

TeleTrust – Bundesverband IT-Sicherheit e.V.

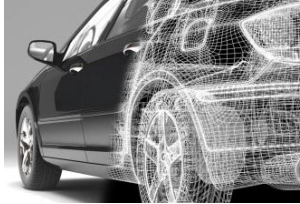
TeleTrust-Workshop "Industrial Security" 2015

München, 11.06.2015

"Safety-related Security – Zusammenhänge, Synergien, Zielkonflikte"

Martin Kaiser

IABG



AUTOMOTIVE



INFOKOM



MOBILITÄT, ENERGIE &
UMWELT



LUFTFAHRT



RAUMFAHRT



VERTEIDIGUNG &
SICHERHEIT

Safety-related Security – Zusammenhänge, Synergien, Zielkonflikte

Martin Kaiser

2015-11-06



CoC SAFETY

IABG is a leading European technology enterprise with the core competencies of analysis, simulation & testing as well as plant operation (safety & security)

87.4 %
SCHWARZ Holding GmbH

12.6 % IABG
Mitarbeiterbeteiligungs AG

IABG

Total operating performance: about €177,2 million* - Staff: approx. 1000
(about 10% thereof investments in research and development, facilities, HR development)

Automotive



Employees:
about 120

Development and operation of mechatronic test systems for OEM & suppliers

InfoCom



Employees:
about 130

Development and operation of secure ICT systems

Mobility, Energy & Environment



Employees:
about 100

Environmental solutions, protection, electro-mobility and change in energy policy.

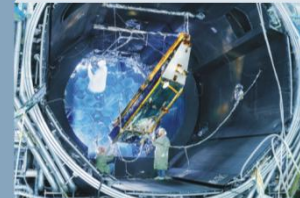
Aeronautics



Employees:
about 160

Fatigue strength tests for complete airframes and components

Space



Employees:
about 130

Operation of ESA coordinated Space Test Centres in Ottobrunn and Noordwijk

Defence & Security



Employees:
about 370

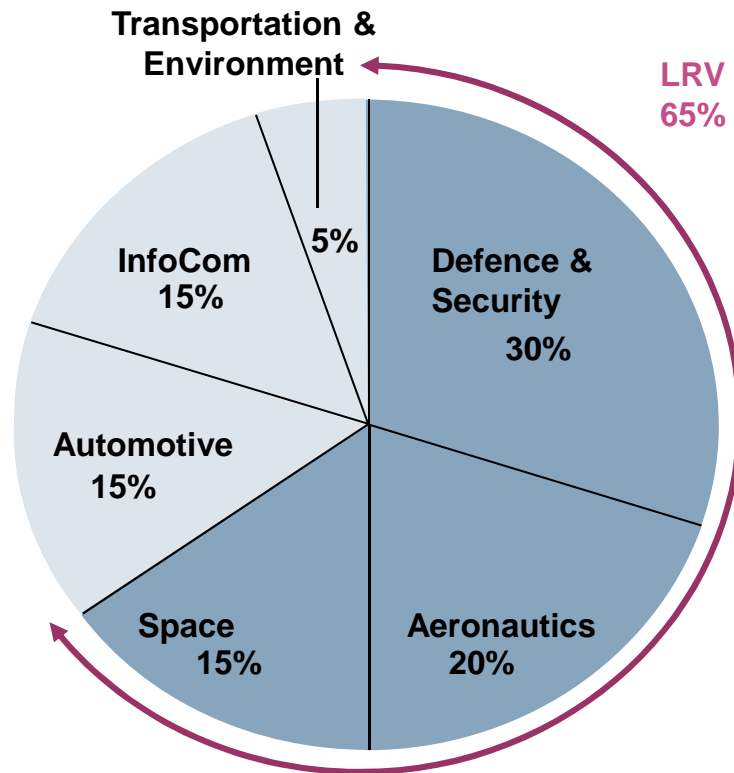
Operation of military simulation & test systems for analyses and conceptions

* Business year 2012

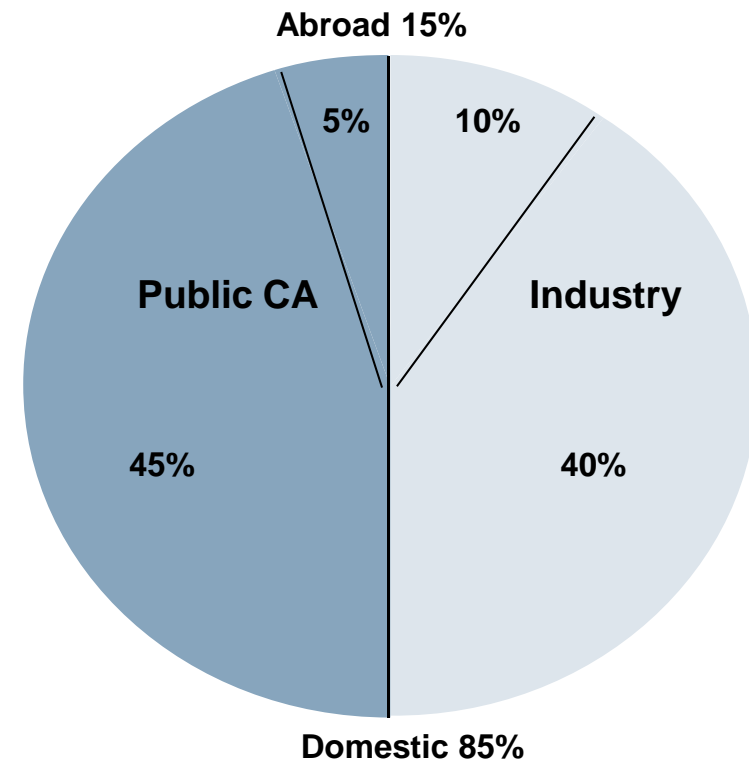
Total operating performance 2012

Business segments

100% ~ €177,2 million



Customers



IABG Infrastructure



IABG Headquarters in Ottobrunn



Berlin



Oberpfaffenhofen



Koblenz



Dresden



Lichtenau



Dresden



Lathen



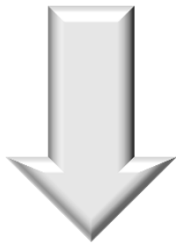
Noordwijk (NL)

