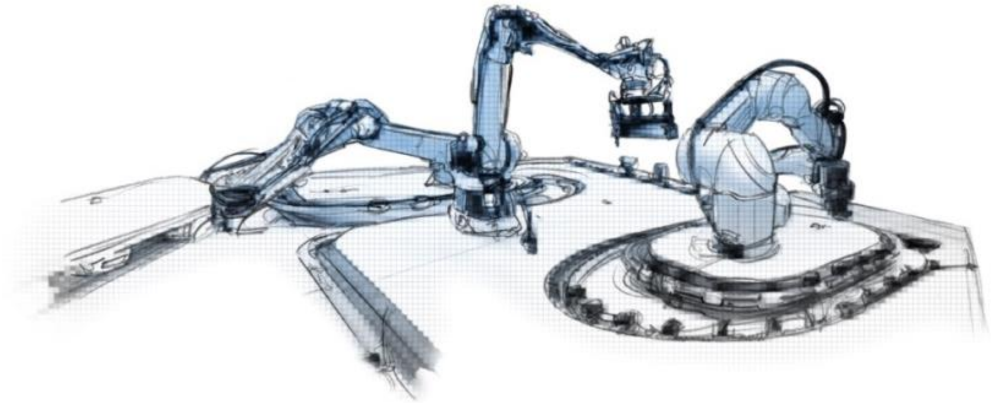


CERT@VDE – The cybersecurity platform for industrial small and medium-sized enterprises (SME)

Andreas Harner, Head of CERT@VDE

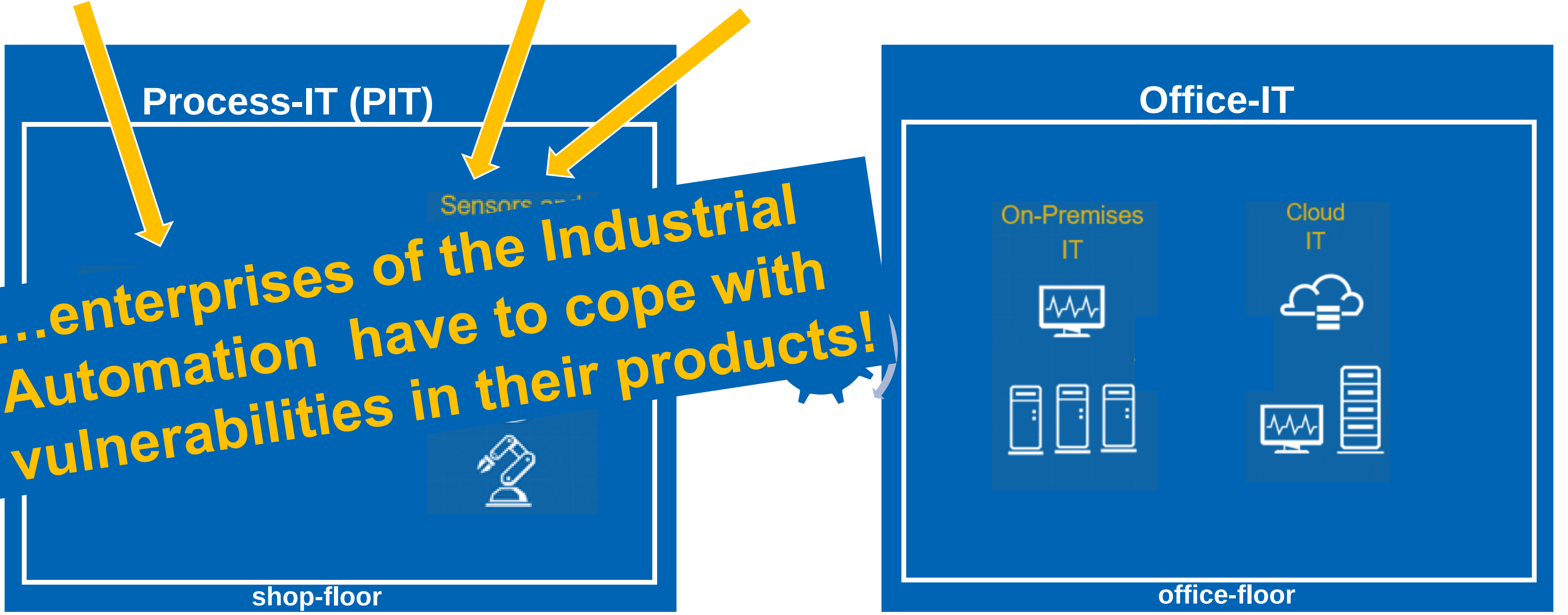
Hamburg, January 2018

Industrial IoT (IIoT) or Industry 4.0

IT based automation devices based on classic operation systems

classic fieldbuses replaced by Ethernet-based buses

Worldwide access to the sensors: through the Cloud!



…enterprises of the Industrial Automation have to cope with vulnerabilities in their products!

