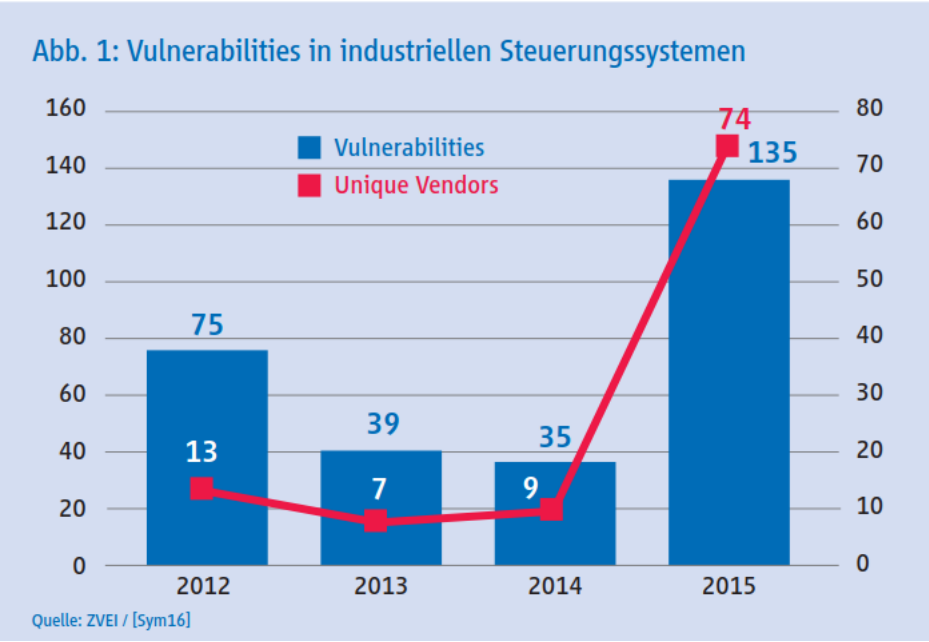
Cybersecurity
CERT@VDE

Andreas Harner

DKE
VDE DIN

Schwachstellenmanagement: Ein paar Zahlen…

Behauptung: „Die Anzahl von Schwachstellen steigt kontinuierlich an!“

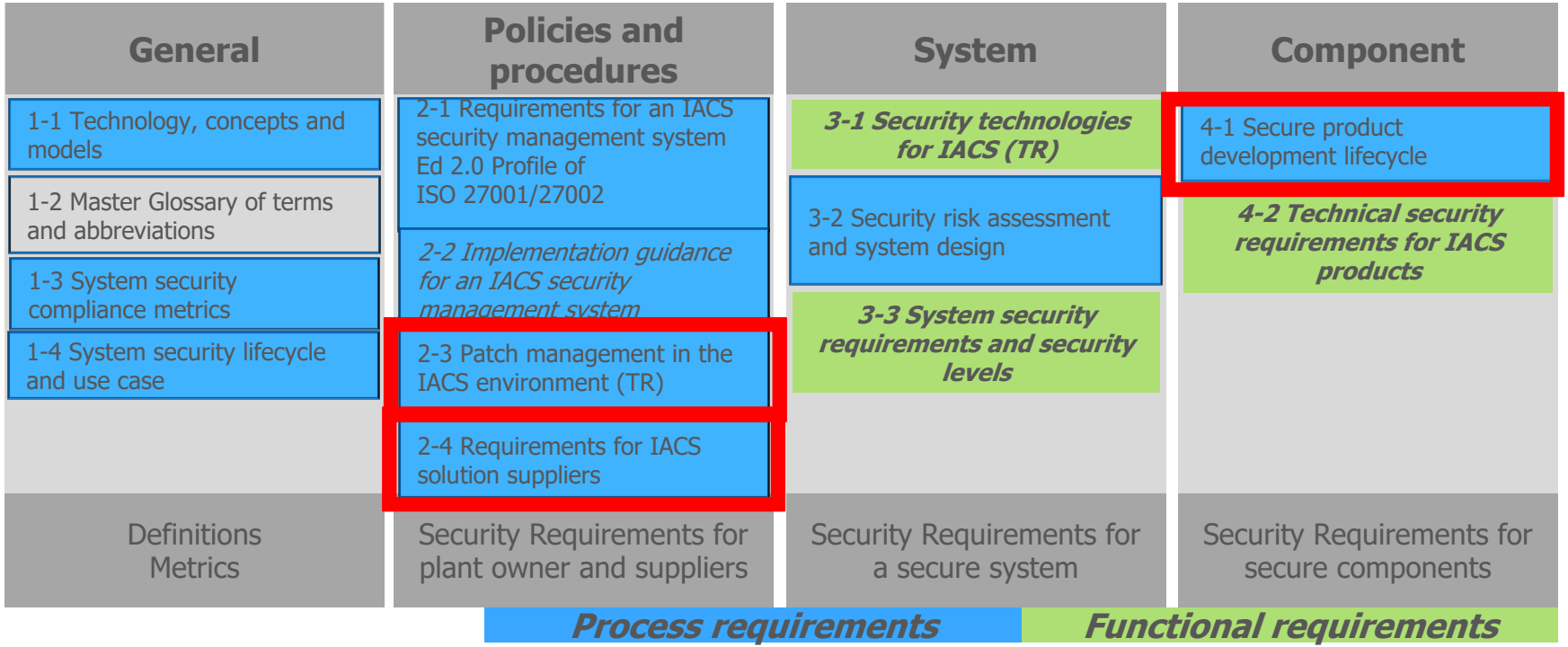


Quelle: ZVEI: Orientierungsleitfaden für Hersteller zur IEC 62443

- Stimmt diese Behauptung?
- Gibt es mehr oder weniger Schwachstellen?
- Gibt es mehr oder weniger Offenlegung?
  - Durch Externe?
  - Durch Interne?

→ Es werden mehr Schwachstellen gefunden!

