汽车行业
基于模型的功能安全分析

ANSYS SBU

会议议程

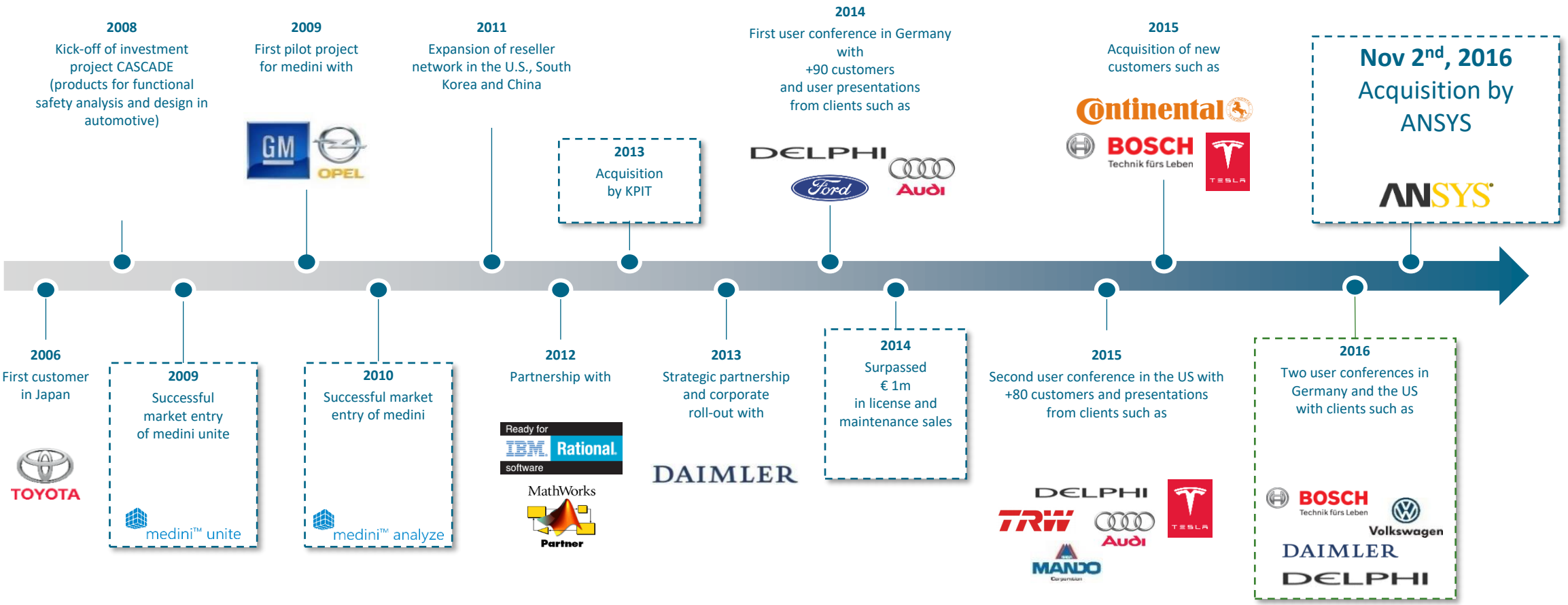
- 汽车领域的安全要求及挑战
- ANSYS medini 基于模型的系统安全解决方案
- ANSYS medini 在完整的ISO 26262 安全生命周期中的应用
- 小结

ANSYS medini: 综合安全分析解决方案

- 汽车功能安全、预期功能安全、信息安全、可靠性工程等综合解决方案的行业领导者
- 基于模型的方法，覆盖全生命周期，支持在概念、系统、软件、PCB、芯片级进行安全分析，确保追踪性和一致性
- 符合安全标准的最佳实践
- 内置大量高效的工程模板、检查单和失效率手册，支持复用和自动化，能够减少高达57%的工作和投入市场的时间

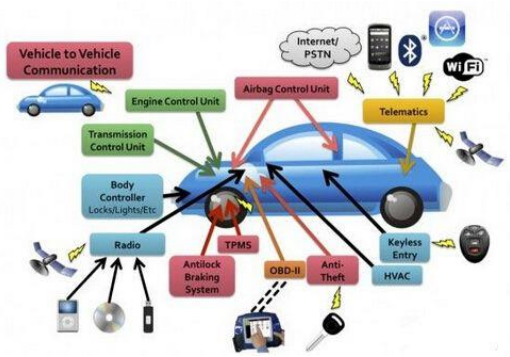
全球250+ 客户

产品历史


2006
First customer in Japan
TOYOTA
2008
Kick-off of investment project CASCADE (products for functional safety analysis and design in automotive)
2009
Successful market entry of medini unite
medini™ unite
2009
First pilot project for medini with
GM
OPEL
2010
Successful market entry of medini
medini™ analyze
2011
Expansion of reseller network in the U.S., South Korea and China
2012
Partnership with
Ready for
IBM Rational
software
MathWorks
Partner
2013
Acquisition by KPIT
2013
Strategic partnership and corporate roll-out with
DAIMLER
2014
First user conference in Germany with +90 customers and user presentations from clients such as
DELPHI
Ford
Audi
2014
Surpassed € 1m in license and maintenance sales
2015
Second user conference in the US with +80 customers and presentations from clients such as
DELPHI
TRW
Audi
TESLA
MANDO
2015
Acquisition of new customers such as
Continental
BOSCH
Technik fürs Leben
TESLA
2016
Two user conferences in Germany and the US with clients such as
BOSCH
Technik fürs Leben
Volkswagen
DAIMLER
DELPHI
Nov 2nd, 2016
Acquisition by ANSYS
ANSYS

汽车行业系统开发中的安全挑战

- 系统**复杂度不断增长**，电子化程度越来越高…



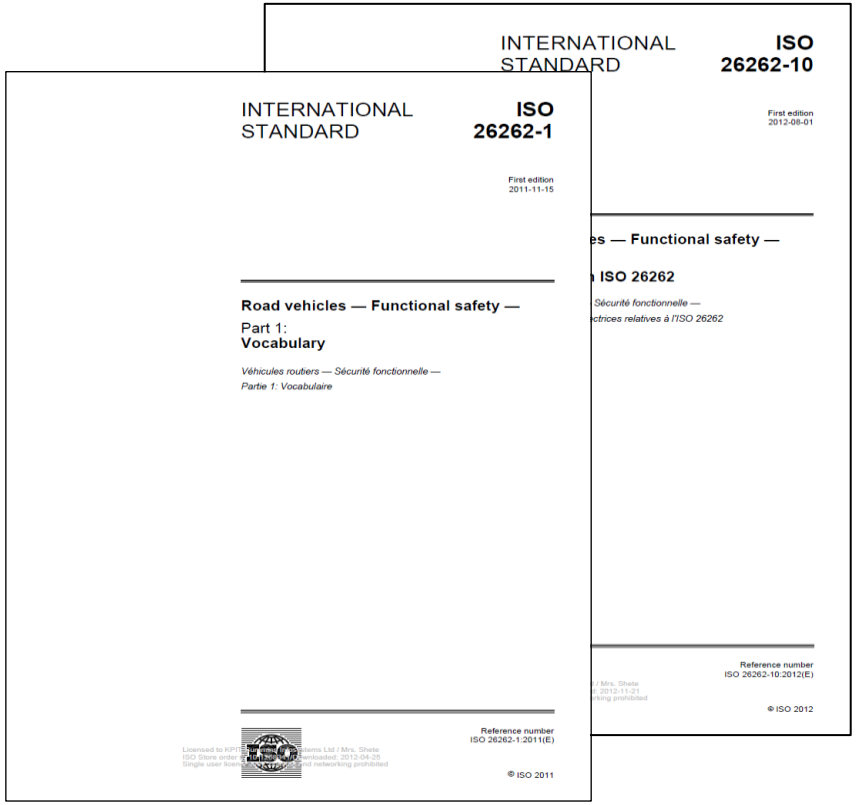
- 电子和软件**不断创新，安全相关的系统越来越多**
  - 自动驾驶 、 ADAS…
  - 主动被动安全系统…
  - 新能源汽车（BMS、CCU、VCU…）
  - 网络应用、信息安全
  - 芯片设计…

- 汽车安全事故增多引起整个行业对功能安全的关注→**安全相关活动贯穿整个开发过程**

汽车行业功能安全标准ISO 26262:2018

ISO-26262

- 汽车行业的功能安全
- 基于风险的特定方法
- 针对电子电气(E/E)系统
- 总重不超过3.5吨的量产乘用车
- *半导体、卡车、大巴和摩托车在2018年新版中涵盖*
- 管理系统失效与随机硬件失效
- 源于 IEC-61508



安全　　→ 不存在不可接受的风险

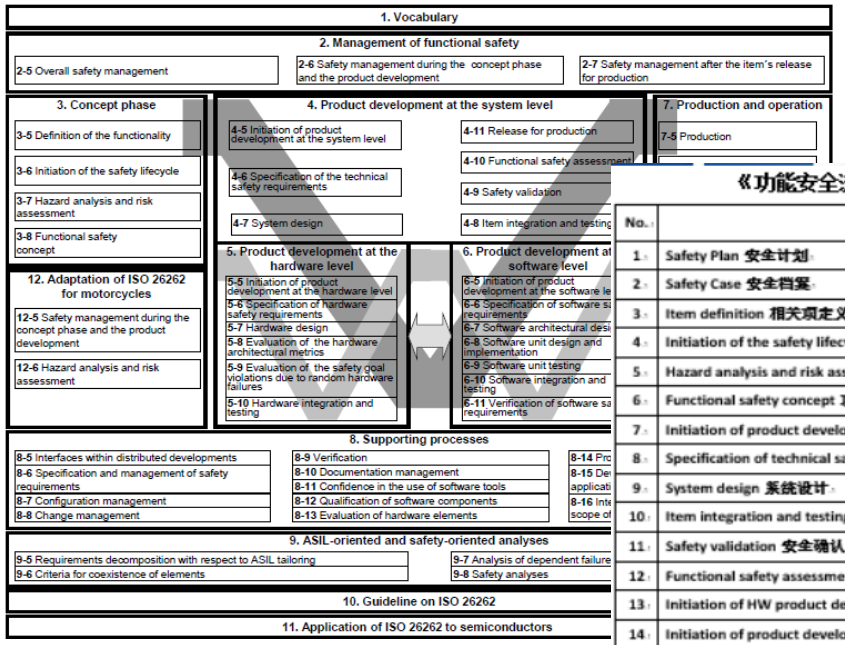
功能安全 →　不存在不可接受的E/E/系统功能失效造成的风险

汽车安全完整性等级　ASIL：QM,A,B,C,D

工程中有哪些功能安全相关活动?

安全活动

- 功能和故障识别
- 危害和可操作性分析– HAZOP
- 危害分析和风险评估– HARA
- 安全完整性等级确定- ASIL
- 安全目标和安全需求定义及管理
- 架构设计：从系统（SysML）到软硬件架构
- 可追溯性和分配



《功能安全流程开发体系》规范的框架

No.	内容
1	Safety Plan 安全计划
2	Safety Case 安全档案
3	Item definition 相关项定义
4	Initiation of the safety lifecycle 安全生命周期启动
5	Hazard analysis and risk assessment 危害分析和风险评估
6	Functional safety concept 功能安全概念
7	Initiation of product development at the system level 启动系统层面产品开发
8	Specification of technical safety requirements 技术安全要求的定义
9	System design 系统设计
10	Item integration and testing 相关项集成和测试
11	Safety validation 安全确认
12	Functional safety assessment 功能安全评估
13	Initiation of HW product development 启动硬件层面产品开发
14	Initiation of product development at the software level 启动软件层面产品开发
15	Specification of SW safety requirements 软件安全要求的定义
16	SW Architecture design 软件架构设计
17	SW Unit design and implementation 软件单元设计和实现
18	SW Unit testing 软件单元测试
19	SW integration and testing 软件集成和测试
20	Verification of SW safety requirements 软件安全要求的验证
21	Interfaces within distributed development 分布式开发接口
22	Specification and management of safety requirements 安全要求的定义和管理
23	Configuration management 配置管理
24	Change management 变更管理
25	Verification 验证
26	Documentation 文档化
27	Confidence in the use of software tools 软件工具置信度
28	Qualification of SW components 软件组件资质
29	Proven In Use argument 在用证明
30	Analysis of dependent failures 相关失效分析
31	Safety analyses 安全分析

安全分析

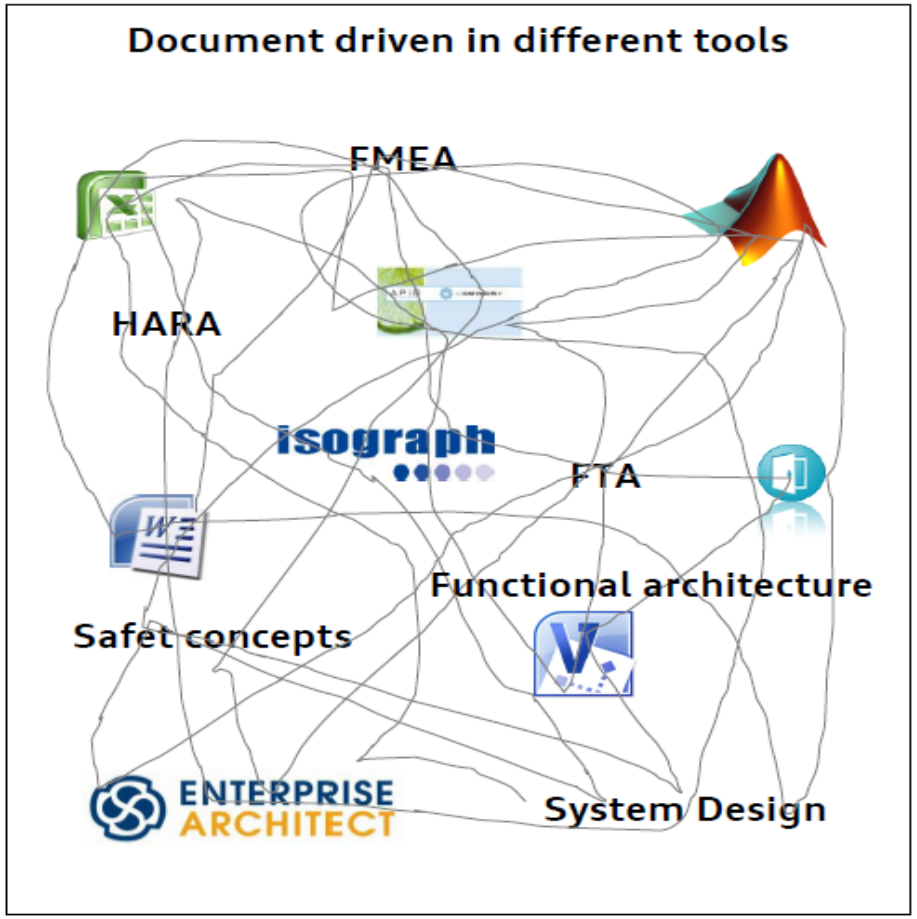
- 故障模式和影响分析– FMEA
- 故障模式，影响和诊断分析– FMEDA
- 故障树分析– FTA (定性&定量)
- 硬件指标计算（可靠性和概率计算）