Security differences between Office-IT and Process-IT

	Process-IT, Industrial Control Systems (ICS)	Office-IT, Office-Systems
Anti-Virus-Programs	unusual / difficult to apply	usual / easy to apply
product life cycle	up to 20 years and longer	3 - 5 years
real-time requirement	very high	low: delays are acceptable
application of patches	not regular / unplanned	regular / planned
security tests / audits	no common practice	planned und partly mandatory
outsourcing	rarely	standard
physical security	varies from low until high	high (esp.Critical Infrastructures)
vulnerability handling	SME: immature	standard

…need of a „coordinating PSIRT“ in Germany for ICS…

PHOENIX CONTACT
INSPIRING INNOVATIONS

BECKHOFF

PEPPERL+FUCHS

Weidmüller

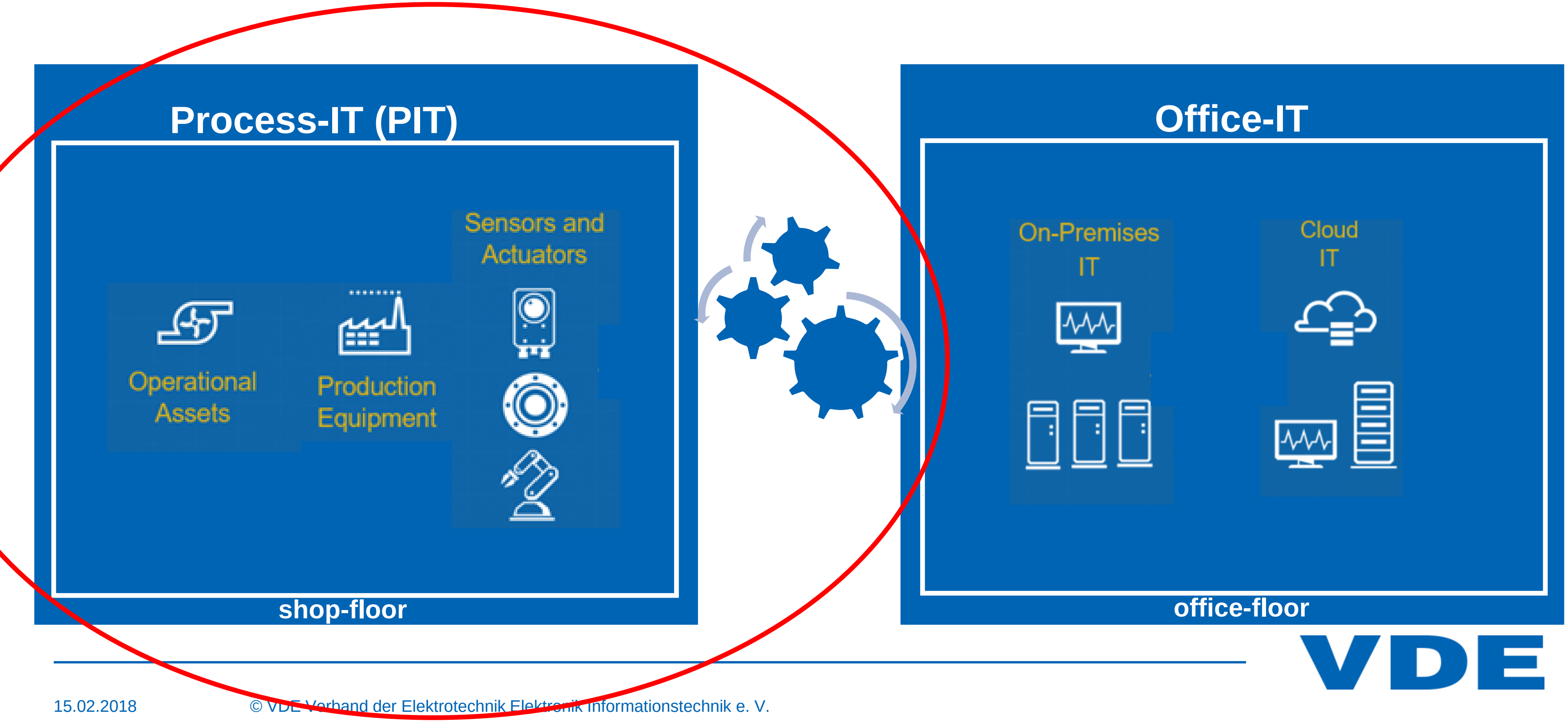
Endress+Hauser

<u>Common Position:</u>

- *„….we, the SMEs of the Industrial Automation need a trusworthy, neutral, independant platform based on an institution with a wellknown reputation…“*
  → VDE e.V. (registered association, non-profit)“

  → Within european time zone – able to speak German – able to speak „Automation“

Scope of CERT@VDE



The VDE e.V. - Association for Electrical, Electronic & Information Technologies

Science,Technology, Innovation

- Knowledge transfer in the VDE network of experts
- Partner for educational and technological policies
- Youth development

Standardisation

- VDE|DKE is the German member of IEC and of CENELEC

Test, Certification

- Interoperability – Safety – Security - Usability

VDE CERT

non-profit

Historical interrupt or „why VDE“?

