

Funktionale Sicherheit Anwendung in Energiespeichersystemen

Christoph Eggert
Hannover, 02.04.2019

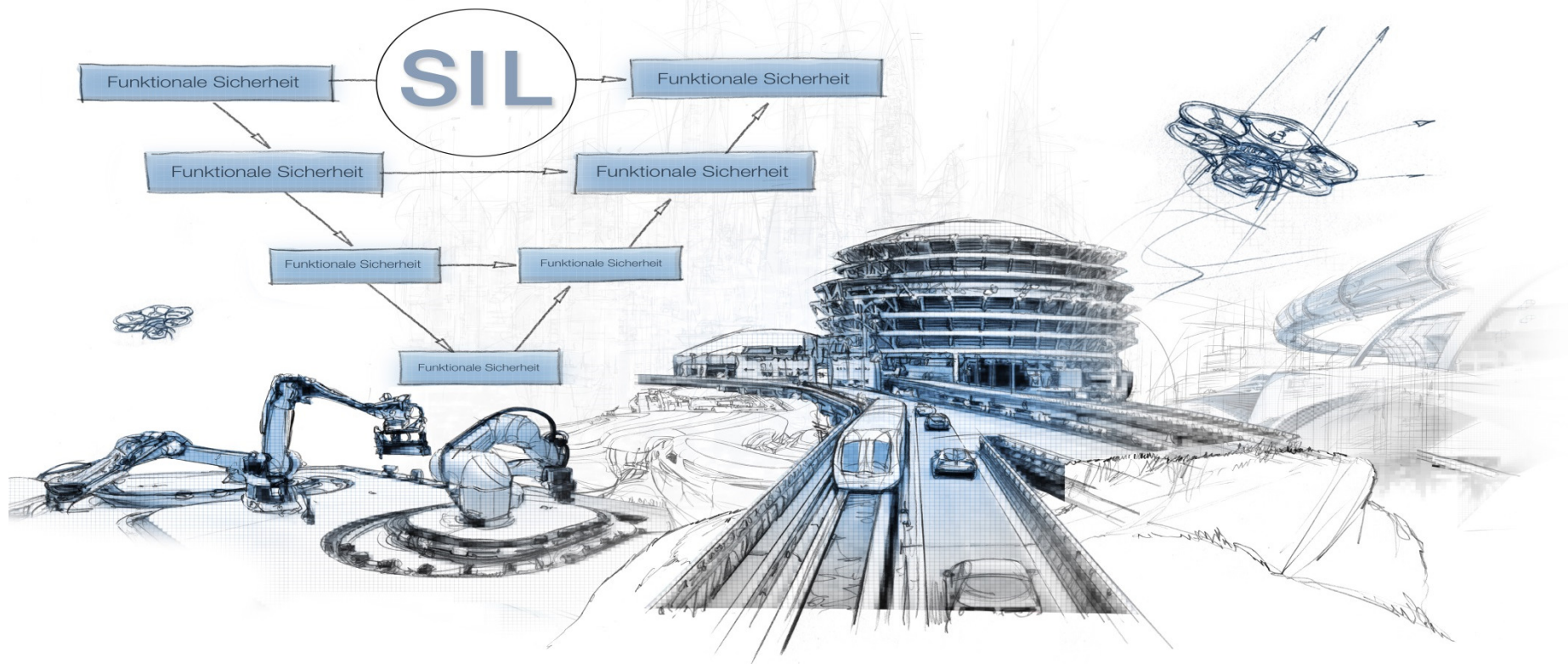


VDE INSTITUT

Agenda



- Was ist Funktionale Sicherheit?
- Beispielhafte Anwendung in Energiespeichersystemen
- Beitrag des VDE – Prüf- & Zertifizierungsinstitutes



Was ist Funktionale Sicherheit?

Definition der funktionalen Sicherheit nach ISO26262-1:

