FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Anpassung der Prozesslandschaft an moderne Safety-Anforderungen

Am Beispiel eines international tätigen Automotive Lieferanten

Erstellt von: Gerald Fritz

Inhalt

- ZKW Group, ZKW Elektronik
- Safety in Automotive
  - Functional Safety ISO 26262
- Safety bei ZKW Elektronik
  - Implementierung & Erfahrungen
  - Werkzeuge zur Unterstützung des Entwicklungsablaufes
  - Problemstelle Reliability Calculation

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

ZKW Group

Anbieter von Premium Lichtsystemen und Elektrik/Elektronik Modulen für Kraftfahrzeuge

- 5920 Mitarbeiter
- 750 Mio Umsatz

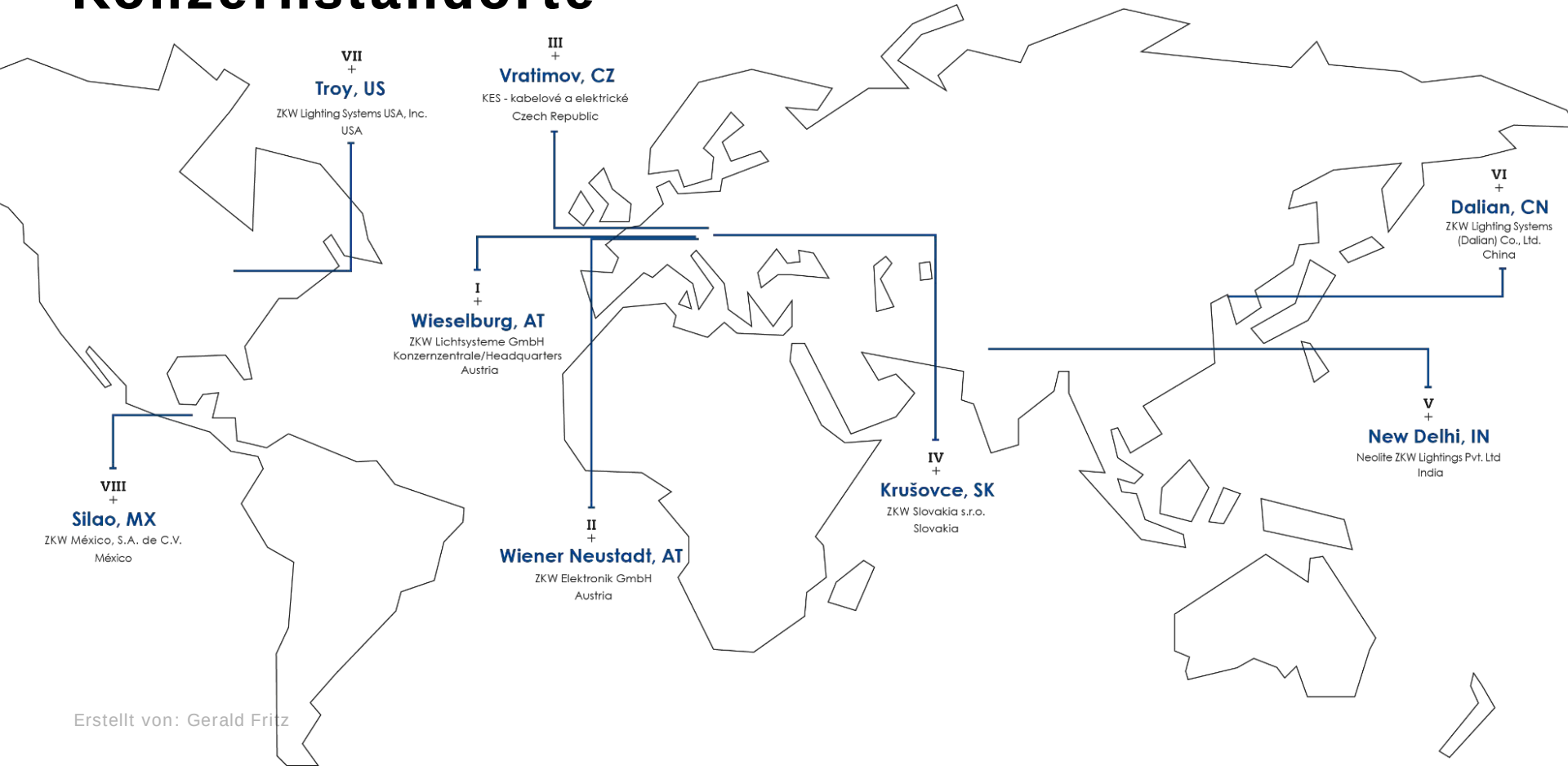
Erstellt von: Gerald Fritz

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Konzernstandorte



Erstellt von: Gerald Fritz

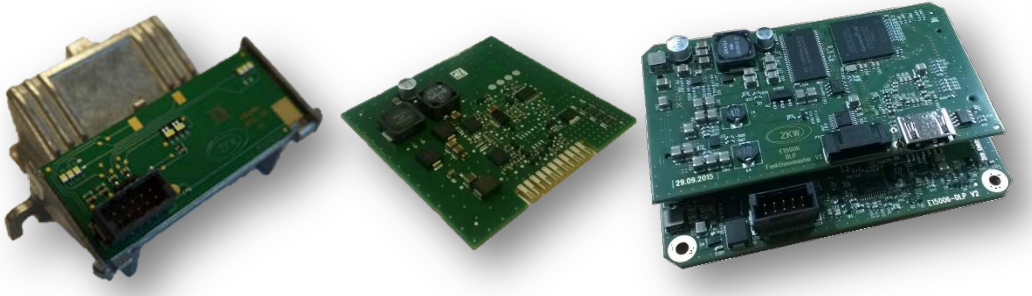
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

