



Smart Elevators 4.0: Security und Safety

SECURITY-4-SAFETY (S4S)

erlift 2017

gsburg, 20. Oktober 2017

ELEVATOR 4.0

NEUE SCHNITTSTELLEN



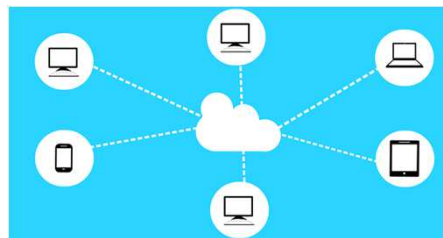
Diagnose



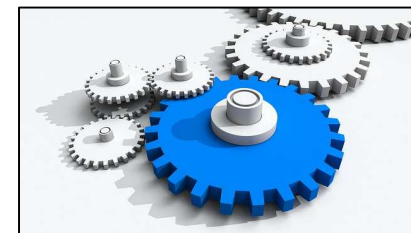
Inhouse Vernetzung



Cloud Anbindung



Fernwartung



ELEVATOR 4.0

NEUE PRÜFMITTEL UND SENSOREN

Bei der Aufzugprüfung können inzwischen viele Werte digital ausgelesen werden.

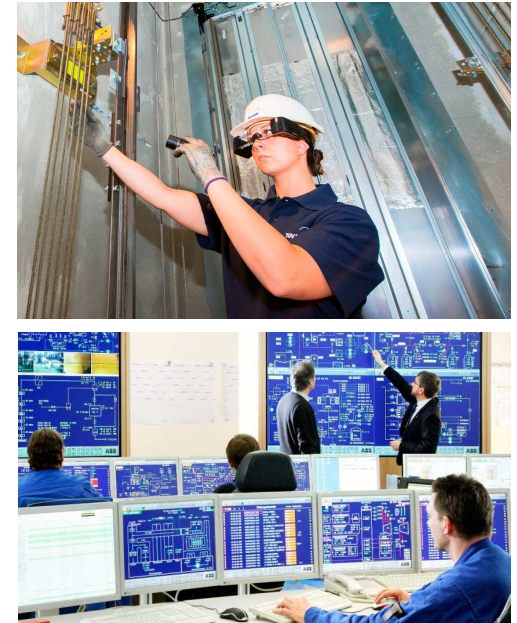
Gestern



Heute

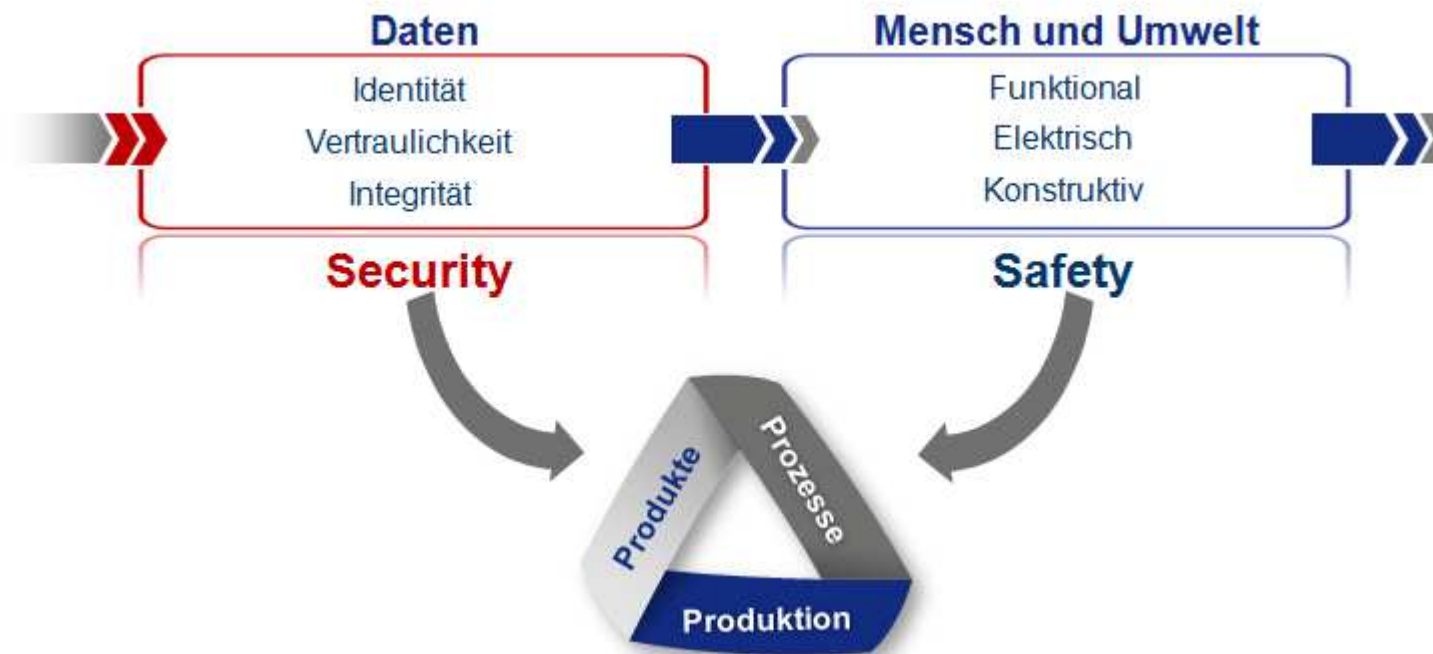


Morgen



SECURITY4SAFETY

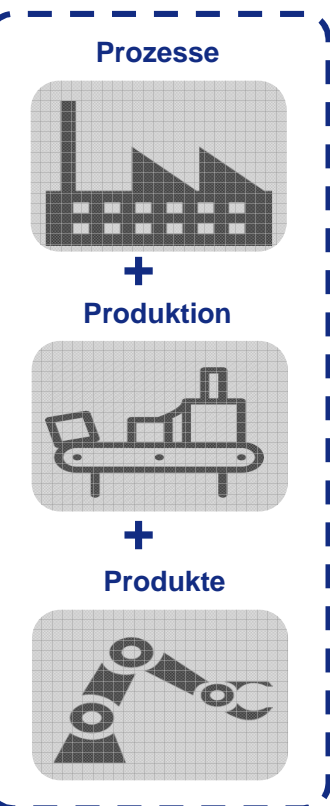
ie analoge und die digitale Welt verschmelzen, sodass neben der funktionalen Sicherheit (Safety) stets auch die IT-Sicherheit (Security) zu prüfen ist.