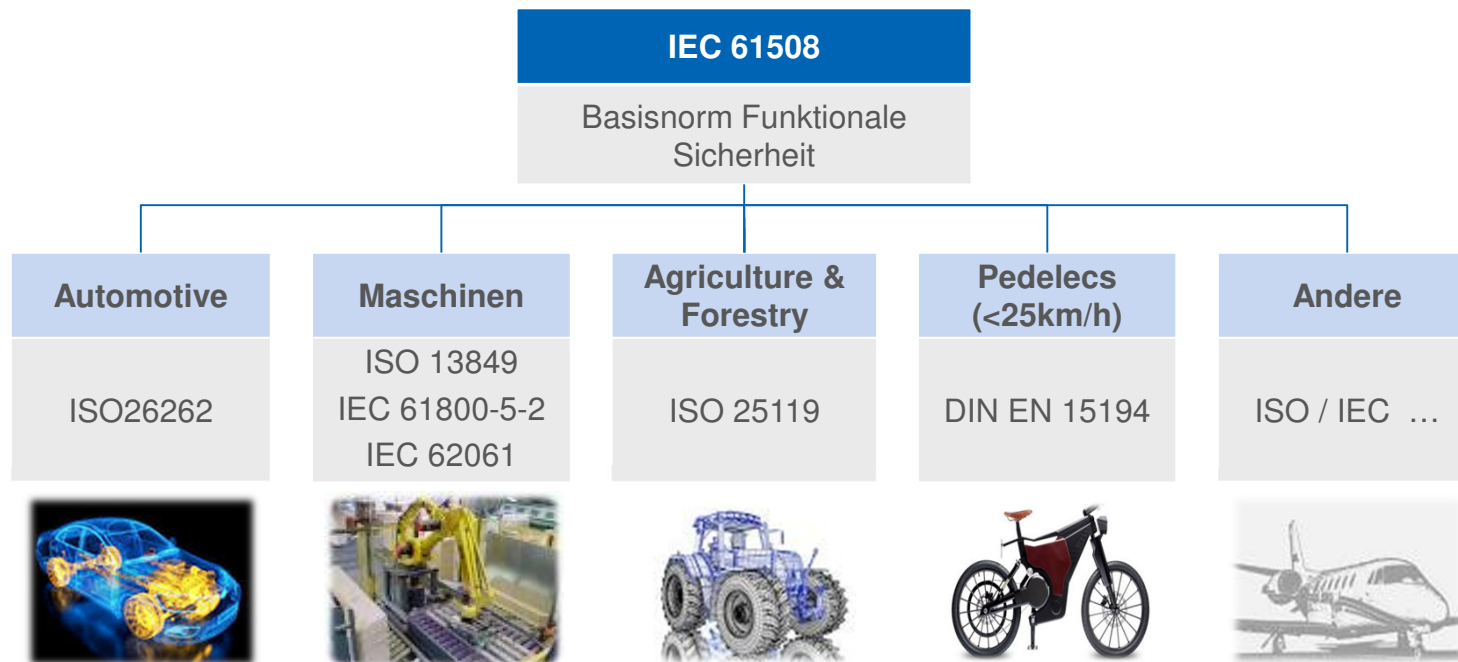


„Absence of **unreasonable risk** due to hazards caused by **malfunctioning behaviour** of **E/E-systems**“

Ein **Risiko** ist hier die **Kombination** aus der **Wahrscheinlichkeit** und dem **Ausmaß eines Schadens**.

