OT goes 2 Cloud: Requirements & Opportunities

Bonn, 10.07.2019

Heiko ADAMCZYK

TLP:Green

Agenda

01 DCSO at a glance

02 Terms

03 Standardization

04 Architectural concepts

05 Evaluation approach

06 Conclusion

DCSO
ENGINEERING SECURITY

Collaboration & Enablement

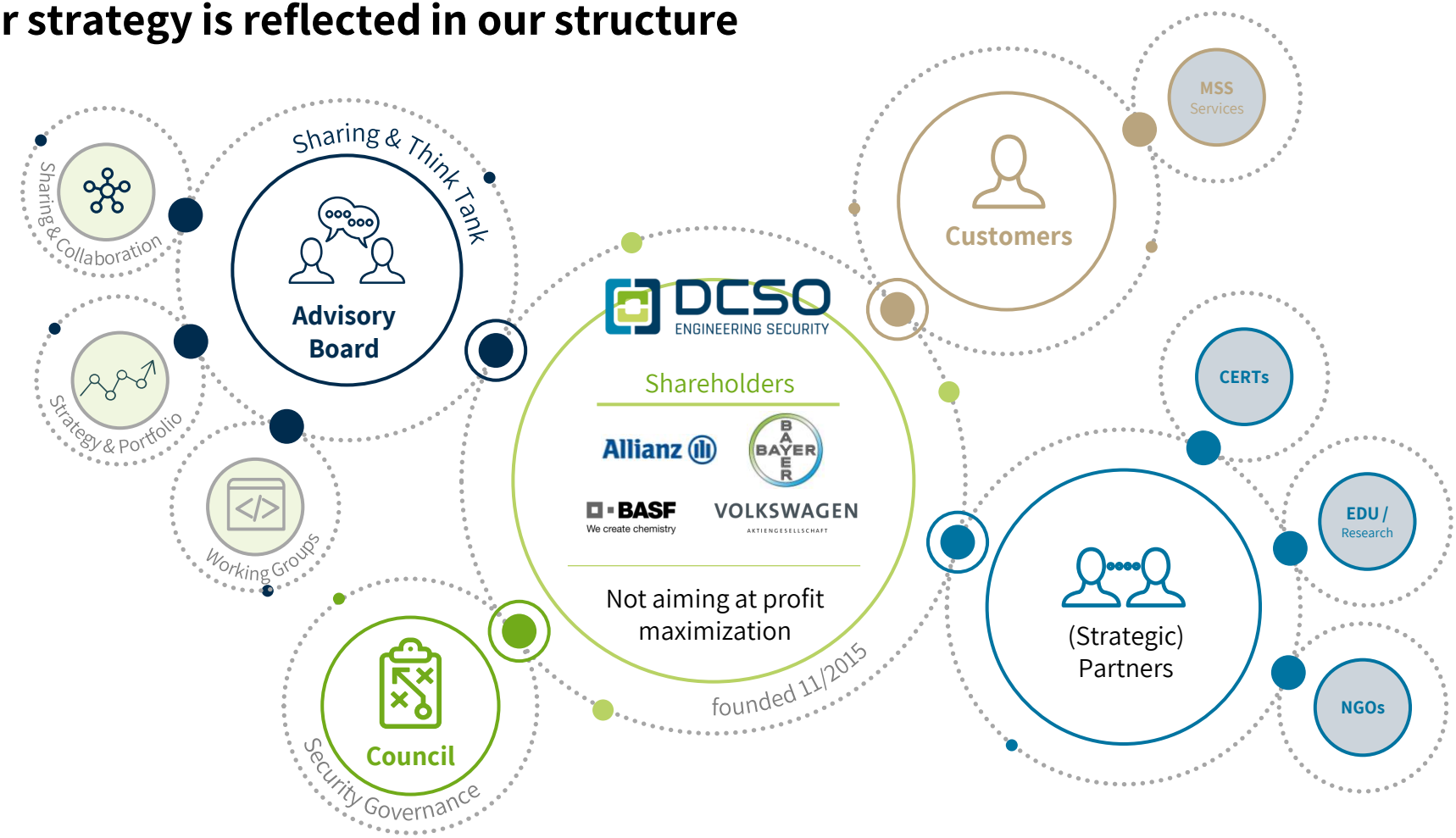
VISION | MISSION

WE ARE THE LEADING ENABLER OF COMMUNITY-DRIVEN CYBER-DEFENSE.

Engineering Security Together.

TLP:Green

Our strategy is reflected in our structure



Our Drivers: Collaboration, Neutrality, Expertise and Efficiency

Neutral and **Independent**

- No market bias through vendor neutral position
- Vendors cannot request DCSO to assess products

Managed Services

- Raised efficiency through best-of-breed aggregation
- Unique Services
- World-wide delivered managed analytics

Cross-Industry **Collaboration**

- Joint Advisory Board projects
- Prototyping and Proof-of-Concept Engineering

Competence Center

- Help with strategic decisions
- Subject Matter Consultancy & Assessment

DCSO Advisory Board - Members

Terms

System

User, organization, technical

Security Objectives

Availability confidentiality, integrity

Causal Chain

Threat → vulnerability → damage

Risk Management

Effective, economically, reasonable elimination of vulnerabilities

Why standardization is so important:

INNOVATION

- Systematic development of new or expansion of existing subject areas

SUPPORT

- Strategic implementation within companies, at the same time proof of implementation to the outside world

HOLISTIC APPROACH

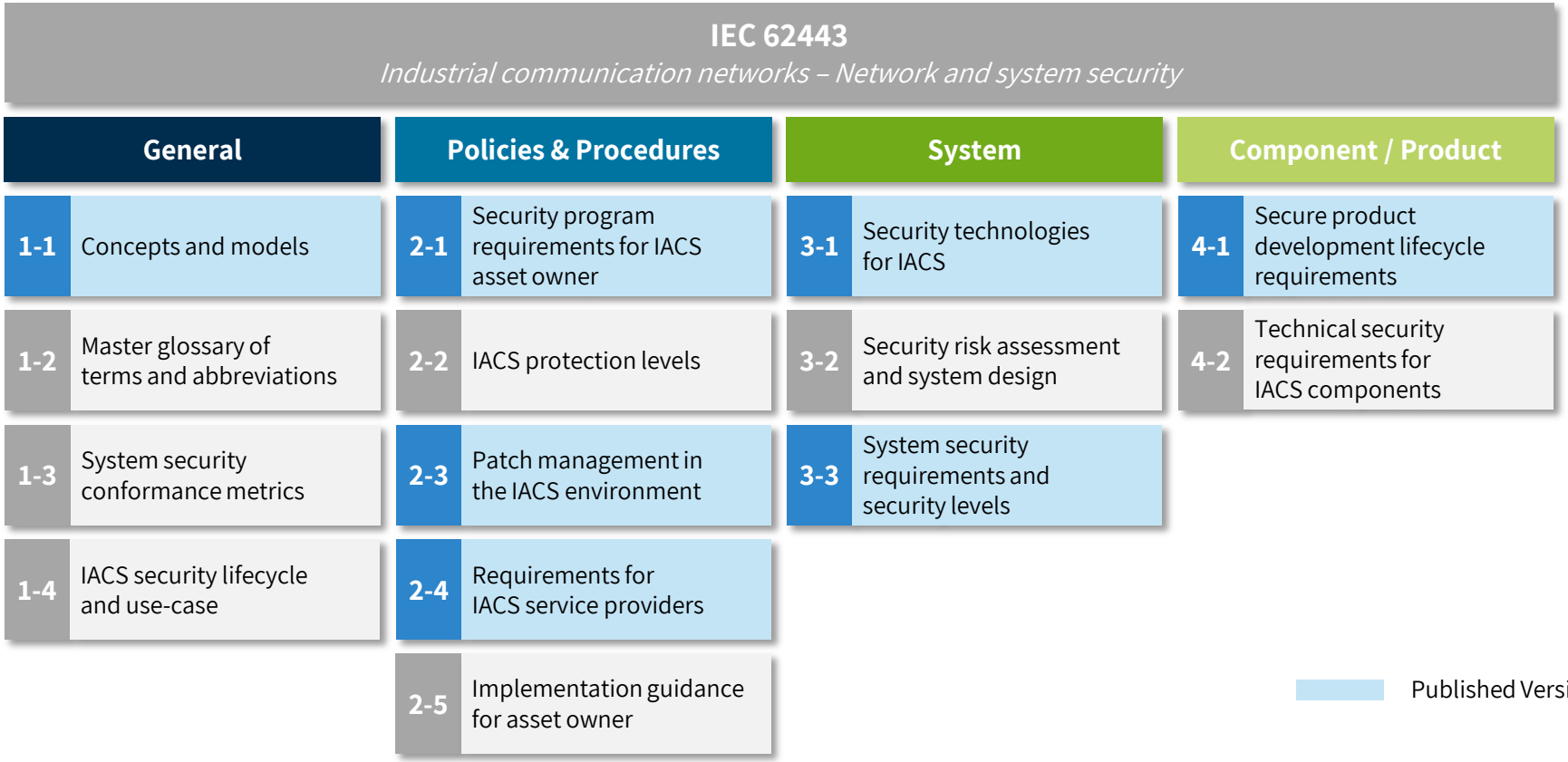
- Information security always for the entire system and consideration of the entire life cycle
  (from design, procurement, operation, maintenance)