MASCHINEN FABRIK OERLIKON
KRAFTUEBERTRAGUNG LAUFFEN-FRANKFURT
175Km
ALLGEMEINE ELECTRICITÄTS GESELLSCHAFT

Fußnote: Von Unknown, dead. - Scan from Original, Gemeinfrei

Quelle: https://commons.wikimedia.org/w/index.php?curid=1733600

1879

- Foundation of the first “Berliner Elektrotechnik-Vereins“: Proposed by Werner v. Siemens:

→ **Safety…** for electrical systems

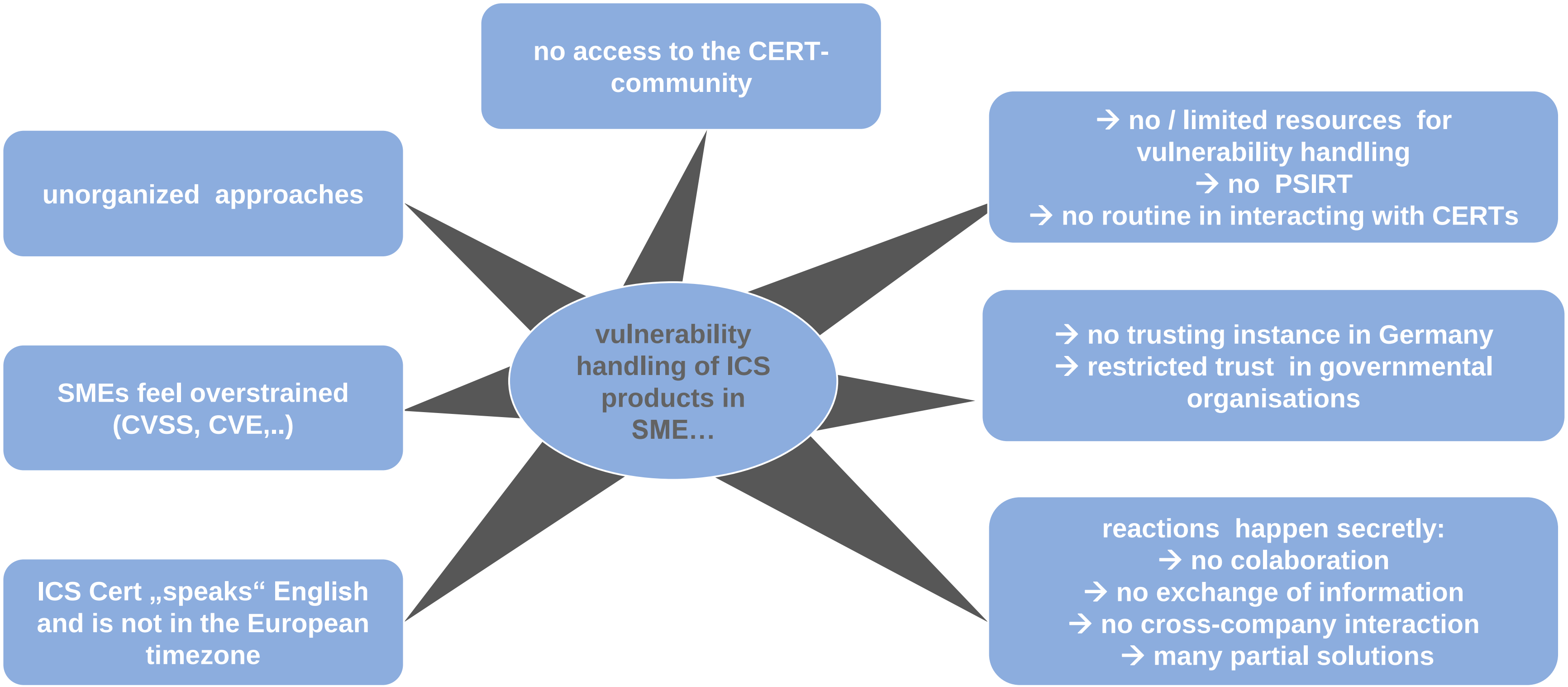
→ **Exchange of information …** between power operators and manufacturers

1893

- Foundation of VDE
(by Adolf Slaby and Georg Wilhelm von Siemens)

Electrical Safety → Functional Safety → Cybersecurity

Today‘s situation: vulnerability handling in SMEs



vulnerability handling of ICS products in SME…

no access to the CERT-community

unorganized approaches

SMEs feel overstrained (CVSS, CVE,..)