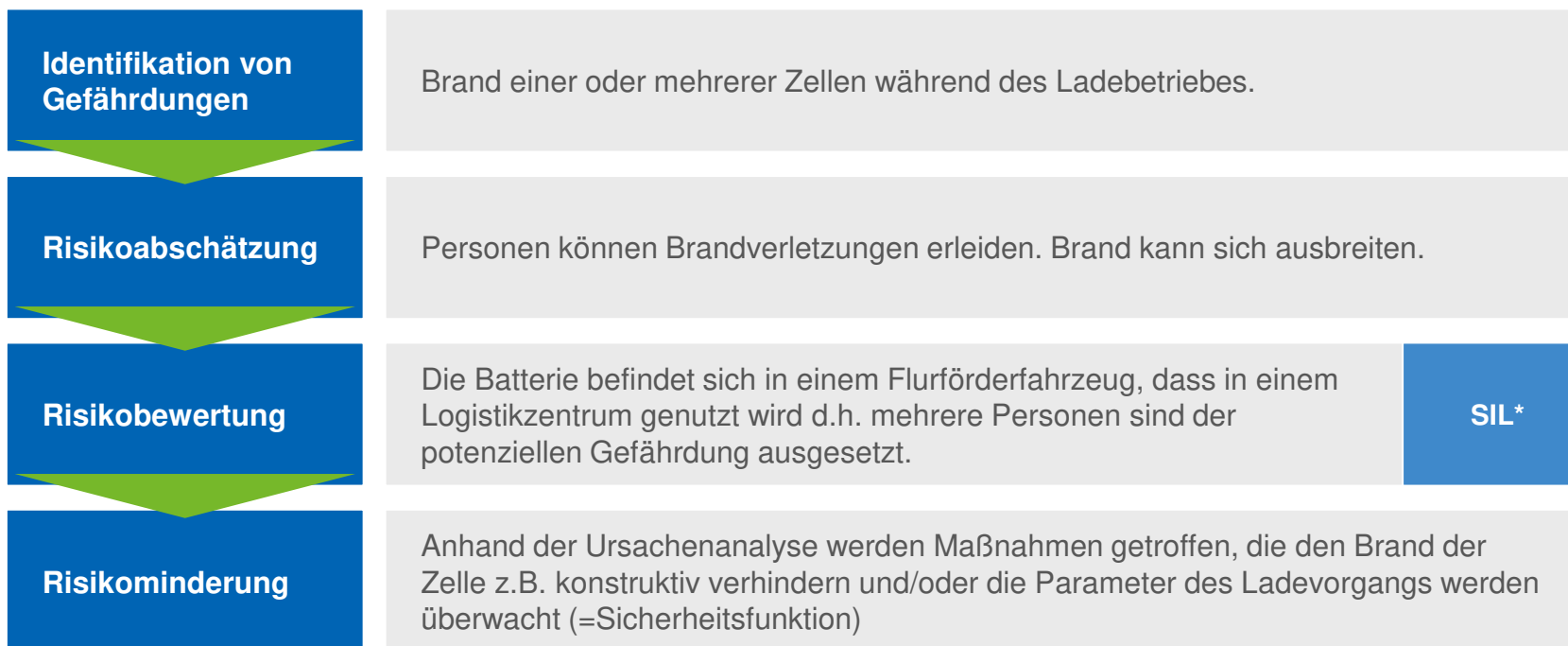
Quelle: [1] ISO26262-1

Funktionale Sicherheit – Relevante Standards



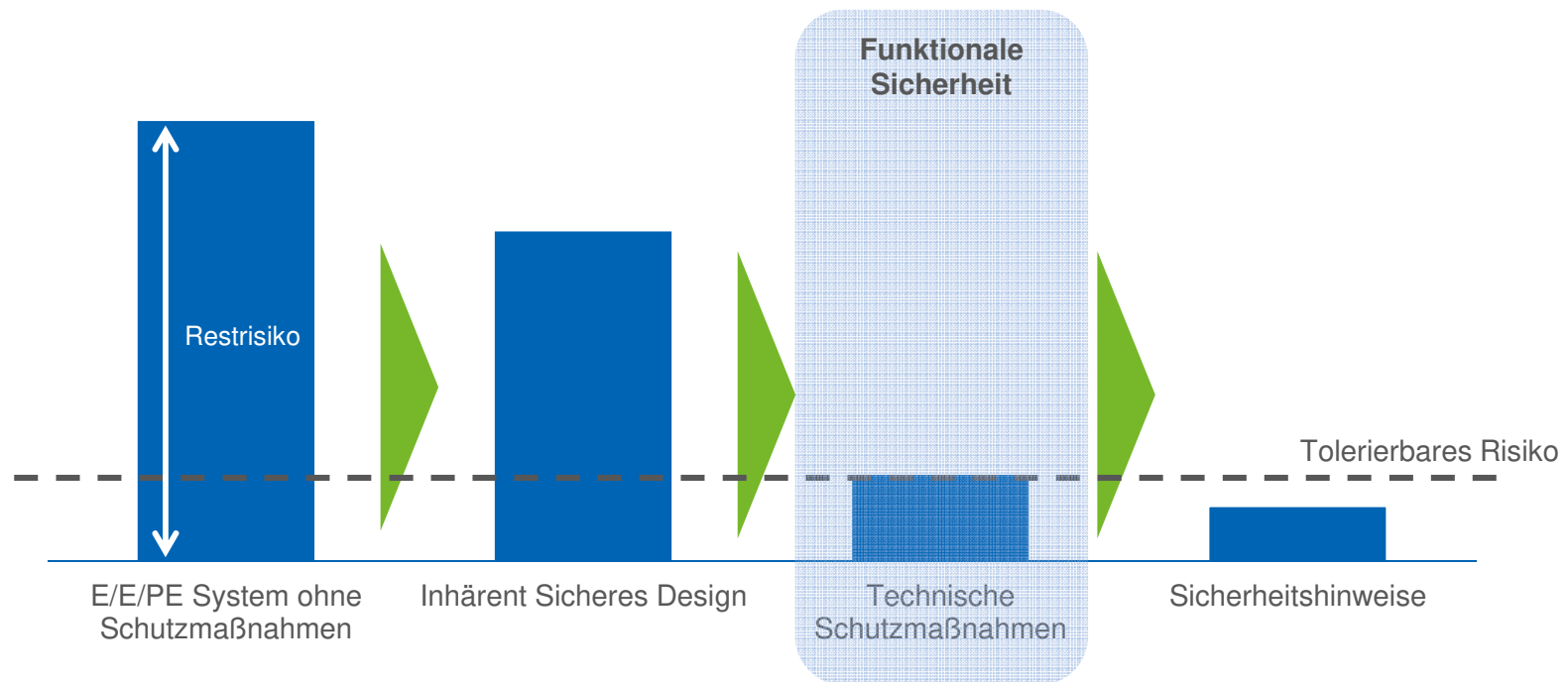
Die **neue Niederspannungsrichtlinie LVD** (seit 20. April 2016) fordert die Durchführung und Dokumentation einer **geeigneten Gefährdungs- & Risikoanalyse**.