IEC 62443: Normative Anforderungen

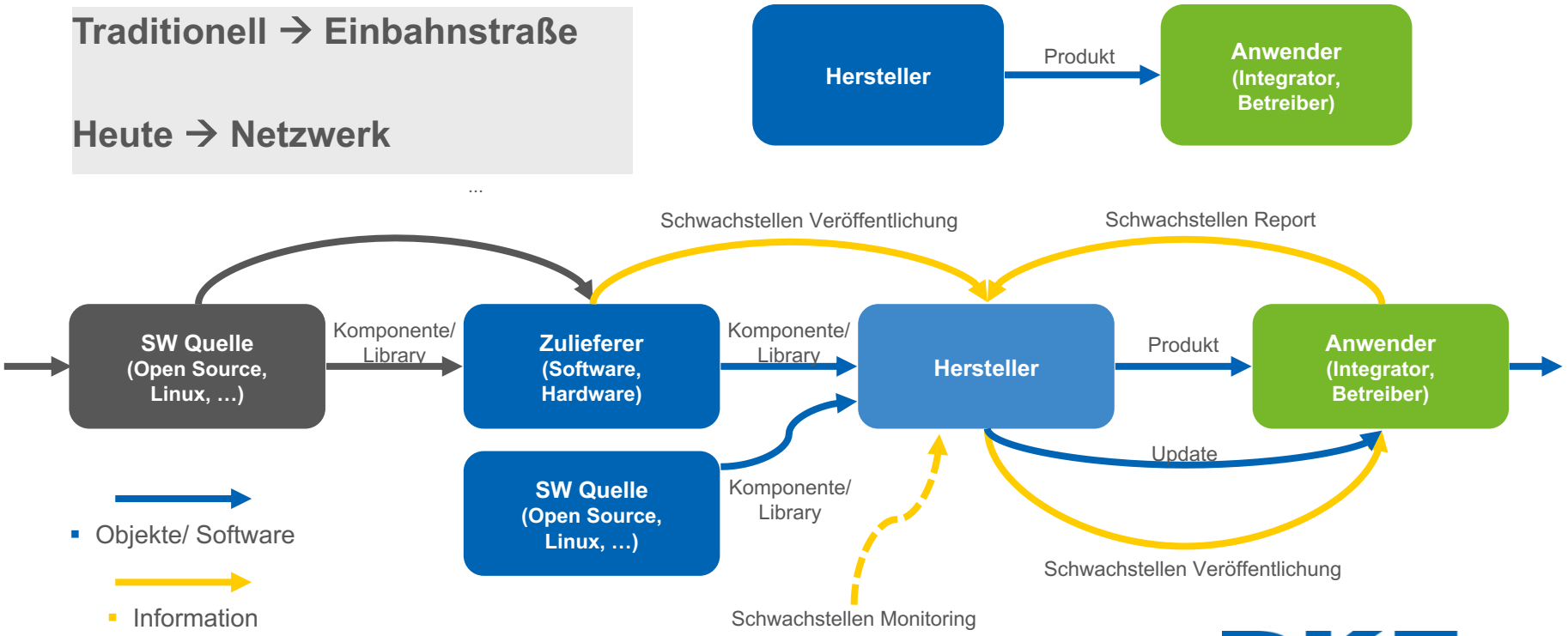


Motivation für CERT@VDE: Beziehung Hersteller - Kunde

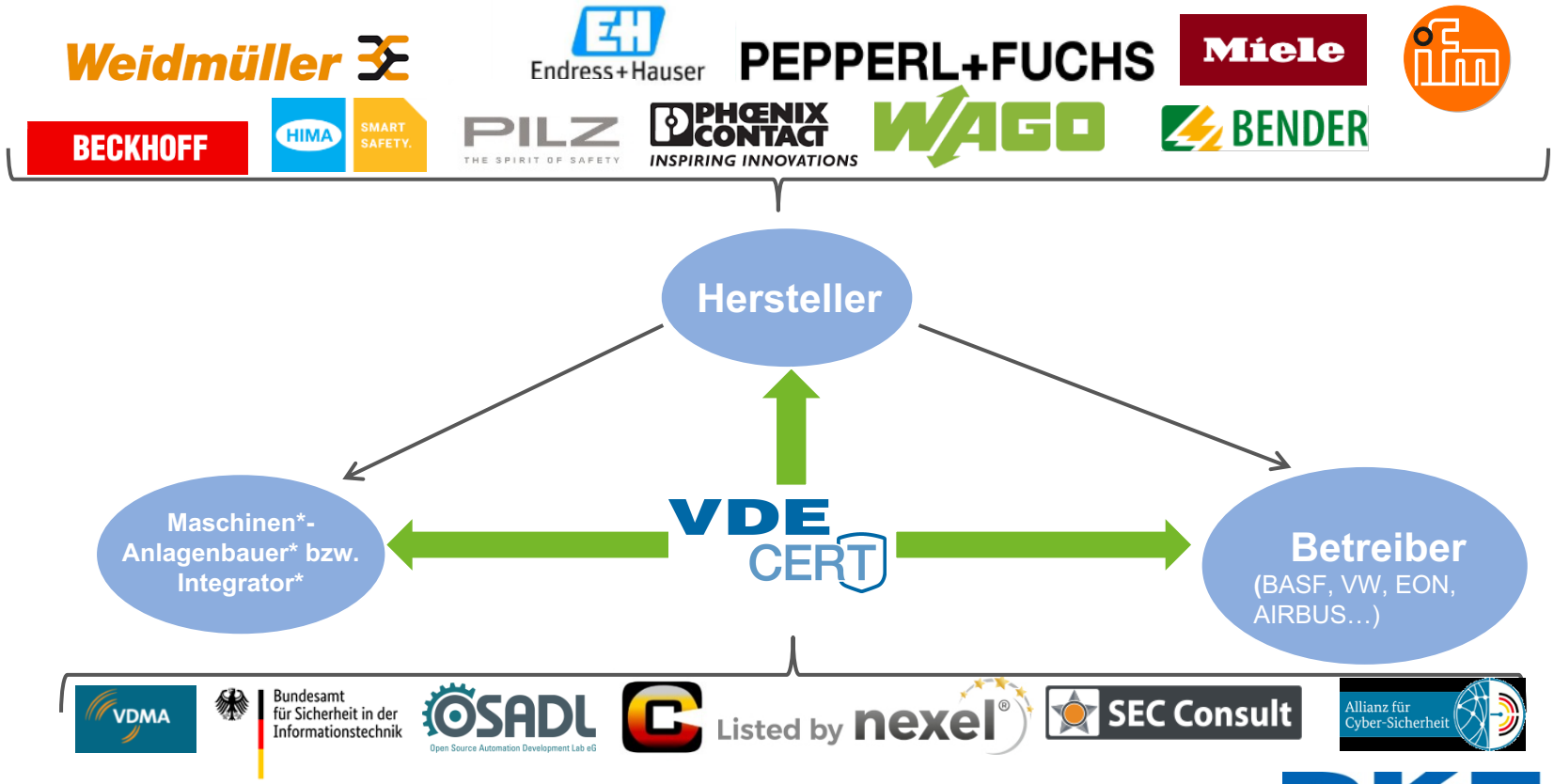
Traditionell → Einbahnstraße

Heute → Netzwerk

...



CERT@VDE als koordinierendes Produkt-CERT (PSIRT)



CERT@VDE und IoT Inspector
Schwachstellen in Firmware auf der Spur

DKE
VDE DIN

CERT@VDE im VDE

Wissenschaft Technologien Innovationen

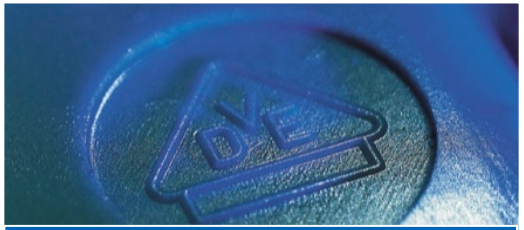
- Wissenstransfer im Expertennetzwerk
- Technologie- und Bildungspolitik
- Nachwuchsförderung

