Willkommen

Komponentenentwicklung nach IEC 62443: Prozesse, Funktionen und Bewertung

PHOENIX CONTACT
INSPIRING INNOVATIONS

Kurzvorstellung Phoenix Contact

Dr. Lutz Jänicke – Corporate Product & Solution Security Officer

- 2002-2015 Innominate Security Technologies AG (jetzt: Phoenix Contact Cyber Security GmbH)
  - CTO; IT-Sicherheitsbeauftragter
- 2016- Corporate Product & Solution Security Officer
  - Phoenix Contact Gruppe/Digital Processes & Solutions
- Plattform Industrie 4.0
  - AG Sicherheit vernetzter Systeme; UAG Sichere Kommunikation für Industrie 4.0
- DKE
  - UK 931.1 IT-Sicherheit in der Automatisierungstechnik (→ IEC 62443)
  - TBKON Cybersecurity
  - TBINK AK „Safety & Security“
  - Beirat CERT@VDE
- ZVEI
  - Arbeitskreis Cybersicherheit; Lenkungskreis Industrial Security
- VDMA
  - Arbeitskreis Cybersecurity; Arbeitskreis „Sichere Fernwartung“

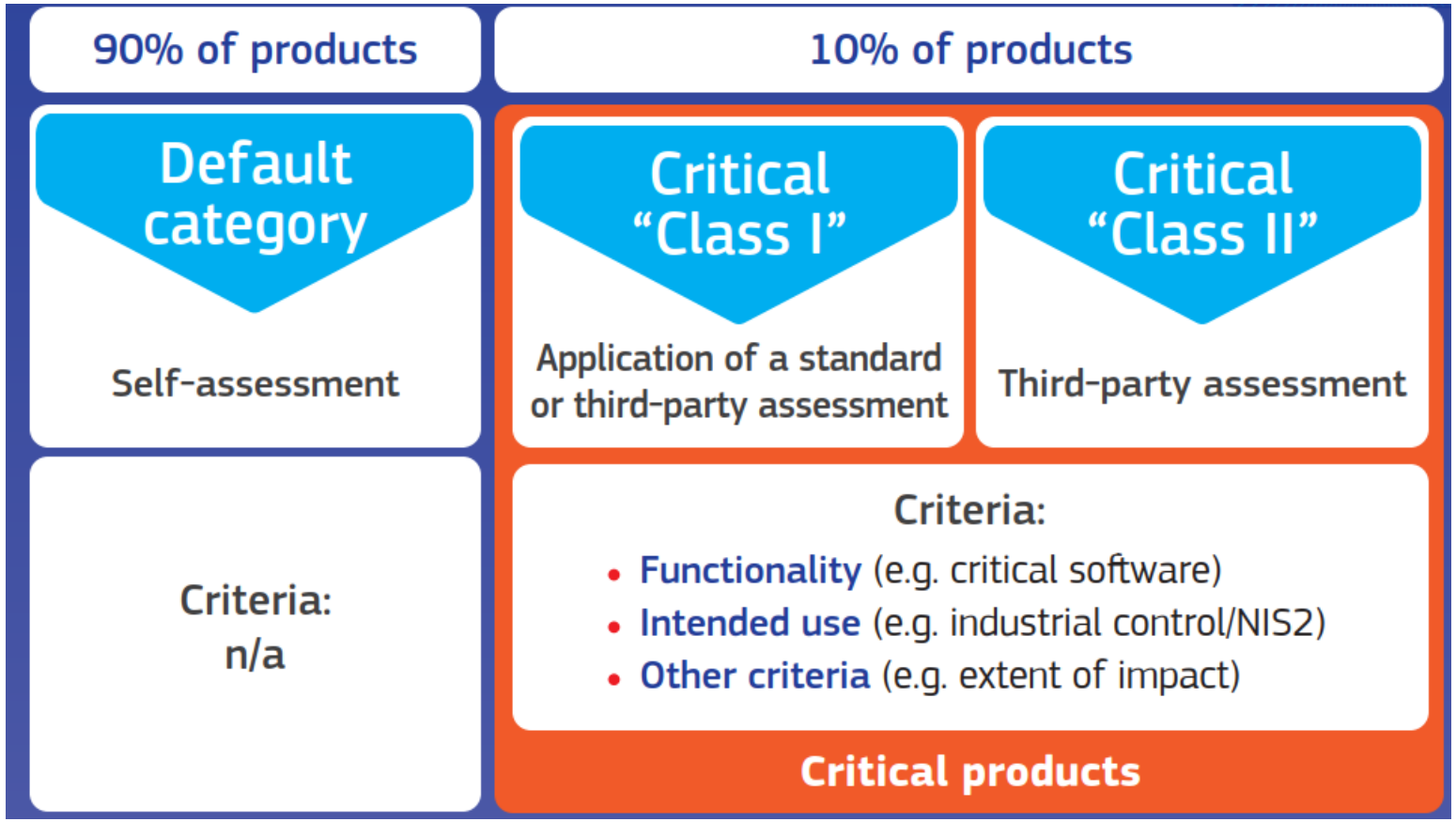
Aktuelles Thema

EU Cyber Resilience Act

September 2022: Proposal for EU Cyber Resilience Act published

Quelle: Cyber Resilience Act - Factsheet | Shaping Europe's digital future (europa.eu)