ZKW Elektronik

Kompetenzzentrum der ZKW Group für Elektronikentwicklung und -produktion

- Gegründet 2013
- 175 Mitarbeiter



Erstellt von: Gerald Fritz

Safety in Automotive

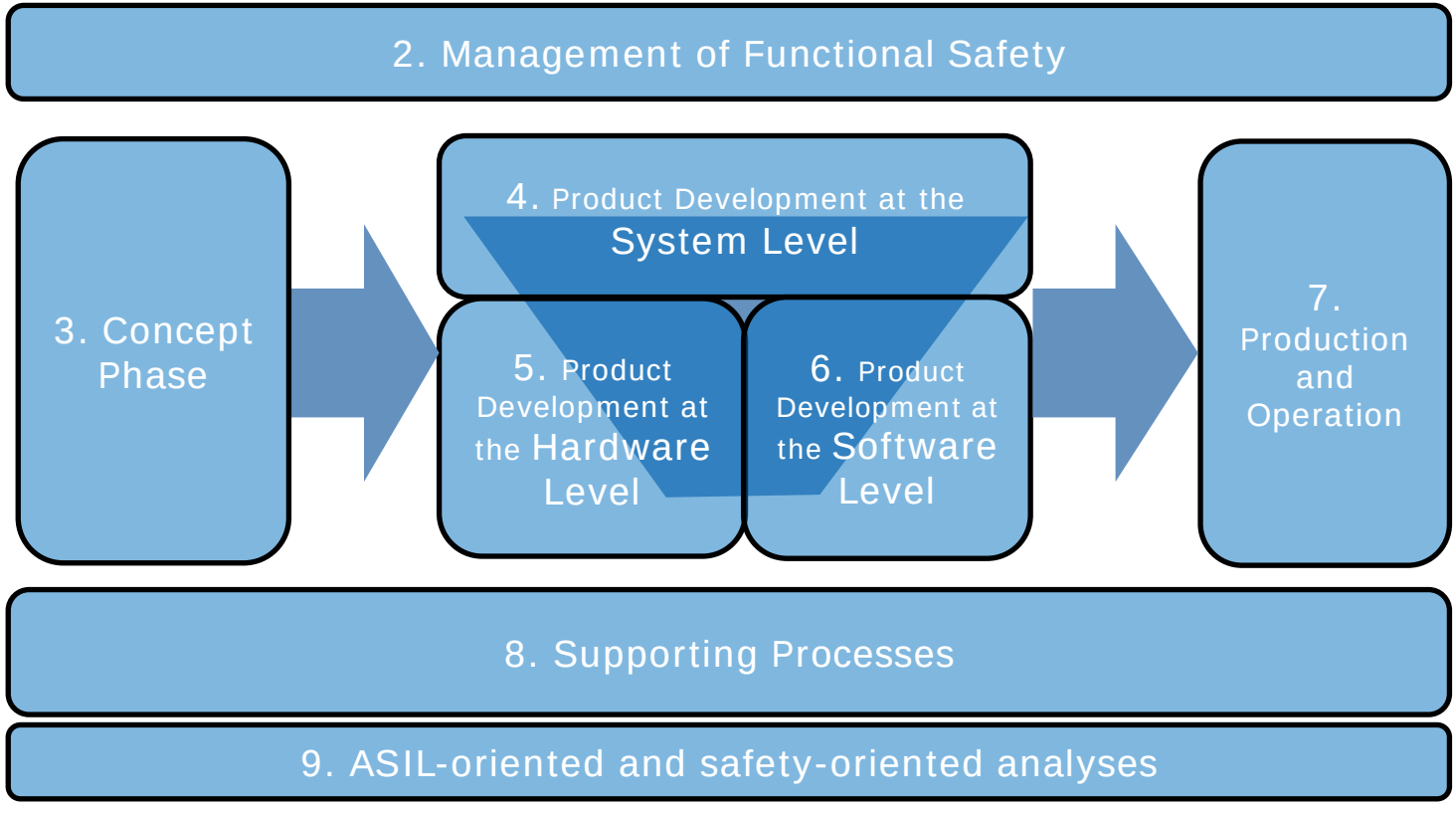
ISO 26262 Road vehicles – Functional Safety
herausgegeben m. **November 2011**
Die ISO 26262 basiert auf der IEC 61508 und wurde speziell für EE-Systeme (Elektrik/Elektronik) in Automotive angepasst.

Scope / Geltungsbereich
Wird bei sicherheitskritischen Systeme mit einem oder mehreren EE Systemen bei Serienproduktions Fahrzeugen unter 3500kg angewandt