安全项目管理

- 安全证据链的组织、报告
- 安全计划、安全案例

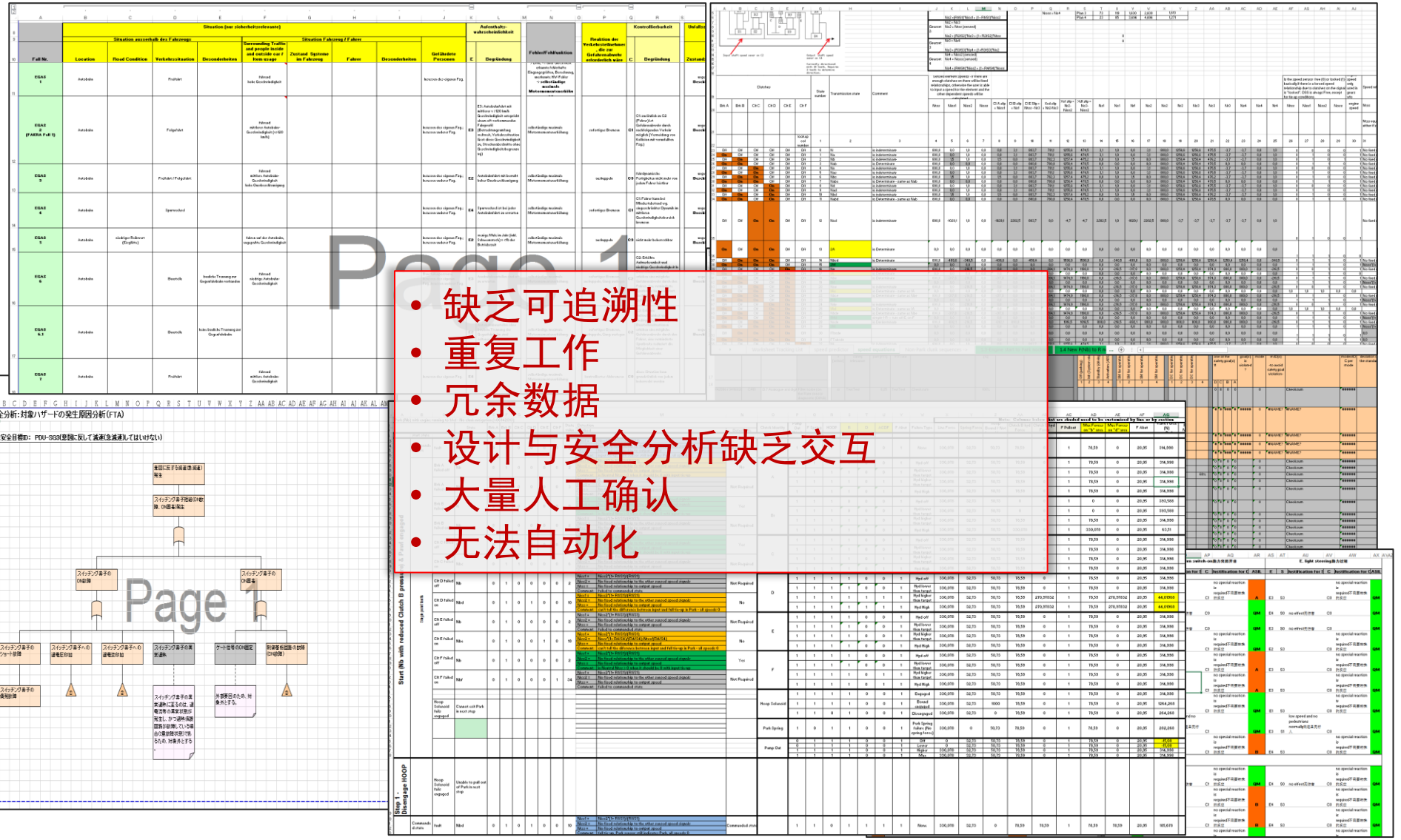
…目前大多采用的手段是excel 及单任务工具 …

实际工程中安全分析是怎样做的：多个点工具分别完成单个任务



- is...
  - Consistency is difficult to visualize
  - Time-consuming
  - complex

功能安全开发挑战



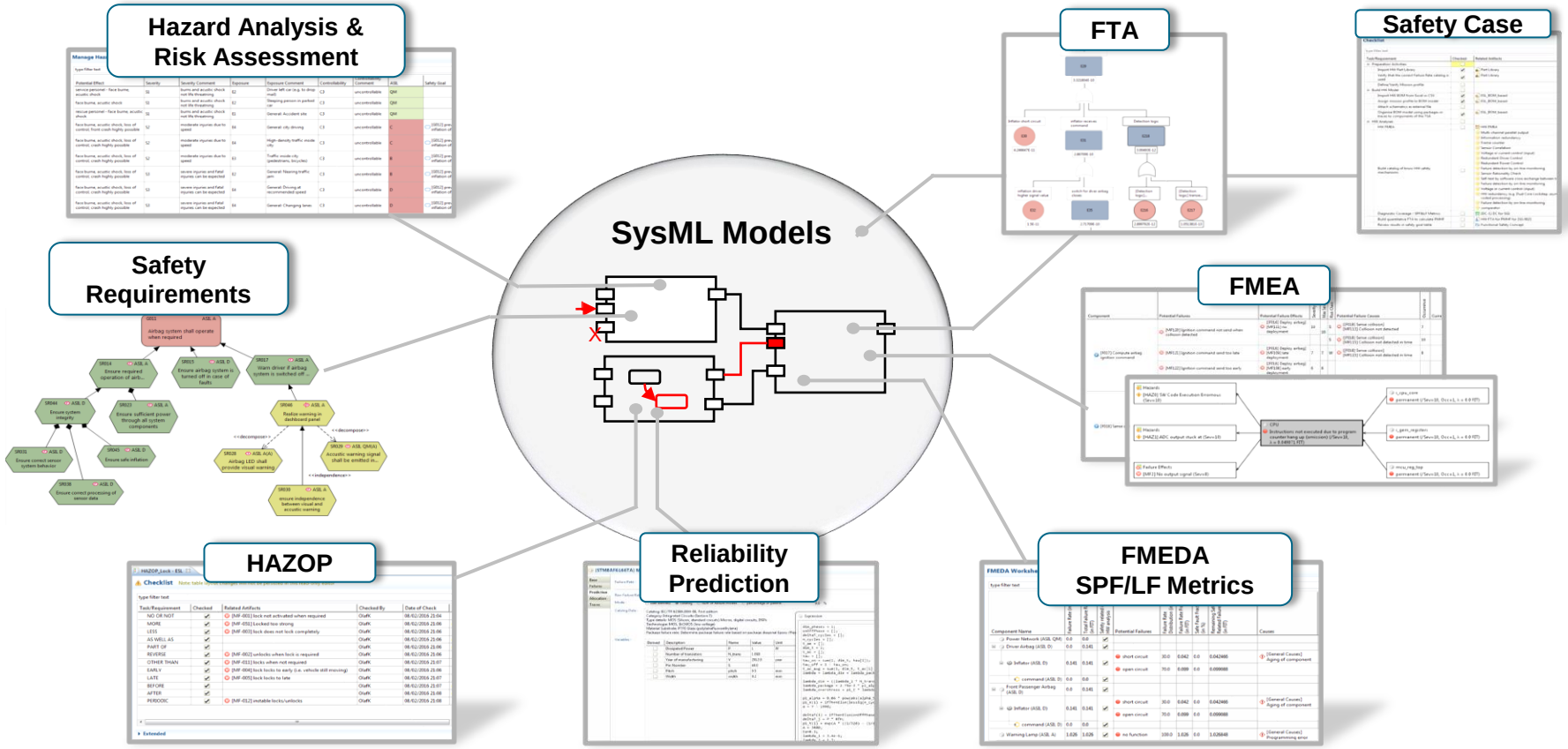
- 缺乏可追溯性
- 重复工作
- 冗余数据
- 设计与安全分析缺乏交互
- 大量人工确认
- 无法自动化

会议议程

- 汽车领域的安全要求及挑战
- ANSYS medini 基于模型的系统安全解决方案
- ANSYS medini 在完整的ISO 26262 安全生命周期中的应用
- 小结