Aufgrund der Verschmelzung von funktionaler und IT-Sicherheit können die bisher getrennt voneinander betrachteten Arbeitsfelder nicht mehr singulär bearbeitet werden.

SECURITY4SAFETY

ine reine Produkt- oder Systemprüfung ist nicht mehr sicher. Die IT-Netze, Zonen und Organisations-Strukturen, in denen die Produkte der Systeme eingebunden sind, müssen notwendigerweise mitgeprüft werden.



GANZHEITLICHE BETRACHTUNG ZUM NACHWEIS DES STANDS DER TECHNIK:

Informationssicherheits-Managementsystem

- > Betrachtung und Bewertung von Organisation und Prozessen
- > ISO 27001 als Grundvoraussetzung für I4.0 („die ISO 9001 der digitalen Transformation“)
- > ISO 2700x als Nachweis zum Stand der Technik
- > Information Security Readiness (ISO 2700x in drei Stufen)

System- und Komponentenbetrachtung

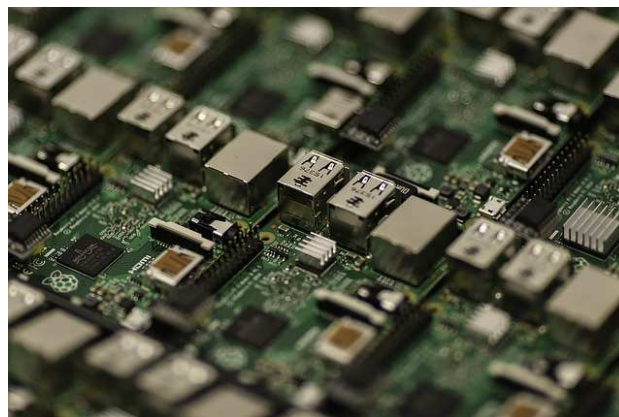
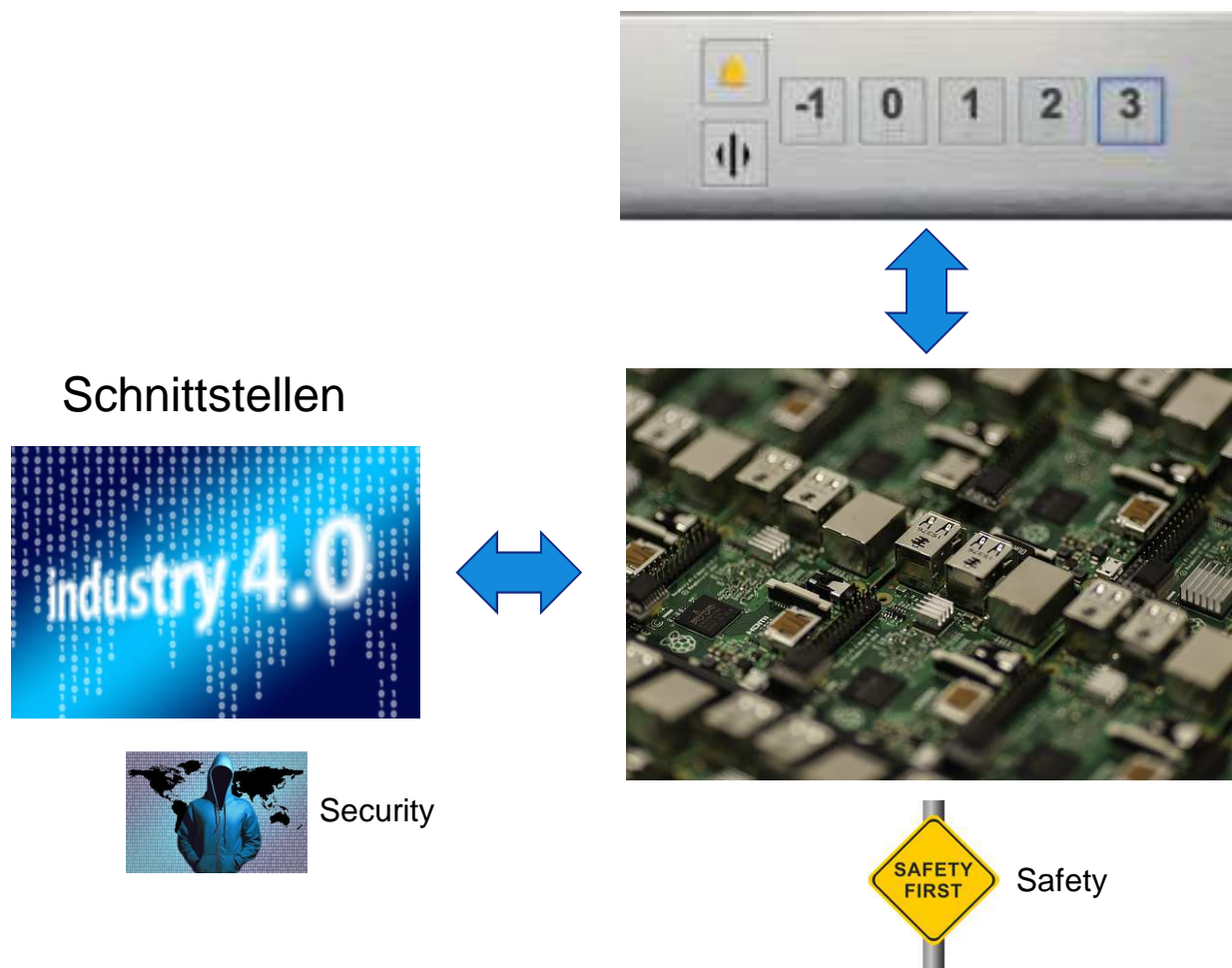
- > Ganzheitliche Security- und Safety Risikobetrachtung (S4S-Risk-Analyse)
- > Umsetzung von Best Practices
- > Umsetzung von normativen Anforderungen gem. Industrial Security (IEC 62443)
- > Konzeptprüfung
- > Penetration Tests (Überprüfung der Wirksamkeit der Techniken und Maßnahmen)