D.h. davon ausgenommen sind Nutzfahrzeuge über 3,5t und einspurige Fahrzeuge (Abwandlungen in Arbeit)

Functional Safety
Stellt nicht die grundlegende Funktionalität der Systeme sicher, ebenso sind Gefährdungen durch beispielsweise Feuer, Rauch oder Stromschläge nicht direkt durch die ISO 26262 adressiert.

ISO 26262 Überblick



ASILs & Decomposition

ASIL	PMFH	FIT
Automotive Safety Integrity Level	Probabilistic Metric for random Hardware Failures	Fehler pro Milliarde Betriebsstunden
QM		
A		
B	$<10^{-7}$	100
C	$<10^{-7}$	100
D	$<10^{-8}$	10

Ermittlung ASIL

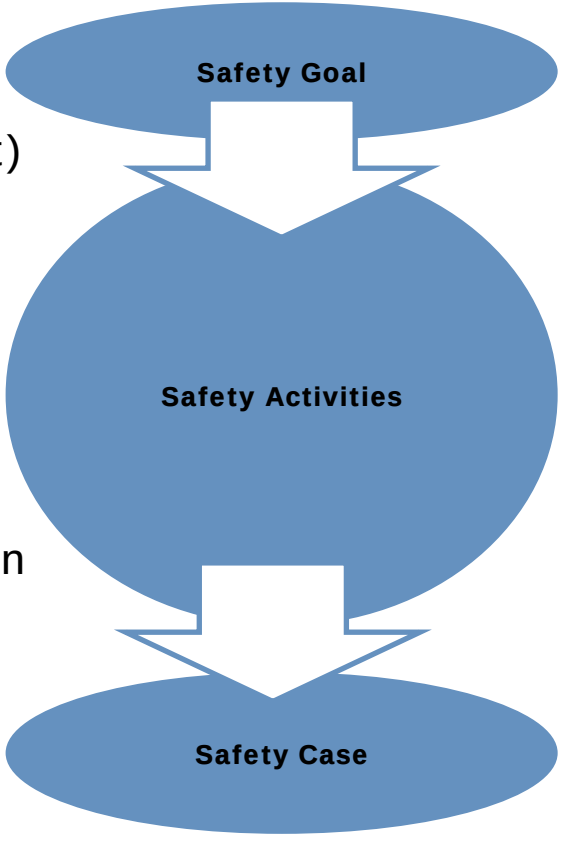
- Wird zumeist von den OEMs vorgenommen (System Level)