INTEROPERABILITY

- Technical specifications create open systems with guaranteed characteristics (multivendor solutions)

variety & diversity | overlapping | simplicity | applicability | degree of updating | interaction

Standard: IEC 62443 „Network and system security”



IEC 62443: Essential Aspects

IEC 62443

Industrial communication networks – Network and system security

General

1-1	Concepts, Models
1-2	Terminology
1-3	Conformance Metrics
1-4	Lifecycle Use-cases

Policies & Procedures

2-1	• Organization • Training / awareness • Continuity plan • Policies, procedures • Personnel security • Physical security • Network segmentation • Account administration • Authentication • Authorization • Risk management & implementation • System development & maintenance • Information documentation management • Incident planning & response
2-3	• Patch management

System

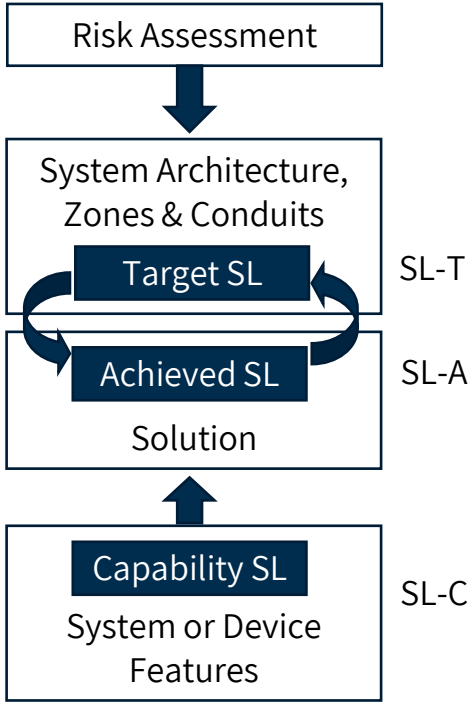
3-2	• System architecture & network segmentation • Zones and conduits • Security levels for systems
3-3	• Access control • Use control • Data integrity • Data confidentiality • Restrict data flow • Timely response to an event • Resource availability

Component / Product

4-1	• Product development process
4-2	• PLCs • HMI devices • PC stations • Firewalls • Gateways • Switches • Functions • Applications • Data

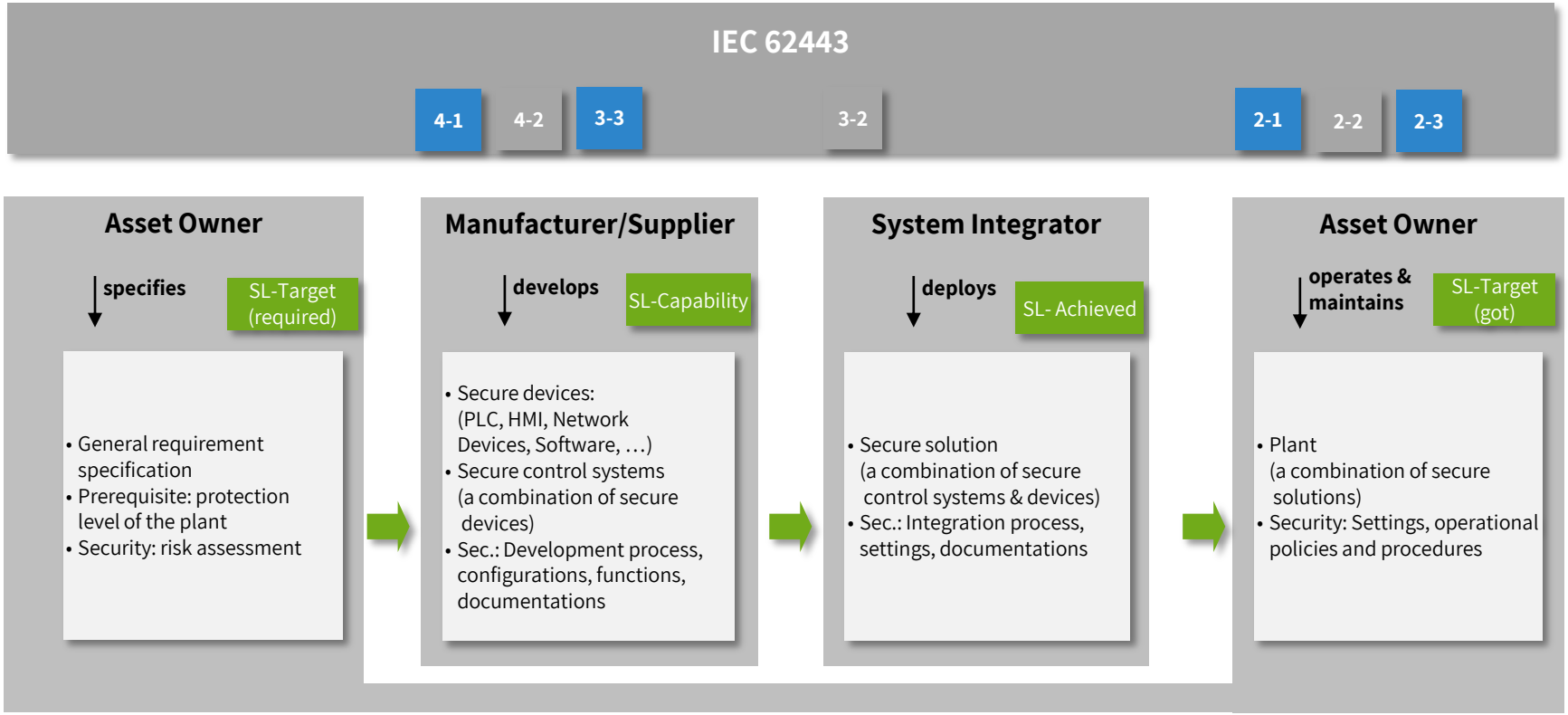
IEC 62443 – Security Level

IEC 62443-1-1: 4 Security Level defined	
SL 1	Protection against **casual or coincidental violation**
SL 2	Protection against **intentional violation** using simple mean
SL 3	Protection against **intentional violation** using sophisticated means
SL 4	Protection against **intentional violation** using sophisticated means with extended resources



