Regional Standards (BSI)
- IT-Sicherheitsgesetz (KRITISV – security for critical infrastructures)
- IEC 80001 (Risk assessments for medical devices)
- ...



NTT

NTT DATA

cybersecurity solutions

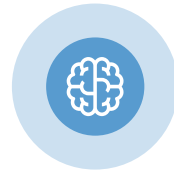
NTT OT-Security Project Approach

Security Visibility Across Your ICS Environment

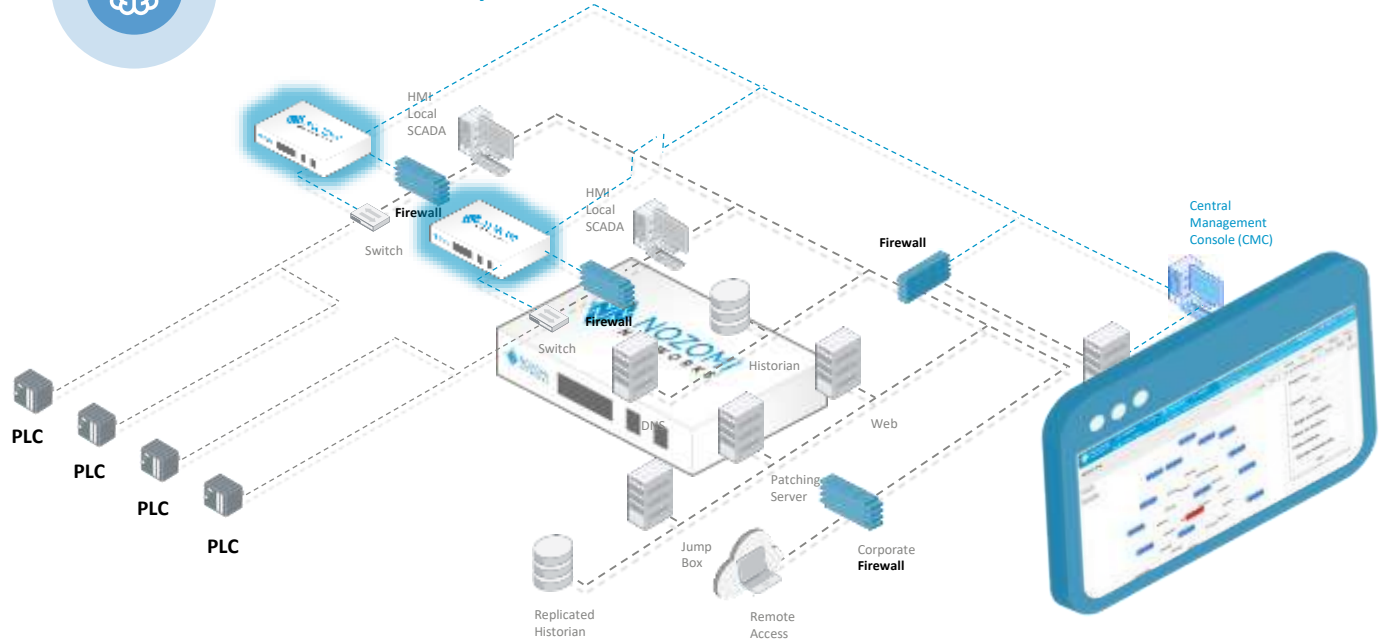


NTT DATA
TECHNOLOGY VISION

	Vendor	Rockwell Eng
	IP	192.168.0.10.12
	OS	Windows 7 / 2008 R2
	Patch Vuln	?
	Vendor	Honeywell
	IP	192.168.0.251.2
	Firmware	12.028
	Module #	0123
	Vendor	ABB
	IP	172.16.80.205
	Firmware	4.380
	Module #	0423
	Vendor	Schneider Electric
	IP	10.172.58.231
	Firmware	16.020
	Module #	8990
	Vendor	Rockwell
	IP	172.21.230.1
	Firmware	?
	Module #	?