Severity class	Probability class	Controllability class		
		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

Safety Flow

- HARA → Festlegung der Safety Goals
- Definition der Functional Safety Requirements (Konzept)
- Umsetzung mittels Technical Safety Requirements (Entwicklung)
- Safety Assessments (Validierung)
- Zusammenfassung der Arbeitsergebnisse der Konzept- und Produktentwicklung im Safety Case

- Begleitende qualitative und quantitative Safety Analysen
  - FMEA (qualitativ und quantitativ)
  - FTA (qualitative und quantitative)
  - HAZOP (Hazard and Operability study)
  - Reliability Block Diagrams
  - Markov Models



FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Projekt ISO 26262 bei ZKW Elektronik

Planung & Vorarbeit

- Übergreifendes Projektteam definieren (ZKW)
- Projektteams an den Standorten (ZKW E)
- Auswahl Implementierungspartner
- Policy & Culture definieren

Trainings & Definition

- Trainings der Projektteams zur ISO 26262
- Erarbeitung der Prozesse im Unternehmen und Integration

Implementation & Evaluierung

- Implementierung im ersten Targetprojekt
- Interne und Externe Assessments

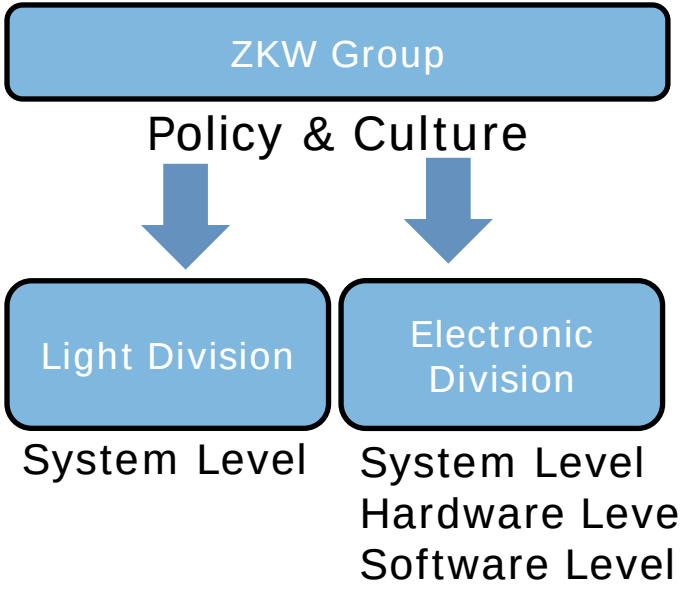
Verbesserung & Verbreitung

- Einarbeitung der erhobenen Verbesserungspotential
- Trainings anhand des definierten Prozesses im Unternehmen
- Definition von standardisierten Templates

Erstellt von: Gerald Fritz

Commitment des Unternehmens

- Auftrag der Unternehmensführung
- Zentrale Koordination der Safety Aktivitäten und Umsetzung der Anforderungen
- Fachspezifische Unterscheidungen in Abläufen und Umfang der Prozesse