IEC 62443-1-1 Draft 6, Edition 2, September 2016

IEC 62443: Life Cycle Approach



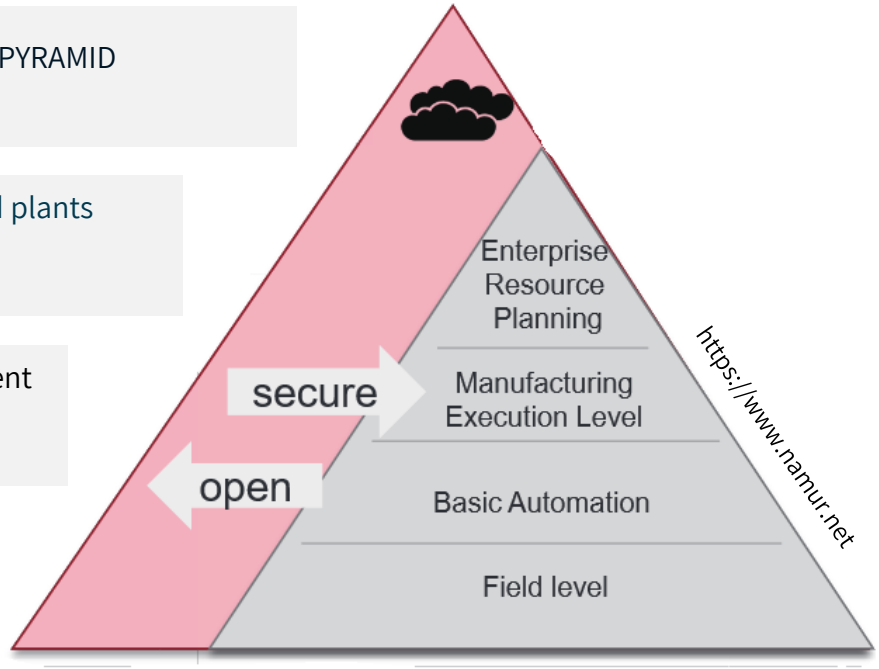
Case 1: NAMUR Open Architecture (NOA)

A A combined solution with well ACCEPTED AUTOMATION PYRAMID and OPENNESS TO NEW TECHNOLOGIES

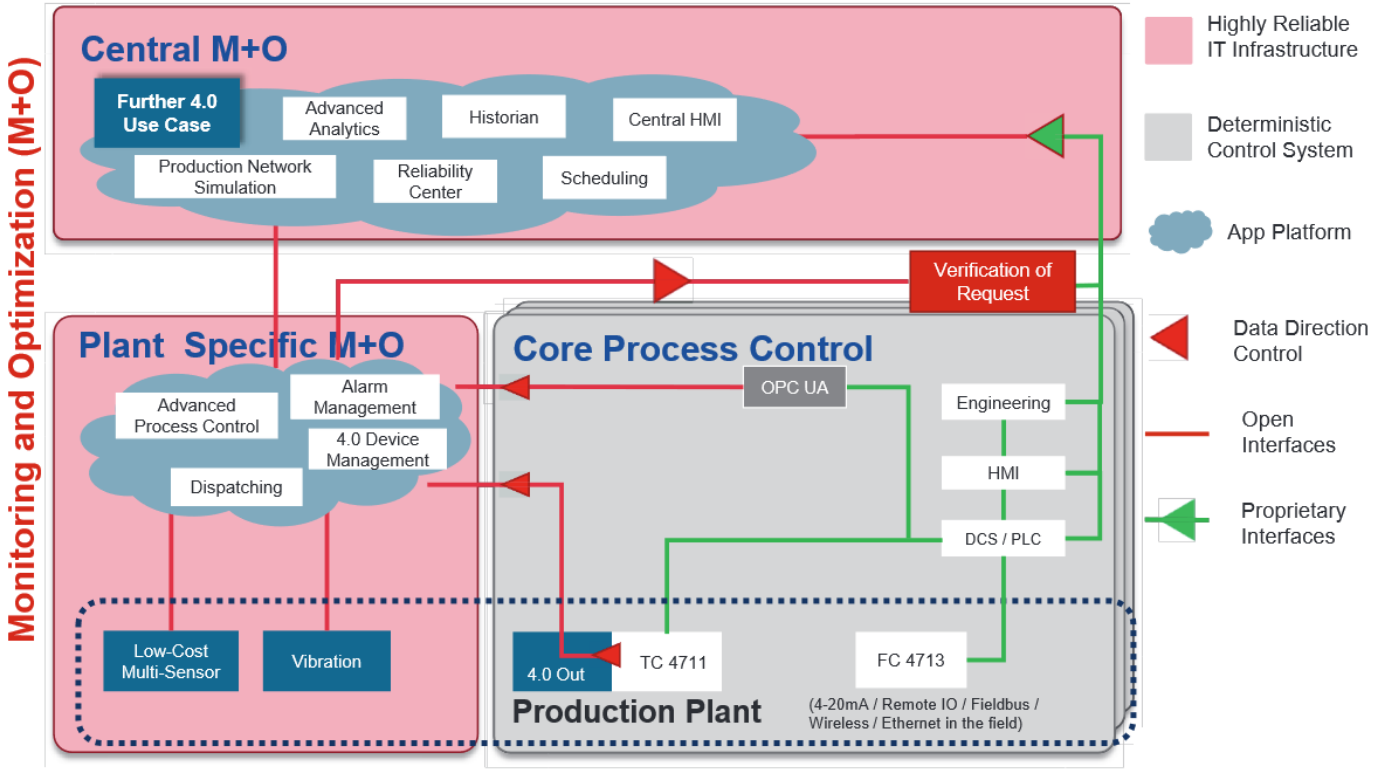
I Enables INNOVATIVE SOLUTIONS for green- & brownfield plants but the PROCESS CONTROL CORE REMAINS LARGELY UNAFFECTED

C CORE PROCESS CONTROL: with execution of measurement & control tasks, batch functions, acquisition of sensor values, HMI for plant operators

M MONITORING AND OPTIMIZATION: with execution monitoring & optimization tasks, new sensors for advanced functions, enterprise applications

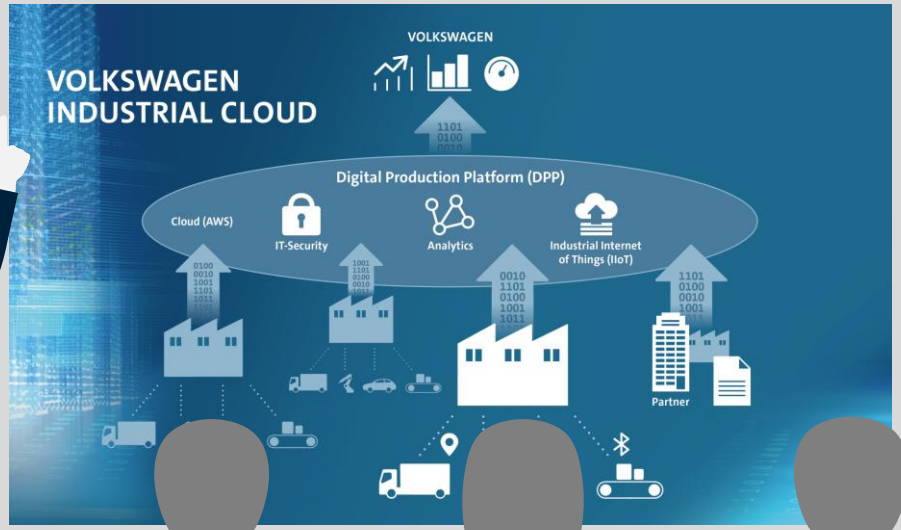


Case 1: NAMUR Open Architecture (NOA)



https://www.namur.net

Case 2: Volkswagen Digital Production Platform (DPP)



Reducing of factory costs:
- Increasing productivity & quality

Improving risk resilience in OT:
- Improving transparency through standardized KPI