AI-Enabled
Passive Auto-Discovery



NTT OT Security Assessment Report



NTT DATA

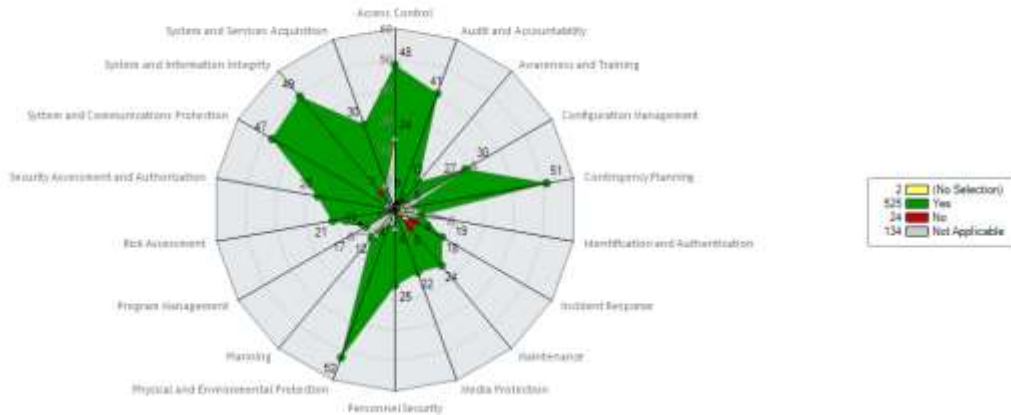
Dashboard: NTTS Risk Assessments

Welcome, Christian Halusa

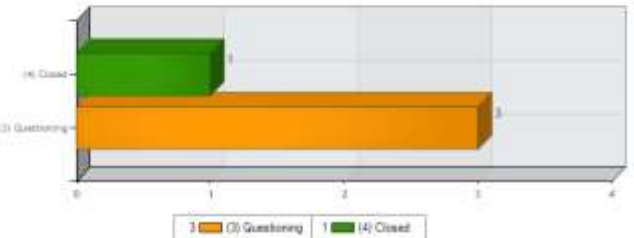
Save Changes Options

Spider chart grouped by sections and answers

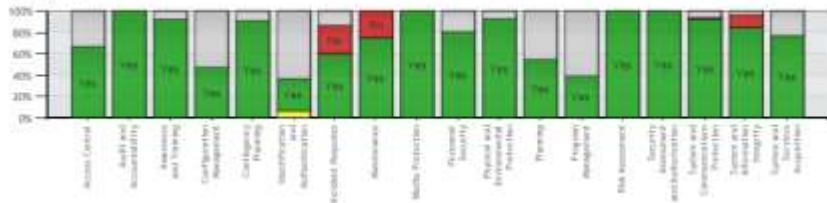
NTTS-RA: Spider chart grouped by sections and answers



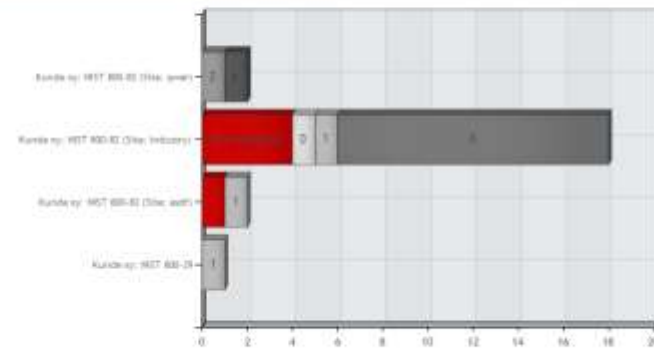
Risk assessment questionnaires grouped by status



Answers grouped by associated sections

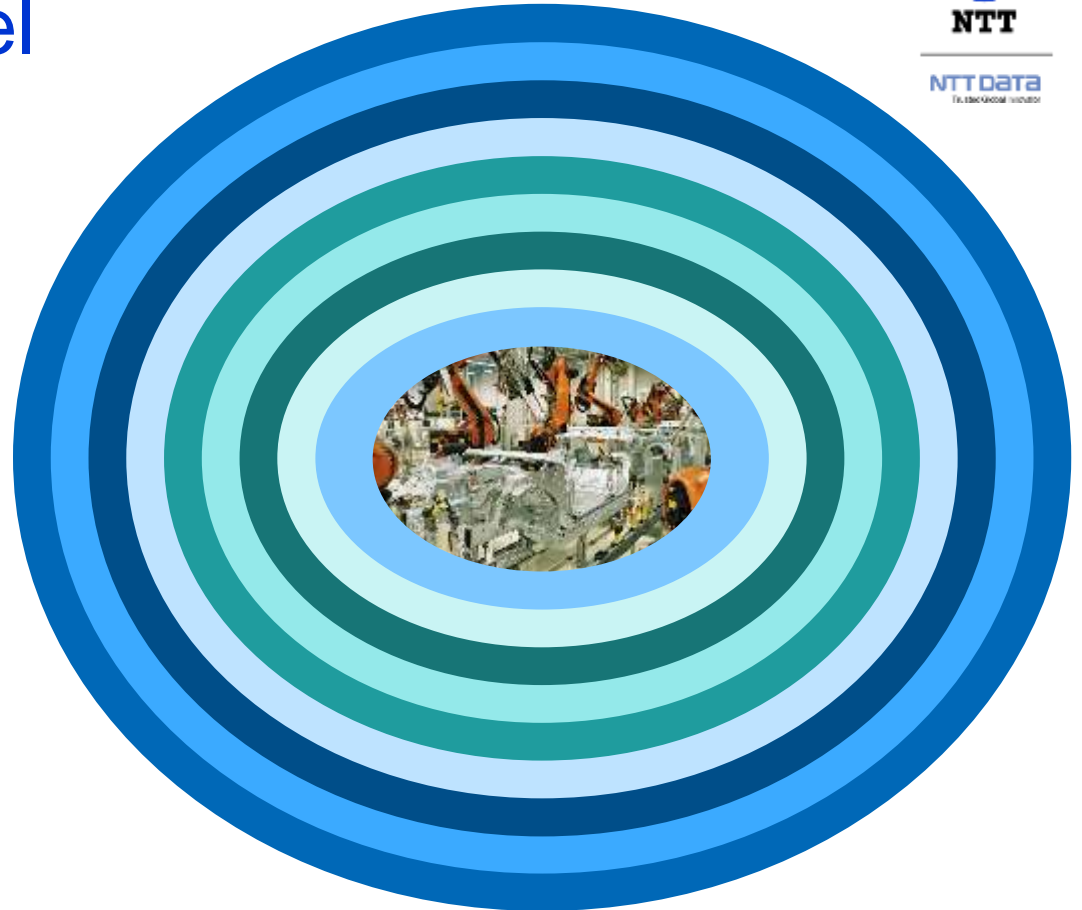



Sections grouped by questionnaires and achieved security level



OT Security Model

- Network Visibility
- Risk Management
- Restrictive Network Segmentation
- Network Threat Detection
- Engineering Workstation / OT-Client Hardening and Application Control
- Patchmanagement of OT-Clients
- Antivirus, EDR – Client
- OT Security Operation Center and Security Operation Processes
- OT Security Awareness





Secure your IoT/OT environment so that the **Internet of Things** does not become the **Internet of Threats**



NTT

NTT DATA

CONNECTING THE WORLD

Thank you

Besuchen Sie uns

Halle: 9

Stand: 9-542