Inhalt

Nr.	Thema
1	Überblick zu Richtlinien und Gesetze / beteiligte Organisationen / Managementebene (jeweils safety-related)
2	Schutzebenenkonzept / generische Aspekte: Vergleich Safety-Security (à Workshopdiskussion)
3	Normungsfragen am Beispiel Risikoanalyse / xLevel, Safety-Security (à Workshopdiskussion)
4	Typische Einstufung von Sicherheitsfunktionen; Rückwirkungsfreiheit (à Workshopdiskussion)
5	Zielkonflikte Safety-Security bei Anforderungen und Analysen
6	Synergien bei Prozessen, Anforderungen und Test (à Workshopdiskussion)
7	Zertifikate aus Anwendersicht (à Workshopdiskussion)
8	VDE Anwendungsregel Safety & Security; Normenliste

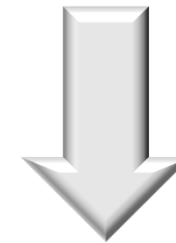
1.1 Regulatory Requirements and Certification

Mandatory application of EC directives and
ECE regulations (in Europe)



Laws in specific Country / Europe / World

Declaration* of
conformity to e.g.
Machinery Directive
2006/42/EC



Example (Germany):
Produktsicherheitsgesetz
(ProdSG)

* Assessment procedures :

- “internal checks” (annex VIII)
- Full quality assurance (annex X)
- EC type examination (annex IX) à NB à ZLS (Germany)

To be distinguished from certificates à laboratory à DAkkS (Germany)

1.2 Regulatory Requirements and Certification

■ Authorities and Organisations

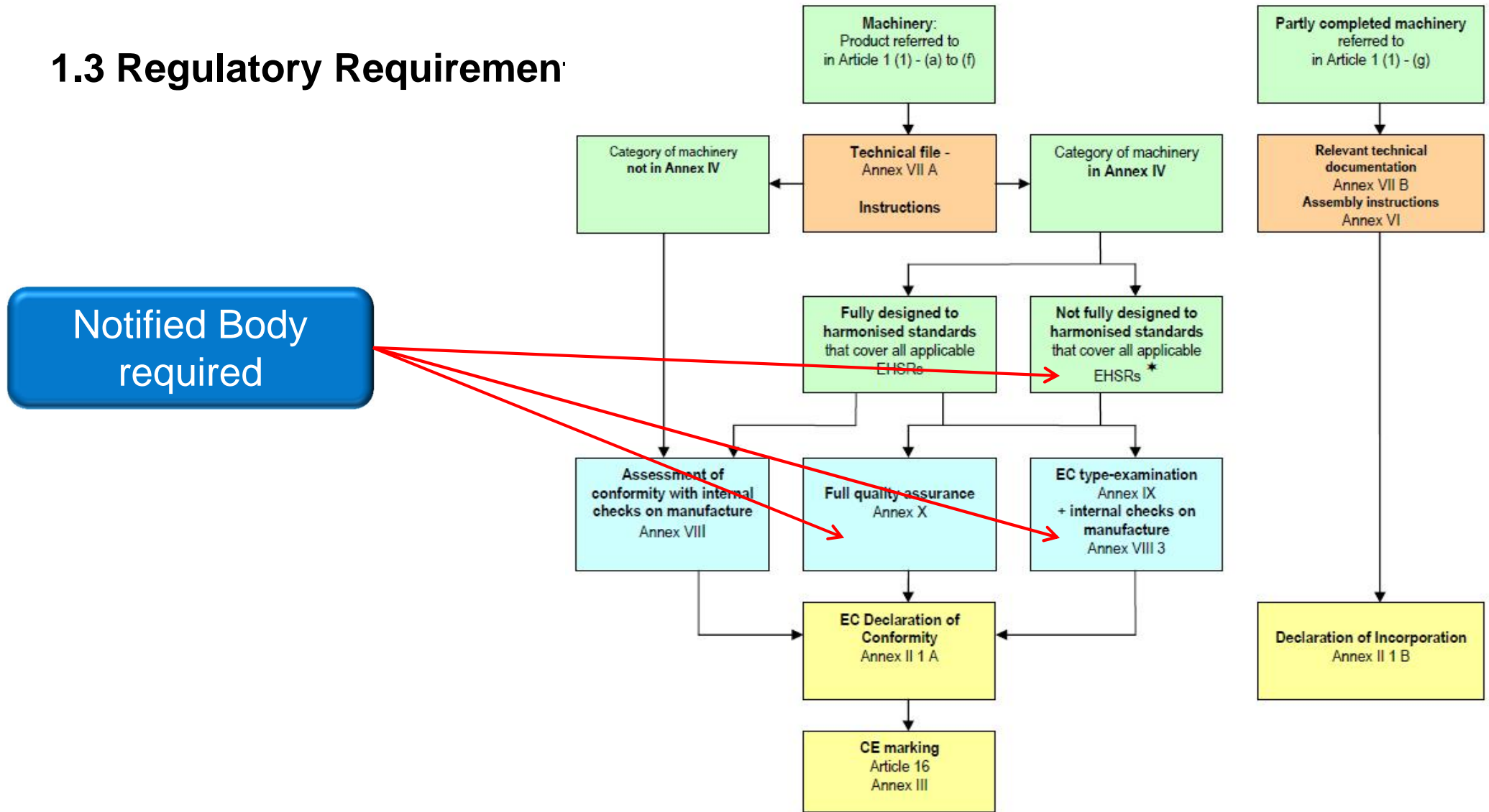
- ProdSG à [Bundesministerium für Arbeit und Soziales: BMAS](#)
- BetrSichV (together with ProdSG / Notified Bodies) for e.g. pressure vessels, lifts, ... à Zugelassene Überwachungsstelle (ZÜS) à ZLS
- BAuA (Bundesanstalt für Arbeitsschutz und Arbeitsmedizin) as communication hub
- Market surveillance à Länderbehörden (Gewerbeaufsicht)