Keine Prüfung ohne IT-Security

- > Rechtssicheres und dem Stand der Technik entsprechendes Inverkehrbringen und Betreiben von smarten Systemen/Produkten ist ohne Bewertung der IT-Security nicht möglich

Security Prozess-, System-, und Komponentenbewertungen als integraler Bestandteil von Industrie 4.0

SECURITY4SAFETY FÜR PRODUKTE (Z.B. AUFZUGSSTEUERUNGEN)



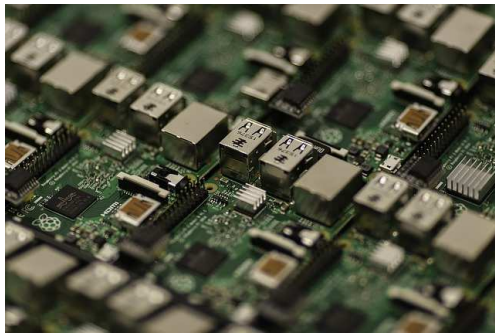
Safety



SECURITY4SAFETY

UNTERSCHIEDLICHE BETRACHTUNGEN

Hardware



Software



Schnittstellen



Safety



- Hardware Ausfall
- Systematische HW + SW Fehler
- Übertragungsfehler (Schnittstellen)
- Soft Errors

Security



- Datendiebstahl
- Viren
- SW Manipulation
- Hacking



**Safety und Security Bedrohungen
müssen gemeinsam betrachtet werden !**



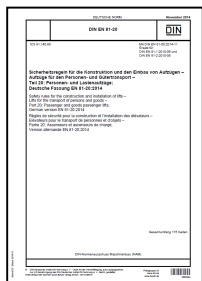
Datenschutz-Recht

Wie kann ich die Software Applikation sicher entwickeln ?

SECURITY4SAFETY NORMEN

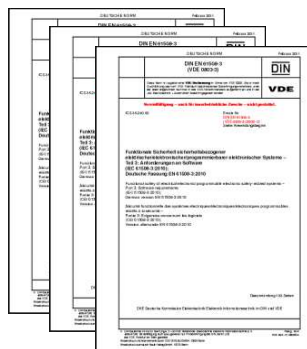


DIN EN 81



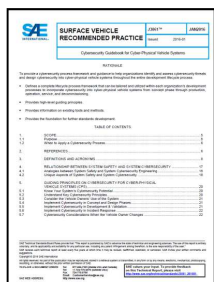
Elevator

IEC 61508-1/2/3



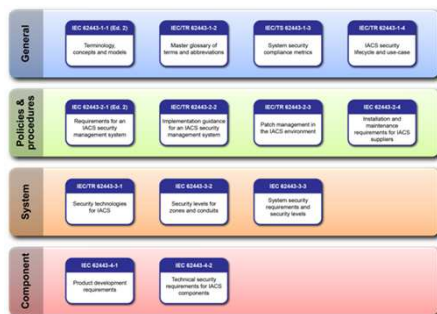
generisch

J3061 (ISO 26262)



Cybersecurity Guidebook for
Cyber-Physical Vehicle Systems

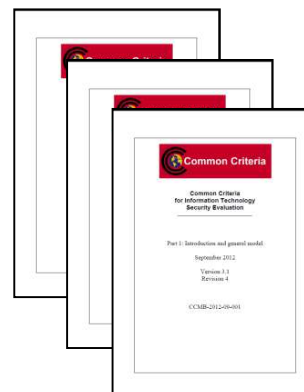
IEC 62443-X



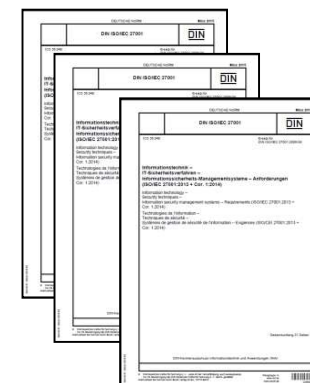
Industrial Security (weitgehend im Draft Status)



Common Criteria 1-3



DIN ISO IEC 2700X

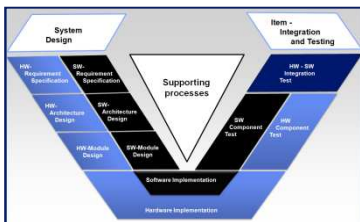


Klassische Security Normen



Wie ist die Vorgehensweise zur Erstellung
sicherer Software ?