Improved IT Operations in OT:
- Standardized, central OS approach

Big Challenge:
- Large number of IoT platforms along the hole supplier chain

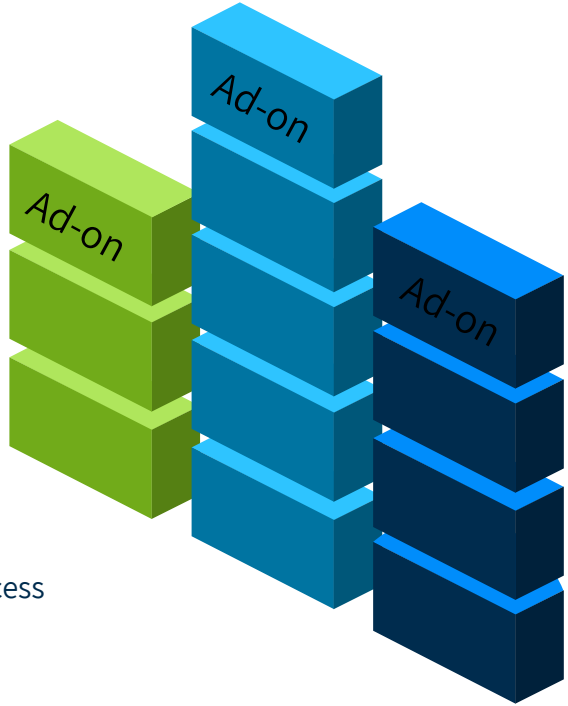
www.volkswagen-newsroom.com

Case 2: Volkswagen Digital Production Platform (DPP)

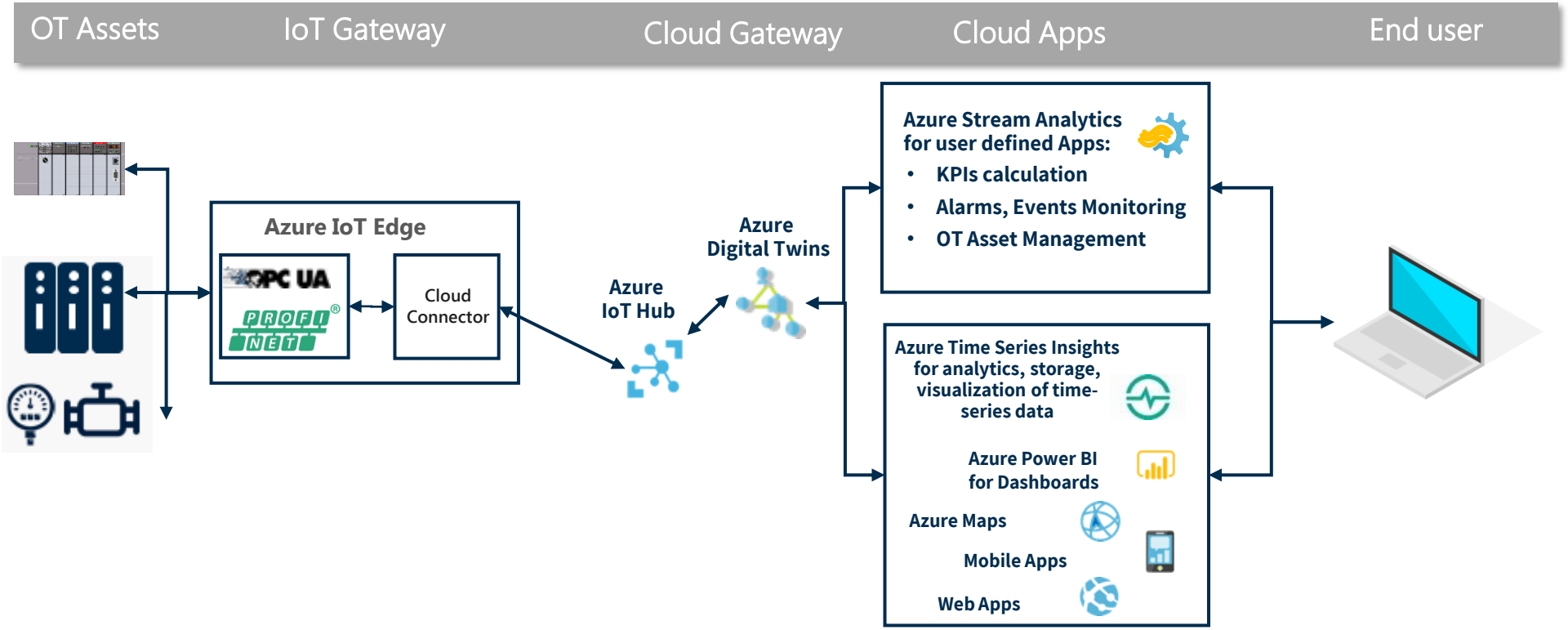
Support of commissioning and acceptance of plants

Monitoring of system status and development of KPIs

Monitoring of product quality (via production data acquisition) and optimization of the production process (via parameterization of systems)



Case 3: Evaluation Scenario



Evaluation based on IEC 62443-3-3 (in combination: ISO/IEC 27001 & 27027)

Evaluation: based on IEC 62443-3-3 System Security Req. & Security Levels

Foundational Requirements (FRs)

"A small set of Foundational Requirements shall be used to derive the full scope of detailed Technical and Program Requirements."

- **Identification & authentication**
- **Use control**
- **System integrity**
- **Data confidentiality**
- **Restricted data flow**
- **Timely response to events**
- **Resource availability**

- SR 1.1 Human user identification and authentication
- SR 1.2 Software process and device identification and authentication
- SR 1.3 Account management
- SR 1.4 Identifier management
- SR 1.5 Authenticator management
- SR 1.6 Wireless access management
- SR 1.7 Strength of password-based authentication
- SR 1.8 Public key infrastructure (PKI) certificates
- SR 1.9 Strength of public key authentication
- SR 1.10 Authenticator feedback
- SR 1.11 Unsuccessful login attempts
- SR 1.12 System use notification
- SR 1.13 Access via untrusted networks

