Speziell angepasste Gefahrenanalyse / Risikobewertung für die Automobilindustrie nach ISO DIS 26262-3

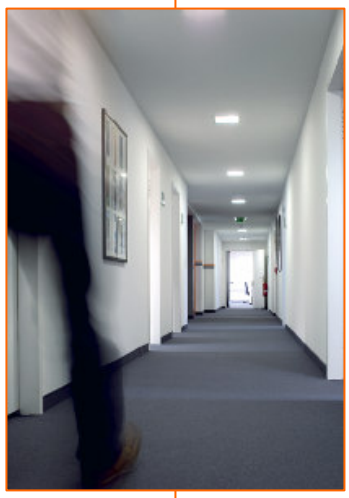
Gudrun Neumann, SGS Germany GmbH

Stand: 22/06/2010

WHEN YOU NEED TO BE SURE

SGS

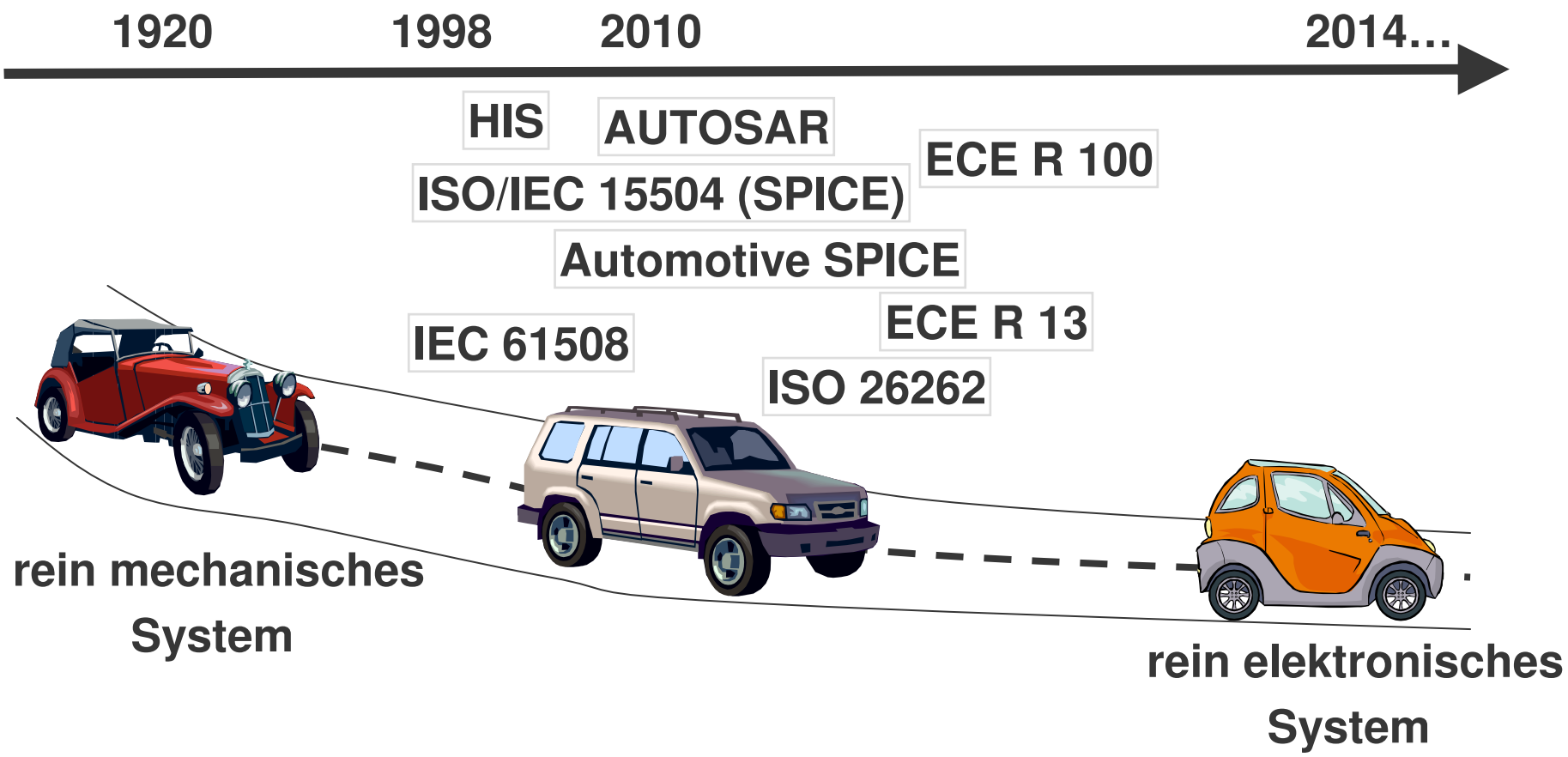
Vorstellung SGS Daten & Fakten



SGS - Société Générale de Surveillance

- 1878 in Rouen – Frankreich gegründet
- 1919 Umzug nach Genf
- Weltweit über 59.000 Mitarbeiter
- Globales Netzwerk aus mehr als 1.000 Niederlassungen und Laboren in über 140 Ländern
- Umsatz 2009: 4,7 Milliarden CHF