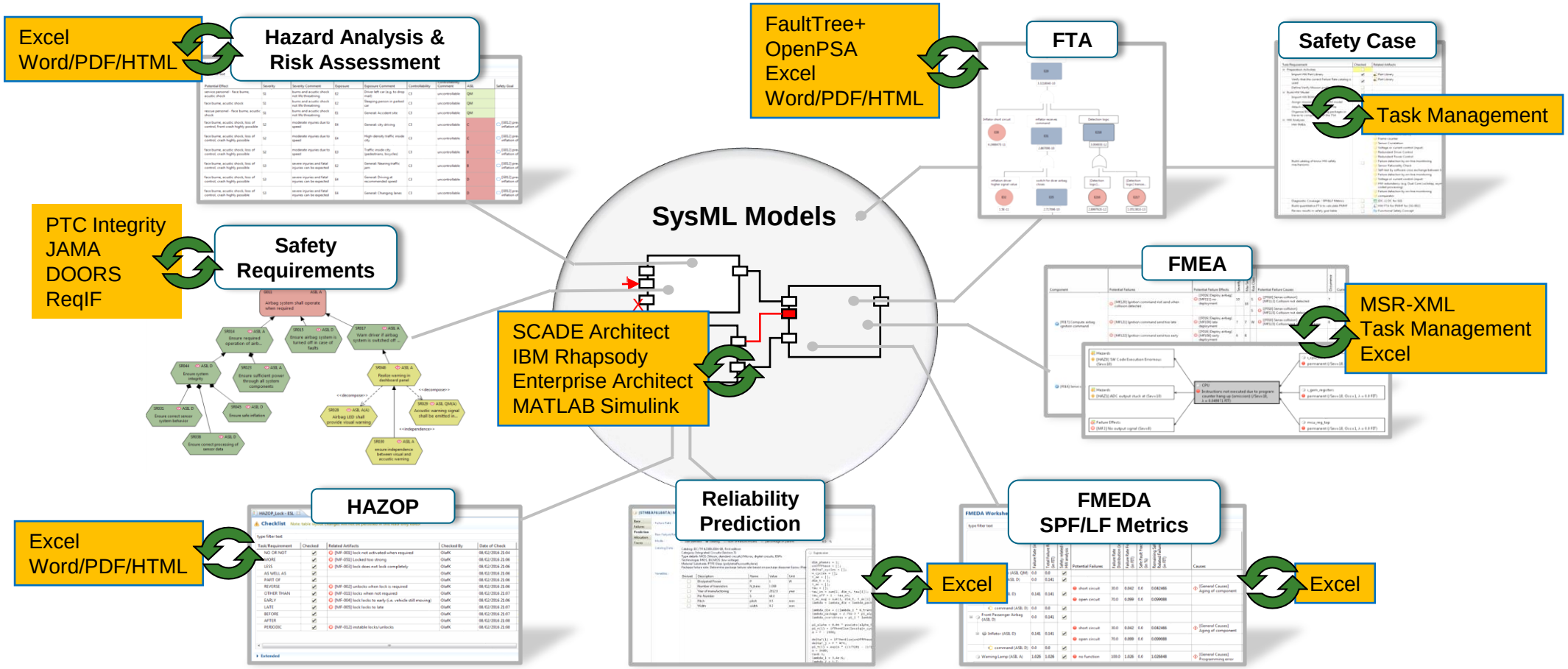
medini: 基于模型的系统安全分析

高质量的系统架构设计与可靠性和安全性分析方法相结合



基于模型的方法确保一致性、可跟踪性和高效率

medini: 丰富的工具接口

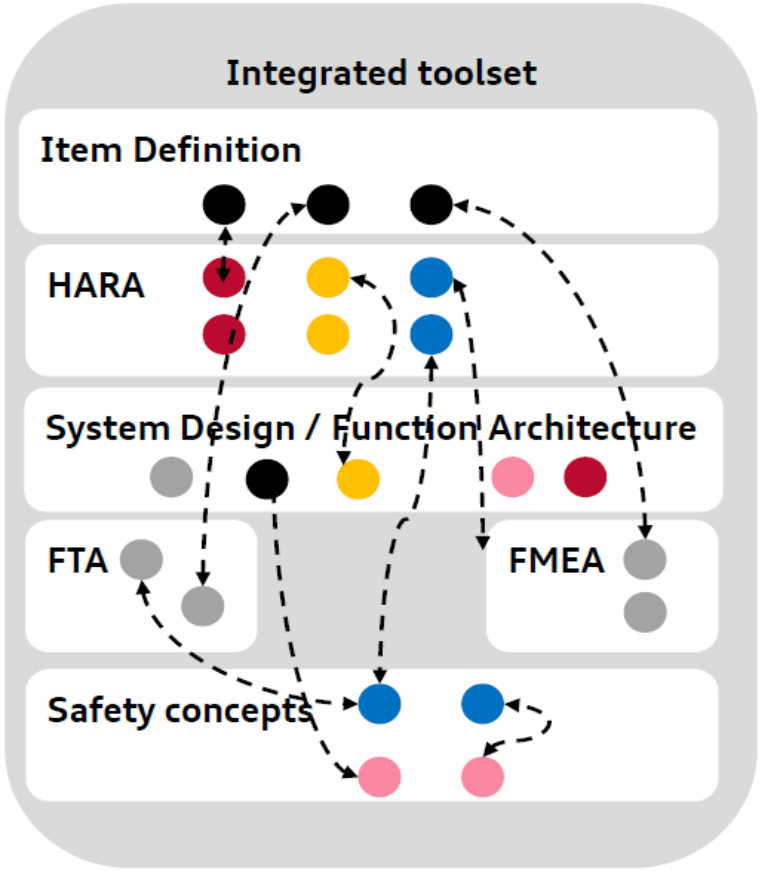


开放的接口，保证工作的无缝衔接

确保安全生命周期的追溯性和一致性

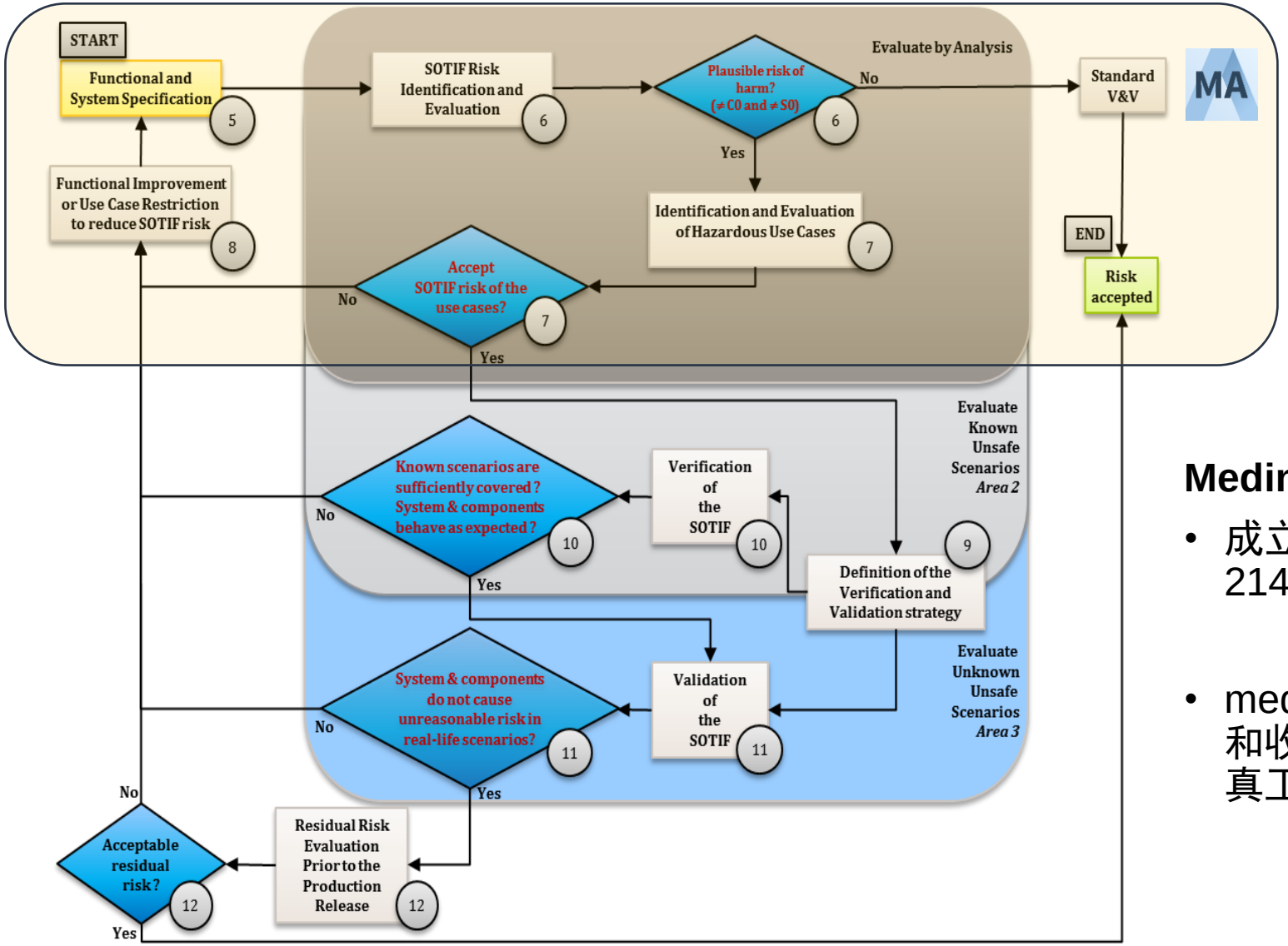
Determination of a suitable tool

Instance links in Medini analyze



- Instance links as a connection between artefacts
- Defined links as attributes of models
- Development of instance links bettween random artefacts
- Advantages of instance links
  - Avoid duplicates
  - No updates necessary
  - Visualization of implicit knowledge
  - Visualization of interconnections

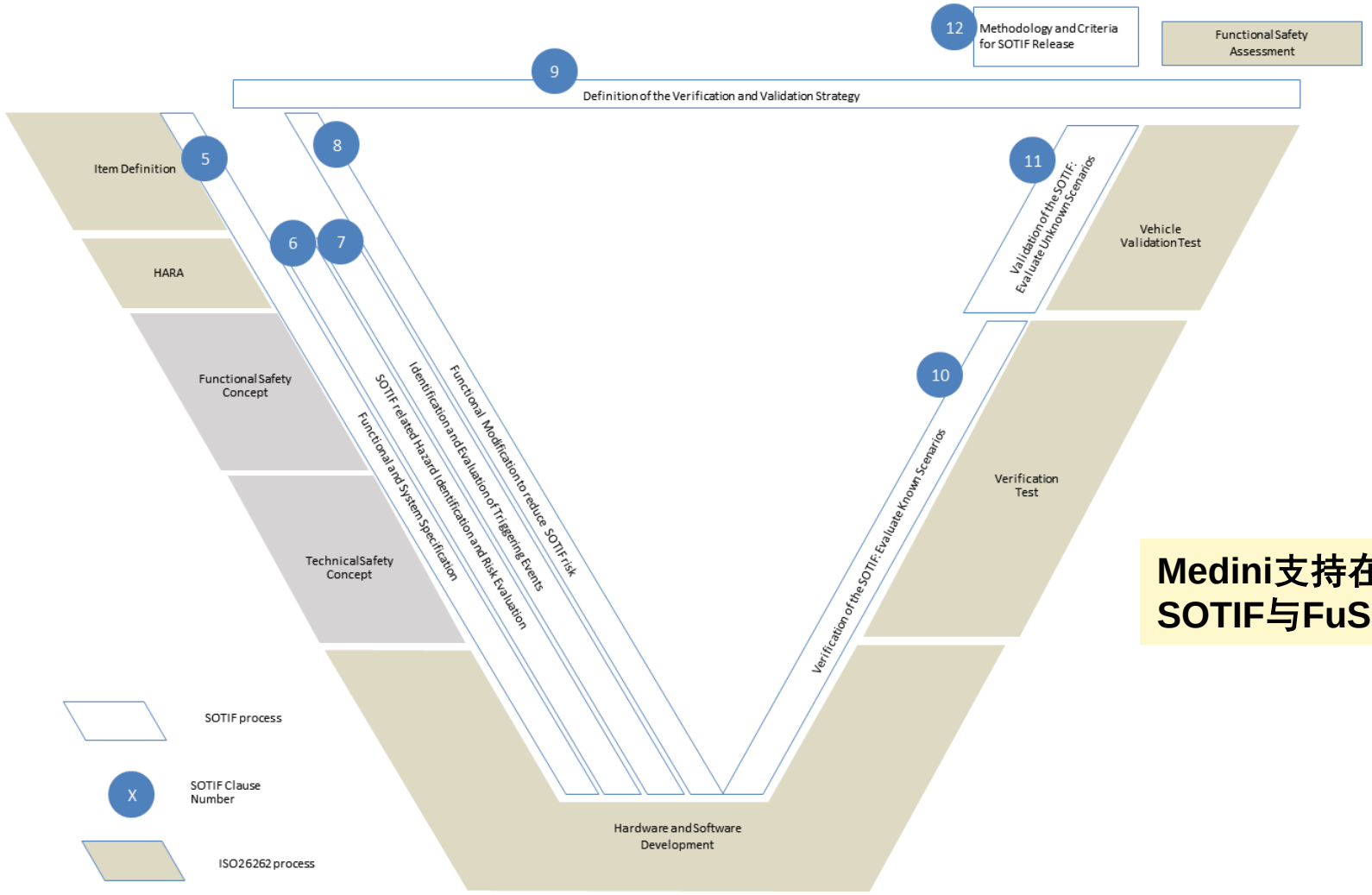
Medini预期功能安全解决方案



Medini优势：

- 成立SOTIF / ADAS / AV工作组，参与ISO PAS 21448标准制定，随时更新保持与标准同步
- medini的范围是分析活动以及V / V数据的准备和收集，测试验证工作可由ANSYS 自动驾驶仿真工具链完成，覆盖SOTIF全流程

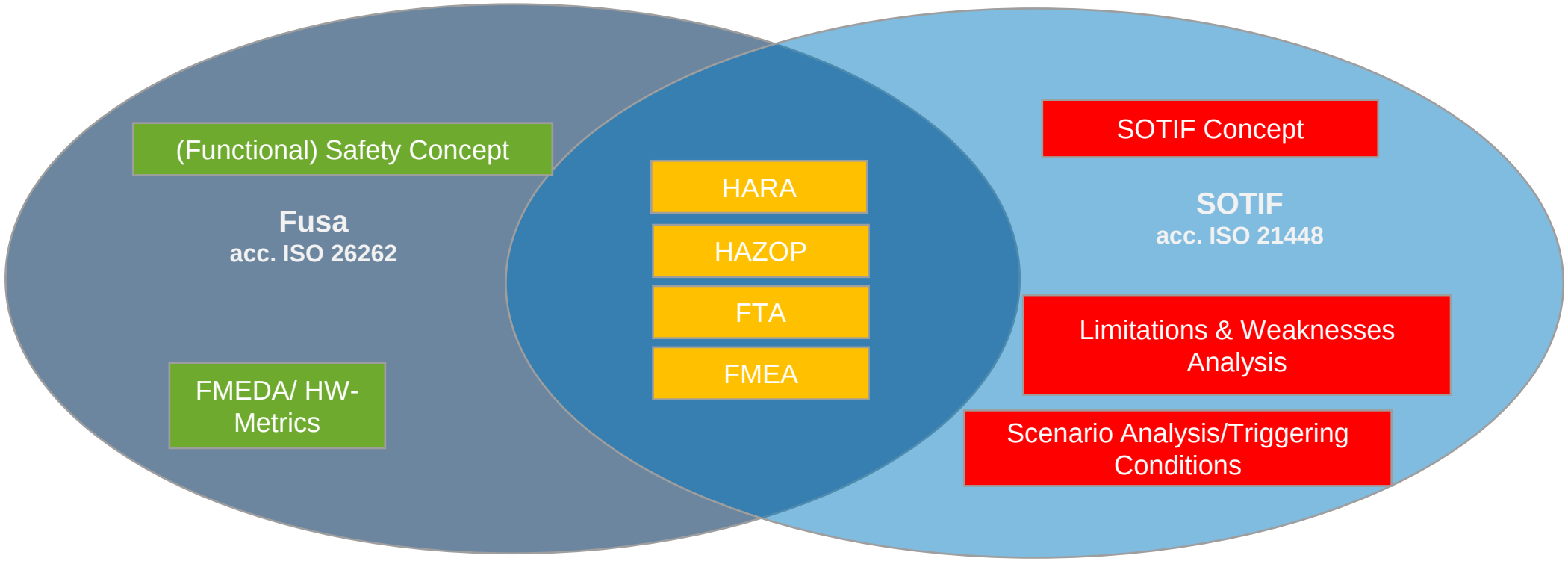
ISO26262与ISO21448的结合



Medini支持在同一操作环境下对SOTIF与FuSa结合进行安全分析

ISO 21448附录A提出了一种FuSa和SOTIF的结合流程，并就如何使两者融合提出了一些建议

FuSa与SOTIF分析方法对比



medini 传统功能
medini 传统功能对SOTIF的更新支持
medini 针对SOTIF的最新功能

medini analyze 信息安全特性

基于SysML语言建模

- 架构建模
- 资产识别
- 为资产分配安全属性（保密性、完整性、可用性等）

攻击树

- 图形化的攻击树编辑器
- 将攻击路径自动衍生到威胁分析表
- 提供自动布局和支持通过多个图表处理大型攻击树

威胁分析表

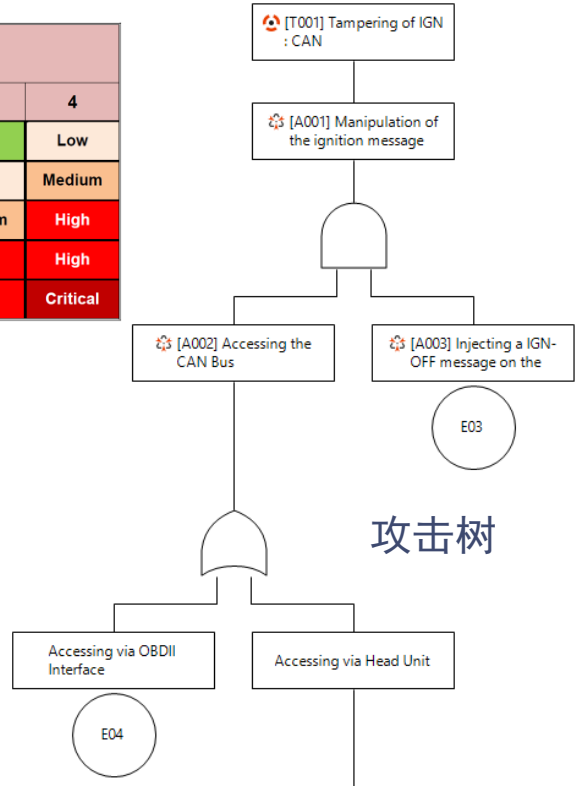
- 可自定义的威胁识别，评估和处理表
- 来自其他分析的自动衍生（攻击树）

信息安全目标与需求管理

- 定义和管理（安全）目标和要求
- 使用GSN的图形编辑器
- 使用图表实现需求的层次结构化和追溯性的可视化

Security Level (SL)	Impact Level (IL)					
Threat Level (TL)		0	1	2	3	4
	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