Evaluation: based on IEC 62443-3-3 System Security Req. & Security Levels

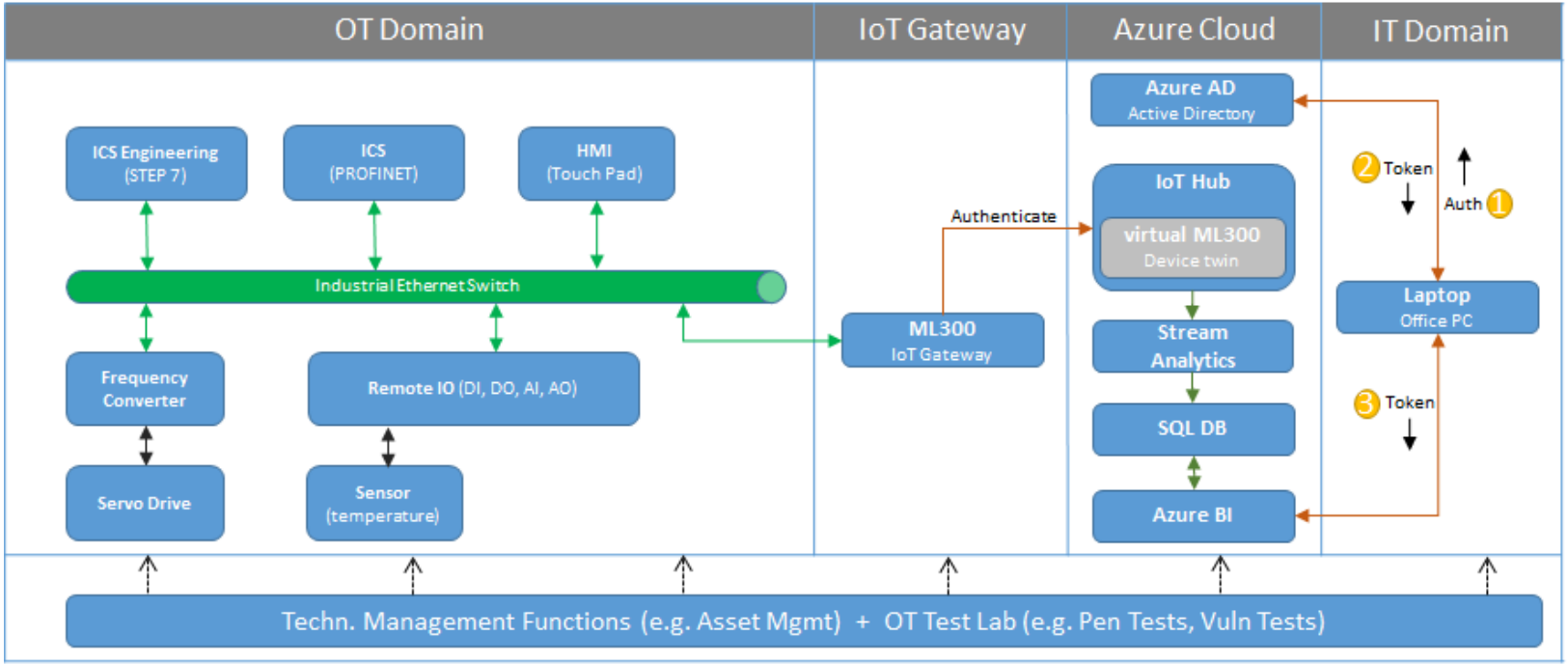
	SL1	SL2	SL3	SL4
FR 1 – Identification and Authentication Control (IAC)				
SR 1.1 – Human user identification and authentication	X	X	X	X
The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.				
RE (1) Unique identification and authentication		X	X	X
The control system shall provide the capability to uniquely identify and authenticate all human users.				
RE (2) Multifactor authentication for untrusted networks			X	X
The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 4.14, SR 1.12 – Access via untrusted networks).				
RE (3) Multifactor authentication for all networks				X
The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				

Evaluation: based on IEC 62443-3-3 System Security Req. & Security Levels

	SL1	SL2	SL3	SL4
FR 1 – Identification and Authentication Control (IAC)				
SR 1.2 – Software process & device ident. & authentication		X	X	X
The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.				
RE (1) Unique identification and authentication			X	X
The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.				

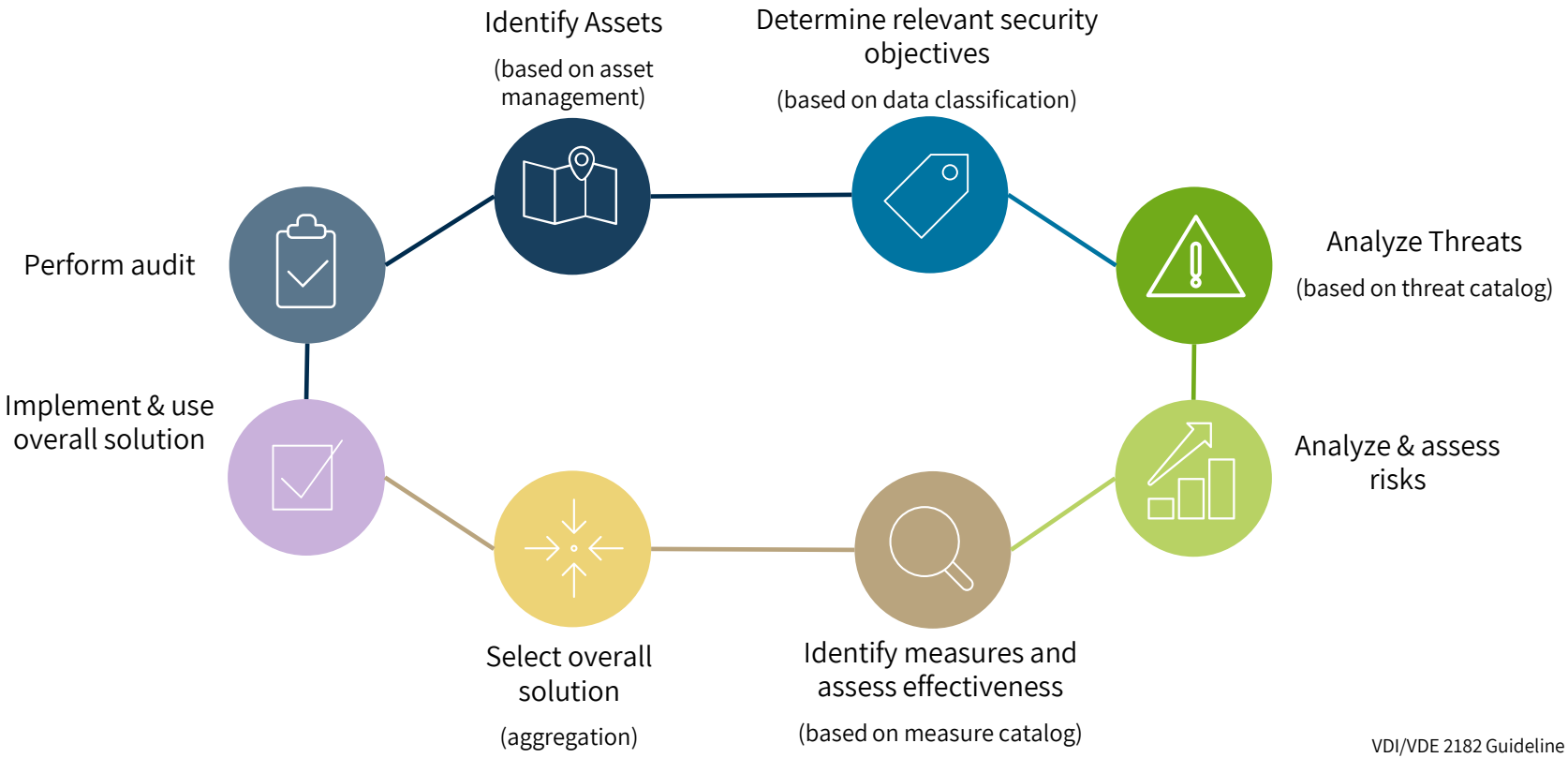
Implementation of Evaluation Scenario

Gain experience, start deeper analysis of security architecture & functions (aws & azure certification)



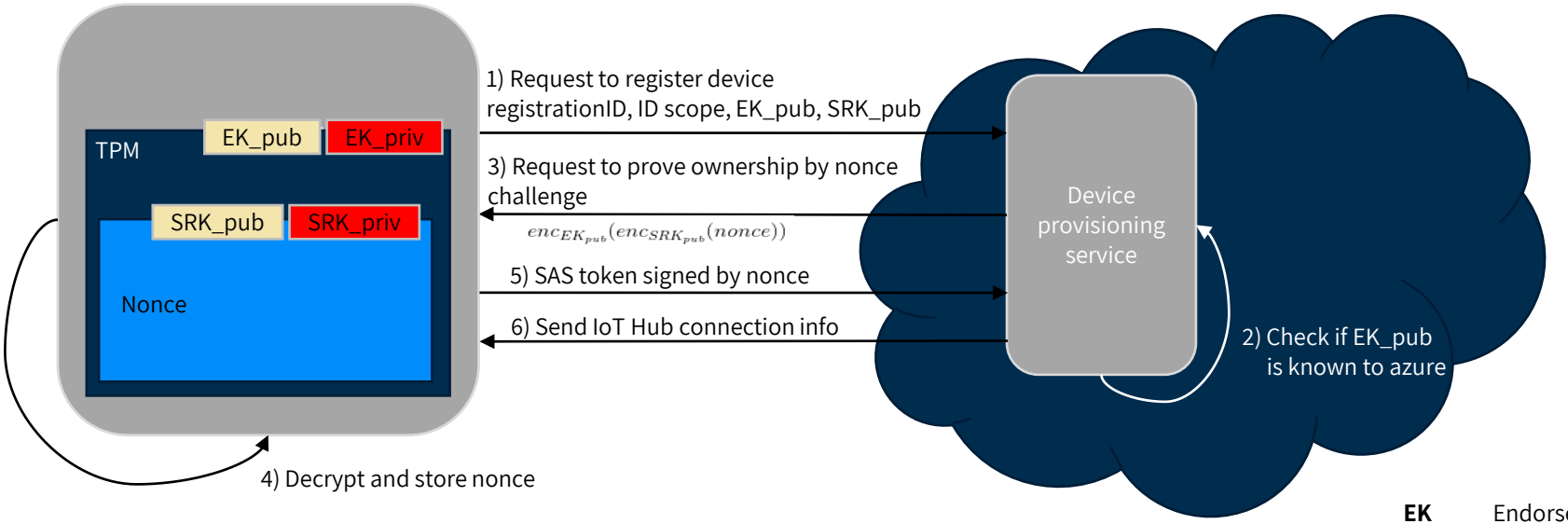
Evaluation: following a systematic approach