- Certifying test laboratories à DAkkS à ILAC

■ Standards and Assessments

- “state of the scientific and technical knowledge”
- Harmonized standards (listed in official journal), e.g. ISO 13849, IEC 62061
- IEC 61511, IEC 61508, ISO 26262, ISO 25119 are **not** harmonized but well known

1.3 Regulatory Requirements



Article 12(3) and (4) procedures for Annex IV machinery

extracted from „guide_application_directive_2006-42-ec-2nd_edit_6-2010_en.pdf“

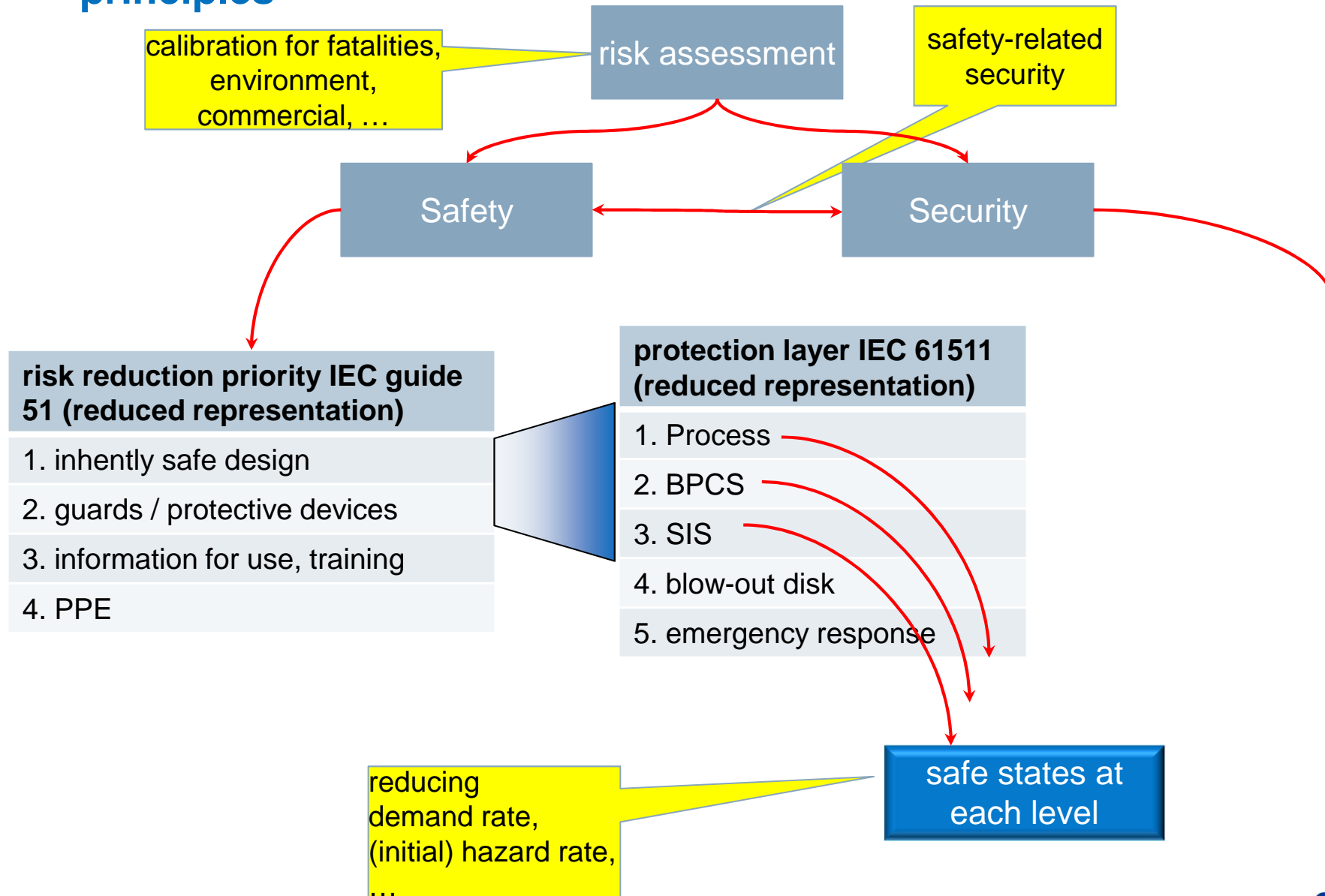
* Harmonised standards are not available, the harmonised standards do not cover all the applicable EHSRs or the harmonised standards are not applied or are only partially applied.