风险图



攻击树

威胁分析和风险评估表

Threat Scenarios

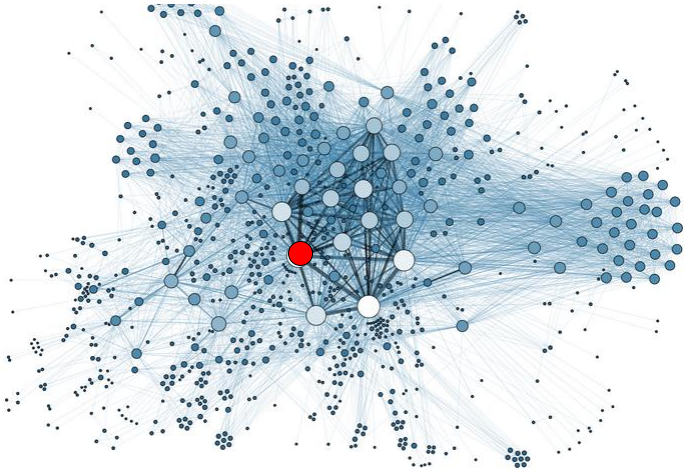
Risk Treatment ☑ Risk Assesment ☑

type filter text

ID	Threat	Asset	Safety Impact	Financial Impact	Operational Impact	Privacy and Legislative Impact	Severity Level	Equipment	Expertise	Knowledge about TOE	Window of Opportunity	Likelihood Level	Security Level
TS001	[T001] Tampering of IGN : CAN	IGN : CAN	High	Medium	High	None	Critical	Bespoke	Expert	Restricted	Small	Low	Medium

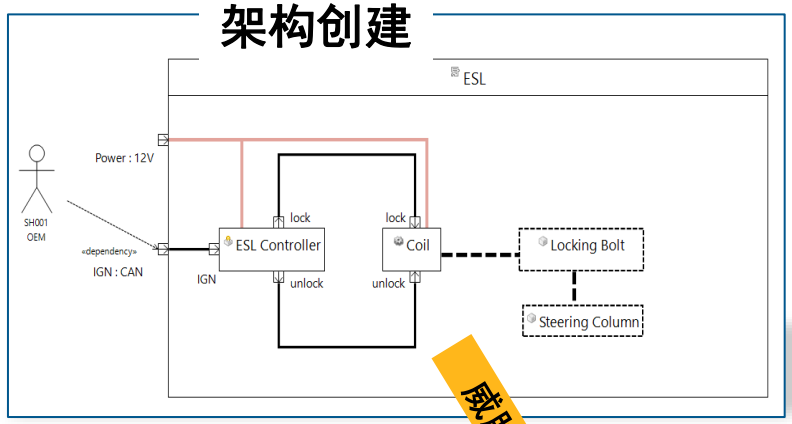
如何系统性的去做信息安全分析

- 识别系统中的资产及其重要的安全属性
- 系统地识别可被利用来执行攻击的系统威胁
- 了解潜在成功攻击的后果
- 估计攻击的可能性（例如，执行攻击所需的成本）
- 将风险与每种威胁相关联
- 根据已识别的风险计划并执行适当的安全措施
- 避免过度设计和低估



Medini信息安全分析工作流程

架构创建



威胁的衍生

威胁识别

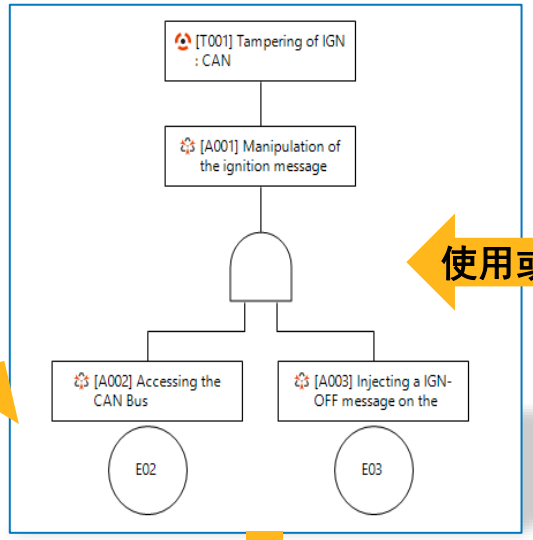
Identified Threats

type filter text

ID	Name	Assets	To Be Assessed	Category
T001	Tampering of IGN : CAN	ESL::IGN : CAN	☑	Tampering

攻击场景

攻击树



使用或派生

攻击目录

Attacks

type filter text

ID	Name	Category
A001	Manipulation of the ignition message	Tampering
A002	Accessing the CAN Bus	Tampering
A003	Injecting a IGN-OFF message on the CAN	Tampering

推导出威胁评估

威胁评估与处理

Threat Scenarios

type filter text

ID	Threat	Asset	Severity Level	Likelihood Level	Security Level	Treatment Options	Measures	Affected Design Elements	Requirements
TS001	[T001] Tampering of IGN : CAN	IGN : CAN	Critical	Low	Medium	Mitigation	Encryption Authentication		[Sec-01] Encrypt Ignitition Message on the CAN-Bus

medini 针对半导体的解决方案

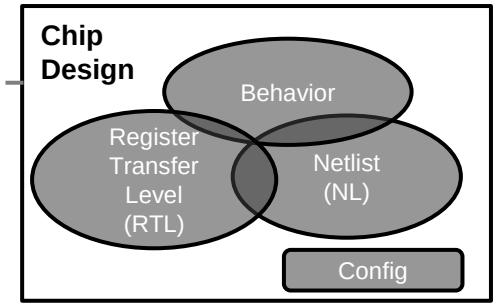
medini™ analyze

Design Tools
Redhawk, CADENCE, Synopsys

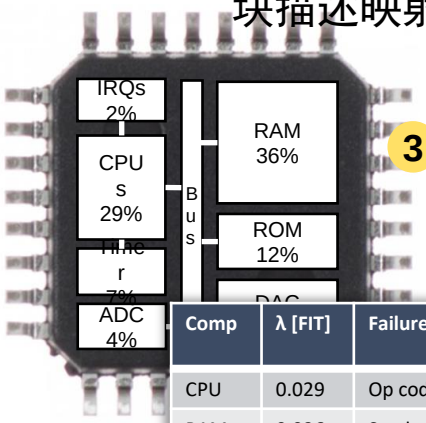
0 定义高层架构模型

1 导出包含 die area/gate counts 的设计数据

Design Hierarchy (XML)



2 导入设计数据并与高层模块描述映射



3 失效率预计: 根据映射关系自动分布至各模块

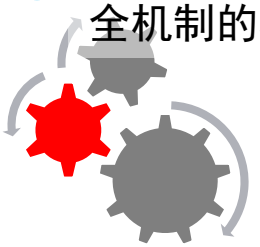
Comp	λ [FIT]	Failure	SM	Critical?	...
CPU	0.029	Op code	SM_Lockstep	X	
RAM	0.036	Stuck at	ECC	X	
				Σ SPF/LF	

4 执行 FMEDA，计算 SPF/LF metrics, safe fault fractions, 等

5 从FMEDA生成故障列表，以进行故障注入模拟

Fault Injection Data (XML)