EU CRA: Mandatory Security for Products



Quelle: Cyber Resilience Act - Factsheet | Shaping Europe's digital future (europa.eu)

EU CRA: Essential Requirements (Annex I)

- designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks
- **delivered** without any known exploitable vulnerabilities
- Risk based
  - secure by default configuration
  - protection from unauthorized access
  - protect confidentiality of data
  - Protect integrity of data, programs, configuration
  - protect the availability of essential functions
  - designed, developed and produced to limit attack surfaces
  - designed, developed and produced to reduce the impact of an incident
  - provide security related information by recording and/or monitoring
  - ensure that vulnerabilities can be addressed through security updates

EU CRA: Vulnerability Management (Annex II)

- identify and document vulnerabilities and components contained in the product, including by drawing up a **software bill of materials**
- address and remediate vulnerabilities without delay, including by providing security updates
- apply effective and regular tests and reviews of the security
- (if) security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge
- … Prozesse für Advisories etc
- Article 10, Paragraph 6:
- When placing a product with digital elements on the market, and for the **expected product lifetime** or for a period of **five years** from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Was sind harmonisierte Normen?

Harmonisierte Normen stellen durch besondere Merkmale eine gesonderte Form von europäischen Normen (EN) dar. Der Begriff "harmonisierte Norm" wurde von der Europäischen Kommission im Rahmen der Neuen Konzeption (New Approach) festgelegt. Per Definition fallen unter die Kategorie einer harmonisierten Norm alle Normen, die

- von der Europäischen Kommission und der Europäischen Freihandelsassoziation (EFTA) an eine der anerkannten europäischen Normungsorganisationen (**CEN**, **CENELEC** oder **ETSI**) in Auftrag gegeben wurden;
- im Amtsblatt der Europäischen Union (Official Journal) veröffentlicht wurden.

Von der EU-Kommission in Auftrag gegebene Normen werden auch als „mandatierte Normen“ bezeichnet. Europäische Normen (EN) sind alle Normen, die von den europäischen Normungsorganisationen erarbeitet werden. Erst durch die Listung im Amtsblatt der Europäischen Union werden sie zu harmonisierten (Europäischen) Normen.

Diese harmonisierten Normen enthalten im Konsens erarbeitete Lösungen für die Einhaltung von rechtlichen Bestimmungen der einschlägigen Harmonisierungsgesetze der Europäischen Union. Die Anwendung von Normen ist freiwillig. Wenn harmonisierte Normen angewendet werden besteht die Vermutung der Konformität mit den entsprechenden rechtlichen Anforderungen. Darüber hinaus können Hersteller, Konformitätsbewertungsstellen oder andere Wirtschaftsakteure durch die Anwendung dieser Normen nachweisen, dass Produkte, Dienstleistungen oder Verfahren der EU-Rechtsvorschrift entsprechen, unter der die harmonisierte Norm gelistet ist.

Quelle: Harmonisierte Normen – Europäischer Rechtsrahmen (dke.de)

IEC 62443

IEC 62443: Zukünftige Struktur

General	Policies and procedures	System	Component	Profiles	Evaluation
1-1 Technology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS (TR)	4-1 Secure product development lifecycle		6-1 Security evaluation methodology for IEC 62443 – Part 2-4 (TS)
1-2 Master Glossary of terms and abbreviations	2-2 Security Protection Rating	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS products		6-2 Security evaluation methodology for IEC 62443 – Part 4-2 (TS)
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				
1-5 Rules for IEC 62443 Profiles (TS)	2-5 Implementation Guidance for IACS Asset Owners				
Definitions Metrics	Security Requirements for plant owner and suppliers	Security Requirements for a secure system	Security Requirements for secure components	Profiles for IACS solution suppliers (and more?)	Evaluation methodologies for conformity assessment