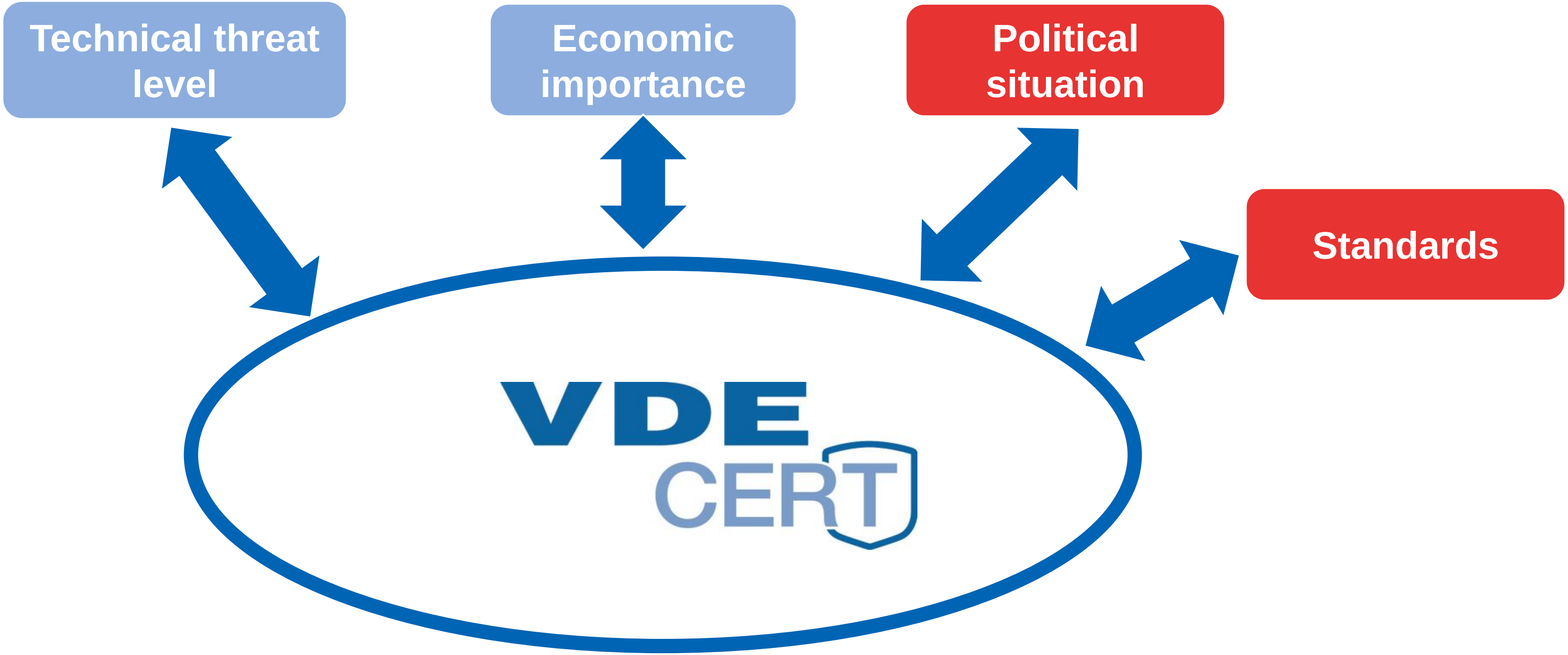
ICS Cert „speaks“ English and is not in the European timezone

→ no / limited resources for vulnerability handling
→ no PSIRT
→ no routine in interacting with CERTs