Colour code: Product category Documents Procedure Declaration – marking

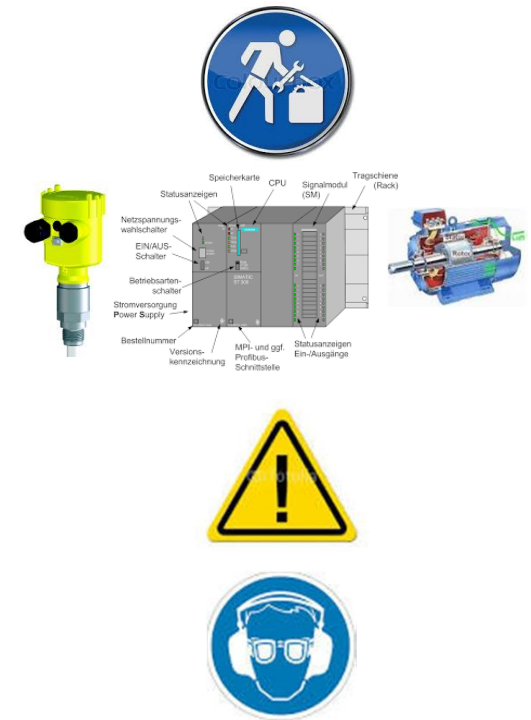
1.4 Management level

- safety / security culture
 - IEC 62879 Ed. 1.0 „Human factors and functional safety“
 - ...
- ISMS / IACS SMS (ISO / IEC 27001 / 2, IEC 62443-2-1, ...)
- FSM (Management of Functional Safety)
 - IEC 61508 part 1
 - ISO 26262 part 2
 - ~~■ ISO 13849~~
 - IEC 61511-1 clause 5
 - IEC 62061 clause 4

2.1 From risk assessment to safe states at different levels – generic principles



2.2 Design Measures to attain safety

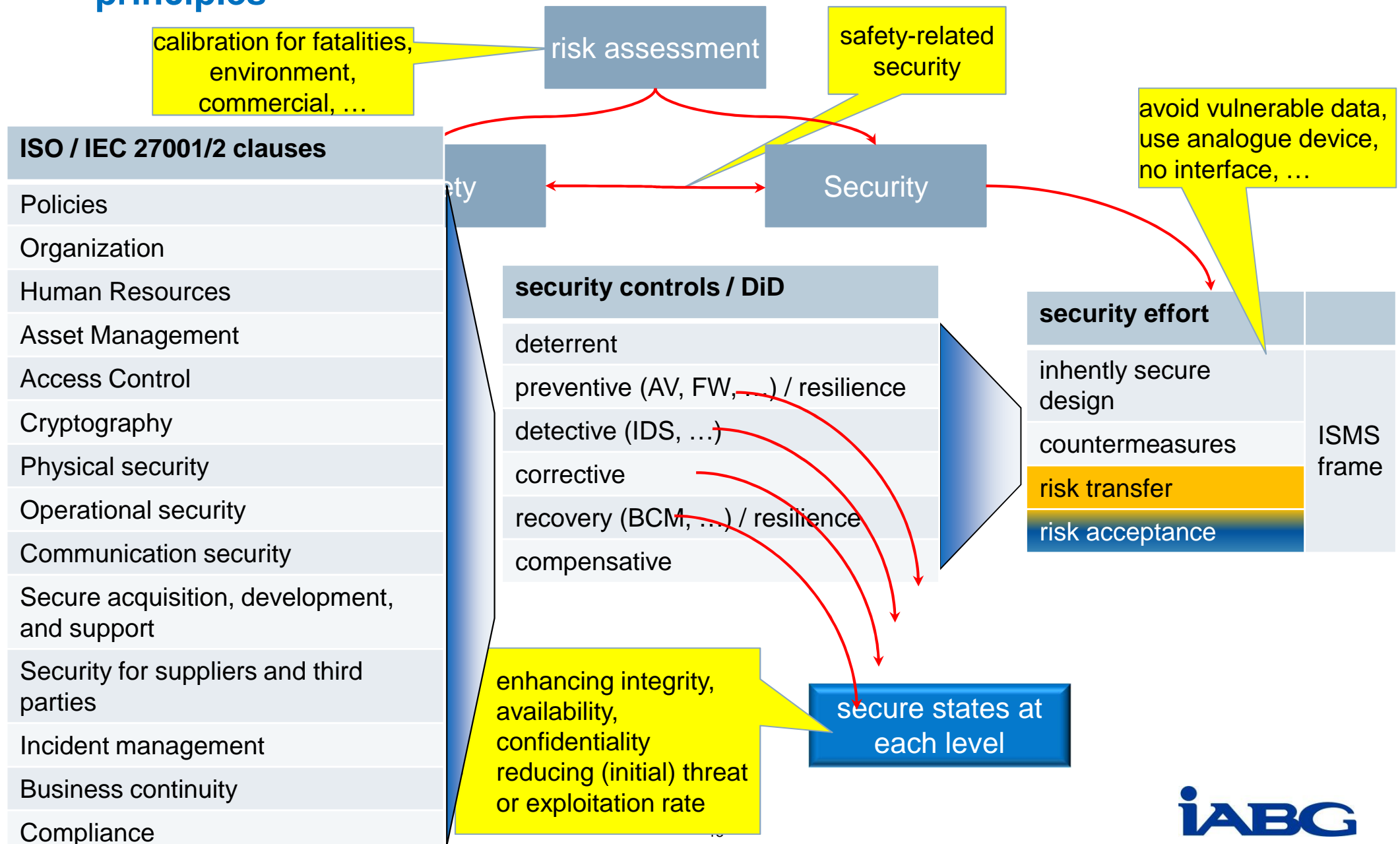


- Inherently safe design (avoid risks)
- Electronically design (E/E/PE* systems to control / mitigate risks)
- Other measures (warning signs, manuals and similar à information on residual risk)