OT Risk Management based on VDI/VDE 2182



Process 1: Asset Identification

Identify critical assets, analysis of their functions (focus lies on external interfaces)



EK	Endorsement Key
SRK	Storage Root Key
pub	Public portion of key
priv	Private portion of key
enc	Encryption

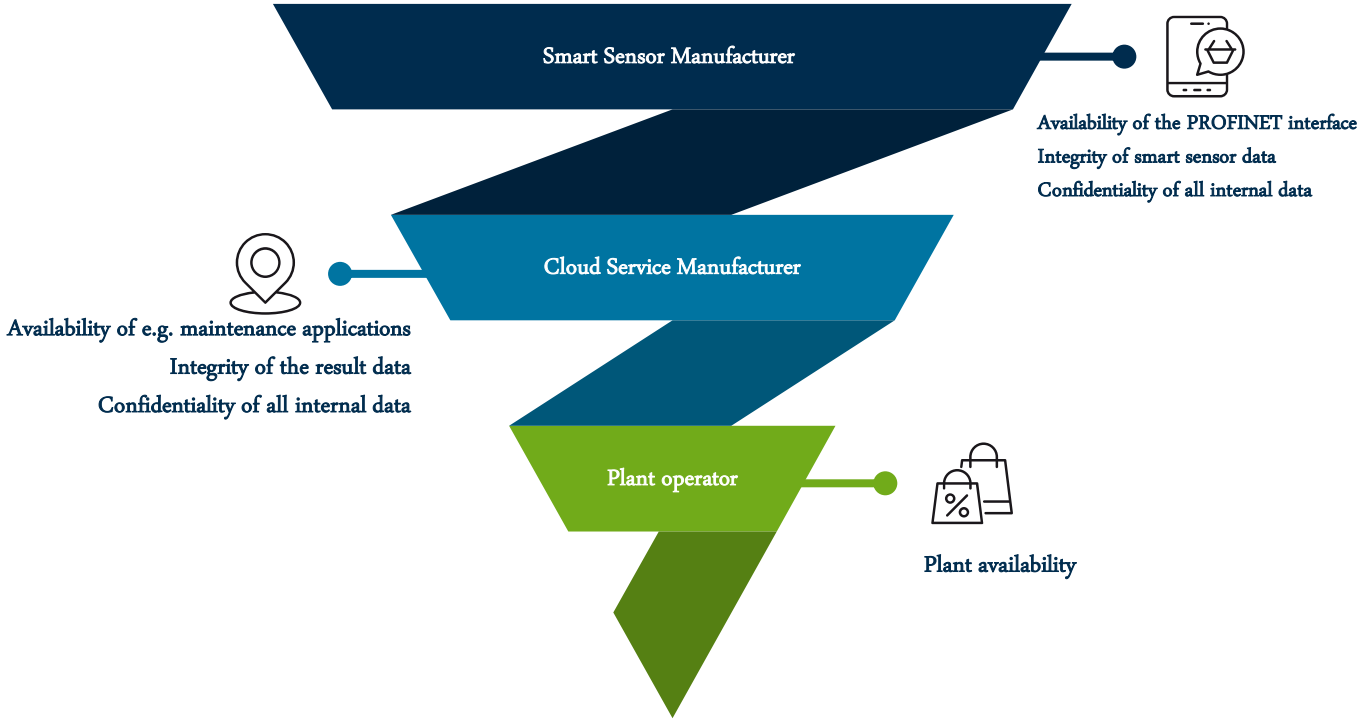
Process 1: Asset Identification

Identify critical assets, document their functions (capabilities according IEC 624433-3)

FR	FR Title	SR	SR Title	SL1	SL2	SL3	SL4
FR 1	Identification and authentication control	SR 1.1	Human user identification and authentication				
FR 1	Identification and authentication control	SR 1.2	Software process and device identification and authentication				
FR 1	Identification and authentication control	SR 1.3	Account management				
FR 1	Identification and authentication control	SR 1.4	Identifier management				
FR 1	Identification and authentication control	SR 1.5	Authenticator management				
FR 1	Identification and authentication control	SR 1.6	Wireless access management				