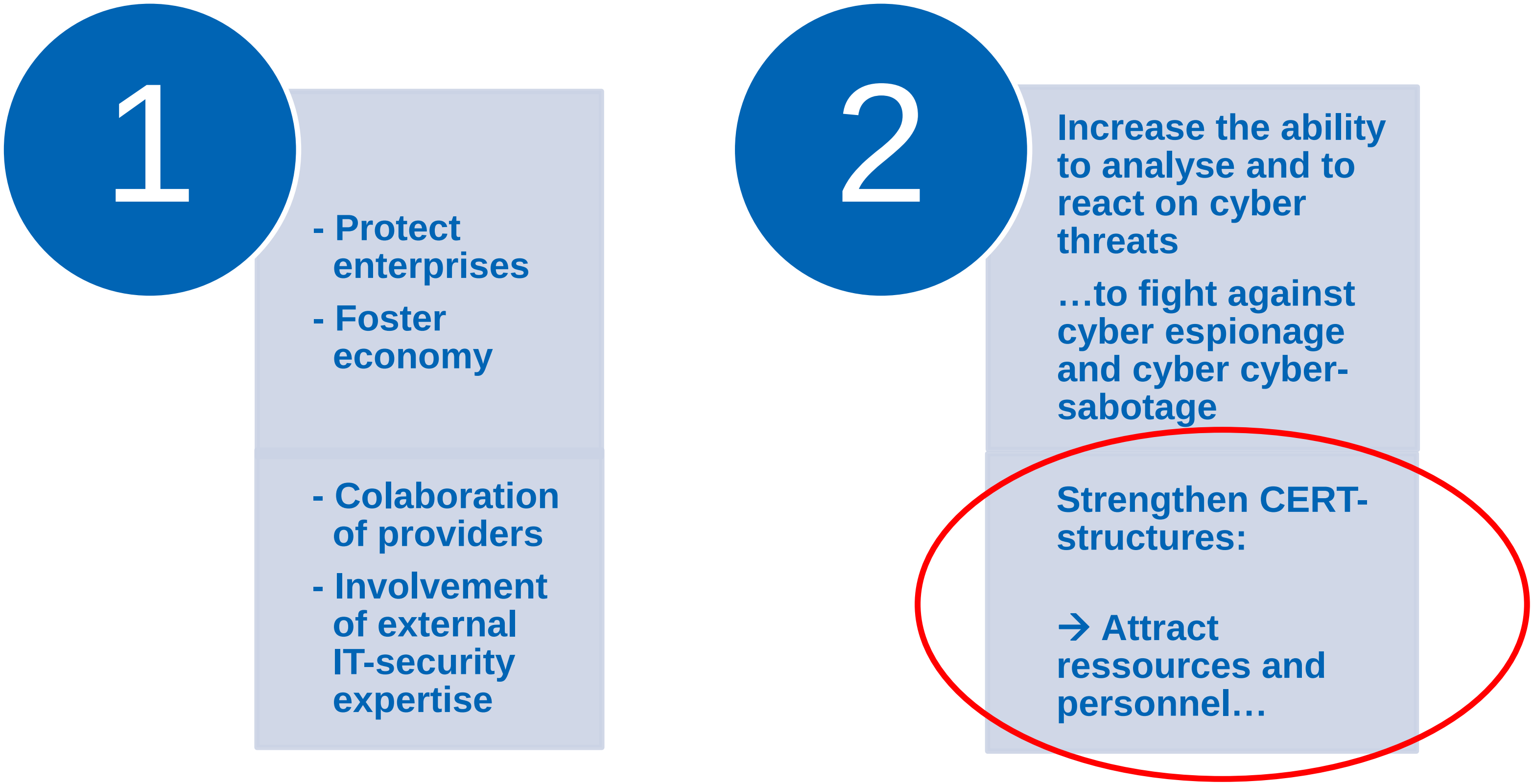
→ no trusting instance in Germany
→ restricted trust in governmental organisations

reactions happen secretly:
→ no colaboration
→ no exchange of information
→ no cross-company interaction
→ many partial solutions

Further drivers for CERT@VDE



Germany: National Cybersecurity-Strategy (2016)



1

- Protect enterprises
- Foster economy

- Colaboration of providers
- Involvement of external IT-security expertise

2

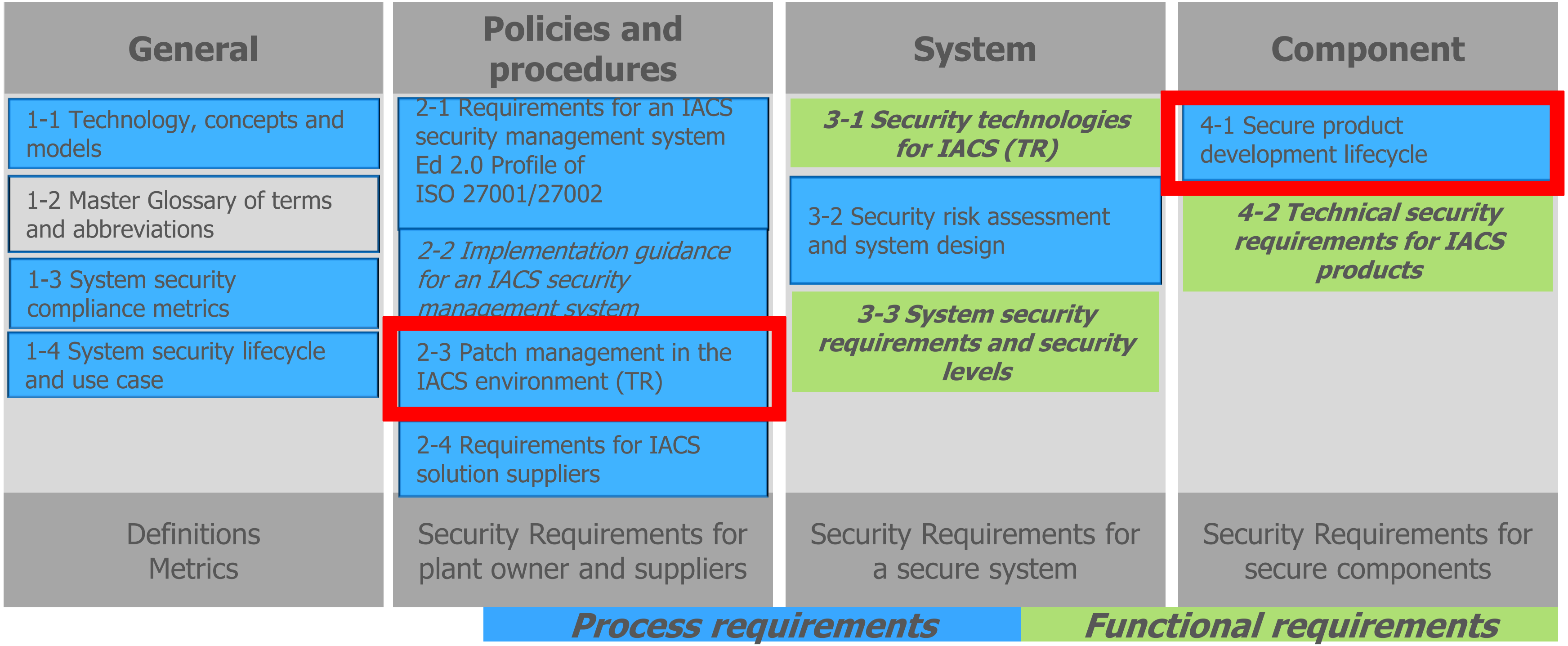
Increase the ability to analyse and to react on cyber threats