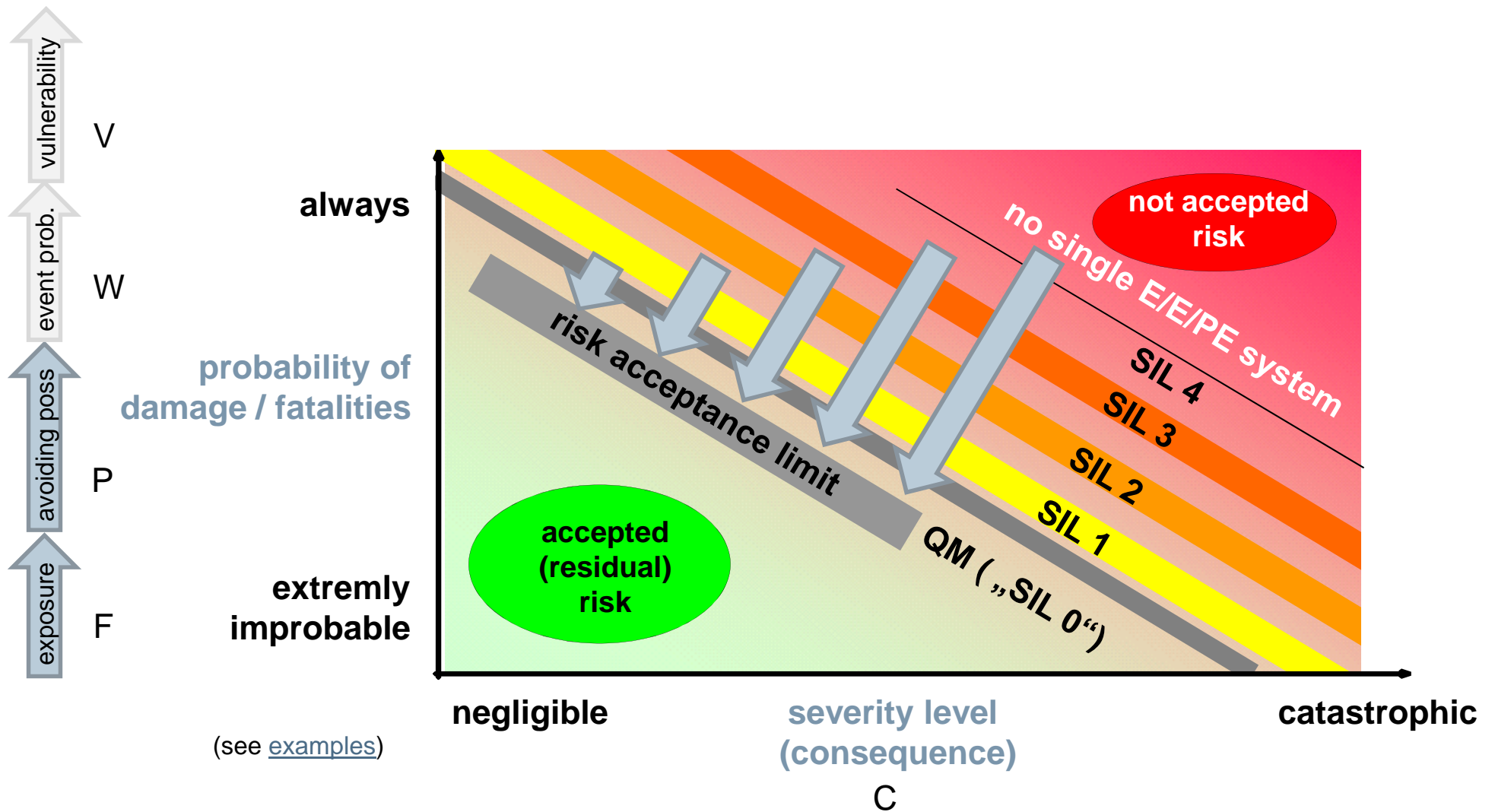


*electrical / electronic / programmable electronic

2.3 From risk assessment to safe states at different levels – generic principles



3.1 Risk Assessment



3.2 Risk Assessment Procedures – Risk Graph Calibration (Example)

Deepwater
Horizon (2010)



Risk matrix for single hazard tolerability



Safety (onsite)	Reputation/ Environment	Commercial	Severity Level	<10-6 /yr	10-6 – 10-5/yr	10-5 – 10-4/yr	10-4 – 10-3/yr	0.001- 0.01/yr	0.01- 0.1/yr	0.1-1/yr	>1/yr
>200 fatalities	Global outrage >1,000,000 bbl oil spill	≥ \$10bn	A	Medium	High	High	High	High			
>50 fatalities	International outrage across a region >100,000 bbl oil spill	\$1bn to <\$10bn	B	Medium	Medium	High	High	High			
>10 fatalities	Severe national outrage. >10,000 bbl oil spill	\$100m to <\$1bn	C	CRR (Low)	Medium	Medium	High	High			
1-10 fatalities	National outrage. >1,000 bbl oil spill	\$10m to <\$100m	D	CRR (Low)	CRR (Low)	Medium	Medium	High	High	High	High
≥1 disabling injuries	State outrage. Onsite release with prolonged damage or offsite release with immediate remediation	\$1m to <\$10m	E				Medium	Medium	High	High	High
≥1 lost time injuries	Local outrage. Onsite release with immediate remediation	\$100k to <\$1m	F				CRR (Low)	Medium	Medium	High	High
≥1 first aid injuries	No community outrage. Contained onsite release	<\$100k	G				CRR (Low)	CRR (Low)	Medium	Medium	High