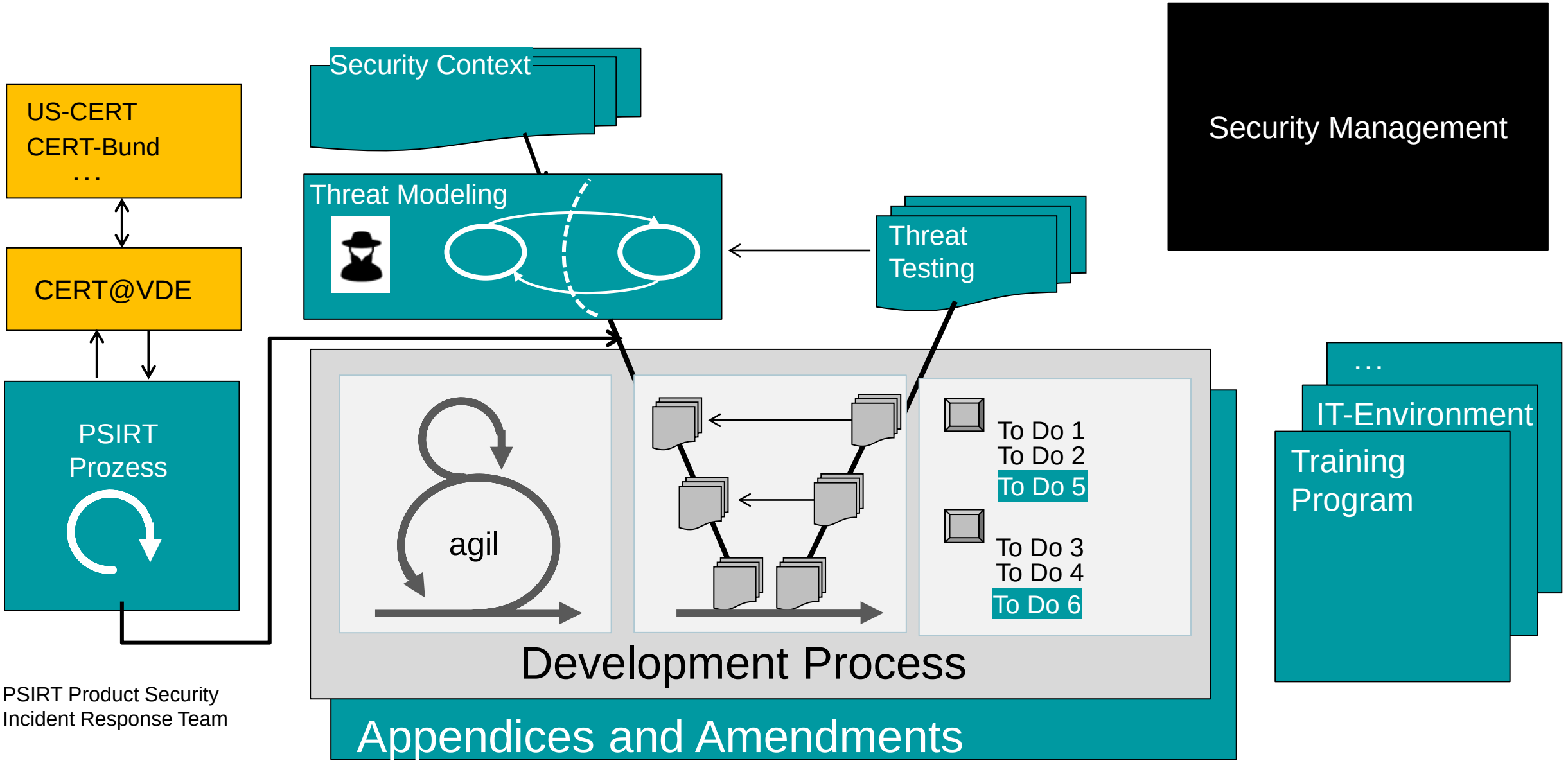
Process requirements ***Functional requirements***