…to fight against cyber espionage and cyber cyber-sabotage

Strengthen CERT-structures:

→ Attract ressources and personnel…

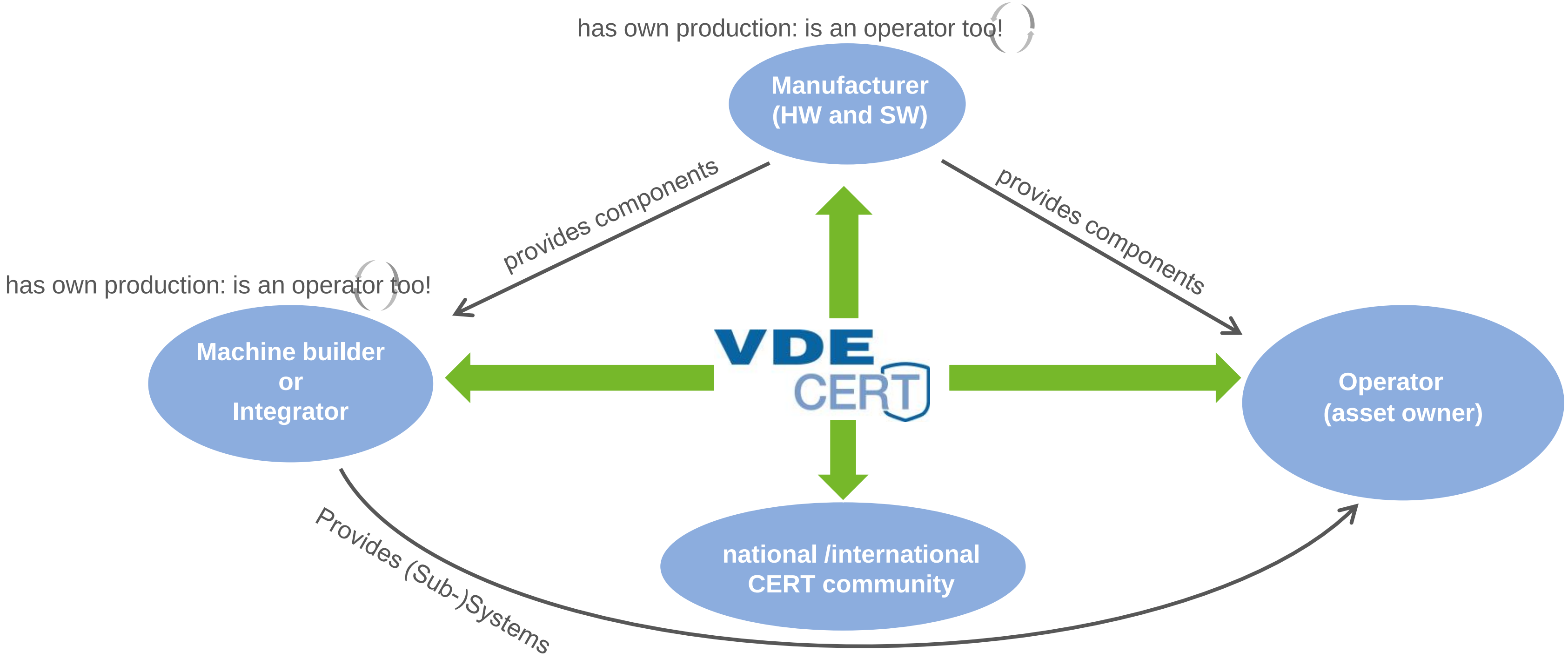
IEC 62443:
Normative requirements in standards for industrial security



General	Policies and procedures	System	Component
1-1 Technology, concepts and models	2-1 Requirements for an IACS security management system Ed 2.0 Profile of ISO 27001/27002	***3-1 Security technologies for IACS (TR)***	4-1 Secure product development lifecycle
1-2 Master Glossary of terms and abbreviations	*2-2 Implementation guidance for an IACS security management system*	3-2 Security risk assessment and system design	***4-2 Technical security requirements for IACS products***
1-3 System security compliance metrics	2-3 Patch management in the IACS environment (TR)	***3-3 System security requirements and security levels***	
1-4 System security lifecycle and use case	2-4 Requirements for IACS solution suppliers		
Definitions Metrics	Security Requirements for plant owner and suppliers	Security Requirements for a secure system	Security Requirements for secure components

Process requirements ***Functional requirements***

Closing the gap: CERT@VDE



Added values for CERT@VDE cooperation partners

- **cross-company** discussions and interaction on the trustworthy and secure environment of CERT@VDE *(anonymous, if required)* → **motivates to collaborate!**
- **information hub between CERT community and automation industry**

qualified information exchange between manufacturers, operators, integrators and CERT community
→ **Responses** to threats/detected vulnerabilities: **structured and faster**!