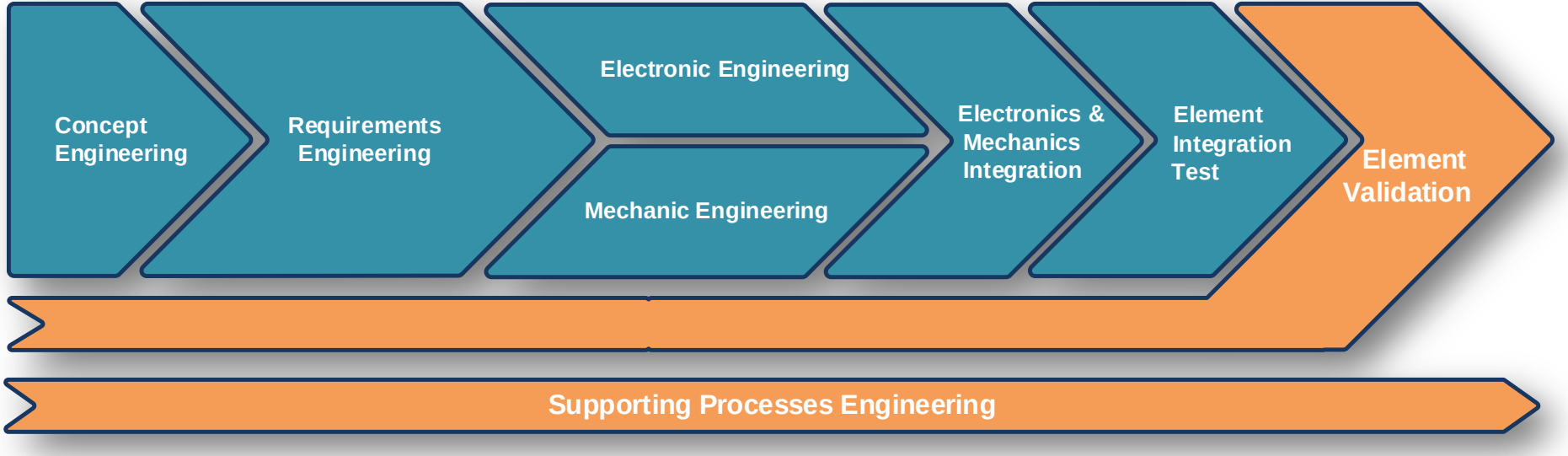


FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Integration in die Prozesslandschaft



Prozesslandschaft, Anforderungen

Integration der Safety spezifischen Punkte in den jeweiligen Prozess

- Beispielsweise wird ein Safety Requirement wird über ein Attribut identifiziert
- Die Verifikation und Validierung erfolgt zusätzlich nach Safety-Kritierien

Zusammenfassung

- Prozesseinführung ist ein Veränderungsprozess
- „Culture“ schaffen
- Entscheidungsträger in den betroffenen Bereichen einbinden
- Automotive Systemlieferanten
  - Mechatronische Systeme, alle sind betroffen
- QM Basisprozesse müssen etabliert sein
- Safety Anforderungen in Abläufe integrieren
- Lead Project eng einbinden und unterstützen
- Akzeptanz der Abläufe auch über integrierte Toollösungen erleichtern