Gefährdungs- und Risikoanalyse



Fußnote: *Sicherheitsintegritätslevel nach IEC61508

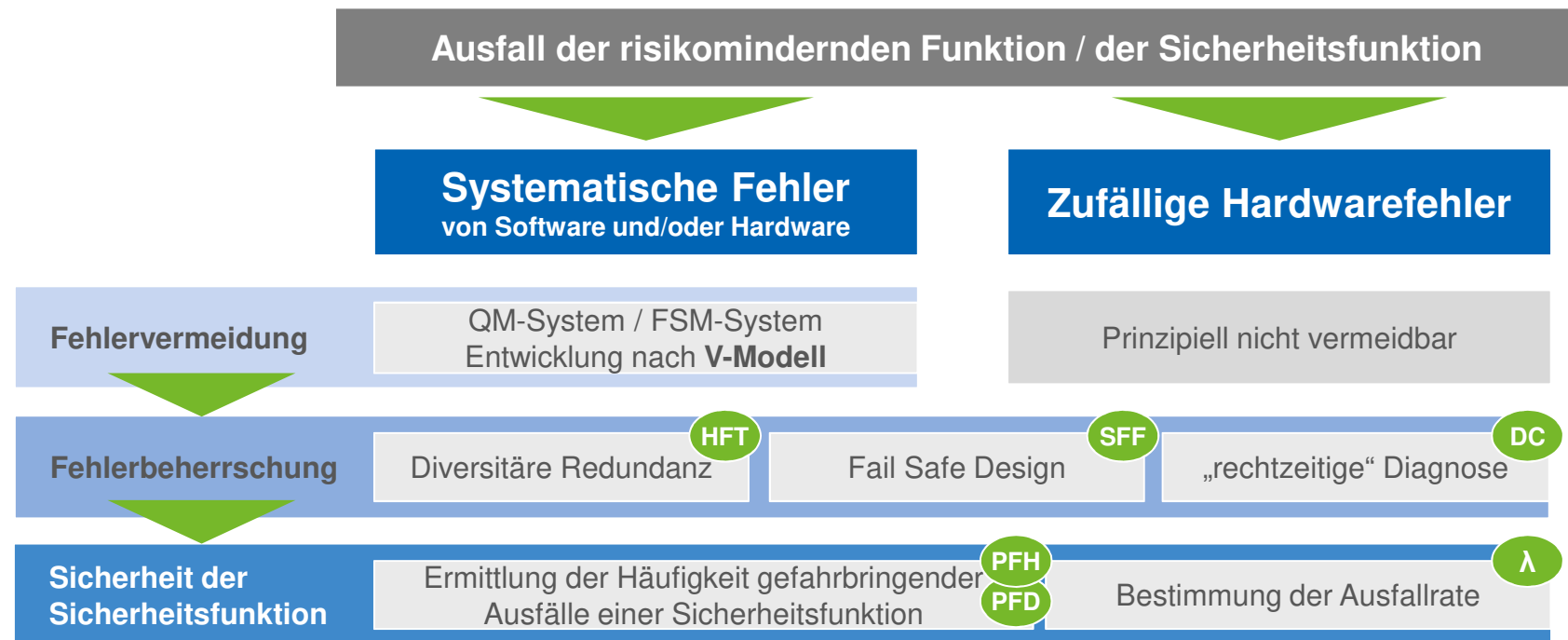
Mehrstufige Risikoreduzierung



Realisierung von Sicherheitsfunktionen



Sichere Auslegung von Sicherheitsfunktionen



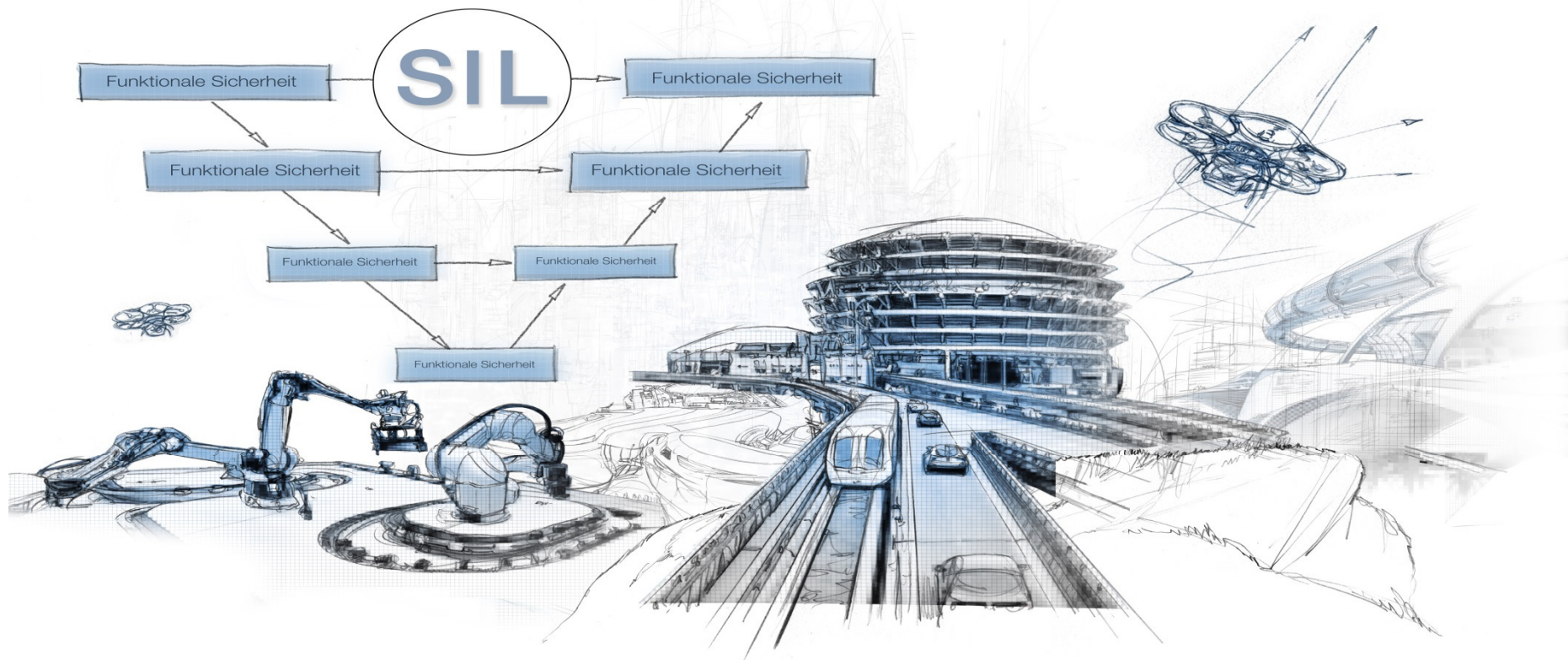
Anforderungen an Sicherheitsfunktionen in Abhängigkeit des zu erreichenden Sicherheitsintegritätslevels