Normen Standards Grundlagen

- Internationale Normen und Standards

VDE CERT

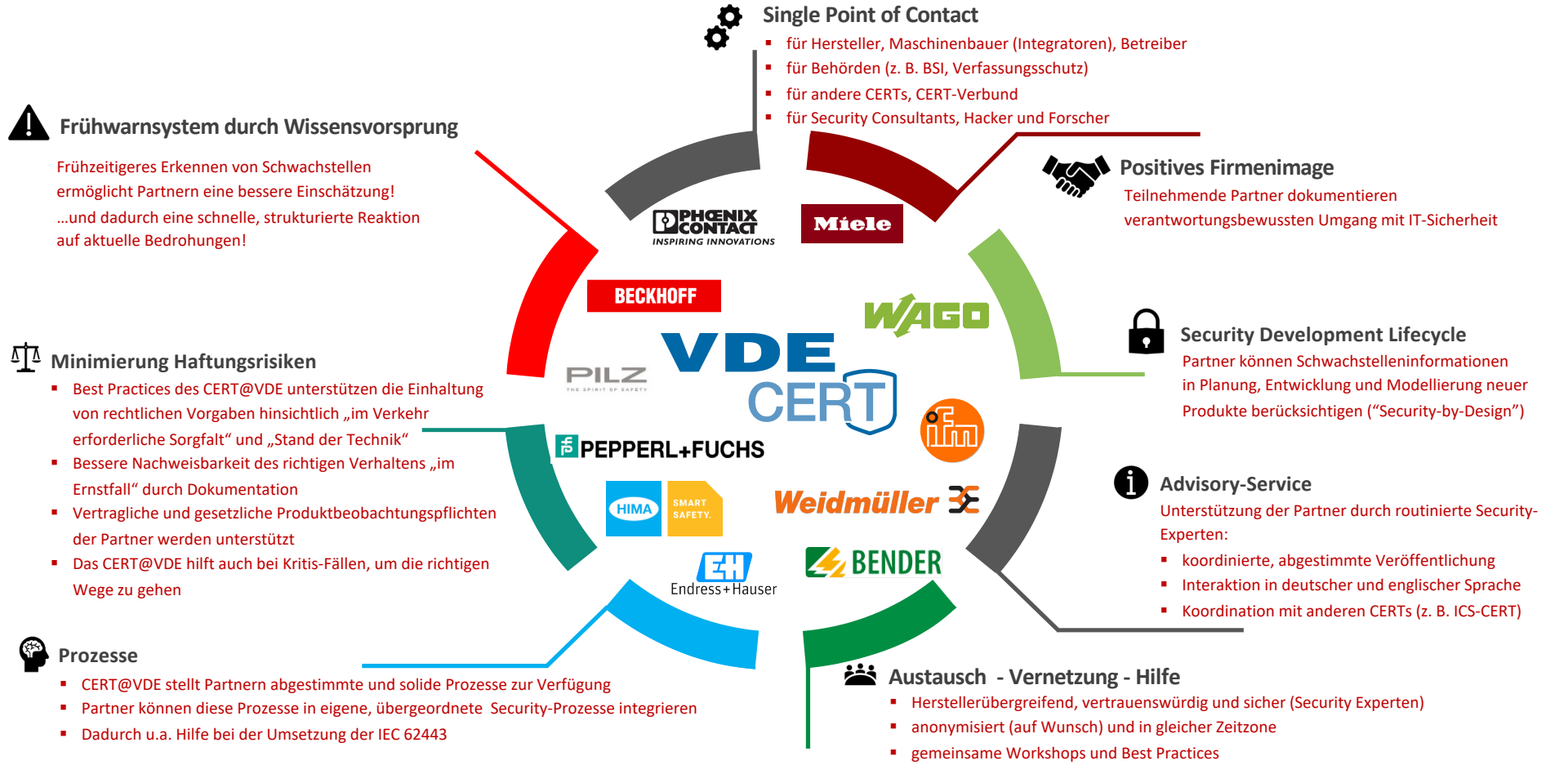
gemeinnützig



Prüfung Sicherheit Verbraucherschutz

- Produktprüfung und Zertifizierung

CERT@VDE – Mitmachen und Vorteile nutzen!



Single Point of Contact

- für Hersteller, Maschinenbauer (Integratoren), Betreiber
- für Behörden (z. B. BSI, Verfassungsschutz)
- für andere CERTs, CERT-Verbund
- für Security Consultants, Hacker und Forscher

Frühwarnsystem durch Wissensvorsprung

Frühzeitigeres Erkennen von Schwachstellen ermöglicht Partnern eine bessere Einschätzung!
…und dadurch eine schnelle, strukturierte Reaktion auf aktuelle Bedrohungen!

Positives Firmenimage

Teilnehmende Partner dokumentieren verantwortungsbewussten Umgang mit IT-Sicherheit

Minimierung Haftungsrisiken

- Best Practices des CERT@VDE unterstützen die Einhaltung von rechtlichen Vorgaben hinsichtlich „im Verkehr erforderliche Sorgfalt“ und „Stand der Technik“
- Bessere Nachweisbarkeit des richtigen Verhaltens „im Ernstfall“ durch Dokumentation
- Vertragliche und gesetzliche Produktbeobachtungspflichten der Partner werden unterstützt
- Das CERT@VDE hilft auch bei Kritis-Fällen, um die richtigen Wege zu gehen

Security Development Lifecycle

Partner können Schwachstelleninformationen in Planung, Entwicklung und Modellierung neuer Produkte berücksichtigen (“Security-by-Design”)

Advisory-Service

Unterstützung der Partner durch routinierte Security-Experten:

- koordinierte, abgestimmte Veröffentlichung
- Interaktion in deutscher und englischer Sprache
- Koordination mit anderen CERTs (z. B. ICS-CERT)