6 执行故障注入以确定安全机制的覆盖范围



7 更新安全机制的诊断覆盖范围和故障注入的安全故障比例

Medini Analyze 系统安全平台
-适用于概念、系统、软硬件全流程应用

主机厂/平台

HAZOP
HARA/FHA/PHA/TARA
Safety Requirements

Tier1 子系统/ECU 供应商

FMEA
FTA
FMEDA/FMECA
DFA
Reliability

半导体厂商

SPF/LF Metrics (FMEDA)
FTA
Reliability

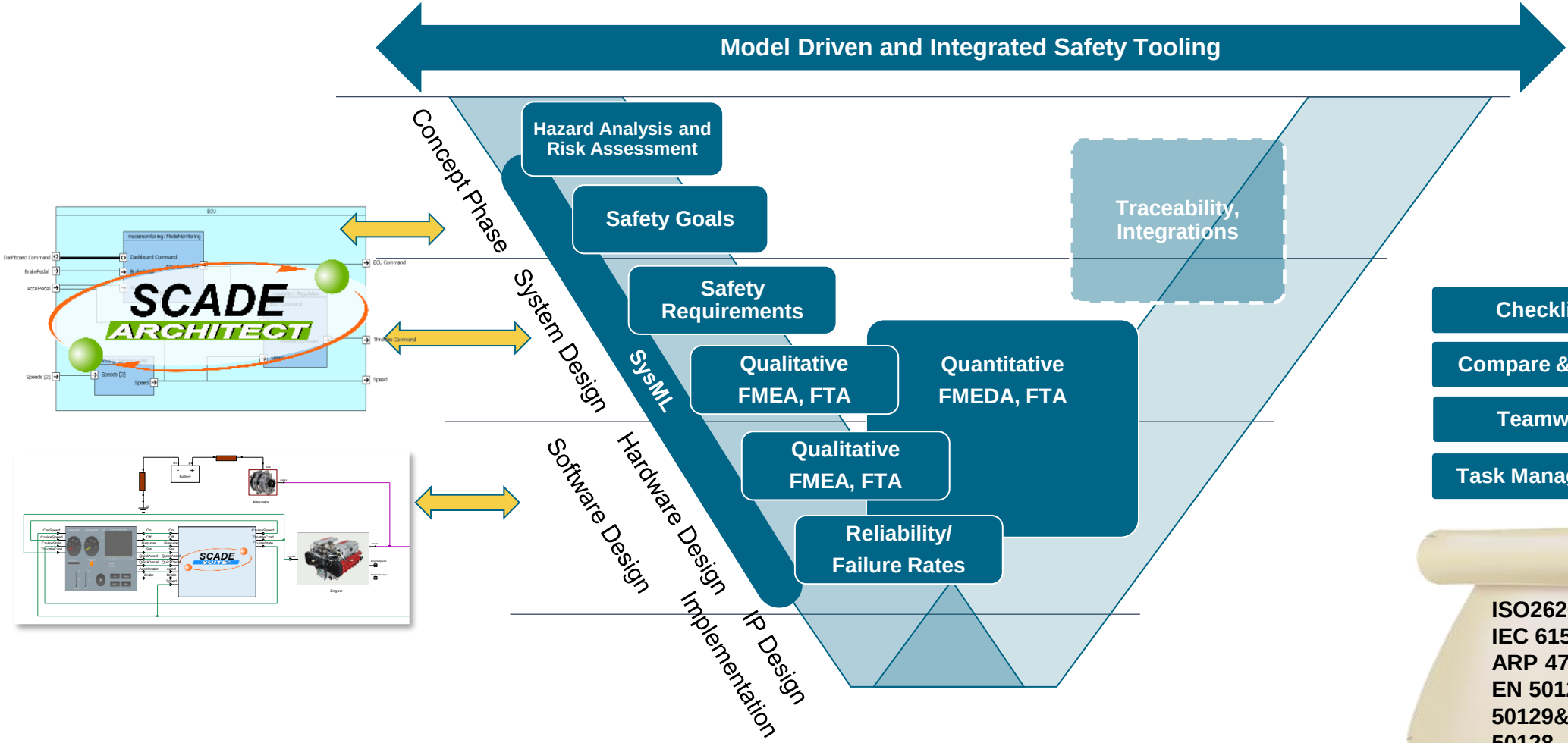
定性到定量分析…平台到半导体芯片

功能安全 + 预期功能安全 + 信息安全

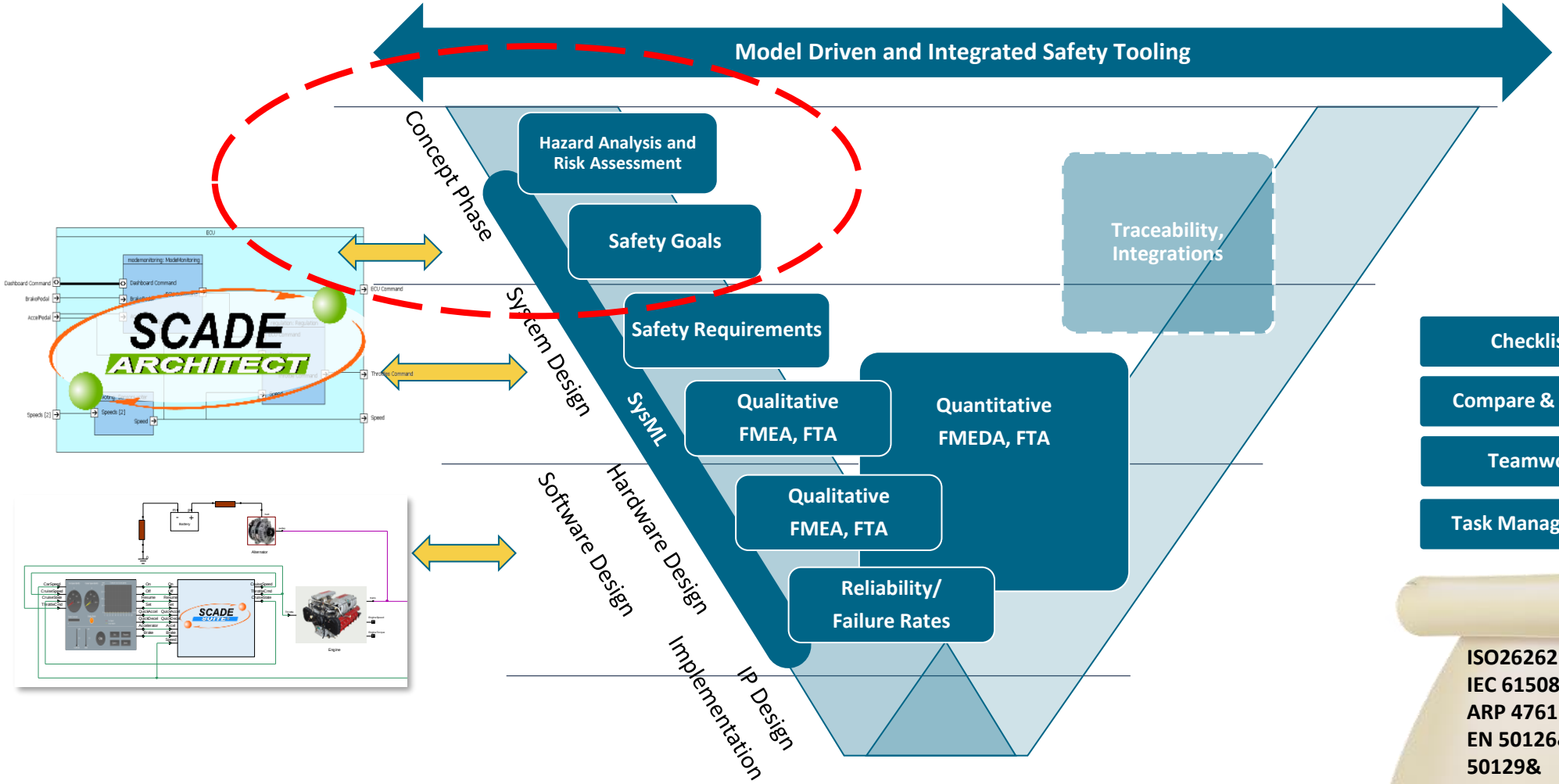
会议议程

- 汽车领域的安全要求及挑战
- ANSYS medini 基于模型的系统安全解决方案
- ANSYS medini 在完整的ISO 26262 安全生命周期中的应用
- 小结

medini覆盖整个功能安全生命周期



概念阶段：基于模型的项目定义、风险评估



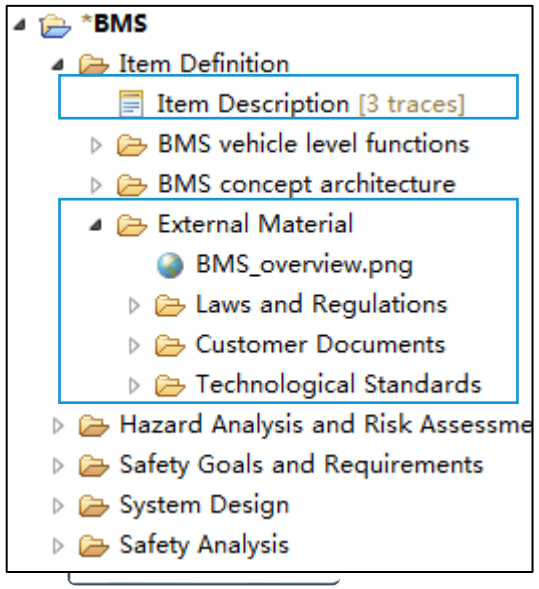
- Checklists
- Compare & Merge
- Teamwork
- Task Management

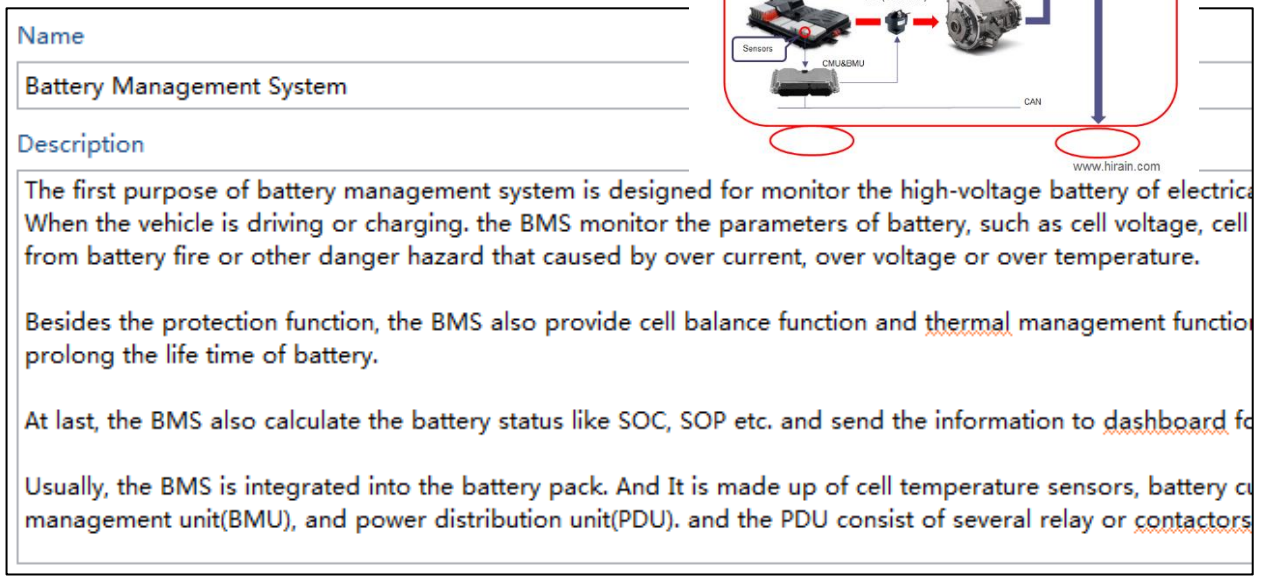
ISO26262
IEC 61508
ARP 4761
EN 50126&
50129&
50128

概念阶段：基于模型的项目定义、风险评估

项目定义 → 危害分析（HARA） → 确定功能安全目标与需求

– 项目定义、描述





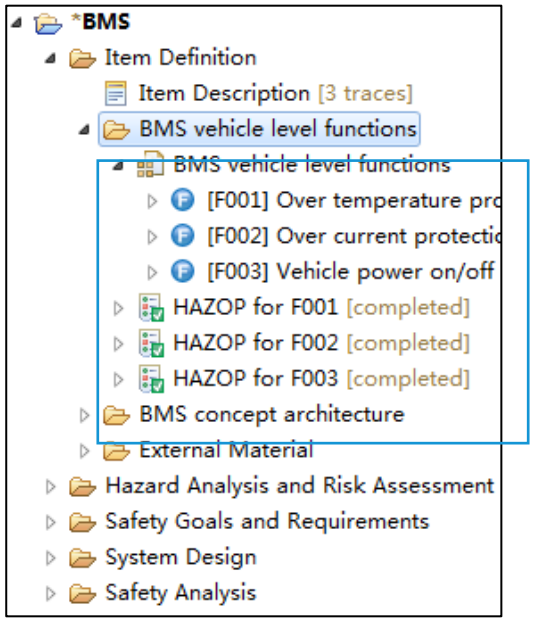
- ✓ 支持中英文双语输入
- ✓ 支持导入外部资料
- ✓ 支持模板的定制化

概念阶段：基于模型的项目定义、风险评估

项目定义 → 危害分析（HARA） → 确定功能安全目标与需求

- 项目定义、描述
- 整车功能建模、故障识别、HAZOP、操作场景

Function → Malfunction



来源： 危害与可操作性分析（**HAZOP**）

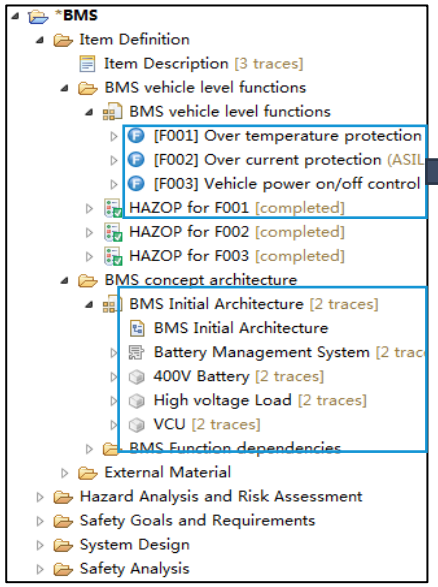
Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note
NO OR NOT	☑	[MF062] Can not open the main positive and negative relay when over temperature occur [MF137] Can not output the power limit value, when temperature is very high	yu.wang	18-2-23 下午6:34	
MORE	☑	[MF138] Output a higher power limit value than required	yu.wang	18-2-23 下午6:34	
LESS	☑	[MF139] Output a lower power limit value than required	yu.wang	18-2-23 下午6:34	
AS WELL AS	☑		yu.wang	18-2-23 下午6:34	NA
PART OF	☑		yu.wang	18-2-23 下午6:34	NA
REVERSE	☑		yu.wang	18-2-23 下午6:34	NA
Unintended	☑	[MF140] Unintended output the power limit value when it is not needed [MF063] unintended close the main positive and negative relay	yu.wang	18-2-23 下午6:34	
OTHER THAN	☑		yu.wang	18-2-23 下午6:34	NA

提供HAZOP分析模板

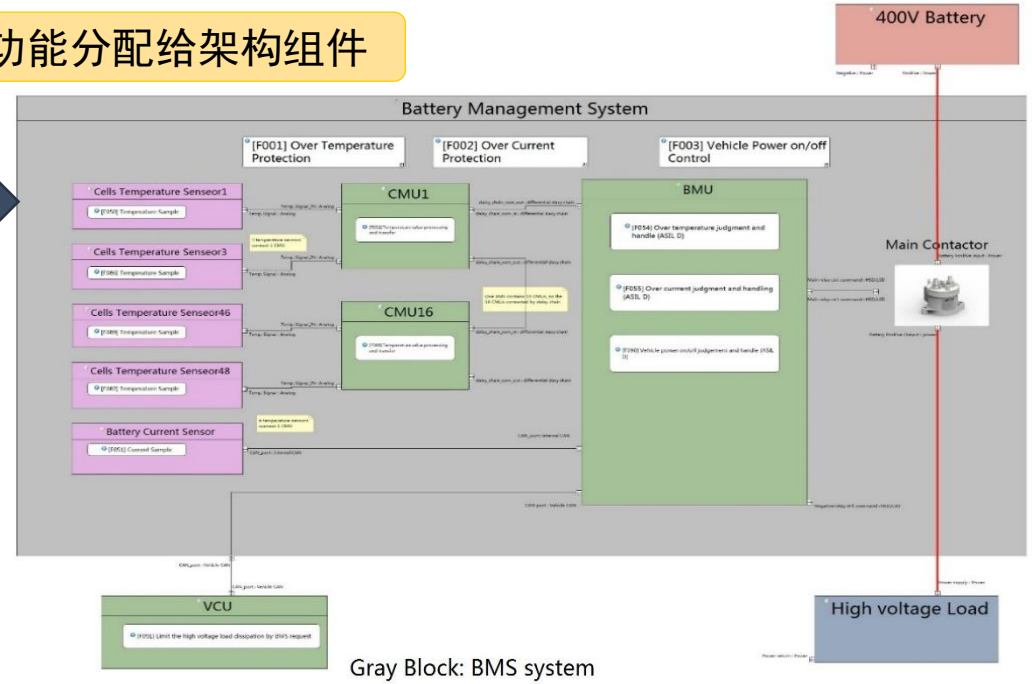
概念阶段：基于模型的项目定义、风险评估

项目定义 → **危害分析（HARA）** → **确定功能安全目标与需求**

- 项目定义、描述
- 整车功能建模、故障识别、HAZOP、操作场景
- SysML初始架构建模



功能分配给架构组件

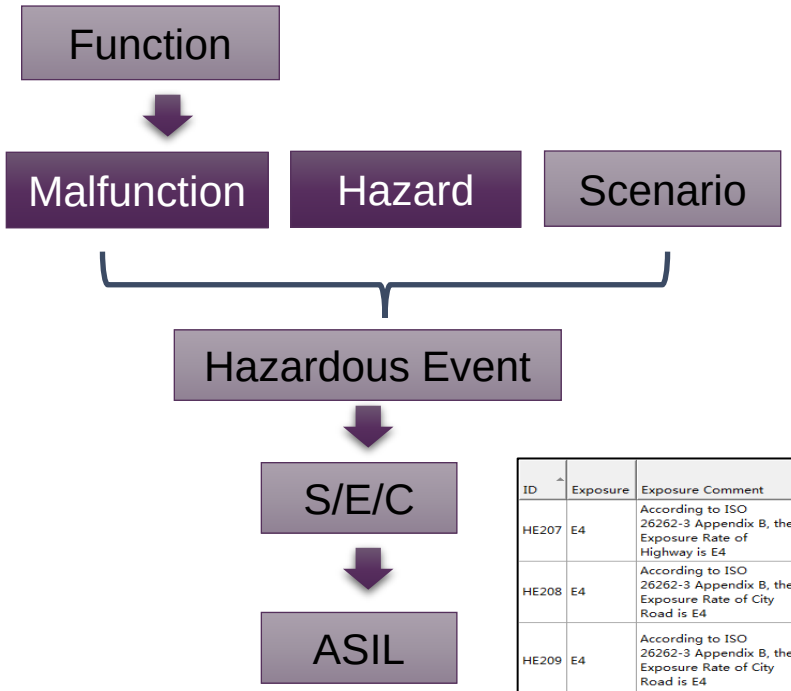


使用SysML建模语言快速建模

Gray Block: BMS system
RED Block: POWER
Green Block: ECU
Pink Block: Sensor
Blue Block: Load