Element 1

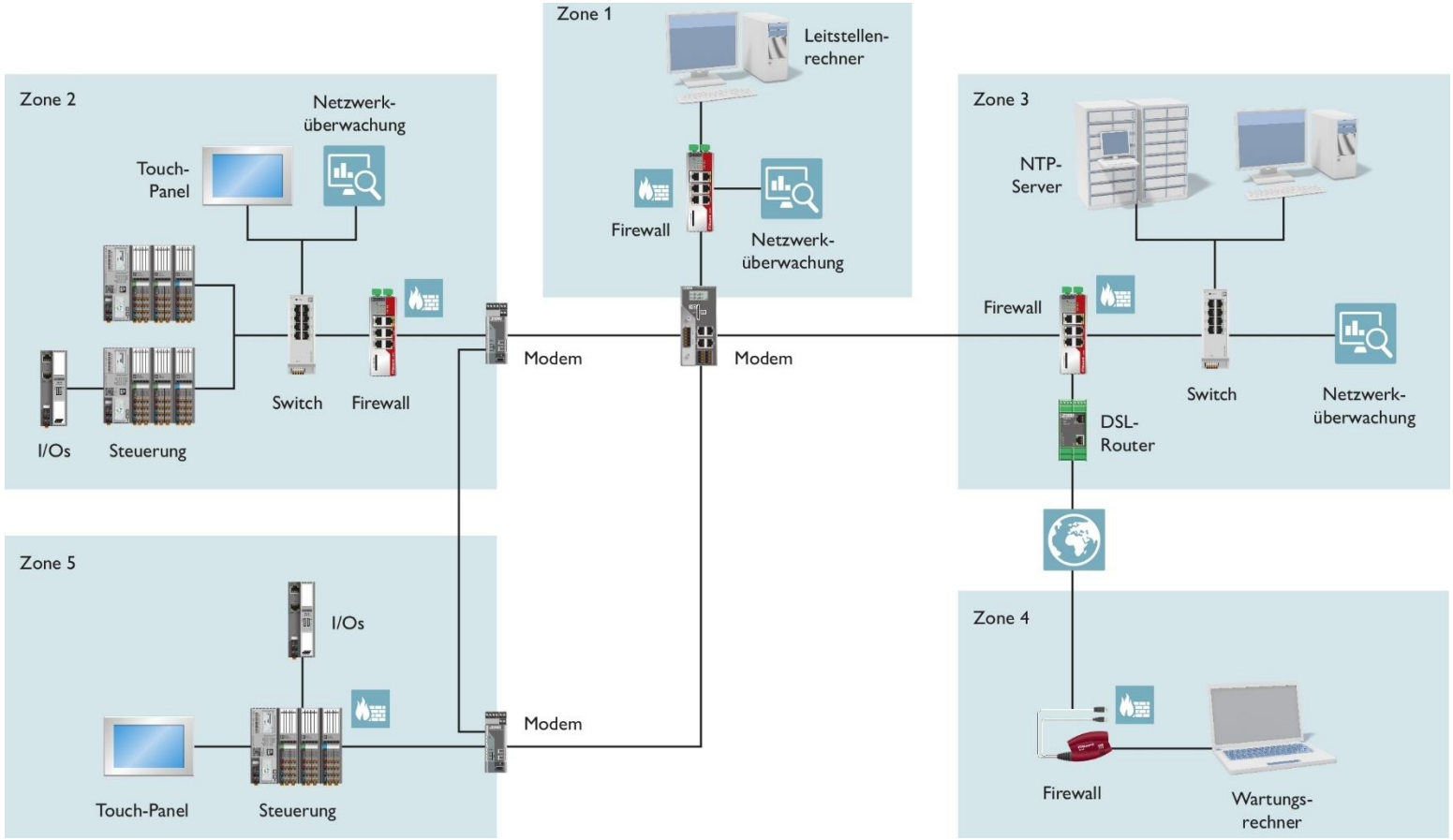
Sicherer Entwicklungsprozess nach IEC 62443-4-1

IEC 62443 4-1 8 Prozessansätze *47 Anforderungen*

1. SM: Verwaltung der IT-Sicherheit
2. SR: Spezifikation der IT-Sicherheitsanforderungen
3. SD: IT-Sicherheit durch den Entwurf
4. SI: Gesicherte Implementierung
5. SVV: Verifikations- und Validierungsprüfung
6. DM: Behandlung von Mängeln in der IT Sicherheit
7. SUM: Verwaltung von IT-Sicherheits-Updates
8. SG: IT-Sicherheitsrichtlinien (Dokumentation)