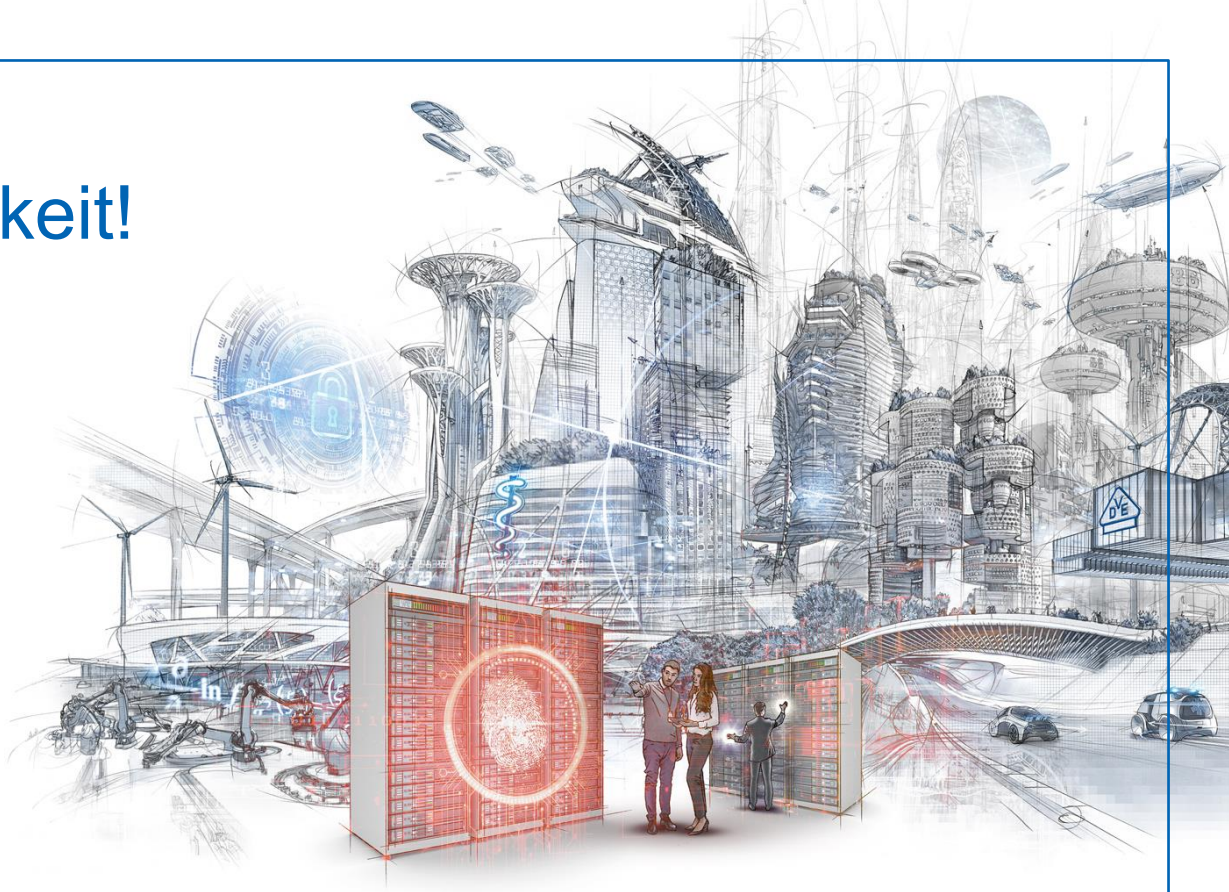
Prozesse

- CERT@VDE stellt Partnern abgestimmte und solide Prozesse zur Verfügung
- Partner können diese Prozesse in eigene, übergeordnete Security-Prozesse integrieren
- Dadurch u.a. Hilfe bei der Umsetzung der IEC 62443

Austausch - Vernetzung - Hilfe

- Herstellerübergreifend, vertrauenswürdig und sicher (Security Experten)
- anonymisiert (auf Wunsch) und in gleicher Zeitzone
- gemeinsame Workshops und Best Practices

Vielen Dank für Ihre Aufmerksamkeit!



Web: https://cert.vde.com

Mail: info@cert.vde.com

Twitter: @certvde

Ihre Ansprechpartner:

Andreas Harner
Abteilungsleiter CERT@VDE
Tel. +49 69 6308-392
andreas.harner@cert.vde.com