概念阶段：基于模型的项目定义、风险评估

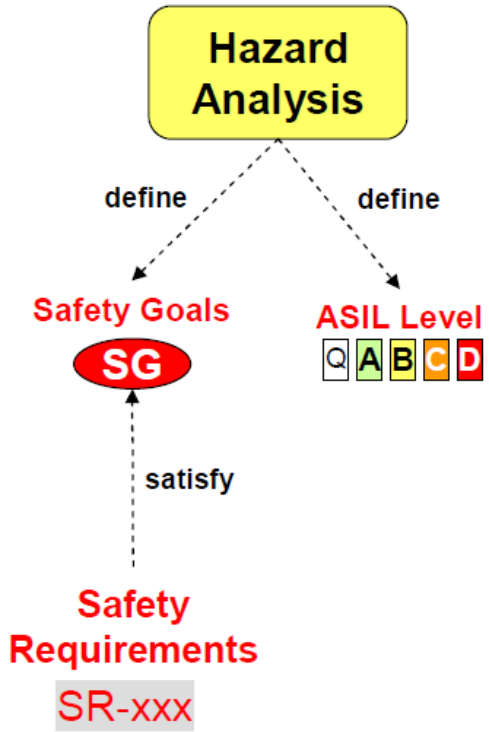
项目定义 → 危害分析（HARA） → 确定功能安全目标与需求



- 结合工具内置的操作场景库，对每个功能自动生成 HARA表
- 识别危害事件的严重度（S）、暴露概率（E）和可控性(C)。
- 提供风险图、自动计算风险分级 （ASIL）

ID	Name	ASIL	Safe State	FTTI
G001	Avoid battery fire caused by over temperature	C	disconnect high voltage circuit	500ms

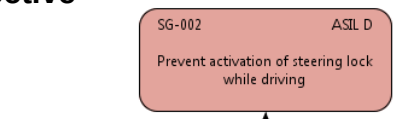
ID	Exposure	Exposure Comment	Malfunctioning Behaviour	Hazard	Potential Effect	Severity	Severity Comment	Controllability	Controllability Comment	ASIL
HE207	E4	According to ISO 26262-3 Appendix B, the Exposure Rate of Highway is E4	[MF062] Loss of Over temperature protection function	[VH02] Battery fire caused by over temperature	Fire in vehicles may cause people to be burned or die	S3	More than 10% of the possibility to AIS5 ~ 6	C2	It takes 30 seconds between the ignition of the battery to the vehicle. More than 90% of drivers can avoid hazards.	C
HE208	E4	According to ISO 26262-3 Appendix B, the Exposure Rate of City Road is E4	[MF062] Loss of Over temperature protection function	[VH02] Battery fire caused by over temperature	Fire in vehicles may cause people to be burned or die	S3	More than 10% of the possibility to AIS5 ~ 6	C2	It takes 30 seconds between the ignition of the battery to the vehicle. More than 90% of drivers can avoid hazards.	C
HE209	E4	According to ISO 26262-3 Appendix B, the Exposure Rate of City Road is E4	[MF062] Loss of Over temperature protection function	[VH02] Battery fire caused by over temperature	Fire in vehicles may cause people to be burned or die	S3	More than 10% of the possibility to AIS5 ~ 6	C1	It takes 30 seconds between the ignition of the battery to the vehicle. More than 99% of people near the vehicle can avoid hazards.	B
HE210	E4	According to ISO 26262-3 Appendix B, the Exposure Rate of Country Road is E4	[MF062] Loss of Over temperature protection function	[VH02] Battery fire caused by over temperature	Fire in vehicles may cause people to be burned or die	S3	More than 10% of the possibility to AIS5 ~ 6	C2	It takes 30 seconds between the ignition of the battery to the vehicle. More than 90% of drivers can avoid hazards.	C
HE211	E4	According to ISO 26262-3 Appendix B, the Exposure Rate of Country Road is E4	[MF062] Loss of Over temperature protection function	[VH02] Battery fire caused by over temperature	Fire in vehicles may cause people to be burned or die	S3	More than 10% of the possibility to AIS5 ~ 6	C1	It takes 30 seconds between the ignition of the battery to the vehicle. More than 99% of people near the vehicle can avoid hazards.	B



概念阶段：基于模型的项目定义、风险评估

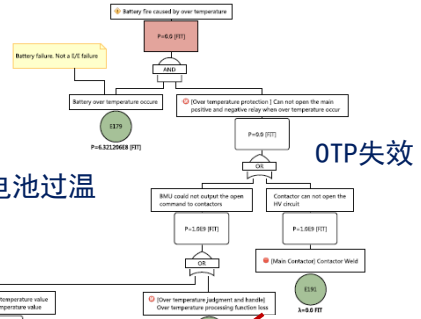
项目定义 → 危害分析（HARA） → 确定功能安全目标与需求

Safety Goal = Top level Safety Objective

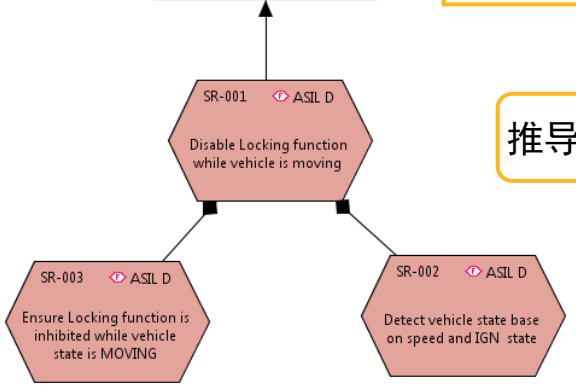


定义安全目标

基于架构进行FTA分析



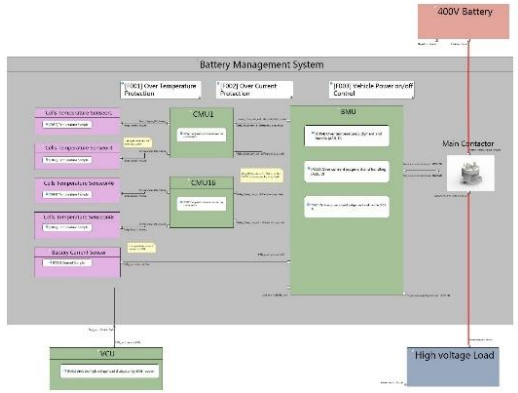
推导安全需求



功能安全需求

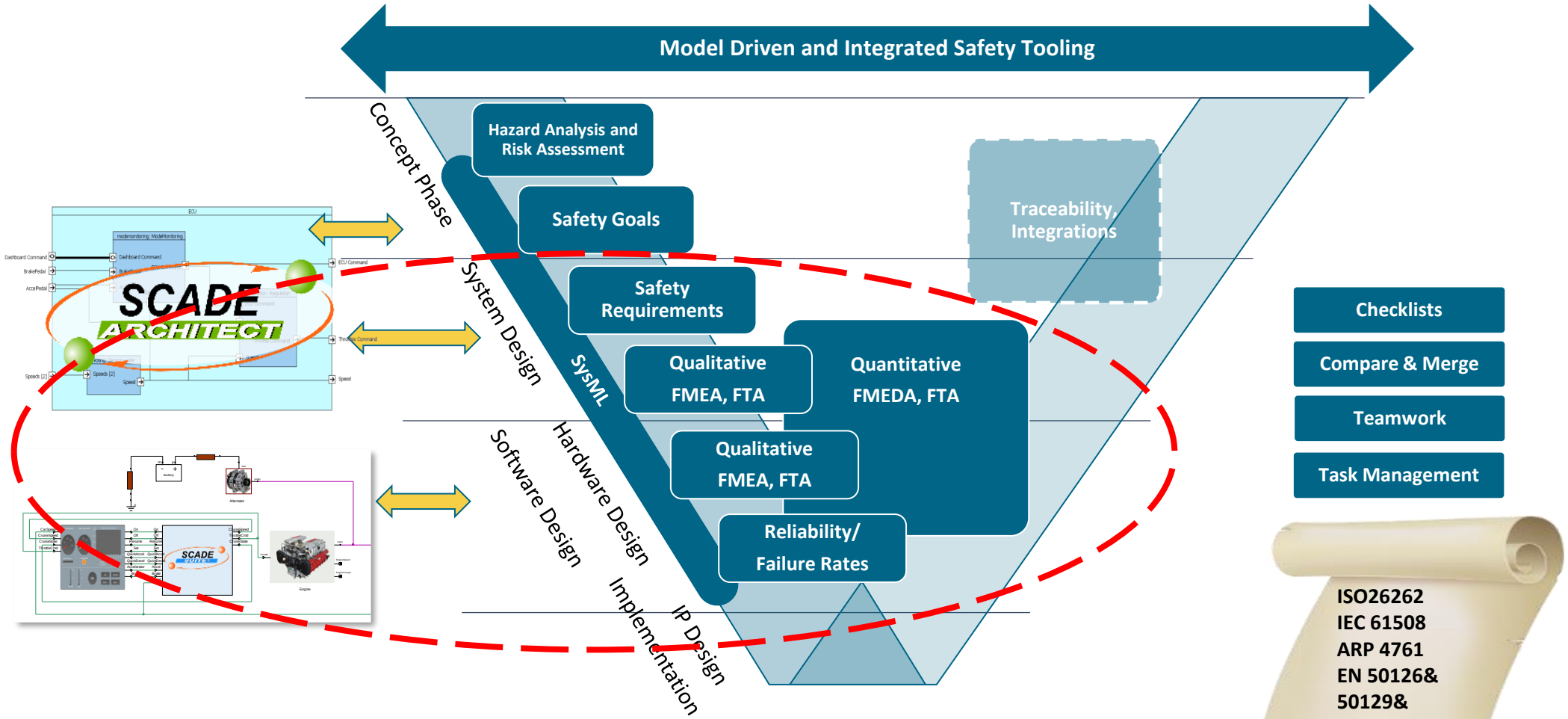
The failure of temperature sensor shall be detected or tolerated	FSR002
The failure of CMU shall be detected or tolerated	FSR004
The failure of BMU shall be detected or tolerated	FSR006
The weld fault of main contactos shall be detected or tolerated	FSR008

- 定义功能安全目标
- 推导功能安全需求 （定性FTA）
- 分配功能安全需求给初始架构
- 支持图形、表格和第三方工具对安全需求的管理

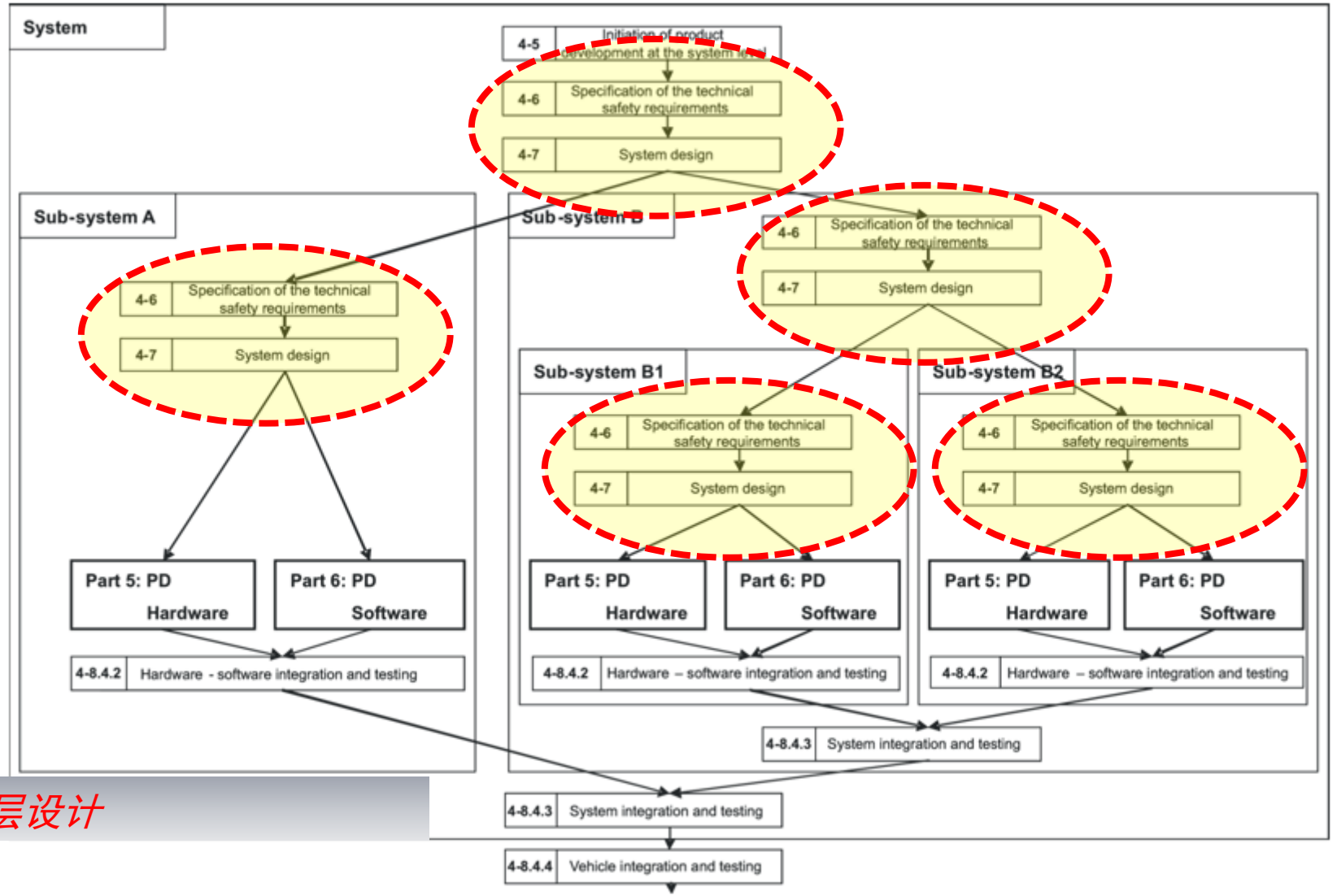


快速对初始架构建模(SysML)