IEE Seminar: SIL Determination Principles and Practical Experience

Savoy Place, London, 28 March 2007

8

From "Calibration of SIL Determination Methods.pdf", London, 2007

3.3 From risk assessment to safety and security requirements within various standards

- ISO IEC 27005 describes consequences and likelihood (experience, statistics, motivation & capabilities)

Table E.1 a)

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

If vulnerability is unknown, „ease of exploitation“ is difficult to estimate

- Also IEC 62443-2-1 knows the risk equation

$$Likelihood_{Event_Occurring} = Likelihood_{Threat_Realized} \times Likelihood_{Vulnerability_Exploited} \quad (A.1)$$

As discussed above, risk is made up of both likelihood and consequence, where consequence is the negative impact the organization experiences due to the specific harm to the organization's asset(s) by the specific threat or vulnerability.

$$Risk = Likelihood_{Event_Occurring} \times Consequence \quad (A.2)$$

3.4 From risk assessment to safety and security requirements within various standards

■ Result of risk assessment, the risk level, is often associated with security levels acc. IEC 62443 (... contents depending on FR)

likelihood calibration

- SL 1 – Prevent ... / protect against ...casual
- SL 2 – Prevent ... / protect against ...simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent ... / protect against ... sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent ... / protect against ... sophisticated means with extended resources, IACS specific skills and high motivation.

3.5 From risk assessment to safety and security requirements within various standards

- IEC 62443-1-1, IEC 62443-2-1, IEC 62443-4-1, IEC 62443-4-2 reference ISO 15408 (equal or stronger than EAL4+ required ¹⁾)

- CC part 3

- EAL2+3: basic attack potential
- EAL4: enhanced-basic attack potential
- EAL5: moderate attack potential
- EAL6+7: high attack potential

can be understood as
SLx implementation
level


- but ... EAL6 talks about „protecting **high value** assets against significant **risks**.“

likelihood calibration

1) 62443-4-2 Technical security requirements for IACS components à 4
Common control system security **constraints** à HW requirements, where + is
AVA_VAN.5

3.6 From risk assessment to safety and security requirements within various standards

- Smart Grid Information Security SL calibration is in contrast severity-oriented ...



Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Abbildung 2: SGIS Security level

(Quelle: [SG-CG/M490/H_Smart Grid Information Security 12/2014])

3.7 From risk assessment to safety and security requirements within various standards

... and resembles BSI Grundschrift 100-2 ...

severity calibration

Schutzbedarfskategorien	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

... where this example reveals a missing link to safety (SILs include a severity **AND** a probability component) ¹

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	<ul style="list-style-type: none"> Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben

1) see also [TBINK comment](#) p.3 („IT-Sicherheitskatalog“ gem. § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG))

4.1 Specific requirements (enhancements), SIL examples

- Typical SILs for power plants range from **SIL1** (overpressure sealing steam) to **SIL3** (overspeed steam turbine, reverse (motor) operation, induced draught, furnace ventilation, fuel feed) → depends on size, other measures and individual system → far more than SCADA, see e.g. [ISO 27019](#)
- Attack / malware may push to SIL4 :
 - factor W (frequency of unwanted event) possibly higher, but consider also ...
 - C (consequence), ...
 - F (exposure higher if physical access unauthorized open to public → [assume freedom from interference, require SLx / EALx or consider new risk assessment ?](#)), ...
 - P, V ; see [risk matrix](#)
- Battery charging at charging station:
 - unintended movement may be [ASIL A](#) or B → C if hacked
- (graceful) degradation requires analysis to avoid dangerous intermediate states

4.2 Specific requirements (freedom from interference)

- (by fault / attack) degraded system :
 - Typical safety solution: „freedom from interference“. Example situations: smart meter → car (unintended movement); cars → grid (DDoS attack on load control for wide grid etc.)
 - For security hard to demonstrate as malware interfaces are not known in advance.
 - Should we assume normatively „freedom from interference“ if a potentially vulnerable system fulfils e.g. EAL 4+ (or higher along with higher SIL ?) acc. to CC / 15408 ?
- IEC 61508-3 clause 7.4 (Software design and development) (guide see [annex F](#))

7.4.2.8 Where the software is to implement both safety and non-safety functions, then all of the software shall be treated as safety-related, unless adequate design measures ensure that the failures of non-safety functions cannot adversely affect safety functions.

7.4.2.9 Where the software is to implement safety functions of different safety integrity levels, then all of the software shall be treated as belonging to the highest safety integrity level, unless adequate independence between the safety functions of the different safety integrity levels can be shown in the design. It shall be demonstrated either (1) that independence is achieved by both in the spatial and temporal domains, or (2) that any violation of independence is controlled. The justification for independence shall be documented.

5. Conflicting objectives and models

■ Security → Safety

- Additional components introducing possible sources of safety-related failures (e.g. virus scanner, firewall)
- Continuous updates of virus data base ; patches → may invalidate safety certificate
- Safety properties (realtime) might be affected (e.g. encryption, timing conflicts, security exceptions,...)