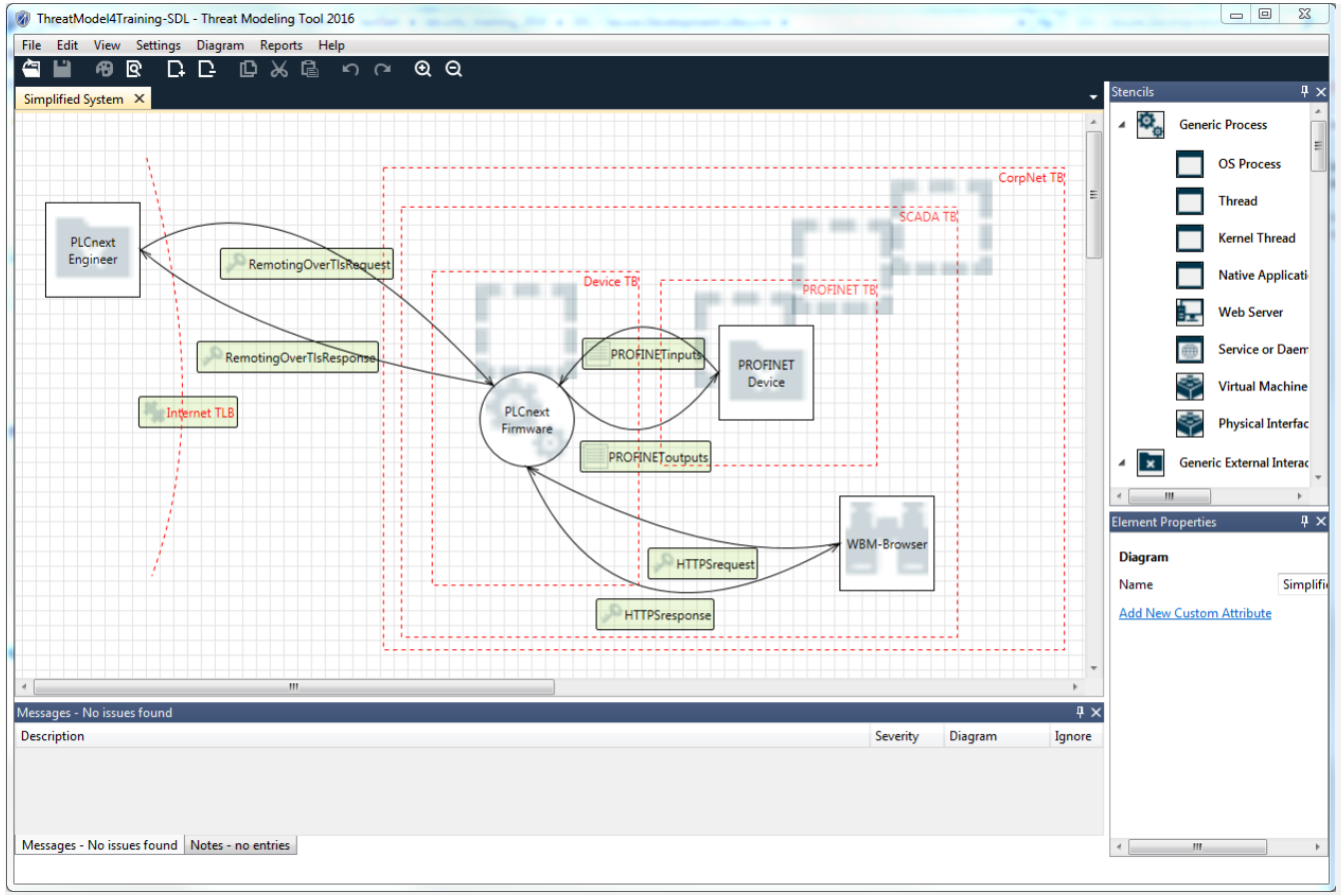


Annahme: Security Context -> Intended Use



- Der Security Context:
  - Beschreibt die Einsatzbedingungen
  - Beschreibt die Umgebung
  - Hält Annahmen die die Umgebung erfüllen muss fest
  - Kann die Anzahl relevanter Threats reduzieren
  - Hilft Threats zu bewerten und zu priorisieren

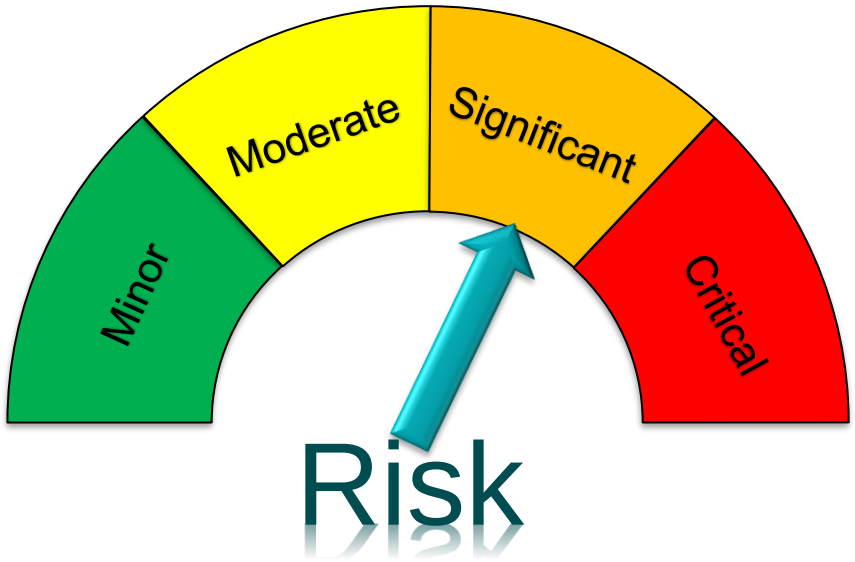
Übersicht - Microsoft Threat Modeling Tool (TMT)