Process 2: Determine relevant security objectives

Security objective in a use case, consider all parties involved



TLP:Green

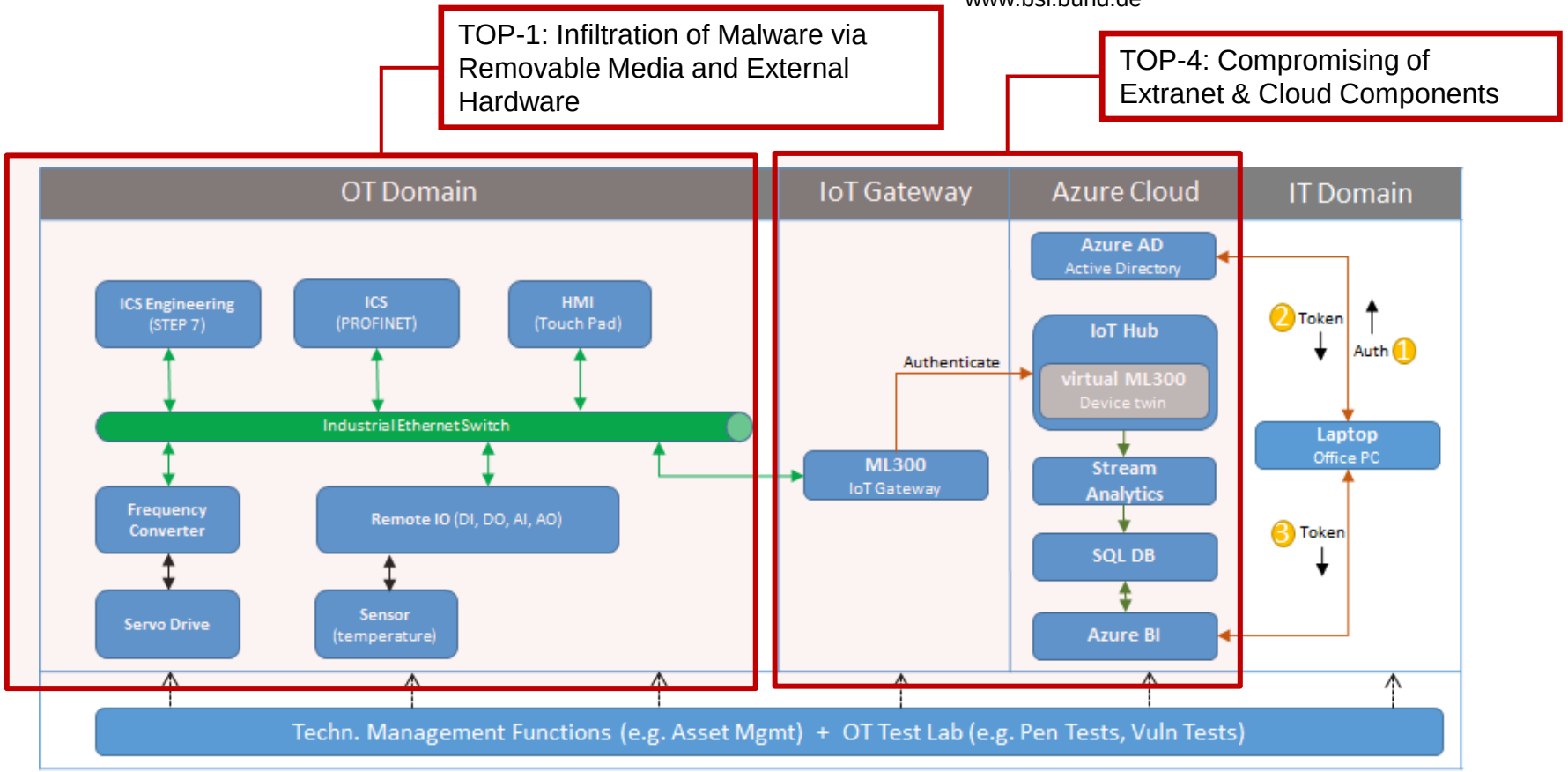
Process 3: Analyze threats

- Threat Catalogues
  - **Open Web Application Security Project (OWASP)** (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
  - **BSI Threat Catalogue** (https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html)

- Threat / Vulnerability databases (constantly updated)
  - **ICS-CERT** (https://ics-cert.us-cert.gov/)
  - **Common Vulnerabilities and Exposures (CVE)** (https://cve.mitre.org/)
  - **Common Weakness Enumeration (CWE)** (https://cwe.mitre.org/)
  - **Open Sourced Vulnerability Database** (http://osvdb.org/)
  - **National Vulnerability Database** (https://nvd.nist.gov/)
  - **Security Focus** (http://www.securityfocus.com/)
  - **Common Attack Pattern Enumeration and Classification (CAPEC)** (https://capec.mitre.org/)

Process 3: Analyze threats

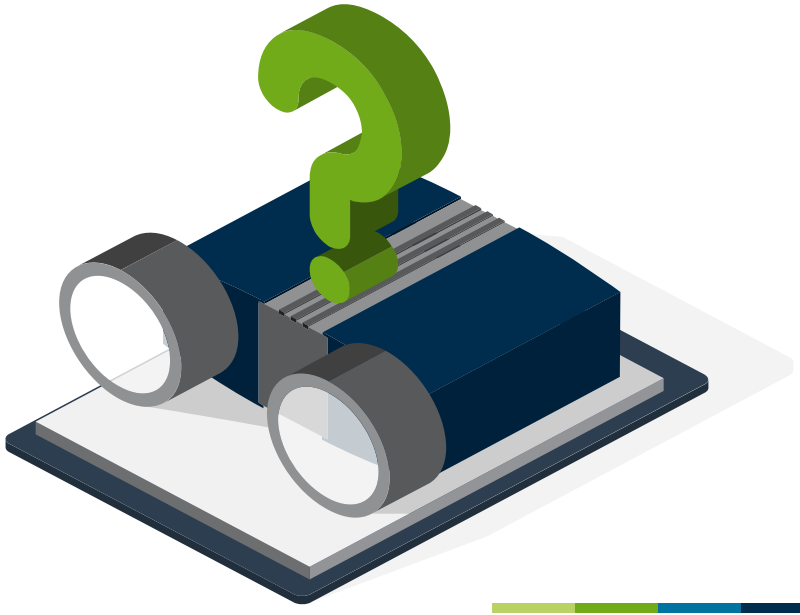
www.bsi.bund.de



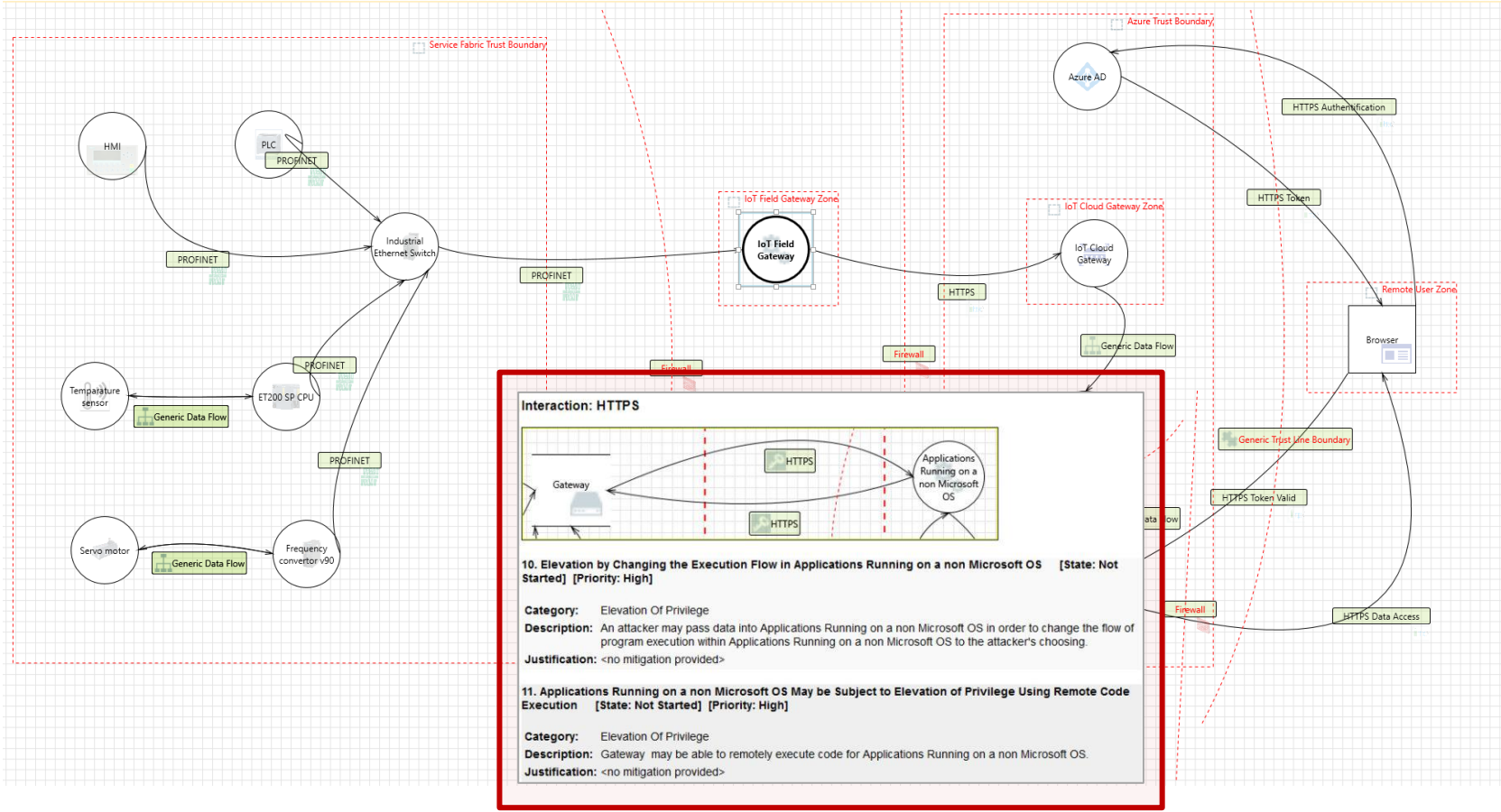
Process 3: Analyze threats

Use of tools, e.g. Microsoft Threat Modelling

- Two parts are needed: the model and the template.
- Model: visual representation (diagram) of the system. It consists of stencils with properties. Stencils are components of a system and can be one of three different types: Targets, Flows and Boundaries
- Targets represent the components of a system, e.g. Switches, PCs, PLCs
- Flows represent the connection between targets, e.g used protocols PROFINET or OPC UA
- Boundaries represent segments, which can be crossed by flows.
- For every stencil, properties can be defined, which are used by the template for the threat assessment