Zeitliche Entwicklung und Evolution



Allgemeines Konzept zur Risikominderung (nach IEC 61508-5)

Rest-Risiko

tolerierbares Risiko

System Risiko

notwendige Risikominderung

ansteigendes Risiko

aktuelle Risikominderung

Durch sicherheits-bezogene Systeme anderer Technologie abgedecktes Teilrisiko

Durch sicherheitsbezogene E/E/PE-Systeme abgedecktes Teilrisiko

Durch externe Einrichtungen abgedecktes Teilrisiko

Durch alle sicherheitsbezogenen Systeme und externe Einrichtungen zur Risikominderung erreichte Risikominderung

Risiko als Funktion

Risiko (R) = ~~F (f, C, S)~~ F(E, C, S)

- f (frequency): Wahrscheinlichkeit des Auftretens des gefährlichen Ereignisses, wobei f = F (E, λ)
  - E (exposure): Häufigkeit und Dauer des Aufenthaltes in der gefährlichen Situation
  - λ (lambda): Ausfallrate, die zu einem gefährlichen Ausfall einer Sicherheitsfunktion führen kann.
- C (controllability): Kontrollierbarkeit der gefährlichen Situation durch eine zeitliche Reaktion der beteiligten Personen
- S (severity): mögliches Schadensausmass

λ ist nach ISO DIS 26262 vernachlässigbar, wenn deren Anforderungen erfüllt sind.

Risikobeurteilungskriterien

- Aufenthaltswahrscheinlichkeit E (Exposure)
  - Von E0 (vernachlässigbar) bis E4 (>10% der durchschnittlichen Betriebsdauer bzw. im Durchschnitt in jeder Fahrsituation)
- Kontrollierbarkeit C (Controllability)
  - Von C0 (Situation gewöhnlich beherrschbar) bis C3 (Sehr schwer oder nicht zu kontrollierende Situation)
- Schadensausmass S (Severity)
  - Von S0 (keine Verletzung) bis S3 (lebensbedrohliche Verletzung)

Schadensausmass S (Severity)

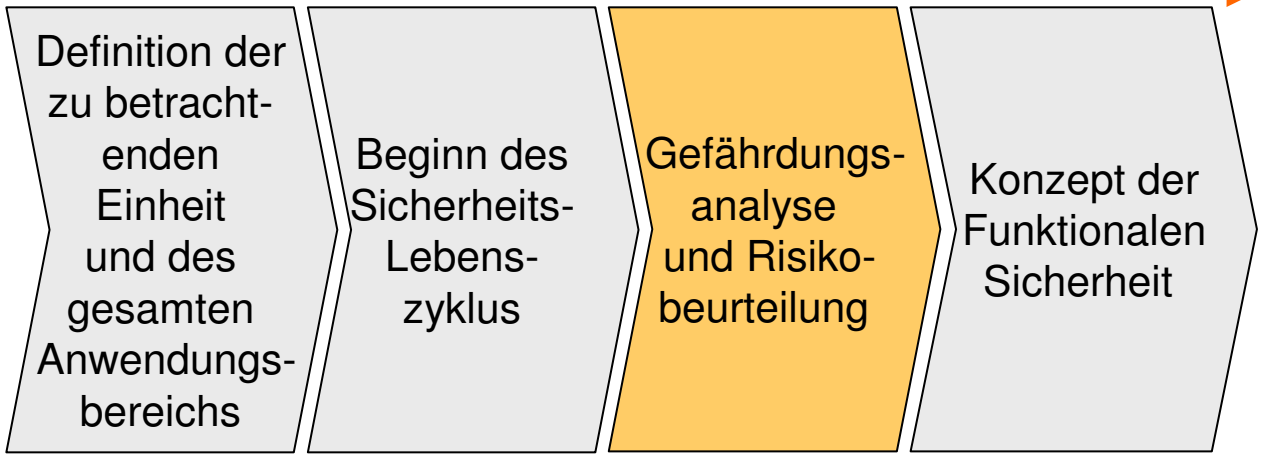
- Klassen von S nach ISO DIS 26262:
  - S0 (keine Verletzung)
  - S1 (leichte Verletzung)
  - S2 (schwere Verletzung)
  - S3 (lebensbedrohliche Verletzung)
- Definition der Klassen spezifisch für die Automobilindustrie; Beispiel eine Zuordnung zur AIS (Abbreviated Injury Scale):