- Kostenloses Tool zur Erstellung von Threat Models
- Basiert auf
  - Datenflussdiagrammen
  - Der STRIDE Analyse
- Generiert automatisch Threats auf Basis
  - Des Datenflussdigramms
  - Regeln in einem editierbaren Template

STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

Threats bewerten - Erklärung



- Die Bewertung eines Threats erfolgt mithilfe der 5 Kriterien:
  - Severity
  - Attack Vector
  - Privileges Required
  - Required Skills
  - Required Resources
- Aus den 5 Einzelwerten wird mithilfe der Zwischenwerte:
  - Exposure
  - Exploitability
  - Likelihood
- Das Gesamtrisiko (Risk) berechnet

Element 2

Unterstützung der Systemsicherheit durch Funktionen nach IEC 62443-4-2

IEC 62443 Foundational Requirements

1. Identifizierung und Authentifikation (IAC)
2. Nutzungskontrolle (UC)
3. Systemintegrität (SI)
4. Vertraulichkeit der Daten (DC)
5. Eingeschränkter Datenfluss (RDF)
6. Rechtzeitige Reaktion auf Ereignisse (TRE)
7. Verfügbarkeit der Ressourcen (RA)

IEC 62443-3-3/-4-2: Security (aber nicht Interoperabilität)

5.5 CR 1.3 – Nutzerkontenverwaltung

5.5.1 Anforderung

Die Komponente muss die Fähigkeit haben, die Verwaltung aller Nutzerkonten zu unterstützen und/oder alle Nutzerkonten unmittelbar nach SR 1.3 in IEC 62443-3-3 [11] zu verwalten.

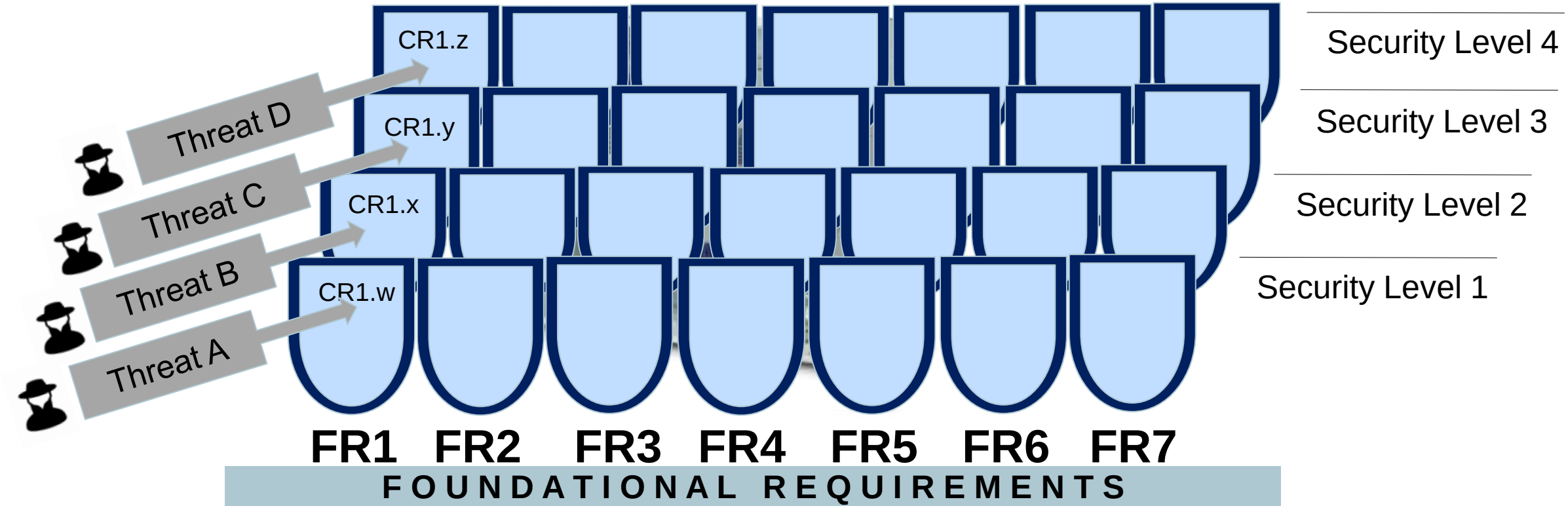
5.5.2 Begründung und zusätzliche Hinweise

Eine Komponente darf diese Fähigkeit zur Verfügung stellen, indem sie in ein Nutzerkontenverwaltungssystem einer höheren Ebene integriert wird.