■ Safety → Security

- Additional components (safety functions) introducing possible sources of vulnerability
- ...

■ Combined view of Safety & Security sometimes desired

- Common quantitative Safety & Security FTA ??
- ...

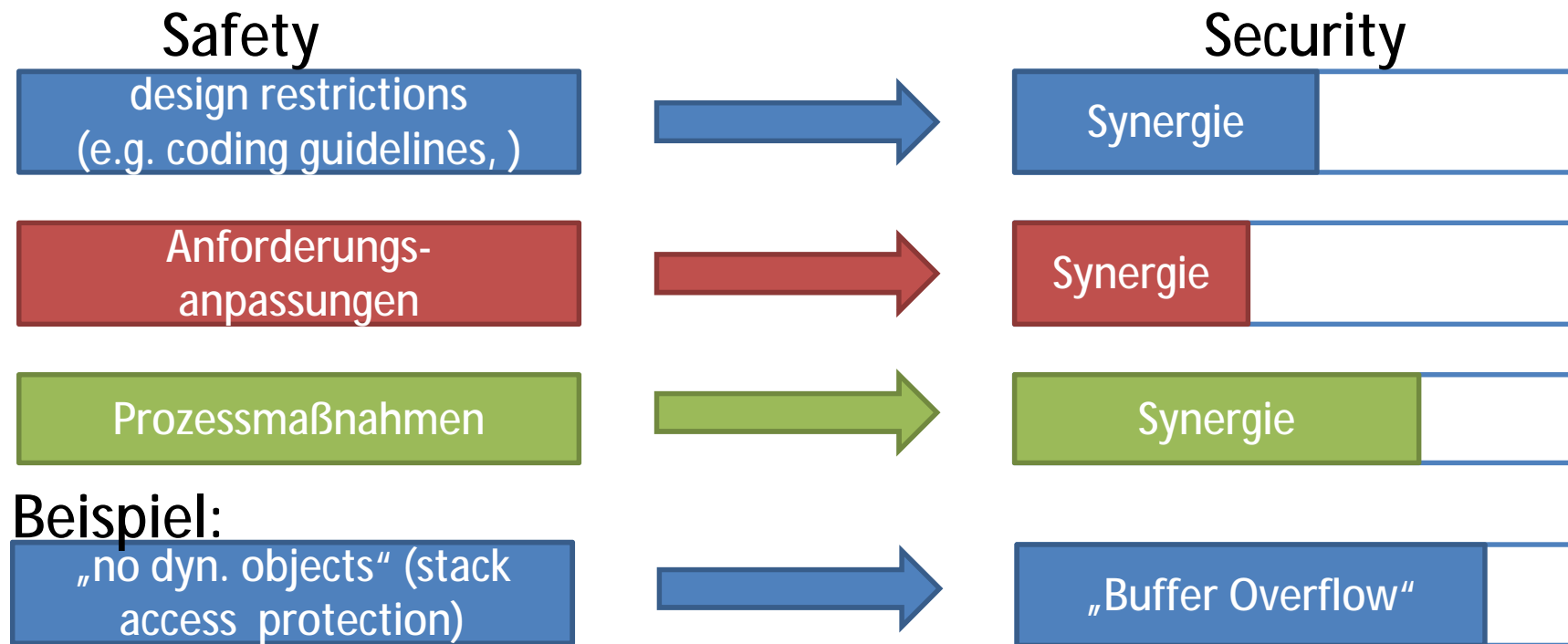
■ Data communication with security and safety (e.g. encryption and CRC / alive crt)

- Is safety layer above security or security layer above safety layer ? → BSC assumption affected
- ...

6.1 Potential Synergies

■ Comparison with safety processes

- Some IEC 61508 requirements and recommendations address already security goals. Examples: risk assessments, safety analyses, requirements management and tracing, design- and coding guidelines...., QM-/CM- reviews / audits, V&V activities



6.2 Potential Synergies: design and test requirements comparison

■ CC part 3 clause 8.1 (EAL overview) ff

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
	ATC_CMC	1	2	3	4	4	5	5

- 8.3 Evaluation assurance level 1 (EAL1) - functionally tested**
- 8.4 Evaluation assurance level 2 (EAL2) - structurally tested.....**
- 8.5 Evaluation assurance level 3 (EAL3) - methodically tested and checked.....**
- 8.6 Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed**
- 8.7 Evaluation assurance level 5 (EAL5) - semiformally designed and tested**
- 8.8 Evaluation assurance level 6 (EAL6) - semiformally verified design and tested**
- 8.9 Evaluation assurance level 7 (EAL7) - formally verified design and tested.....**

resembles
SIL 1..4 range

6.3 Potential Synergies: design and test requirements comparison

■ IEC 61508-3 tab. A.1 (specification) / A.4 (detailed design) / A.5 (module test)

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Semi-formal methods	Table B.7	R	R	HR	HR
1b	Formal methods	B.2.2, C.2.4	---	R	R	HR
2	Forward traceability between the system safety requirements and the software safety requirements	C.2.11	R	R	HR	HR
3	Backward traceability between the safety requirements and the perceived safety needs	C.2.11	R	R	HR	HR
4	Computer-aided specification tools to support appropriate techniques/measures above	B.2.4	R	R	HR	HR

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Structured methods **	C.2.1	HR	HR	HR	HR
1b	Semi-formal methods **	Table B.7	R	HR	HR	HR
1c	Formal design and refinement methods **	B.2.2, C.2.4	---	R	R	HR