Entwicklungs- Prozess



- V-Model (Safety + Security)
- Lebenszyklus
- Risiko-Analyse

Techniken und Maßnahmen



| Verfahren/Strategie ¹⁾ | | Stufe | SL 1 | SL 2 | SL 3 | SL 4 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|------|------|------|------|
| 1 | Funkeinsatz und Black Box Test | 0,5.1, 0,5.2 Tabelle 9.3 | xx | xx | xx | xx |
| 2 | Leistungstest | Tabelle 9.6 | x | x | xx | xx |
| 3 | Einwirkungsgefühl von den Anforderungen an den System- und Softwarezustand der Hardware-Software Integration zu den Spezifikationen der Hardware-Software Integrationen | 0.2.11 | x | x | xx | xx |

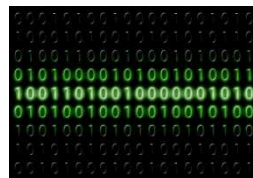
ANMERKUNG 1: Die Integration der programmierten Elektronik ist eine Verifikationsstrategie (siehe Tabelle A.5).

ANMERKUNG 2: Siehe Tabelle C.6.

ANMERKUNG 3: Die Verweissung des internen, nicht externen „Bewertung“ in Stufe 3 (siehe weisse Zelle) beschreibt die Verifikation/Motivation in den Anlagen 9.6 bis 9.7 (siehe Tabelle 9.6).

- Verhindert systematische Fehler
- Authentifizierung
- Signierung

Daten Sicherung



- Fehlerwahrscheinlichkeit
- Datensicherheit
- Kryptographie

Verifikation und Validierung



- Gegenseitige Kontrolle
- **Penetrationstest**
- SW Modul Test
- Integrationstest

Dokumentation

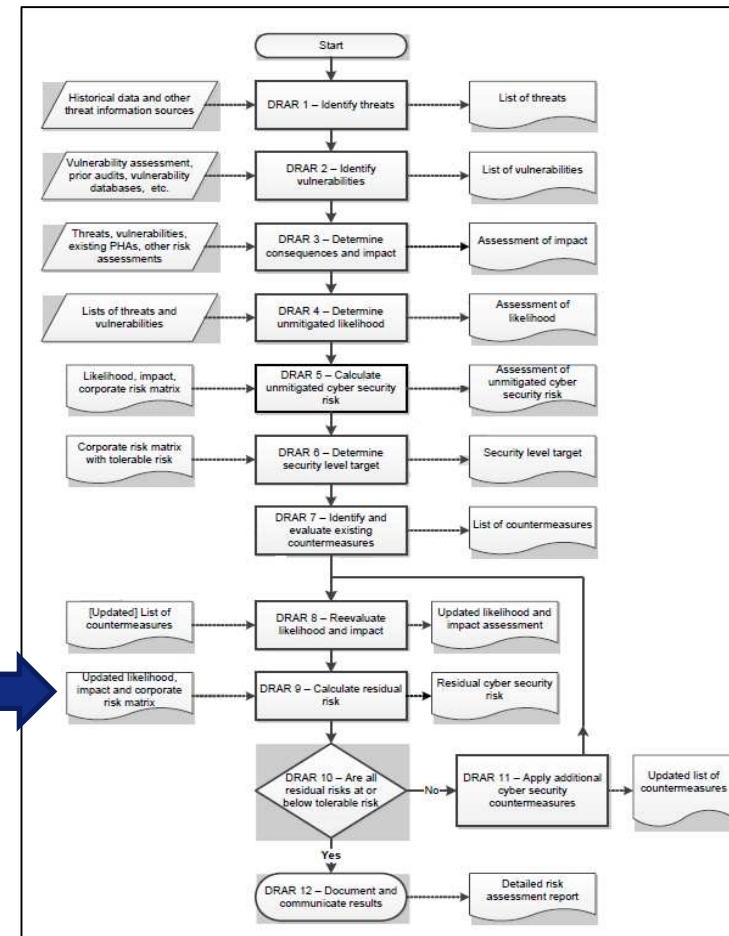
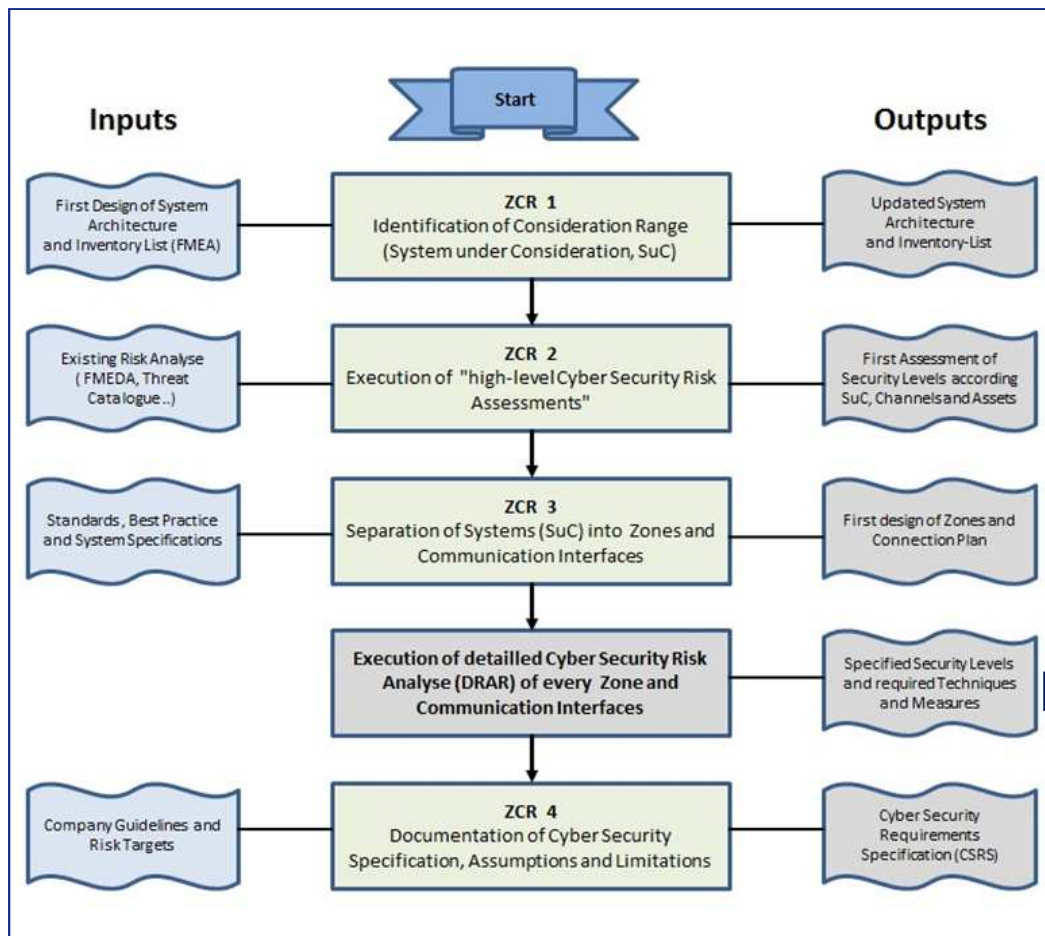
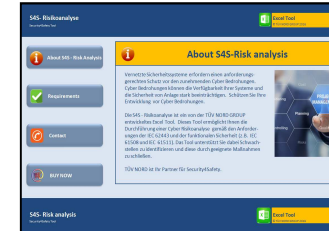