Ein allgemeiner Ansatz für die Erfüllung dieser Anforderung wäre eine Komponente, die die Bewertung der Authentifikation an einen Verzeichnisserver überträgt (z. B. mit einem Protokoll wie RADIUS oder Kerberos), der die nach SR 1.3 in IEC 62443-3-3 [11] geforderten Fähigkeiten der Nutzerkontenverwaltung zur Verfügung stellen.

Quelle: IEC 62443-4-2

IEC 62443-4-2/3-3 Foundational Requirements



CR: Component Requirement

w, x, y, z => SL: Tabelle der funktionalen Maßnahmen

IEC 62443-3-3/-4-2: Security-Anforderung aber umsetzungsoffen

8.3 CR 4.1 – Vertraulichkeit von Informationen

8.3.1 Anforderung

Die Komponente muss

a) die Fähigkeit haben, die Vertraulichkeit von ruhenden Informationen zu schützen, für die ausdrücklich eine Leseberechtigung vorgesehen ist; und

b) den Schutz der Vertraulichkeit von Informationen bei der Übertragung nach SR 4.1 in IEC 62443-3-3 [11] unterstützen.

8.3.2 Begründung und zusätzliche Hinweise

Die Entscheidung, ob eine bestimmte Information geschützt werden sollte oder nicht, hängt vom Zusammenhang ab und kann nicht schon während der Produktentwicklung getroffen werden. Jedoch kann der Umstand, dass eine Organisation den Zugriff auf eine Information durch das Einrichten ausdrücklicher Leseberechtigungen im Automatisierungssystem beschränkt, als ein Indikator dafür angesehen werden, dass diese Information von der Organisation als vertraulich eingestuft wird. Somit sollten alle Informationen, für die die Komponente die Fähigkeit der Einrichtung ausdrücklicher Leseberechtigungen vorsieht, als potentiell vertraulich eingestuft werden und die Komponente sollte daher die Fähigkeit haben, diese zu schützen.

Die Vertraulichkeit von Informationen bei der Übertragung erfordert Fähigkeiten auf der Systemebene, die die Komponente unterstützen muss.

Für den Schutz der Vertraulichkeit gibt 8.5 CR 4.3 – Use of cryptography weitere Informationen.

Quelle: IEC 62443-4-2

IEC 62443-4-2: Security Level -> Fähigkeiten des Angreifers

Funktionale Anforderungen				
Fähigkeiten des Angreifers				
Security Level	**Mittel**	**Ressourcen**	**Fähigkeiten**	**Motivation**
SL-0	keine Gefahr der Beeinträchtigung/Manipulation			
SL-1	zufällige/beiläufige Beeinträchtigung/Manipulation			
SL-2	einfach	begrenzt	allgemein	niedrig
SL-3	ausgefeilt	mittel	Automatisierungs Know-how	mittel
SL-4	ausgefeilt	umfangreich	Automatisierungs Know-how	hoch

IEC 62443-4-2: Security Level -> Fäh

Funktionale Anforderungen				
Fähigkeiten des Angreifers				
Security Level	**Mittel**	**Ressourcen**	**Fä**	
SL-0	keine Gefahr der Beeinträchtigung/Manipulation			
SL-1	zufällige/beiläufige Beeinträchtigung/Manipulation			
SL-2	einfach	begrenzt	allgemein	niedrig
SL-3	ausgefeilt	mittel	Automatisierungs Know-how	mittel
SL-4	ausgefeilt	umfangreich	Automatisierungs Know-how	hoch

Schutz vor den Fähigkeiten von...

SL-1
...jedem Internetnutzer

SL-2
... interessierten Einzelpersonen und Unternehmen mit allgemeinem Sicherheitswissen

SL-3
... Experten und Unternehmen, die effektive, aber kostenorientierte Angriffsszenarien mit klaren Zielen entwickeln und einsetzen (auch kriminelle Energie)

SL-4
... staatlichen Organisationen, die sich darauf konzentrieren, das spezifisch ausgewählte Ziel um fast jeden Preis zu erreichen

Element 3

Bewertung der Security-Umsetzung nach IEC 62443-6-2

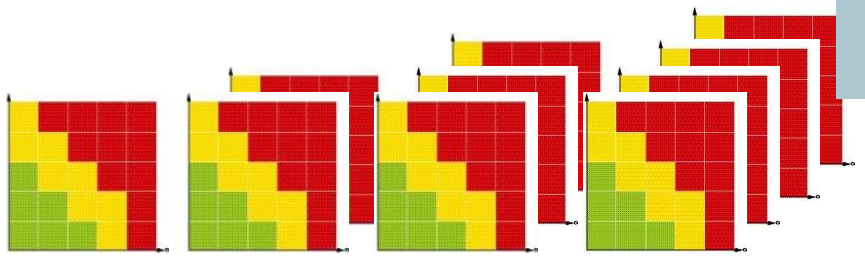
Kombination 4-1 und 4-2 in der Entwicklung von Komponenten