Single Point of Contact:

- for operators to find contact persons of the manufacturers
- for operators to find published security information of all their suppliers in one place
- for manufacurers to adress customers and integrators using their products
- supports the communication with other CERTs (e.g. ICS-CERT) for the constituency
- supports the communication with reporters of vulnerabilities („White-Hat Hacker"…):
  → **„Coordinated Disclosure"**
- collects and provides industry-specific security information for the constituency

Added values for CERT@VDE cooperation partners – II.

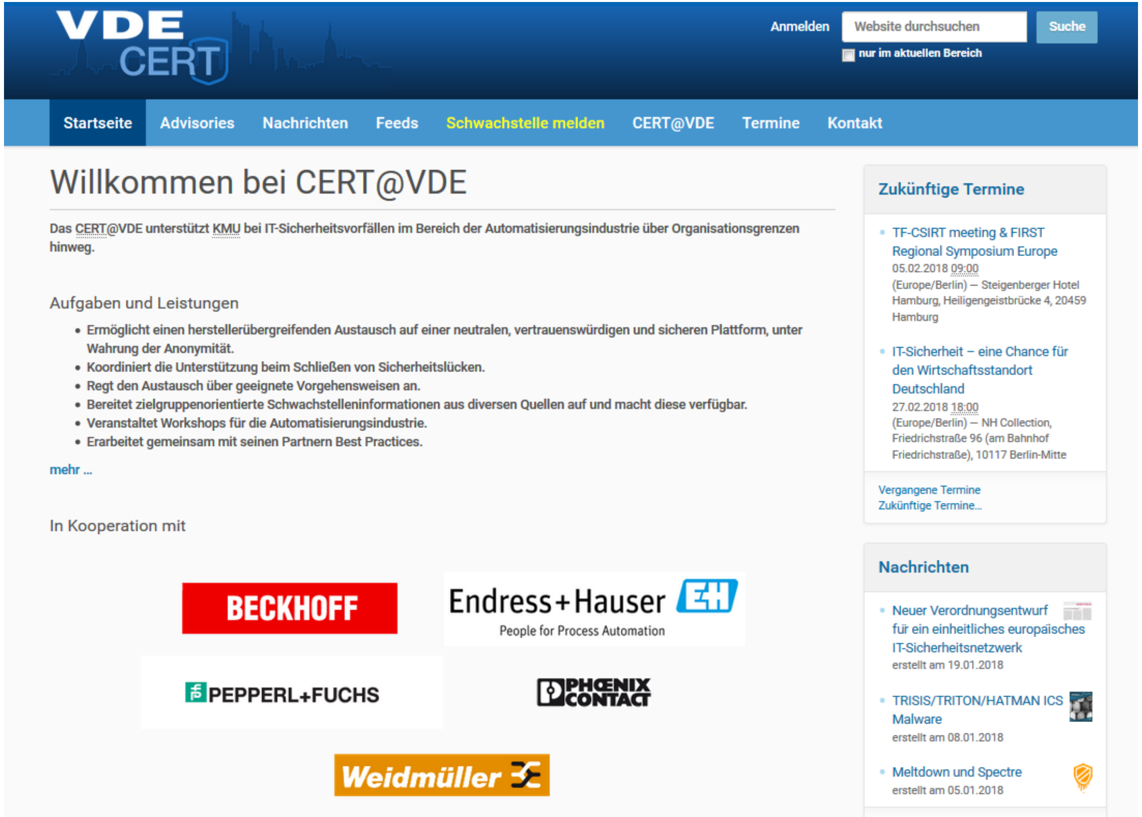
coordination when fixing vulnerabilities and **support** on publication of advisories.
CVE number assignment
(lack of routine in SMEs dealing with CVSS)

elaborate **Best Practices** by the constituency, for the constituency

events and workshops for the automation industry to improve processes, to raise awareness and to promote the importance of CERTs

- **image boost** for the cooperation partners
- **institutionalisation of PSIRT structures** inside the SMEs is encouraged

Status of CERT@VDE



Willkommen bei CERT@VDE

Das CERT@VDE unterstützt KMU bei IT-Sicherheitsvorfällen im Bereich der Automatisierungsindustrie über Organisationsgrenzen hinweg.