Process 3: Analyze threats



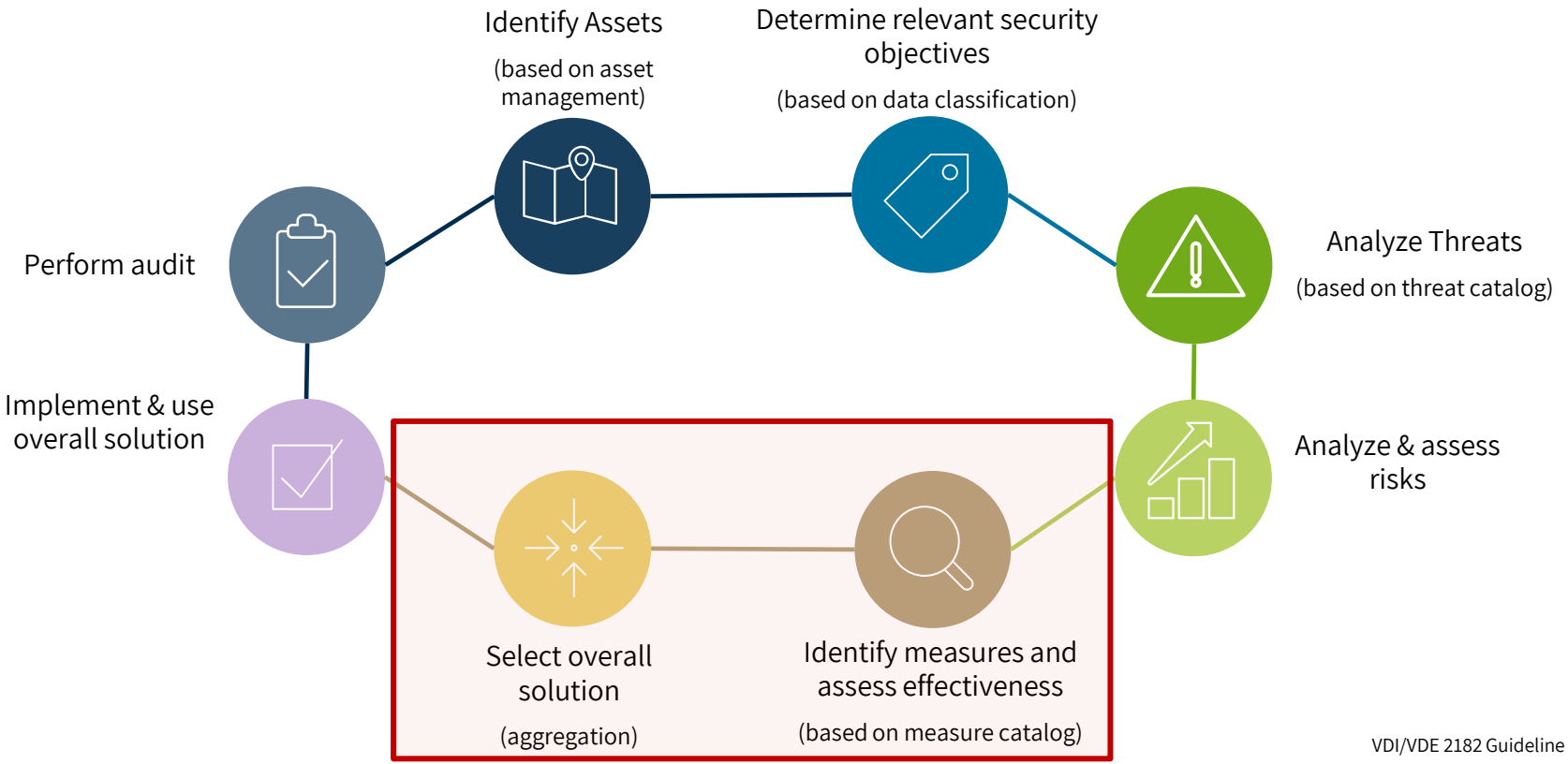
TLP:Green

Process 4: Analysis and access risks

Name	Zone DMZ (critical asset: IoT Gateway)
Function (General)	The system ensures the correct measurement and aggregation of temp sensor values.
Access (via)	Zone „Azure Cloud“ & Zone „OT Domain“
Data Flows (Zone Boundary)	PROFINET, OPC-UA
Assets	SPS (incl. Webserver), agent system, screwdriver
Risk Assessment (high level)	Threats & Vulnerabilities: - relevent threat (output from threat modelling) - Vulnerabilities through the use of standard components (output from vuln. tests) Consequences: - manipulation of the maintenance process, possibly loss of know-how Potential risk: High
Security Requirements (based on IEC 62443-3-3)	FR1 Identification and Authentication FR2 Use Control FR3 System Integrity FR7 Ressource Availability
Security Level SL-T	FR1.2: SL3

Evaluation: next steps

OT Risk Management based on VDI/VDE 2182

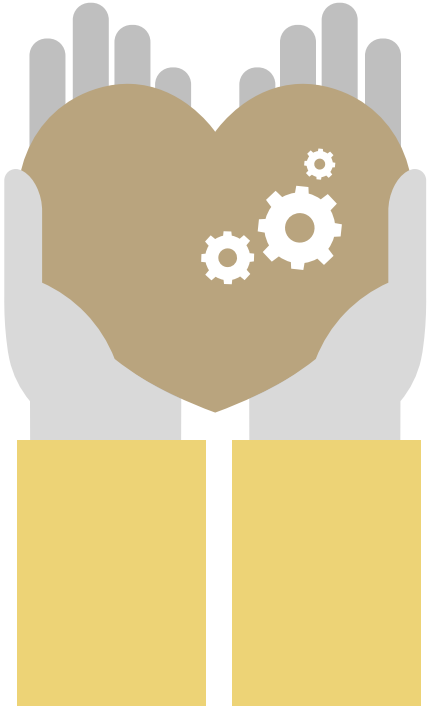


TLP:Green

VDI/VDE 2182 Guideline

Conclusion

- Different cloud based use cases & architectural concepts available
- Well accepted standards & guidelines available
- Todays security concepts doesn’t consider cloud scenarios
- There is a need of deeper investigations to enable secure cloud based solutions



TLP:Green

Questions & Answers

Heiko ADAMCZYK
OT Security Expert

Mob: +49-170-5280522
E-Mail: heiko.adamczyk@dcso.de

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany

E: info@dcso.de

P: +49-30-726219-0

TLP:Green

Cloud-spezifische Bedrohungen

Nicht in ausreichendem Maße isolierte Cloud Ressourcen

- Physikalische Ressourcen durch VMs mehrerer Kunden verwendet

Nur in standardisierter Form angebotene Service Level Agreements (SLA)

- Uneingeschränkte Einsichtnahme aller Daten durch Cloud Service Provider

Anwendung abhängig von Verfügbarkeit des Internet Service Providers

- Sehr hohe Kosten bei maximaler Verfügbarkeit (z.B. Satelliten-Backup)

Ableitung von Risiken

- Zugriff auf wichtiges Know-how des Unternehmens durch Offenlegung
- Manipulation von Daten zwecks Sabotage
- Verfügbarkeit der gesamten Anlage

vgl. ENISA, „Cloud Computing – Benefits, risks, and recommendations for information security“, Nov. 2009