SR und RE	SL 1	SL 2	SL 3	SL 4
FR 4 – Data confidentiality (DC)				
CR 4.1 – Information confidentiality	✓	✓	✓	✓
CR 4.2 – Information persistence				
RE (1) Erase of shared memory resources			✓	✓
RE (2) Erase verification			✓	✓
CR 4.3 – Use of cryptography	✓	✓	✓	✓

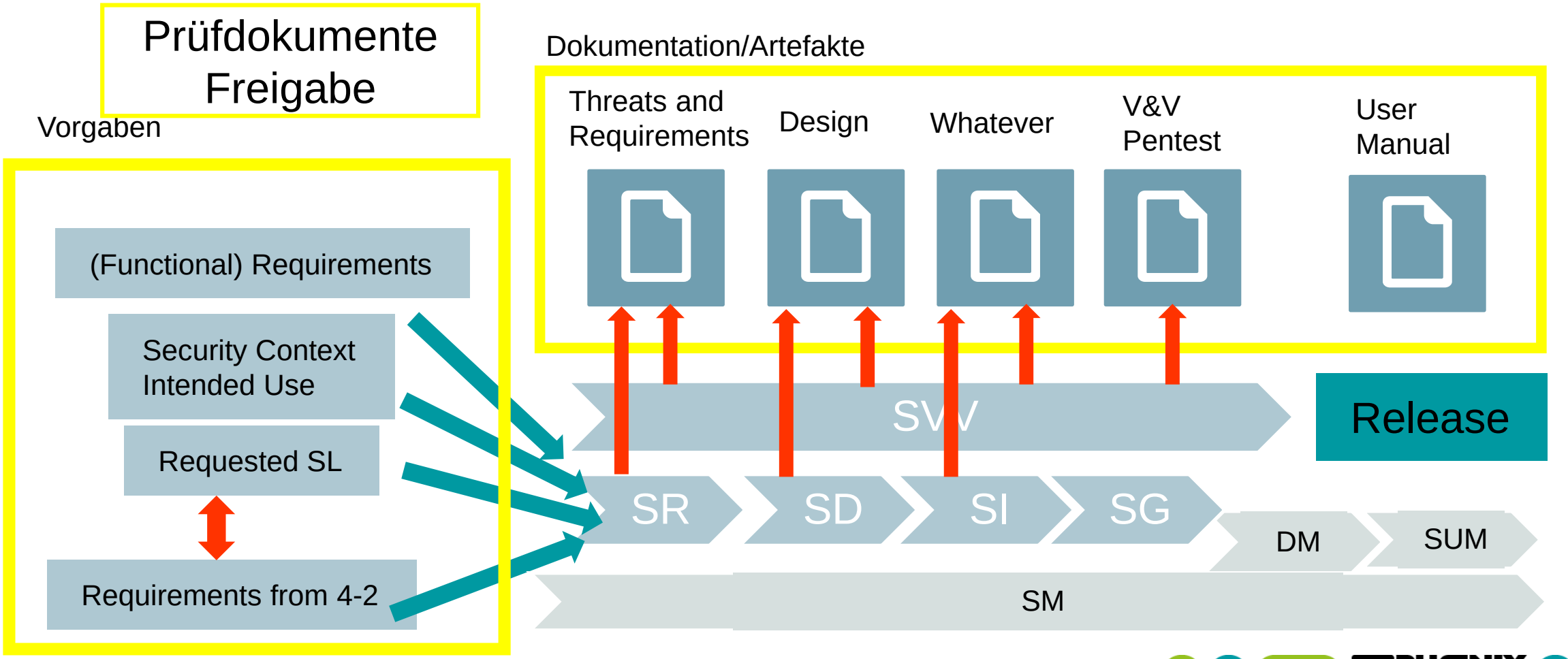
4x gleiche (Meta)-Anforderung

4 unterschiedliche Maßnahmensätze

4x Bedrohungsanalyse (SR) gegen unterschiedliche Angreifer



Kombination 4-1 und 4-2 in der Entwicklung von Komponenten



Danke

Komponentenentwicklung nach IEC 62443: Prozesse, Funktionen und Bewertung

PHOENIX CONTACT
INSPIRING INNOVATIONS