Aufgaben und Leistungen

- Ermöglicht einen herstellerübergreifenden Austausch auf einer neutralen, vertrauenswürdigen und sicheren Plattform, unter Wahrung der Anonymität.
- Koordiniert die Unterstützung beim Schließen von Sicherheitslücken.
- Regt den Austausch über geeignete Vorgehensweisen an.
- Bereitet zielgruppenorientierte Schwachstelleninformationen aus diversen Quellen auf und macht diese verfügbar.
- Veranstaltet Workshops für die Automatisierungsindustrie.
- Erarbeitet gemeinsam mit seinen Partnern Best Practices.

mehr ...

In Kooperation mit

Zukünftige Termine

- TF-CSIRT meeting & FIRST Regional Symposium Europe
  05.02.2018 09:00 (Europe/Berlin) — Steigenberger Hotel Hamburg, Heiligengeistbrücke 4, 20459 Hamburg
- IT-Sicherheit – eine Chance für den Wirtschaftsstandort Deutschland
  27.02.2018 18:00 (Europe/Berlin) — NH Collection, Friedrichstraße 96 (am Bahnhof Friedrichstraße), 10117 Berlin-Mitte

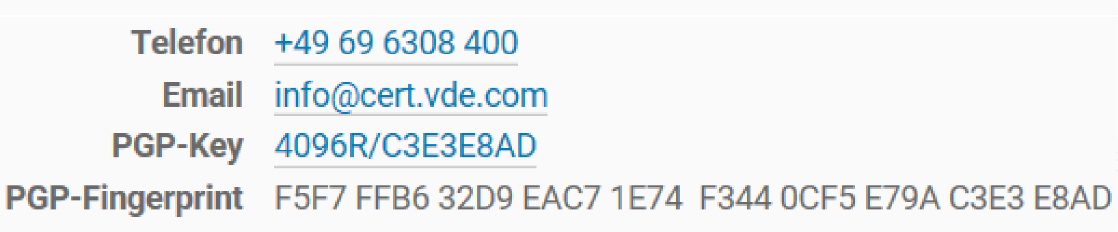
Vergangene Termine
Zukünftige Termine...

Nachrichten

- Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk
  erstellt am 19.01.2018
- TRISIS/TRITON/HATMAN ICS Malware
  erstellt am 08.01.2018
- Meltdown und Spectre
  erstellt am 05.01.2018

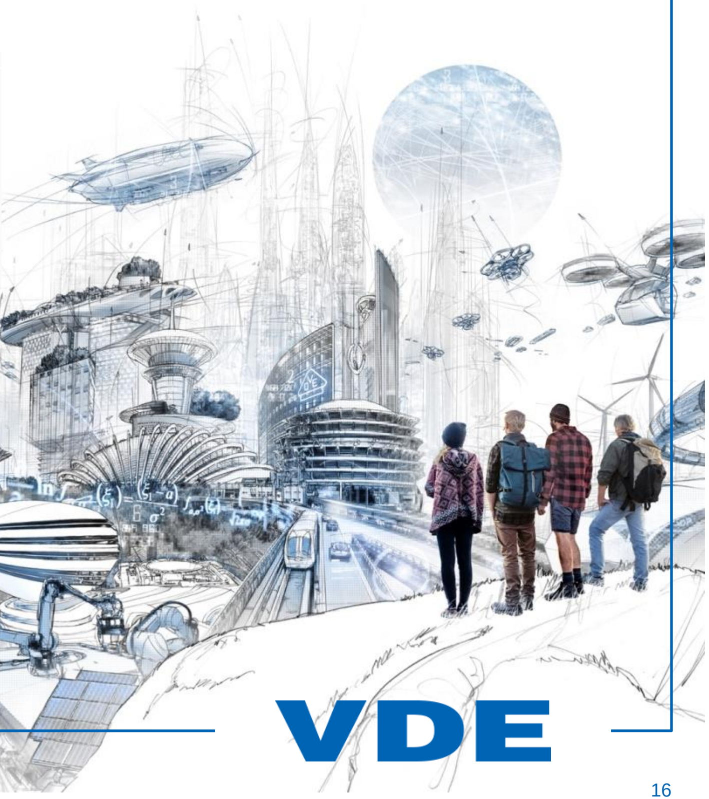
- **Team:**
  1 Head
  2 IT-Sec-Managers
  1 BDM + marketing
- **Web**:
  https://cert.vde.com
- **Advisories**
- Collaboration platform based on „Mattermost“
- **Member:**
  - „Deutscher CERT Verbund“
  - Accredited in „TI-TF-CSIRT“

Thank you for your attention!



Telefon	+49 69 6308 400
Email	info@cert.vde.com
PGP-Key	4096R/C3E3E8AD
PGP-Fingerprint	F5F7 FFB6 32D9 EAC7 1E74 F344 0CF5 E79A C3E3 E8AD

https://cert.vde.com



Andreas Harner

Head of CERT@VDE

Phone: +49 69 6308 392

andreas.harner@vde.com