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

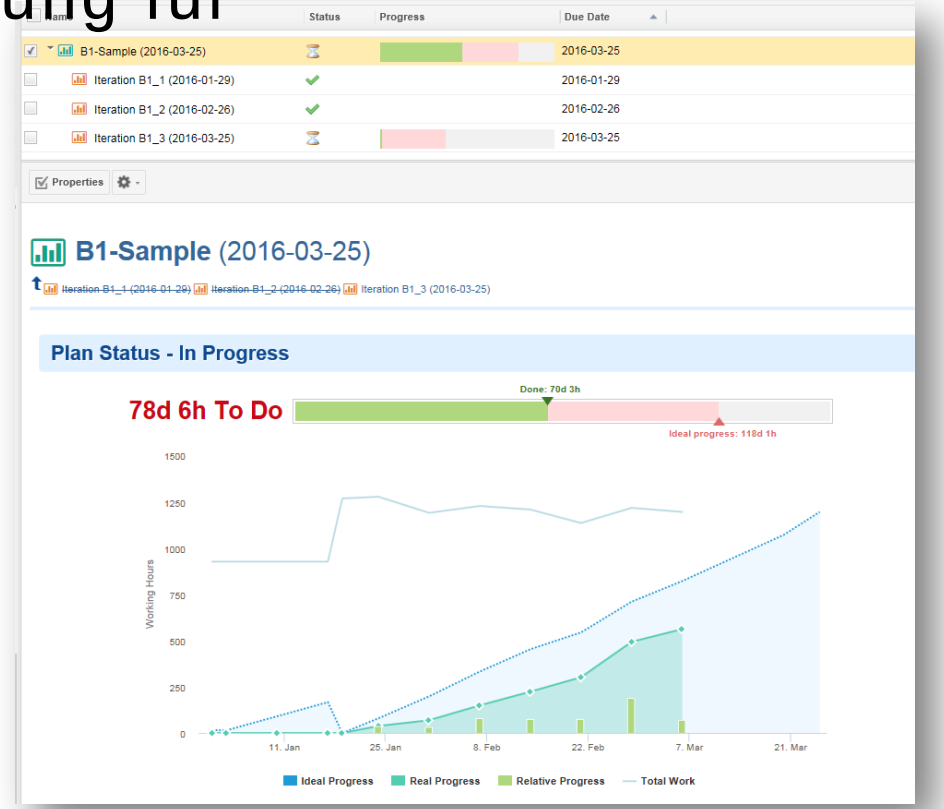
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Werkzeuge zur Unterstützung des Entwickungsablaufes

Eine zentrale Arbeitsumgebung für

- Requirements
- Testfälle
- Traceability
- Reports
- Plandokumente
- Defects
- Change Requests
- Design Descriptions
- Test Reports
- Test Runs
- Reviews
- Quality Assurance Records uvm.