- Nachvollziehbarkeit

SECURITY4SAFETY S4S RISK ANALYSE TOOL

Risiko-Beurteilung nach IEC 62443-3-2 + J3061

Detaillierte Risiko-Analyse zur Bestimmung der Anforderungen

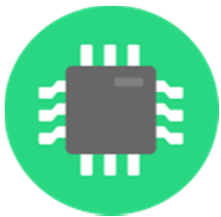


SECURITY4SAFETY

VORGEHEN BEI DER RISIKO ANALYSE / BETRACHTUNGSGEGENSTÄNDE



System
Beschreibung



Inventar



Assets



Bedrohungs-
quelle



Zonen-
betrachtung



Kosten (ROI)



Maßnahmen



Schwachstellen

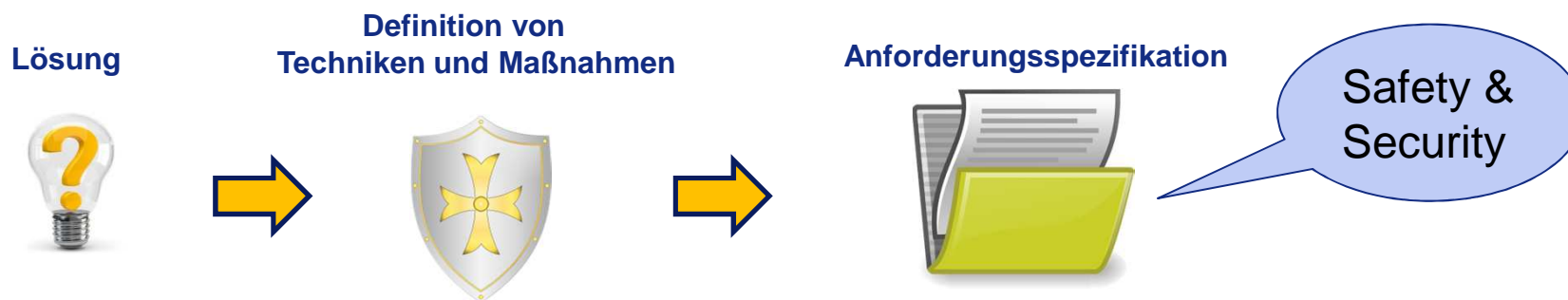
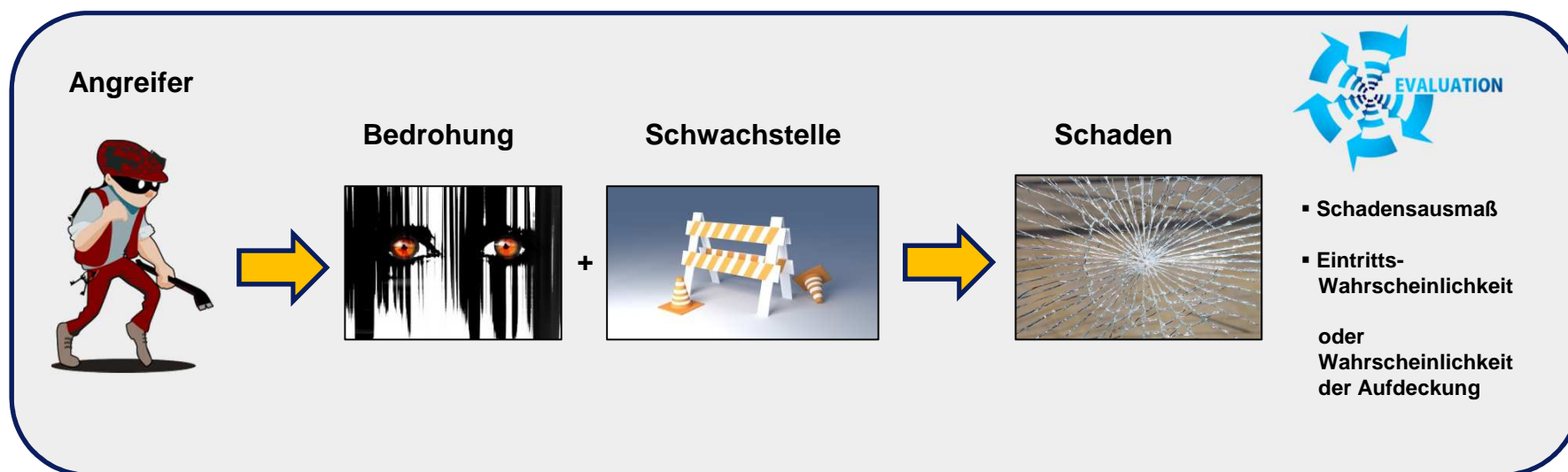