设计阶段：安全需求、系统设计与安全分析交互迭代



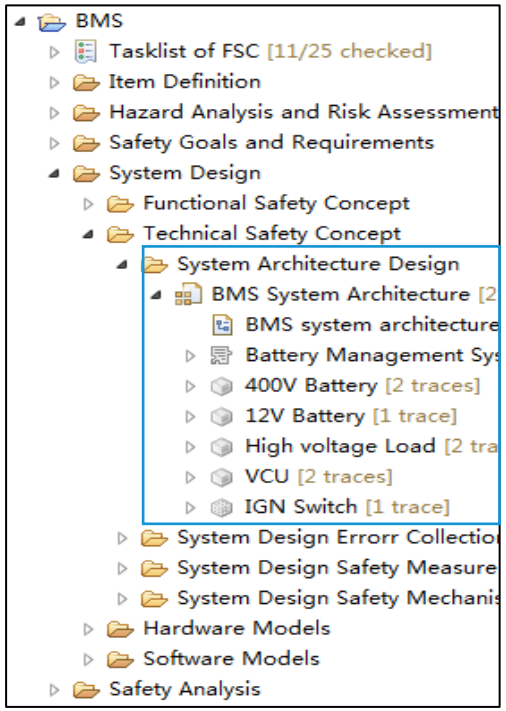
设计阶段（系统）

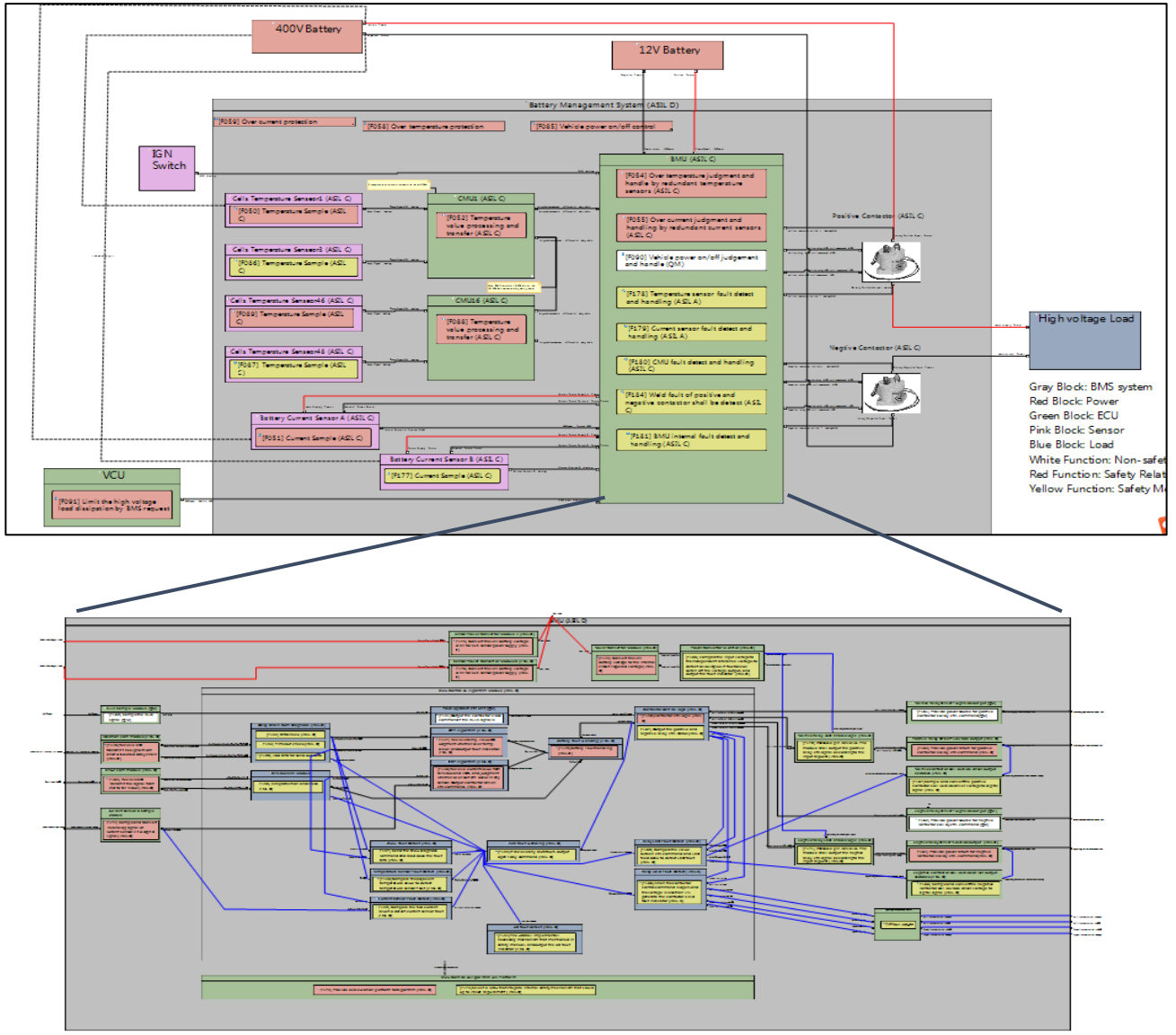

System
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
Sub-system A
4-6 Specification of the technical safety requirements
4-7 System design
Part 5: PD Hardware
Part 6: PD Software
4-8.4.2 Hardware - software integration and testing
Sub-system B
4-6 Specification of the technical safety requirements
4-7 System design
Sub-system B1
4-6 Specification of the technical safety requirements
4-7 System design
Part 5: PD Hardware
Part 6: PD Software
4-8.4.2 Hardware – software integration and testing
Sub-system B2
4-6 Specification of the technical safety requirements
4-7 System design
Part 5: PD Hardware
Part 6: PD Software
4-8.4.2 Hardware – software integration and testing
4-8.4.3 System integration and testing
4-8.4.3 System integration and testing
4-8.4.4 Vehicle integration and testing