Anteil sicherer Ausfälle eines Elements (SFF) (DC)	Hardwarefehlertoleranz (HFT)		
	0	1	2
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Sicherheits-Integritätslevel (SIL)	Mittlere Wahrscheinlichkeit eines gefährbringenden Ausfalls bei Anforderung der Sicherheitsfunktion (PFD _{avg}) (PFD)	Sicherheits-Integritätslevel (SIL)	Mittlere Häufigkeit eines gefährbringenden Ausfalls der Sicherheitsfunktion [h ⁻¹] (PFH) (PFH)
4	≥ 10 ⁻⁵ bis < 10 ⁻⁴	4	≥ 10 ⁻⁹ bis < 10 ⁻⁸
3	≥ 10 ⁻⁴ bis < 10 ⁻³	3	≥ 10 ⁻⁸ bis < 10 ⁻⁷
2	≥ 10 ⁻³ bis < 10 ⁻²	2	≥ 10 ⁻⁷ bis < 10 ⁻⁶
1	≥ 10 ⁻² bis < 10 ⁻¹	1	≥ 10 ⁻⁶ bis < 10 ⁻⁵

Quelle: [2] DIN EN 61508-2



Beispielhafte Anwendung in Energiespeichersystemen

Quelle



VDE-Studie im Rahmen des Förderprojektes „Anforderungen an die funktionale Sicherheit von Batteriemanagementsystemen in Elektrofahrzeugen mit Li-Ionen Batterien“.

Normenunterstützende Untersuchung mit dem Ziel Sicherheitsfunktionen für Batteriemanagementsysteme (BMS) zu erarbeiten, die in Elektrofahrzeugen (z.B. Flurförderfahrzeuge, PEDELECs,...) eingesetzt werden können.

- Risikoanalyse für ein hypothetisches Flurförderfahrzeug
- Berücksichtigung der typischerweise zu erwartenden Anwendung und Betriebsbedingungen
- Erarbeitung eines allg. Vorschlages, der als Mindestanforderung interpretiert werden kann.
- Basis für weitere konkrete Risikoanalysen

VDE



Anforderungen an die funktionale Sicherheit von Batteriemanagementsystemen in Elektrofahrzeugen mit Li-Ionen Batterien (AP6)

Ersteller: Süleyman Berber, Jörg Vössing

Erstelldatum: 2016-04-13

Stand: 2016-04-13

Typische, sicherheitsrelevante Eigenschaften einer LI-IONEN-Batterie



Thermal Runaway



Überladung

(z.B. durch Überhitzung beim Ladevorgang)

Tiefenentladung

(z.B. durch unsachgemäße Lagerung)

Quelle: [3] Berber/Vössing

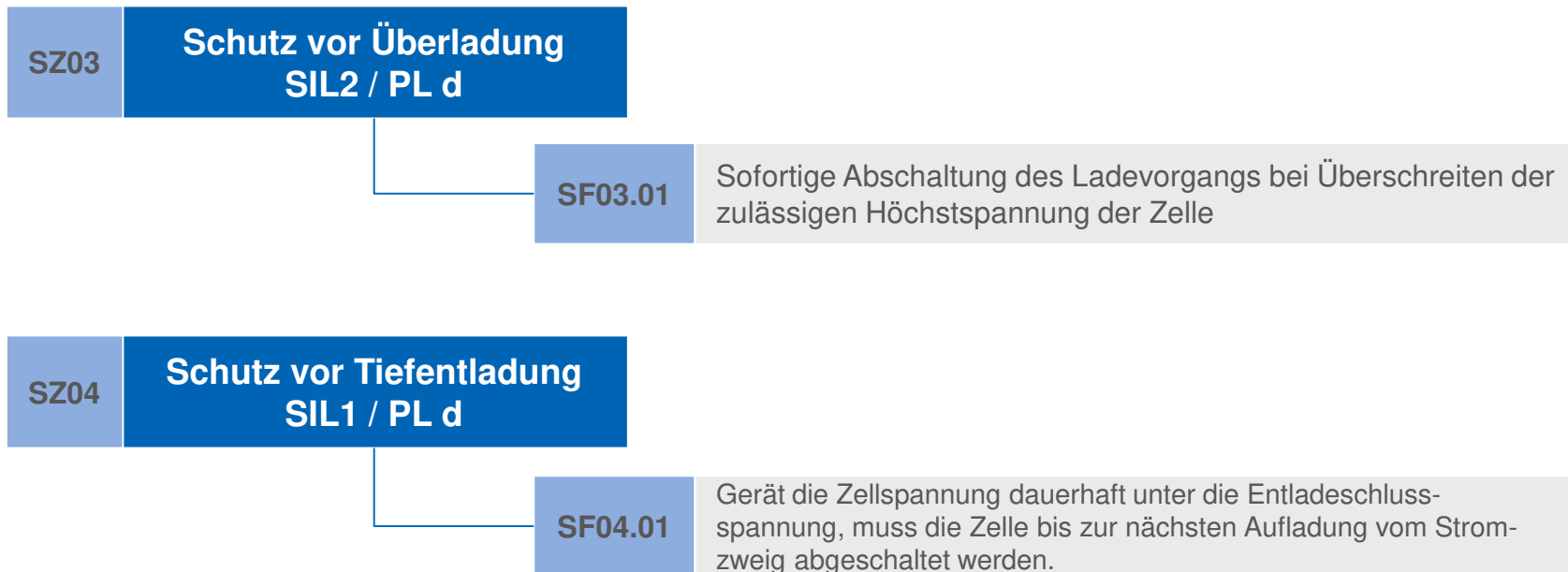
Mögliche Sicherheitsziele für ein LI-IONEN-Energiespeichersystem