Bedrohungen

SECURITY4SAFETY

ERSTER SCHRITT IST DIE ERFASSUNG DER RISIKEN

Erster Schritt: Erkennung des Risikos und Ableitung von geeigneten Techniken und Maßnahmen zur Verhinderung von Schäden



SECURITY4SAFETY

RISIKO BEURTEILUNG / RISIKO-BESTIMMUNG



| Consequence | | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Consequence Description (Hazardous Event) | Impact | | Security measures effecting the specific Treat | Documents | Open |
| | Safety | Financial | | | |
| Infolge des fehlerhaften Grenzwertes wird die Schutzaktion nicht oder zu spät ausgelöst und Schäden an der Anlage sowie dem Personal | 5 | 3 | 8 | Passwort erforderlich Statische Codeanalyse Sicherstellung der Verfügbarkeit [D10] iLSB Nachrichten [D11] LSB Bus [D12] LSB Parametrierung | open |

Auswirkung

Consequence Severity

Damage of persons and environment (Safety)

- S0 No injury. No environment damage.
- S1 Minor injury of one person. Small environment damages.
- S2 Serious permanent injury of one or more persons. Temporary huge environment damages
- S3 Death of more persons. Long term huge environment damages
- S4 Catastrophic Damage. A lot of dead persons

Damage and image damage (Cyber-Security)

- S0 Small damage (< 5 TEuro)
- S1 Moderate damage (5 TEuro .. 10 TEuro)
- S2 Medium damage (10 TEuro .. 50 TEuro)
- S3 High damage (50 TEuro .. 100 TEuro)
- S4 Catastrophic damage (> 100 TEuro)

Ok Cancel

Techniken und Maßnahmen



Set IEC 62443-3-3 Measures

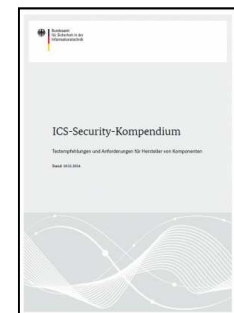
Target SL : SL 3

Foundation Requirement (FR) : FR 1 - Identification and authentication control (IAC)

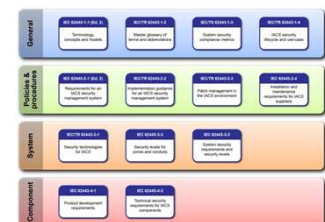
System Requirement (SR):

- SR 1.1 - Human user identification and authentication
- SR 1.1 RE 1 - Unique identification and authentication
- SR 1.1 RE 2 - Multifactor authentication for untrusted networks
- SR 1.2 - Software process and device identification and authentication
- SR 1.2 RE 1 - Unique identification and authentication
- SR 1.3 - Account management
- SR 1.3 RE 1 - Unified account management
- SR 1.4 - Identifier management
- SR 1.5 - Authenticator management
- SR 1.5 RE 1 - Hardware security for software process identity credentials
- SR 1.6 - Wireless access management
- SR 1.6 RE 1 - Unique identification and authentication
- SR 1.7 - Strength of password-based authentication
- SR 1.7 RE 1 - Password generation and lifetime restrictions for human users
- SR 1.8 - Public key infrastructure certificates
- SR 1.9 - Strength of public key authentication
- SR 1.9 RE 1 - Hardware security for 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

Ok Cancel Clear Select All Open Standard



ICS Security Kompendium



IEC 62443-3-3

SECURITY4SAFETY

RISIKO BEURTEILUNG / RISIKO-BESTIMMUNG

| DRAR Level 1 | | | | | | | | |
|--------------|-----------|-----------------------|-----------|-------------------------------|------------------------------------|-----------------|------|------|
| Sensitivity | | | | | | Explanation (E) | Risk | SL-T |
| Expertise | Knowledge | Window of Opportunity | Equipment | Vulnerability of the zone (A) | possibility to discover treats (E) | | | |
| 1 | 3 | 1 | 3 | 7 | 5 | | 280 | SL 3 |



Die Wahrscheinlichkeit den Angriff nicht zu entdecken (E) wird intuitiv im Team festgelegt



Sensitivity / DRAR Level 1

Sensitivity (A)

Expertise (Ex): 1

System knowledge (SK): 1

Time window for attack (TWA): 3

Technique (Tech): 2

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|----|

not critical high thread critical

OK Cancel

Expertise:

- 0 = Several experts
- 1 = One expert
- 2 = Amateur
- 3 = Man on the street

Knowledge:

- 0 = Top secret
- 1 = Developer knowledge
- 2 = Restricted-access knowledge
- 3 = Publicly available knowledge

Window of opportunity:

- 0 = Less (server room)
- 1 = Middle (field)
- 2 = High (office IT)
- 3 = Permanent (Office-IT)

Equipment:

- 0 = Several special tools necessary
- 1 = One special tool necessary
- 2 = Specialised tool
- 3 = Standard equipment

SECURITY4SAFETY

RISIKO BEURTEILUNG / RISIKO-BESTIMMUNG

$$\text{Risk} = A \times E \times B$$

A = probability of occurrence (1 ... 10)

E = weak points (1 ... 10)

B = impact (max (safety+1 + financial+1) * 2- 1)



Security Level / DRAR Level 1

Determination of Cyber-Security-Levels

Effect (B)

| | | 0 | 1 | 2 | 3 | 4 |
|--|--|-----|-----|-----|-----|------|
| | | 0-1 | 2-3 | 4-5 | 6-7 | 8-10 |

Threat (Ax E)

| | 0 | 1 | 2 | 3 | 4 |
|---|--------|------|------|------|------|
| 0 | 0-19 | SL 1 | SL 1 | SL 1 | SL 1 |
| 1 | 20-39 | SL 1 | SL 2 | SL 2 | SL 2 |
| 2 | 40-59 | SL 1 | SL 2 | SL 3 | SL 4 |
| 3 | 60-79 | SL 1 | SL 2 | SL 3 | SL 4 |
| 4 | 80-100 | SL 2 | SL 3 | SL 4 | SL 4 |

48

=> **SL 3**

Info

OK

Ist der safety impact > 0 **muss** eine Gegenmaßnahme getroffen werden !