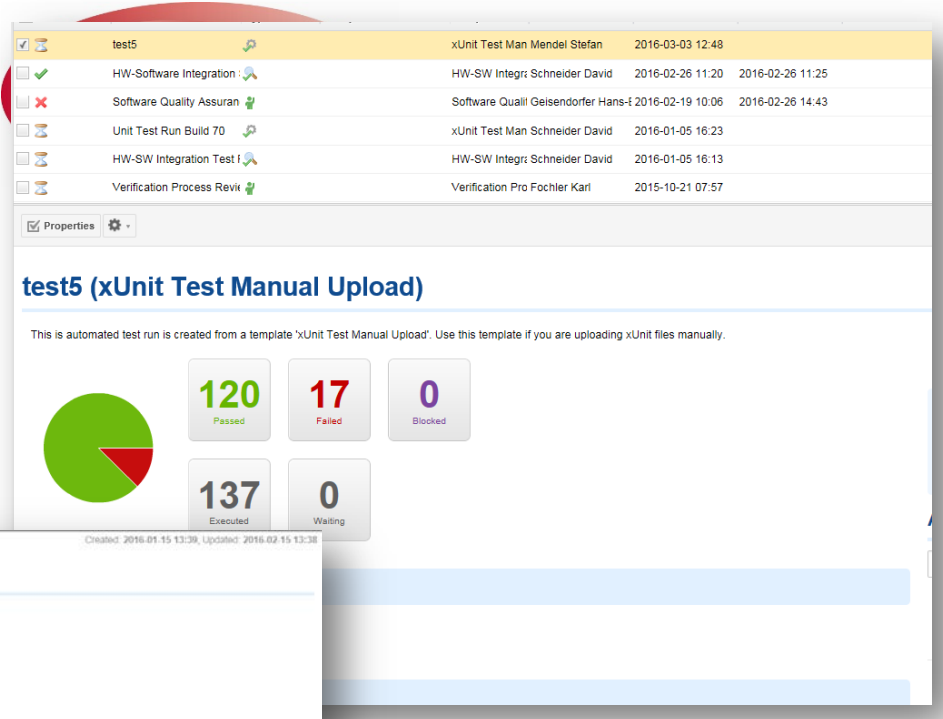


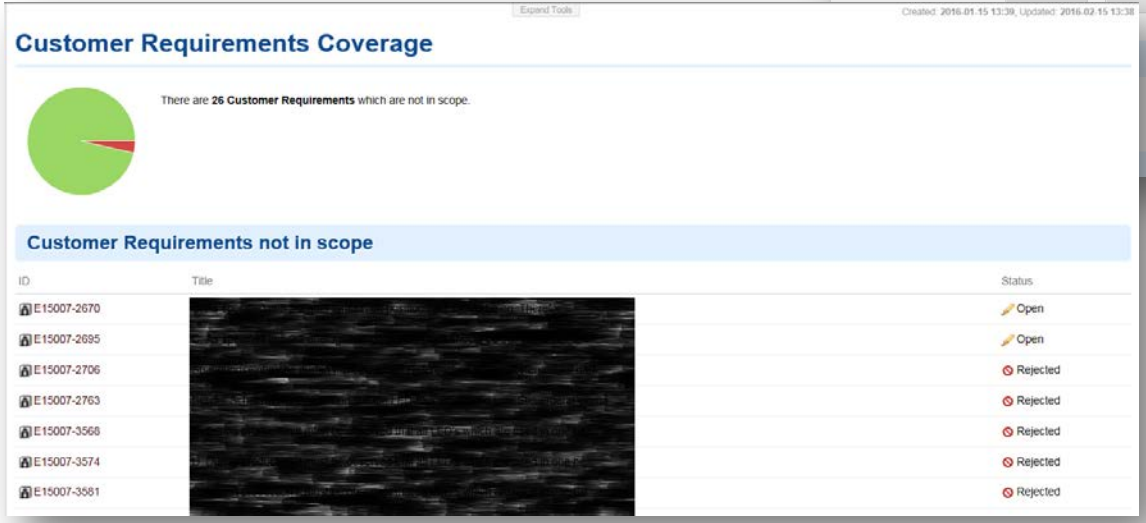
Erstellt von: Gerald Fritz

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

Reports





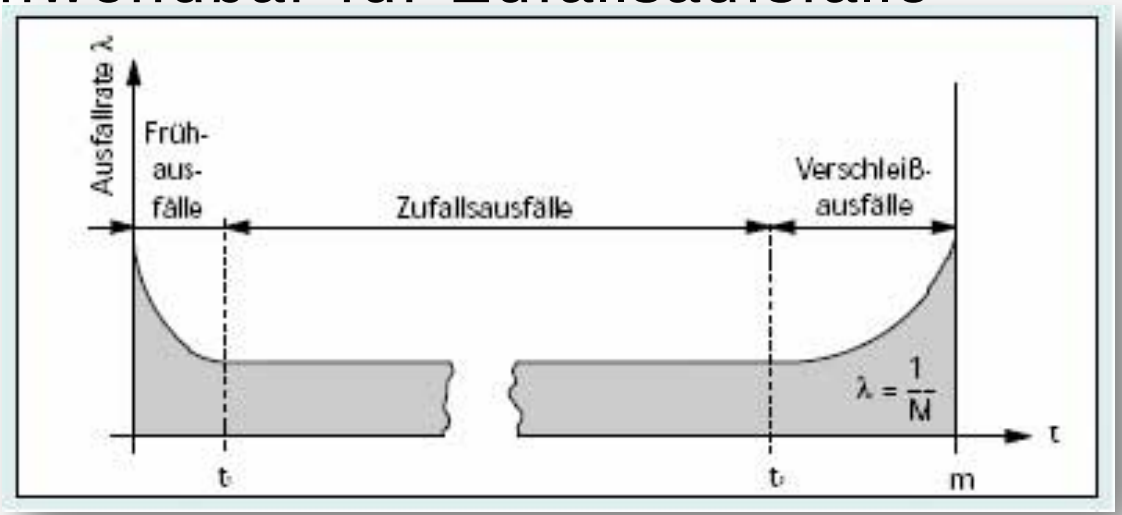
Erstellt von: Gerald Fritz

Problemstelle Reliability Calculation

- Reliability / Zuverlässigkeit von Systemen

Die Wahrscheinlichkeit, dass ein System innerhalb eines Intervass [0,t] fehlerfrei funktioniert.