SZ	Titel	Kurzbeschreibung	SIL *	PL *
01	Schutz vor Übertemperatur	Die Zelle soll im sicheren Temperaturbereich betrieben werden.	2	e
02	Schutz vor Ladung bei Untertemperatur	Die Zelle soll im sicheren Temperaturbereich geladen werden.	2	e
03	Schutz vor Überladung	Die Zelle soll im sicheren Spannungsbereich geladen werden.	2	d
04	Schutz vor Tiefenentladung	Die Zelle soll im sicheren Spannungsbereich betrieben werden.	1	d
05	Schutz vor Überstrom	Die Zelle soll im sicheren Stromstärkebereich betrieben werden.	2	e

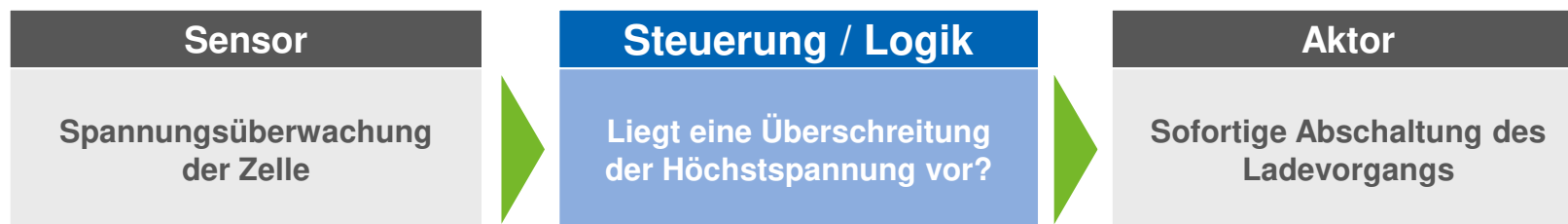
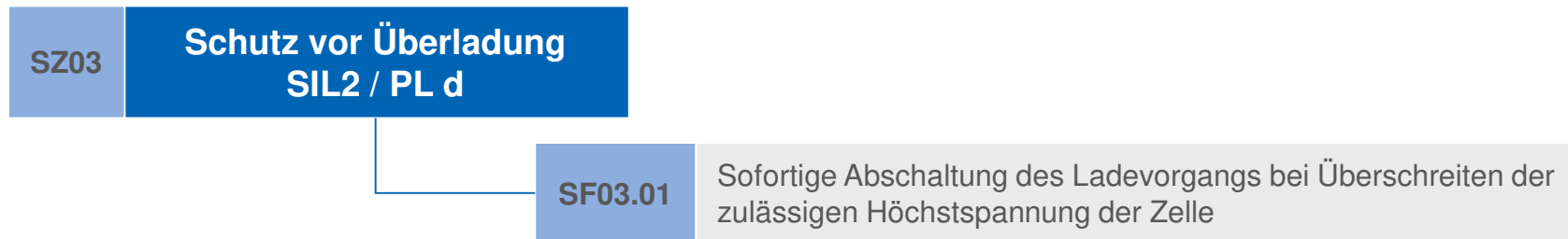
Quelle: [3] Berber/Vössing Fußnote: *SIL nach IEC61508, PL nach ISO13849