SL Level Info

SL 0:
No particular requirements or protective measures

SL 1:
Protection against occasional or accidental violations necessary

SL 2:
Protection against an intentional violation with simple means and low commitment, general abilities and low motivation

SL 3:
Protection against an intentional violation with sophisticated means, medium commitment, automation technology abilities and medium motivation

SL 4:
Protection against an intentional violation with sophisticated means, significant commitment, automation technology abilities and high motivation

OK



SECURITY4SAFETY

Dienstleistungen: Konzeptanalyse + Konformitätsprüfung

Anforderungs-Spezifikation



Software Design



Safety + Security
Konzept Analyse



Konformität zu IEC 62443-3-3

IEC 62443-3-3 / Foundation Requirements (FR) and System Requirements (SR)

FR 1 – Identification and authentication control (IAC)

FR 2 – Use control (UC)



FR 3 – System integrity (SI)

FR 4 – Data confidentiality (DC)

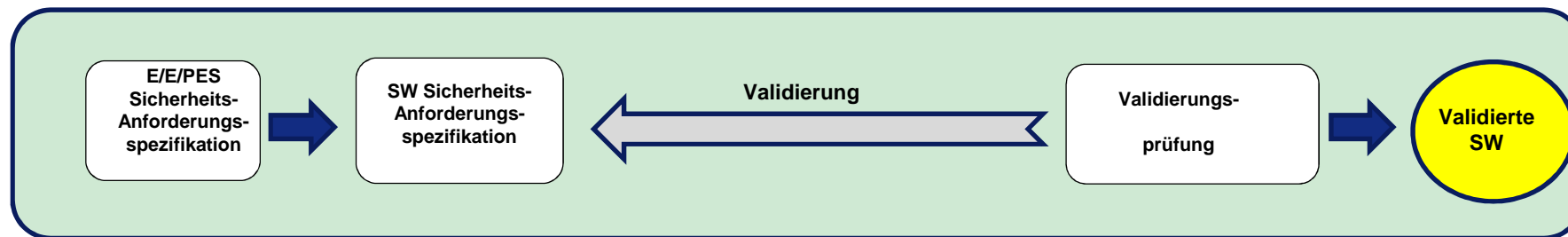
FR 5 – Restructured data flow (RDF)

FR 6 – Timely response to events (TRE)

FR 7 – Resource availability (RA)

|  | | Inspection according IEC 62443-3-3:2015 | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|-------------------------------------------------------------------------------------|------------|--------|------------|-----------------------|---------------------|----------------------|-------------------|---|-------------------|---|--------|---|------------------|---|--------|---|-----------|---|---------|----|-------------|---|---|----|----------------------------|---|---|------------------------|--|--|--|
| Requirements | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System under Consideration: | | | | | | Customer: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <div><div><div>0.0%</div><div>0.0%</div><div>0.0%</div><div>0.0%</div><div>100.0%</div></div><div></div></div> <table><thead><tr><th>Result</th><th>Assessment</th><th>Weight</th><th>Compliance</th></tr></thead><tbody><tr><td>0</td><td>Not fulfilled</td><td>0</td><td>0-10%</td></tr><tr><td>1</td><td>Partial fulfilled</td><td><</td><td>10-50%</td></tr><tr><td>2</td><td>Mostly fulfilled</td><td>></td><td>51-85%</td></tr><tr><td>3</td><td>Fulfilled</td><td>+</td><td>86-100%</td></tr><tr><td>50</td><td>Not checked</td><td>-</td><td>-</td></tr><tr><td>45</td><td>Not relevant or applicable</td><td>-</td><td>-</td></tr></tbody></table> | | | | | | Result | Assessment | Weight | Compliance | 0 | Not fulfilled | 0 | 0-10% | 1 | Partial fulfilled | < | 10-50% | 2 | Mostly fulfilled | > | 51-85% | 3 | Fulfilled | + | 86-100% | 50 | Not checked | - | - | 45 | Not relevant or applicable | - | - | weighted results: 0,0% | | | |
| Result | Assessment | Weight | Compliance | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | Not fulfilled | 0 | 0-10% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Partial fulfilled | < | 10-50% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Mostly fulfilled | > | 51-85% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Fulfilled | + | 86-100% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 50 | Not checked | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 45 | Not relevant or applicable | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Chapter | Type | Sub-Chapters | Requirements | Results | Remarks | SL-1 | SL-2 | SL-3 | SL-4 | Comments | Reference-Documents | Links | Customer Comments | | | | | | | | | | | | | | | | | | | | | | | | |
| SR1TRE1-Human user identification and authentication | R | 5.3.3.1 | SR 1.1 RE 1 – Unique identification and authentication The control system shall provide the capability to uniquely identify and authenticate all human users. | | | | | | | | | open | | | | | | | | | | | | | | | | | | | | | | | | | |
| SR1TRE2-Human user identification and authentication | R | 5.3.3.2 | SR 1.1 RE 2 – Multifactor authentication for untrusted networks The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks). NOTE: See 5.7.3.5.7.3.1, SR 1.5 – Authenticator management, RE 5.7.3.1 for enhanced authenticator management for software processes. | | | | | | | not required for SL 2 | | open | | | | | | | | | | | | | | | | | | | | | | | | | |