Berechnung nur anwendbar für Zufallsaufsfälle



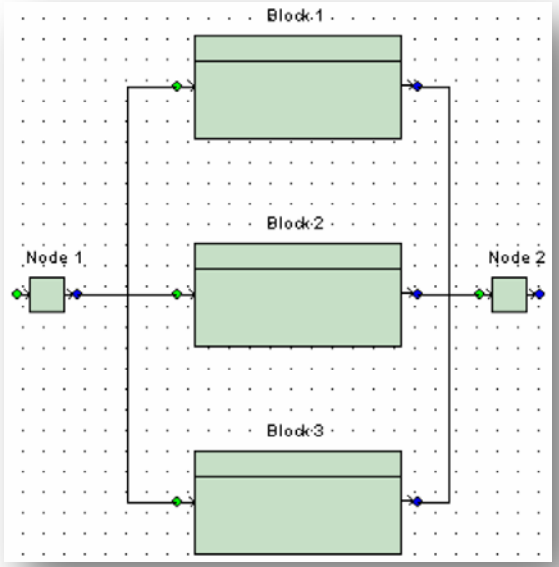
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

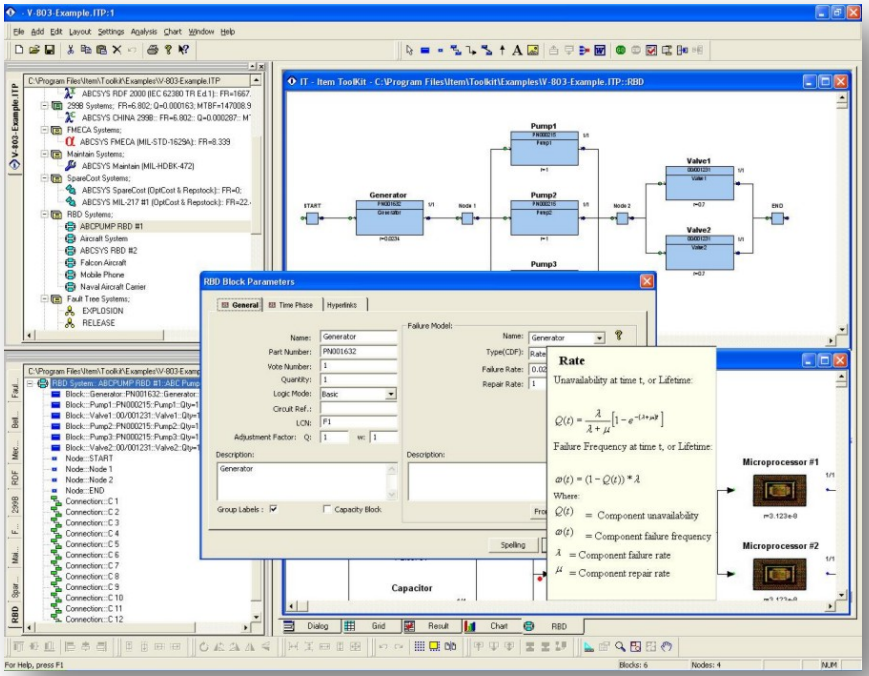
> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

ZKW

Problemstelle Reliability Calculation

Definition der System bzw. Elektronikarchitektur (Redundanzen, Komplexität) mittels RBD





Erstellt von: Gerald Fritz

Problemstelle Reliability Calculation

Target: 100 FIT

Automotive: Bauelemente nach AEC-Q qualifiziert

- FIT Rate eines neuen Bauelements

“insufficient field data as the parts are new...”

“based upon lifetesting, in the amounts as prescribed by AEC-Q100, with 0 failures found, we can calculate a failure rate <10FIT, with 60% Confidence Level, at a junction temperature of 55°C with an activation energy of 0.7eV”

- Berechnung in der Applikation:

Handbücher zur Bestimmung der FIT Raten der Bauelemente wie MIL HDBK 217 oder IEC 62380:2004

Ergibt bei z.B. 85°C Junction Temperature 80 FIT.