Mögliche Sicherheitsfunktionen

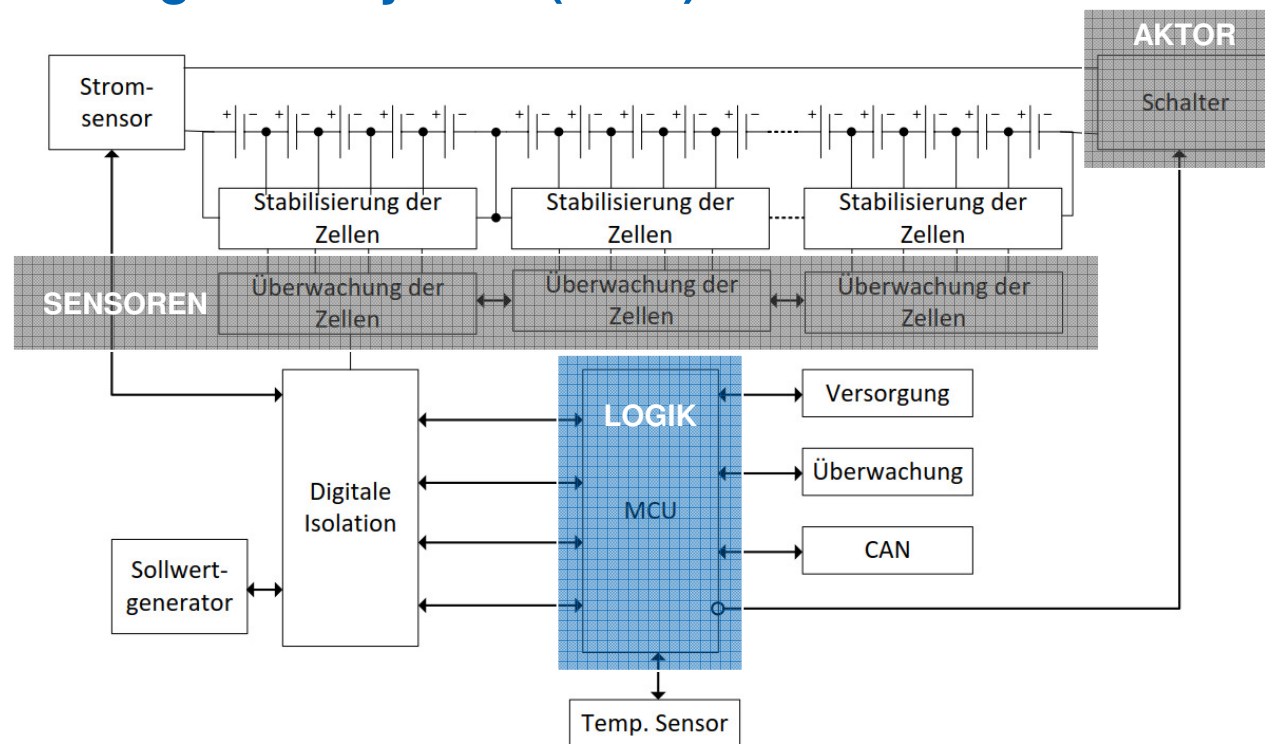


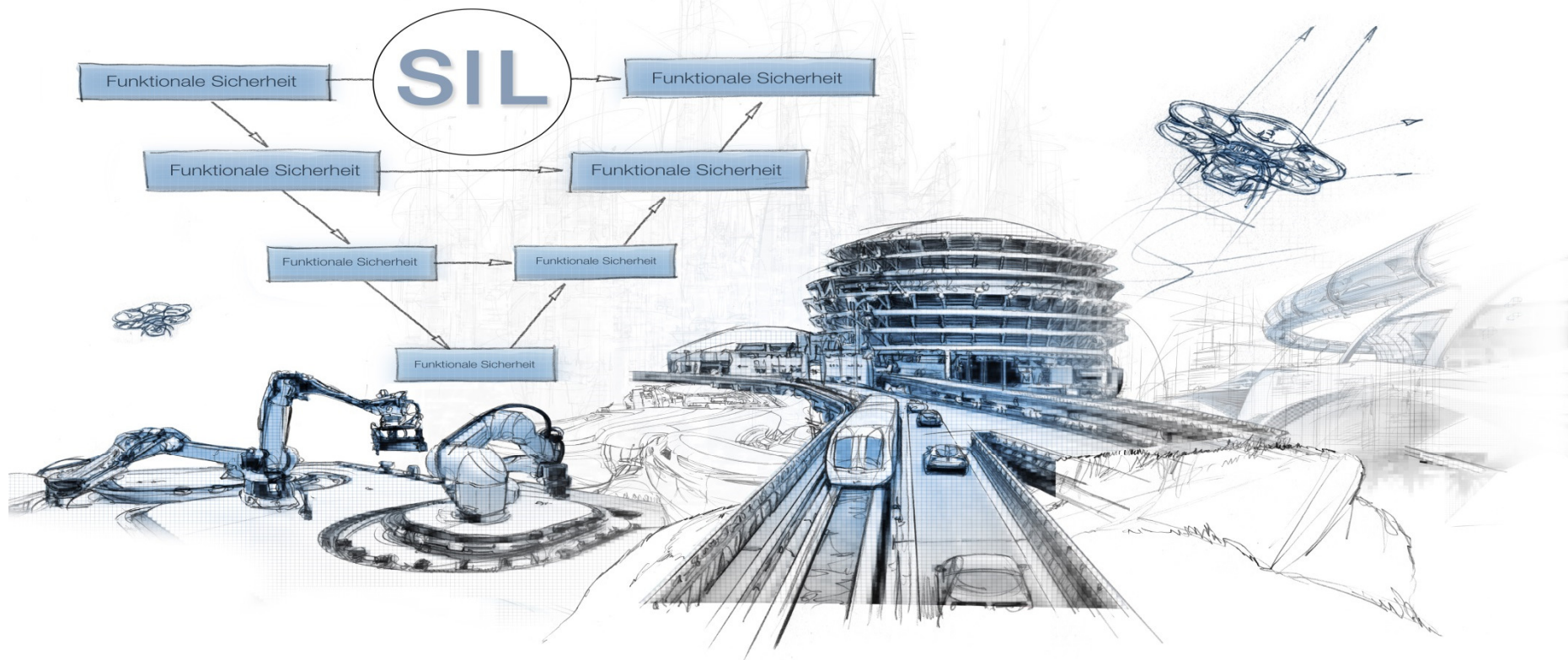
Quelle: [3] Berber/Vössing

Beispielhafte Umsetzung einer Sicherheitsfunktion



Umsetzung der Sicherheitsfunktion in einem Batteriemanagementsystem (BMS)





Beitrag des VDE – Prüf- & Zertifizierungsinstitutes

VDE INSTITUT

Beitrag des VDE – Prüf- & Zertifizierungsinstitutes



www.VDEinfo.com
ID. 49000000



www.VDEinfo.com

- Normen fordern die Beurteilung durch eine **unabhängige Drittstelle** für Systeme, die **höhere Risiken (ab SIL3)** mit sich bringen können (Maschinen, Steuerungen, Leitsysteme, Fahrzeuge...)
- Die **Zertifizierung** der Funktionalen Sicherheit ist ein wichtiger Beitrag, um die **Sicherheit des Produkts**, aber auch seine Konformität mit dem Stand der Technik darzustellen

Das VDE **Eigenschaftszertifikat** „Funktionale Sicherheit“

- Die Zertifizierung ist nach verschiedenen Normen für **Produkte und Systeme** möglich
- Die Zertifizierung erfolgt nur, wenn die **generelle Sicherheit des Produkts** außer Frage steht
- Neben der Zertifizierung kann der VDE **weitere Unterstützung** für den Kunden leisten

VDE INSTITUT

Beitrag des VDE – Prüf- & Zertifizierungsinstitutes



Training	Projektdefinition
Training zu Grundlagen der Funktionalen Sicherheit beim Kunden.	Workshop zur Projektdefinition einschließlich Beratung bezüglich anwendbarer Normen.
Gefährdungs- und Risikoanalyse	Entwicklungsbegleitung
Moderation und methodische Bewertung von Gefährdungs- und Risikoanalysen .	Entwicklungsbegleitende Bewertung der Funktionalen Sicherheit während der einzelnen Phasen des Sicherheits-Lebenszyklus‘
Prozessanalyse	Informationen
Prozessanalyse zur Erlangung eines effizienten Funktionalen Sicherheitsmanagementsystems.	Information über aktuelle Entwicklungen in der Normung zu Funktionaler Sicherheit.

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Christoph Eggert

Smarte Technologien und Industrie (IoT)
Funktionale Sicherheit & Risikoanalysen

Tel.	+49 69 8306-209