Klasse	**S0**	**S1**	**S2**	**S3**
Referenz für einfache Verletzungen (nach AIS Skala)	AIS 0	> 10% Wahrscheinlichkeit von AIS 1-6 (und nicht S2 oder S3)	> 10% Wahrscheinlichkeit von AIS 3-6 (und nicht S3)	> 10% Wahrscheinlichkeit von AIS 5-6

„Stand der Technik“ für die Automobilindustrie

- ISO DIS 26262 (inklusive Teil 3, Kapitel 7 Gefährdungsanalyse und Risikobeurteilung (GuR))

Sicherheits- Lebenszyklus Zeitachse



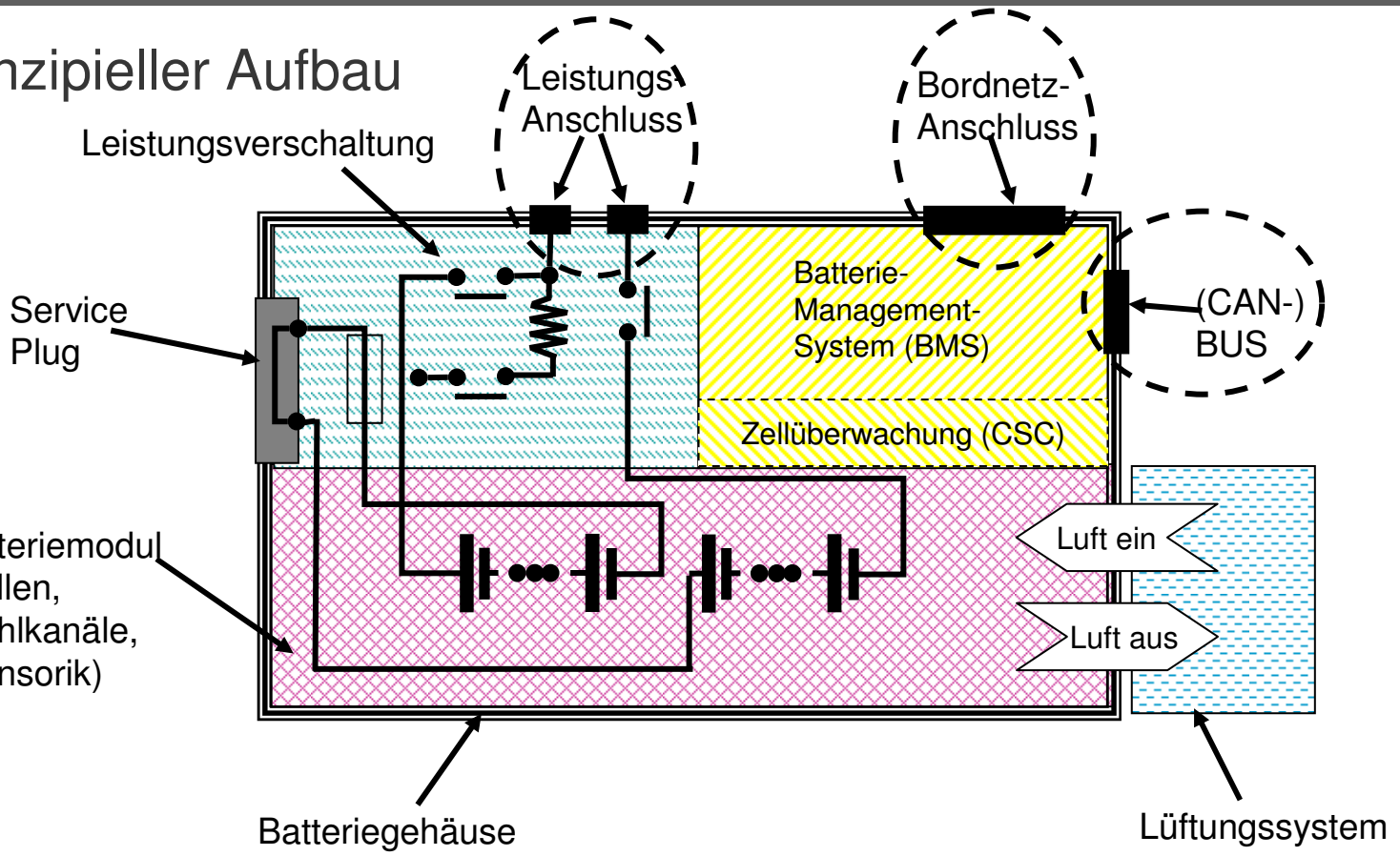
Vorgehensweise
Gefahrenanalyse und Risikobeurteilung (GuR)

Notwendige Schritte:

- Systemdefinition
- Festlegung der Grenzen
- Gefahrenanalyse
- Risikobeurteilung
- Zuordnung ASIL (Automotive Safety Integrity Level)
- Definition sicherer Zustand und Sicherheitsziel
- Verifikation der GuR
- Konzept zur Funktionalen Sicherheit

Systemdefinition
Beispiel eines Li-Ionen Batteriesystem

Prinzipieller Aufbau



Festlegung der Grenzen

- Betriebsbedingte Situationen
  - Verkehrssituationen und Fahrzeugnutzung
  - Umweltbedingungen
  - Vorhersehbares Verhalten des Fahrers
  - Interaktionen mit anderen Systemen des Fahrzeugs
- Betriebsmodi
  - Herstellung
  - Normalbetrieb
  - Service des Fahrzeugs
  - Entsorgung des Fahrzeugs

Gefahrenanalyse
Beispiele eines Li-Ionen Batteriesystem

Fehlfunktion

- Fehler im „Batterie Management System“ (BMS) führt zu einem kritischen Zustand der Batterie

Gefährdungsszenario I

- Parkendes Fahrzeug im Freien
- Batterie brennt oder explodiert

Gefährdungsszenario II

- Parkendes Fahrzeug in Garage neben Wohnhaus
- Batterie brennt oder explodiert
- Brand bleibt unentdeckt

Risikobeurteilungskriterien

- Aufenthaltswahrscheinlichkeit E (Exposure)
  - Von E0 (vernachlässigbar) bis E4 (>10% der durchschnittlichen Betriebsdauer bzw. im Durchschnitt in jeder Fahrsituation)
- Kontrollierbarkeit C (Controllability)
  - Von C0 (Situation gewöhnlich beherrschbar) bis C3 (Sehr schwer oder nicht zu kontrollierende Situation)
- Schadensausmass S (Severity)
  - Von S0 (keine Verletzung) bis S3 (lebensbedrohliche Verletzung)

Risikobeurteilung
Beispiele eines Li-Ionen Batteriesystem

Gefährdungsszenario I

- Schadensausmass: S1 (Gefahr für Passanten)
- Aufenthaltswahrscheinlichkeit: E4 (Hohe Wahrscheinlichkeit)
- Kontrollierbarkeit: C1 (einfach beherrschbar)

Gefährdungsszenario II

- Schadensausmass: S3 (Übergreifen von Feuer auf Wohngebäude)
- Aufenthaltswahrscheinlichkeit: E2 (Wenig wahrscheinlich)
- Kontrollierbarkeit: C3 (Sehr schwer oder nicht zu kontrollierende Situation)

Zuordnung ASIL
(Automotive Safety Integrity Level)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Definition sicherer Zustand und Sicherheitsziels Verifikation der GuR

- Definition des sicheren Zustandes

  Für beide Gefährdungsszenarien unseres Beispiels ist „Batterie brennt nicht und explodiert nicht“ der sichere Zustand.

- Definition des Sicherheitsziels

  Für beide Gefährdungsszenarien unseres Beispiels ist „Fehlfunktion des BMS führt nicht zu einem kritischen Zustand des Batteriesystems“ das Sicherheitsziel.

- Die Verifikation der GuR erfolgt durch Review der Dokumentation durch eine unabhängige Person oder Organisation.
- Eine Risikominimierung kann durch konstruktive, funktionale oder hinweisende Massnahmen erreicht werden.

Konzept zur Funktionalen Sicherheit
Beispiele eines Li-Ionen Batteriesystem

- Konstruktive Massnahmen
  - In diesem Fall wurden keine konstruktiven Massnahmen definiert.
- Funktionale Massnahmen
  - Überwachung des BMS auf Fehlfunktion und unabhängige Temperaturüberwachung
- Hinweisende Massnahmen
  - Regelmäßige Überwachung des Systems im Handbuch vorgegeben (z.B. durch Service, Hauptuntersuchung)
- Externe Einrichtungen zur Risikominimierung

Zusammenfassung

Gefahrenanalyse und Risikobeurteilung dient der

- Risikominimierung auf ein akzeptierbares Ausmass
- Identifikation aller sicherheitsrelevanten Funktionen
- Zuordnung eines ASIL und damit der sicherheitsrelevanten Anforderungen zu jeder Funktion

Vorteile

- Anforderungen an die Qualität und die Testtiefe ist durch den ASIL vorgegeben
- Vereinfachung der Wartung, da sicherheitsrelevante Funktionen klar definiert

Vielen Dank für Ihre Aufmerksamkeit!

SGS Germany GmbH
Gudrun Neumann
Hofmannstr. 50 · 81739 München
Telefon: +49 (0)89 787475-216
Telefax: +49 (0)89 787475-217

Internet: www.sgs-cqe.com
E-Mail: gudrun.neumann@sgs.com

WHEN YOU NEED TO BE SURE

SGS