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Probabilistic testing	C.5.1	---	R	R	R
2	Dynamic analysis and testing	B.6.5 Table B.2	R	HR	HR	HR
3	Data recording and analysis	C.5.2	HR	HR	HR	HR
4	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	HR	HR	HR
5	Performance testing	Table B.6	R	R	HR	HR

6.4 Potential Synergies: design and test requirements comparison

■ IEC 61508-2 tab. B.1 („effectiveness“)

61508-2 © IEC:2010

– 65 –

Table B.3 – Techniques and measures to avoid faults during E/E/PE system integration (see 7.5)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Functional testing	B.5.1	M high	M high	M high	M high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Field experience	B.5.4	R low	R low	R medium	R high
	Statistical testing	B.5.3	– low	– low	R medium	R high

7.1 Certificates – supplier / operator view

- IEC 62443-1-1, IEC 62443-2-1, IEC 62443-4-1, IEC 62443-4-2 (drafts) all reference ISO 15408 (equal or stronger than EAL4+ required ¹⁾)
- IEC 61508 states in the foreword ²⁾

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

- Functional safety certificates (product / type specific) are valid for a future period (e.g. 1 year) → a factory inspection updates every year the validity
- Can security certificates for a product predict its sustainable effectiveness ?
- System integrators / operators for power utilities / chemical plants often need
 - functional safety certified components → safe SIS
 - a notified body assessing safety
 - insurance approval for fire (asset) safety
 - ... and security certificates
 - → there seems to be the need for a commonly agreed approach



7.2 Certificates – supplier / operator view

- How will security be demonstrated in the future ?
 - IEC 62443-1-3 (draft) defines conformance metrics à measures some effectiveness of implemented security measures and relates to FRs, but does not directly verify compliance to IEC 62443
 - ISO / IEC 27004 shows a method to derive metrics, and example metrics to assess the effectiveness of ISMS requirements. Relates directly to ISO / IEC 27001 controls.
- Paths to a „secure“ system
 - Normative compliance approach, detached from practice ?
 - Selection of some measures approved in practice à systematic coverage of normative requirements ?
- Moving target à Normative requirements, security by design, complemented by up-to-date measures ?

*) aus „[Trendschau-2.pdf](http://www.oeffentliche-it.de)“, <http://www.oeffentliche-it.de>

8. VDE / DKE Activities

- list of security standards
- <http://smartgridstandardsmap.com/>

Committee	Standard	Title	Chapter (part)	Level of Abstraction (1: restricted, 4: high)				Layers				Target Users/Audience				Sector/Domain	Reference IT Security Standards (Common Industrial List (CIL))	Brief Description
				1	2	3	4	Detection	Identification	Prevention	Protection	Policy	Transfer	Storage	Recovery			
IEC TC 57	IEC 62380-8	Power systems management and associated information exchange - Data and communications security - Part 8: Data-based access control for power system management		x												Energy Automation	IEC 62380-8	TS 200 (TS) prepared to describe role categorization
IEC TC 57	IEC 62380-9	Power systems management and associated information exchange - Data and communications security - Part 9: Key Management		x												Energy Automation	IEC 62380-9	TS 200 (TS) prepared to describe role categorization
IEC TC 65	IEC 62443-2-1	Industrial communication networks - Network and system security - Part 2-1: Terminology, concepts and models				x										Automation	ANSI/HSA-45.01.01.00.00.00, ANSI/HSA-45.01.01.00.00.00, ISO/IEC 27001, ISO/IEC 27002	Technical requirements for 7 categories of technical security controls: security, integrity, confidentiality, availability, non-repudiation, accountability, and privacy
IEC TC 65	IEC 62443-2-2	Industrial communication networks - Network and system security - Part 2-2: Requirements for security and confidentiality														Automation	ANSI/HSA-45.01.01.00.00.00, ANSI/HSA-45.01.01.00.00.00, ISO/IEC 27001, ISO/IEC 27002	Technical requirements for 7 categories of technical security controls: security, integrity, confidentiality, availability, non-repudiation, accountability, and privacy
IEC TC 65	IEC 62443-2-3	Industrial communication networks - Network and system security - Part 2-3: Requirements for security and confidentiality		x												Automation	ANSI/HSA-45.01.01.00.00.00, ANSI/HSA-45.01.01.00.00.00, ISO/IEC 27001, ISO/IEC 27002	Technical requirements for 7 categories of technical security controls: security, integrity, confidentiality, availability, non-repudiation, accountability, and privacy
IEC TC 65	IEC 62443-2-4	Industrial communication networks - Network and system security - Part 2-4: Contribution of IEC 62443-2-4 to the security of IEC 62443-2-1														Automation	ANSI/HSA-45.01.01.00.00.00, ANSI/HSA-45.01.01.00.00.00, ISO/IEC 27001, ISO/IEC 27002	Technical requirements for 7 categories of technical security controls: security, integrity, confidentiality, availability, non-repudiation, accountability, and privacy

- Application Guide VDE-AR : „Zusammenhang zwischen Funktionaler Sicherheit und IT-Sicherheit am Beispiel der Industrieautomation“
- AD-HOC GROUP: FRAMEWORK TOWARD COORDINATING SAFETY, SECURITY

Danke für Ihre
Aufmerksamkeit –
Fragen,
Diskussion ?

Ihr Ansprechpartner

Martin Kaiser

Center of Competence Safety

Phone +49 89 6088-3759

E-Mail kaiser@iabg.de



IABG mbH
Einsteinstrasse 20
85521 Ottobrunn

Phone +49 89 6088-0
E-Mail safety@iabg.de
Web www.iabg.de