SECURITY4SAFETY PENETRATIONSTEST / ÜBERPRÜFUNG DER WIRKSAMKEIT DER MAßNAHMEN

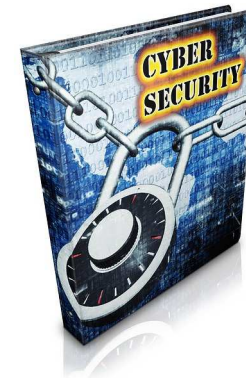


Penetrations-Test

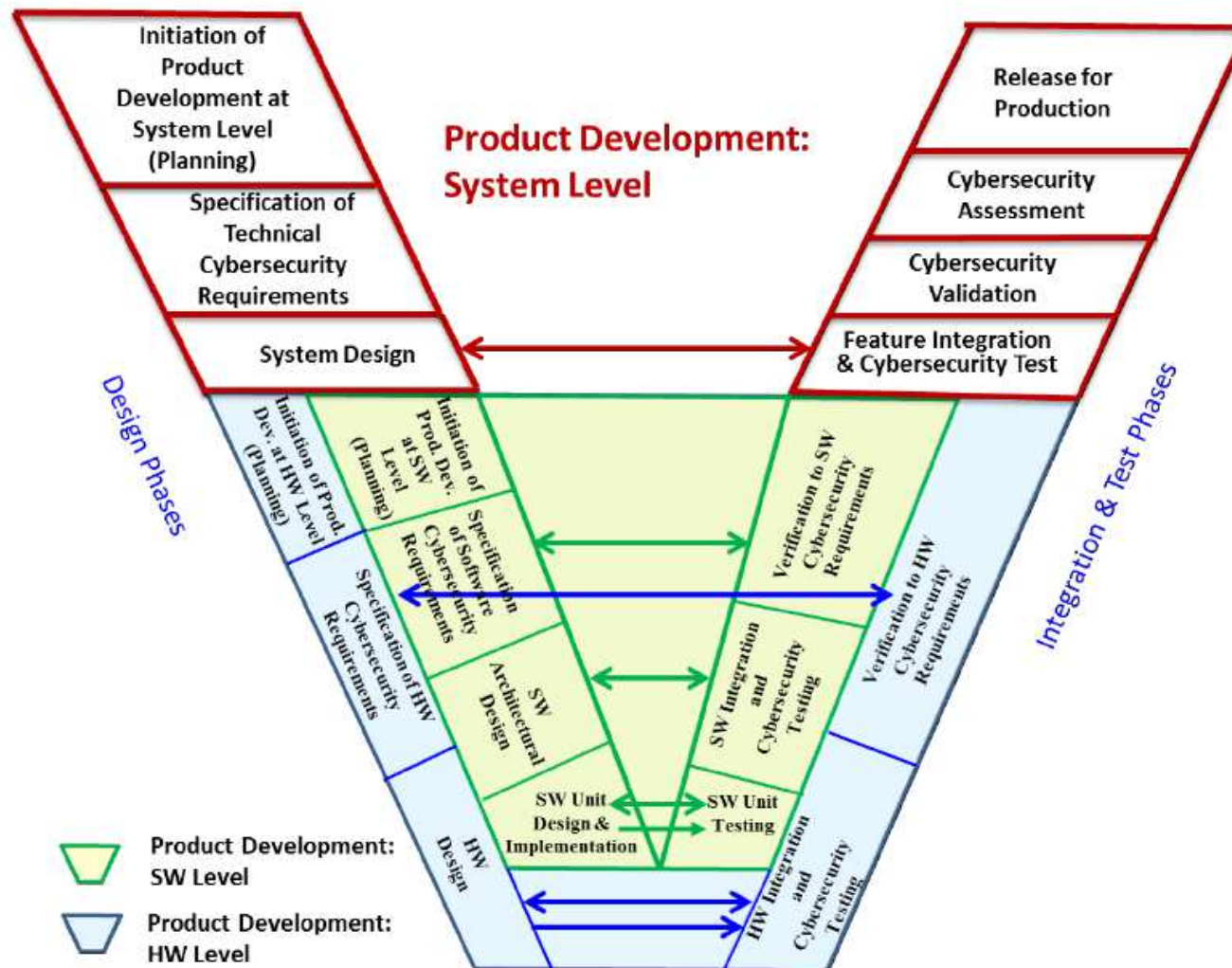
Security



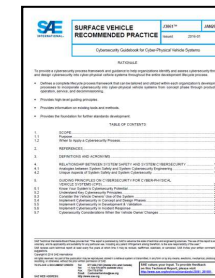
Bericht



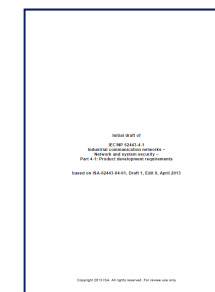
SECURITY4SAFETY PROZESSE



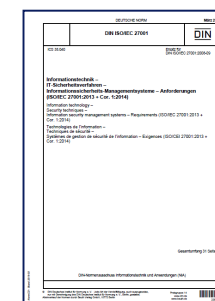
J3061



IEC 62443-4-1



IEC 27001 / 2



SECURITY4SAFETY
PARTNER IM BEREICH SECURITY



<https://www.tuvit.de>



<https://www.secuvera.de>



<http://www.silver-atenade>



Hochschule
Augsburg University of
Applied Sciences

HSAinnoS
Institut für innovative IT-Sicherheit

<https://www.hsasec.de>

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dipl. Ing.(FH) Martin Zeh
Sachverständiger für Funktionale Sicherheit
& Security Manager OBS Manufacturing

TÜV NORD Systems GmbH & Co. KG
Halderstraße 27
86150 Augsburg

Telefon: +49 821 450954-4290
E-Mail: mzeh@tuev-nord.de