Mobil.	+49 170 1874793
Mail.	christoph.eggert@vde.com



VDE INSTITUT

Quellenverzeichnis



[1] ISO26262-1:2011, Road Vehicles – Functional Safety – Part 1: Vocabulary

[2] IEC 61508-2 (VDE 0803-2):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrische/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronischer/programmierbarer elektronischer Systeme

[3] Berber, S. / Vössing, J.: Anforderungen an die funktionale Sicherheit von Batteriemanagementsystemen in Elektrofahrzeugen mit Li-Ionen Batterien. Offenbach 2016.

Glossar (1/2)



Systematischer Fehler

Designfehler, Produktionsfehler, z.B. Ungeeignete Architektur

Zufälliger Hardwarefehler

Zufälliges Zusammentreffen unterschiedlicher Ereignisse z.B. Alterung

HFT - Hardwarefehlertoleranz

Die Hardwarefehlertoleranz (HFT) ist die Fähigkeit eines Systems, eine Sicherheitsfunktion bei Bestehen von Fehlern weiter korrekt auszuführen. Eine HFT von N bedeutet, dass N+1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.

SFF - Safe Failure Fracture / Anteil sicherer Ausfälle

Die Safe Failure Fraction (SFF) beschreibt den prozentualen Anteil von Ausfällen ohne Potenzial, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.

DC - Diagnostic Coverage / Diagnosedeckungsgrad

Anteil der gefahrbringenden Ausfälle, die durch automatische diagnostische Online-Prüfungen erkannt werden.

Glossar (2/2)



PFD - Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung

Sicherheitsbezogene Nichtverfügbarkeit eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion auszuführen, wenn von der EUC oder dem EUC-Leit- und Steuerungssystem eine Anforderung erfolgt.

PFH

Mittlere Häufigkeit eines gefahrbringenden Ausfalls eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion über einen gegebenen Zeitraum auszuführen.

Lambda λ – Ausfallrate

Ausfallwahrscheinlichkeit einer Einheit (einzelne Bauteile oder Systeme).

SIL – Safety Integrity Level

Sicherheitsintegritätslevel nach IEC 61508

PL – Performance Level

Sicherheitsintegritätslevel nach ISO 13849