分层设计

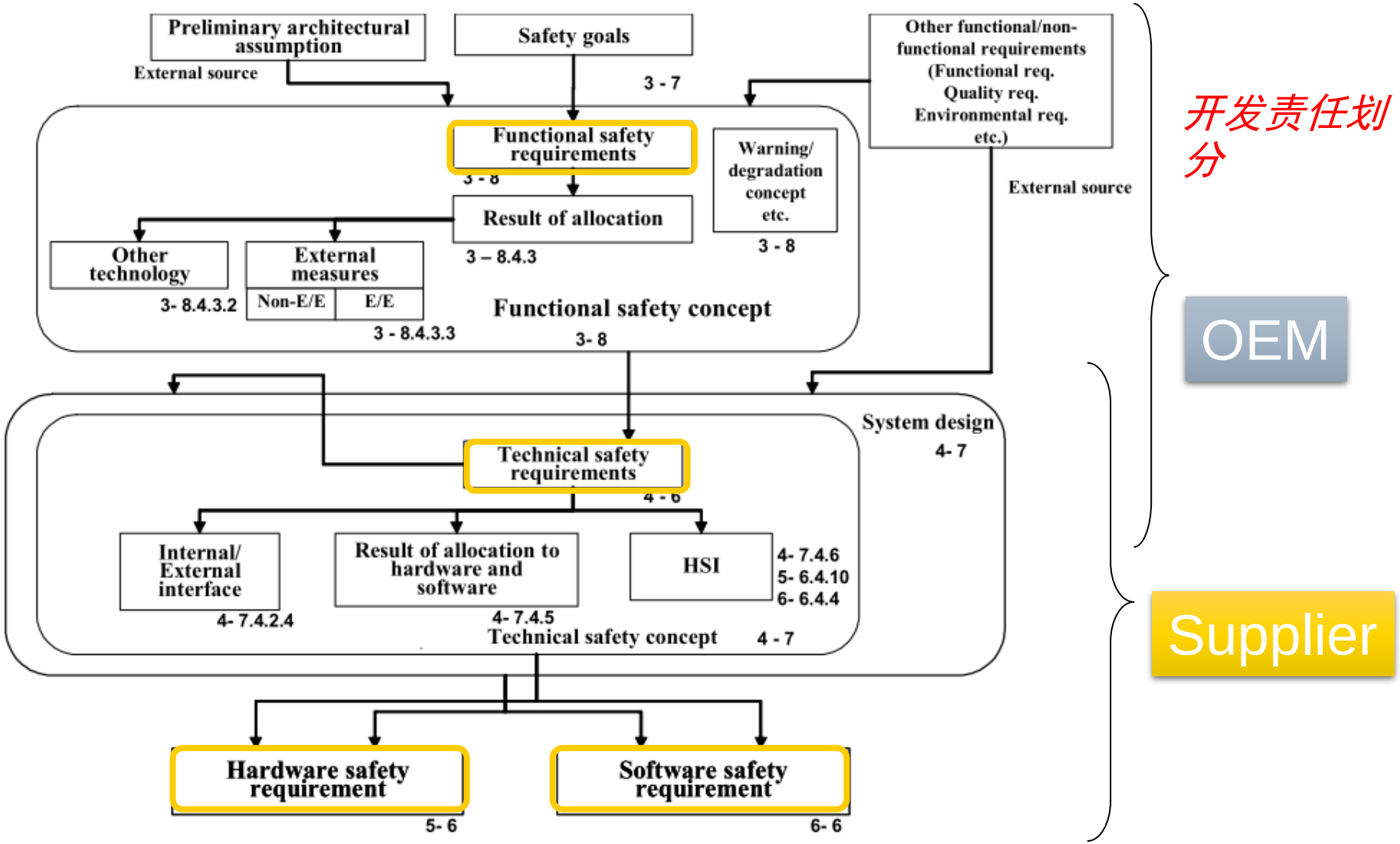
设计阶段（系统）

- 系统设计
  - ✓ 支持在模块中创建功能
  - ✓ 支持分层开发（Sub-system）





安全需求的传递： FSR， TSR， HSR， SSR



开发责任划分

OEM

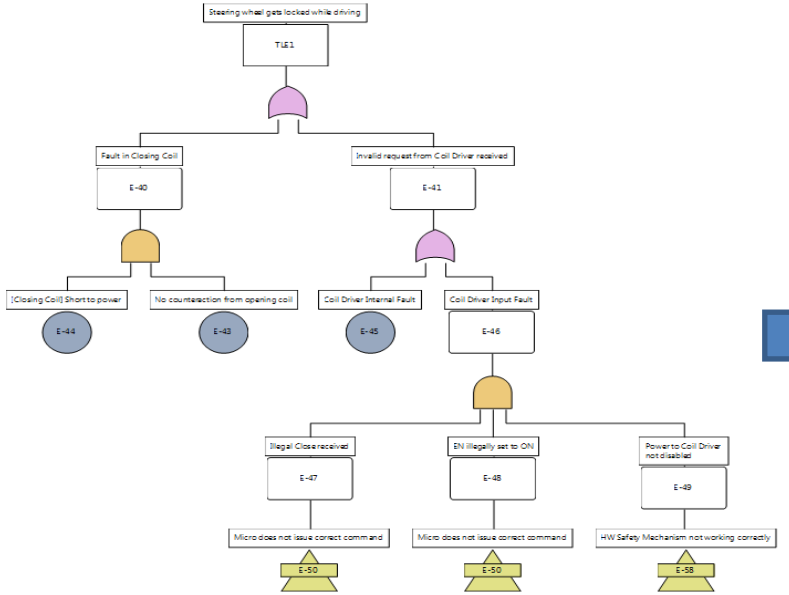
Supplier

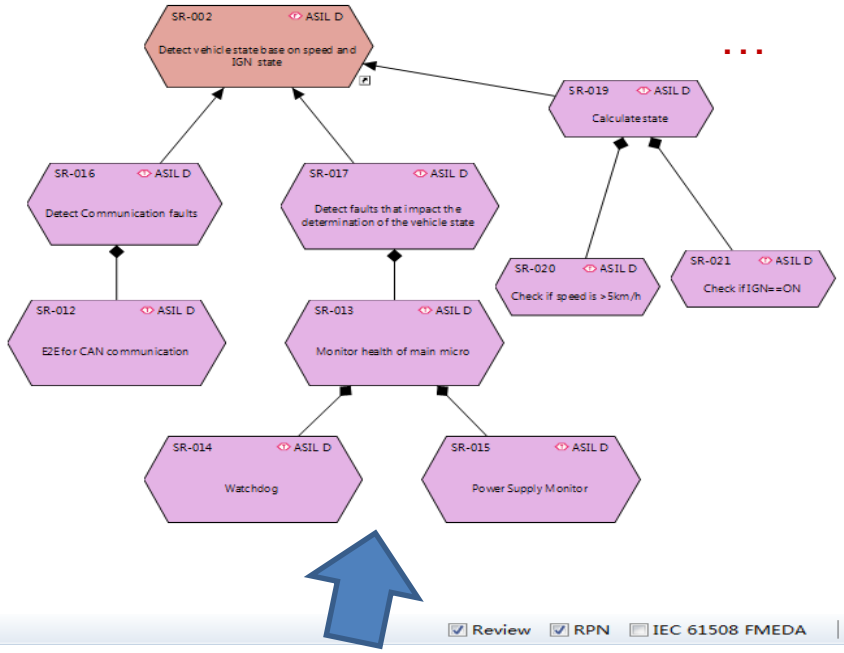
设计阶段（系统）

- 技术安全需求的推导：
  - Basic TSR
  - Diagnosis TSR

源于：

- ✓ FSR
- ✓ FMEA
- ✓ FTA
- …





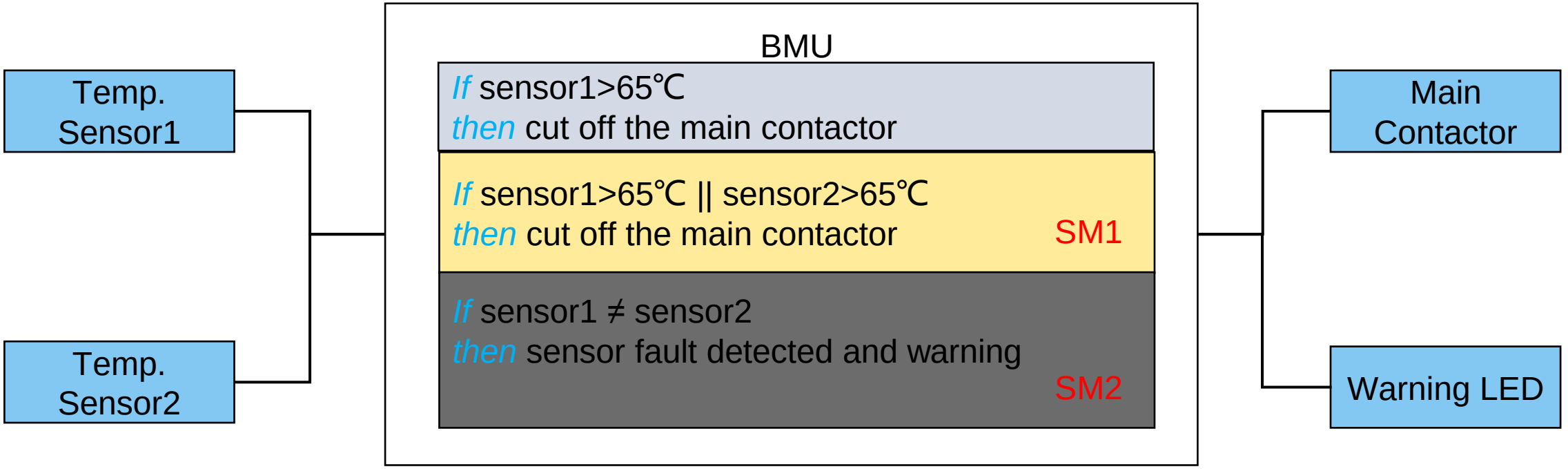
Function FMEA Worksheet — Review ✓ RPN ✓ IEC 61508 FMEDA

type filter text

Component	Potential Failures	Potential Failure Effects	Potential Failure Causes	Current Design Controls Prevention	Current Design Controls Detection	Severity	Occurrenc	Detection	RPN
[F-001] lock steering	[MF-001] lock not activated when required	[Hazards and Top Level Effects] [QU 2] No theft protection	[[F-010] Activate Closing Coil] [MF-017] NO Activation of Closing Co	Water proof sealing	Vibration Test [det: 4]	0	0	4	0
			[[F-005] Derive Command] [MF-037] NO Command issued	Screwing of connector	End-of-Line test [det: 0]		0	0	0
			[[F-006] Supervise Execution] [MF-044] NO Lock State Information	Screwing of connector	End-of-Line test [det: 0]		0	0	0

设计阶段（系统）

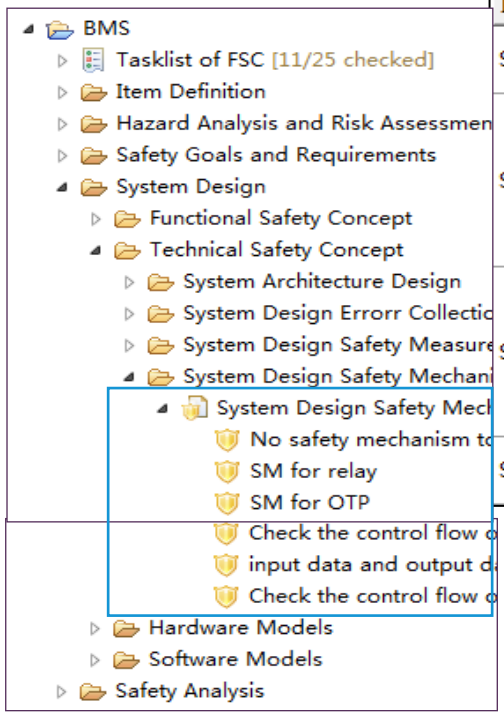
- 技术安全需求的推导：
  - Basic TSR
  - Diagnosis TSR
    - 针对单点故障的安全机制
    - 针对多点潜伏故障的安全机制



设计阶段（系统）

- 技术安全需求的推导：
  - Basic TSR
  - Diagnosis TSR
    - 针对单点故障的安全机制
    - 针对多点潜伏故障的安全机制

- 支持创建安全措施库：提高系统安全设计的效率和可复用性
- 诊断覆盖度（DC）自动分析

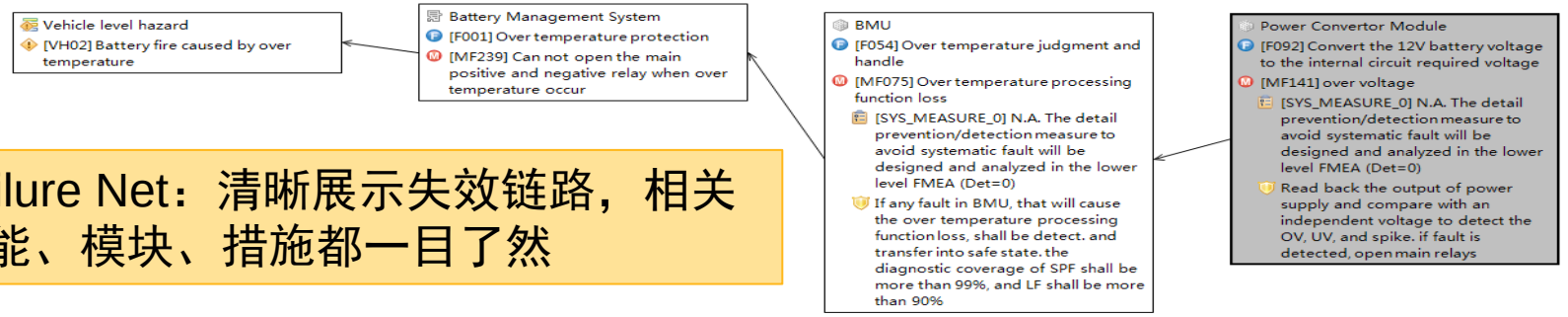


Section Key or Identifier	Safety Mechanism/Measure	Target Date	Status	Description	Det	SPF Diagnostic Coverage (in %)	LF Diagnostic Coverage (in %)
SYS_MECHANISM_1	SM for relay	17-10-17	Completed	Use two redundant relay(main positive and main negative relay) to avoid SPF	0	99.0	99.0
SYS_MECHANISM_2	SM for OTP	17-11-23	Completed	Use two adjacent temperature value to implement the over temperature protection function. if any temperature is morn than 65℃, open the main relays	2	99.0	99.0
SYS_MECHANISM_3	SM for temp. sensor fault detect	17-11-23	Completed	Compare two adjacent temperature value to detect the latent fault, if the temperature value is not the same, open the main relays	2	99.0	99.0
SYS_MECHANISM_4	SM to avoid the LF of relay			Read back the voltage of relay contactor to avoid the LF of relay	0	0.0	0.0

集成ISO26262 Part5 附录D中所有的安全机制

设计阶段（系统）

- 安全分析
  - FMEA
  - FTA



Failure Net：清晰展示失效链路，相关功能、模块、措施都一目了然

- ✓ 支持基于架构一键生成
- ✓ 支持VDA\AIAG等多种标准
- ✓ 同时建立失效网，追溯关系一目了然

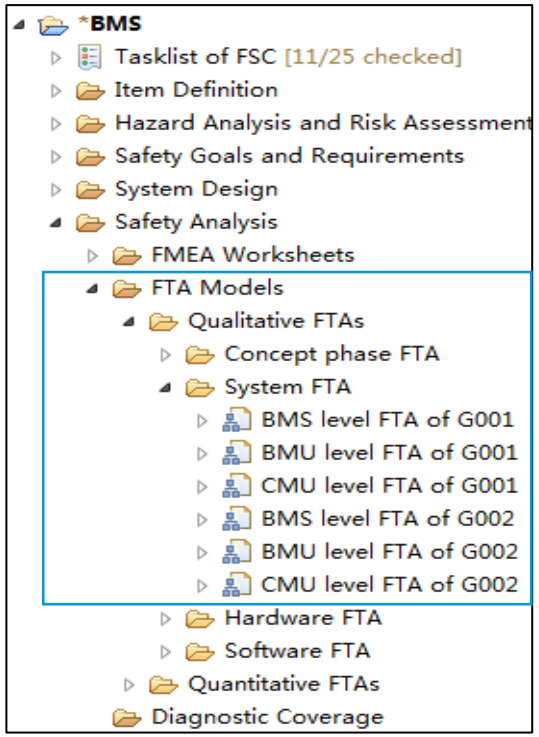
Component/Function	Potential Failures	Potential Failure Effects	Severity	Max Severity	Potential Failure Causes	Occurrence	Current Design Controls Prevention	Current Design Controls Detection	Detection	RPN
[F054] Over temperature judgment and handle	[MF075] Over temperature processing function loss	[[F001] Over temperature protection] [MF239] Can not open the main positive and negative relay when over temperature occur	10	10	[[F092] Convert the 12V battery voltage to the internal circuit required voltage] [MF141] over voltage	2	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA Read back the output of power supply and compare with an independent voltage to detect the OV, UV, and spike. if fault is detected, open main relays	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA	2	40
					[[F092] Convert the 12V battery voltage to the internal circuit required voltage] [MF142] under voltage	2	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA Read back the output of power supply and compare with an independent voltage to detect the OV, UV, and spike. if fault is detected, open main relays	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA	2	40
					[[F092] Convert the 12V battery voltage to the internal circuit required voltage] [MF143] voltage spike	2	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA Read back the output of power supply and compare with an independent voltage to detect the OV, UV, and spike. if fault is detected, open main relays	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA	2	40
					[[F093] Recieve and transmit the signal from and to isolated daisy chain] [MF144] convert function loss	2	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA time out check for daisy chain	[SYS_MEASURE_0] N.A. The detail prevention/detection measure to avoid systematic fault will be designed and analyzed in the lower level FMEA	2	40

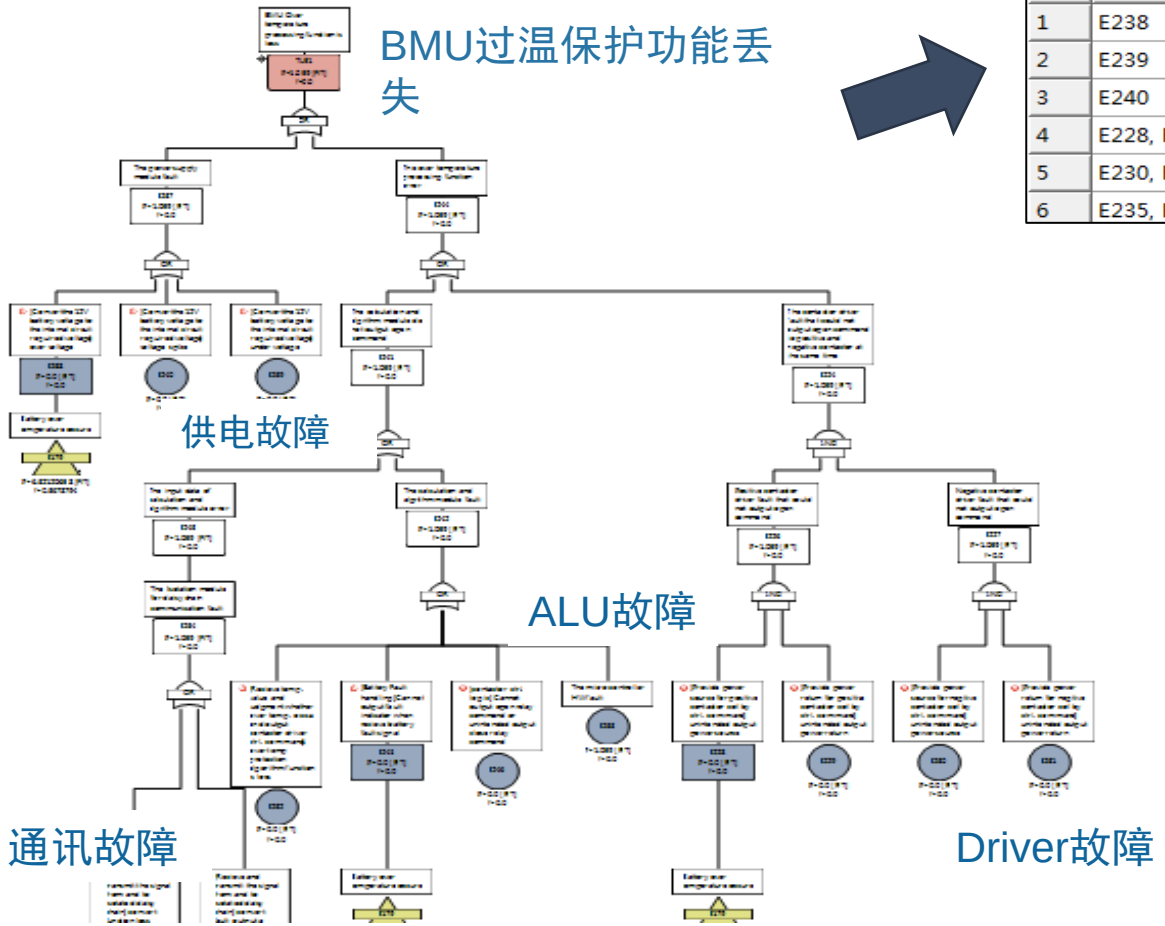
自动生成　　双击选择/自动生成　　双击选择　　自动计算

设计阶段（系统）

- 安全分析
  - FMEA
  - FTA

自动评估最小割集
识别单点和双点故障



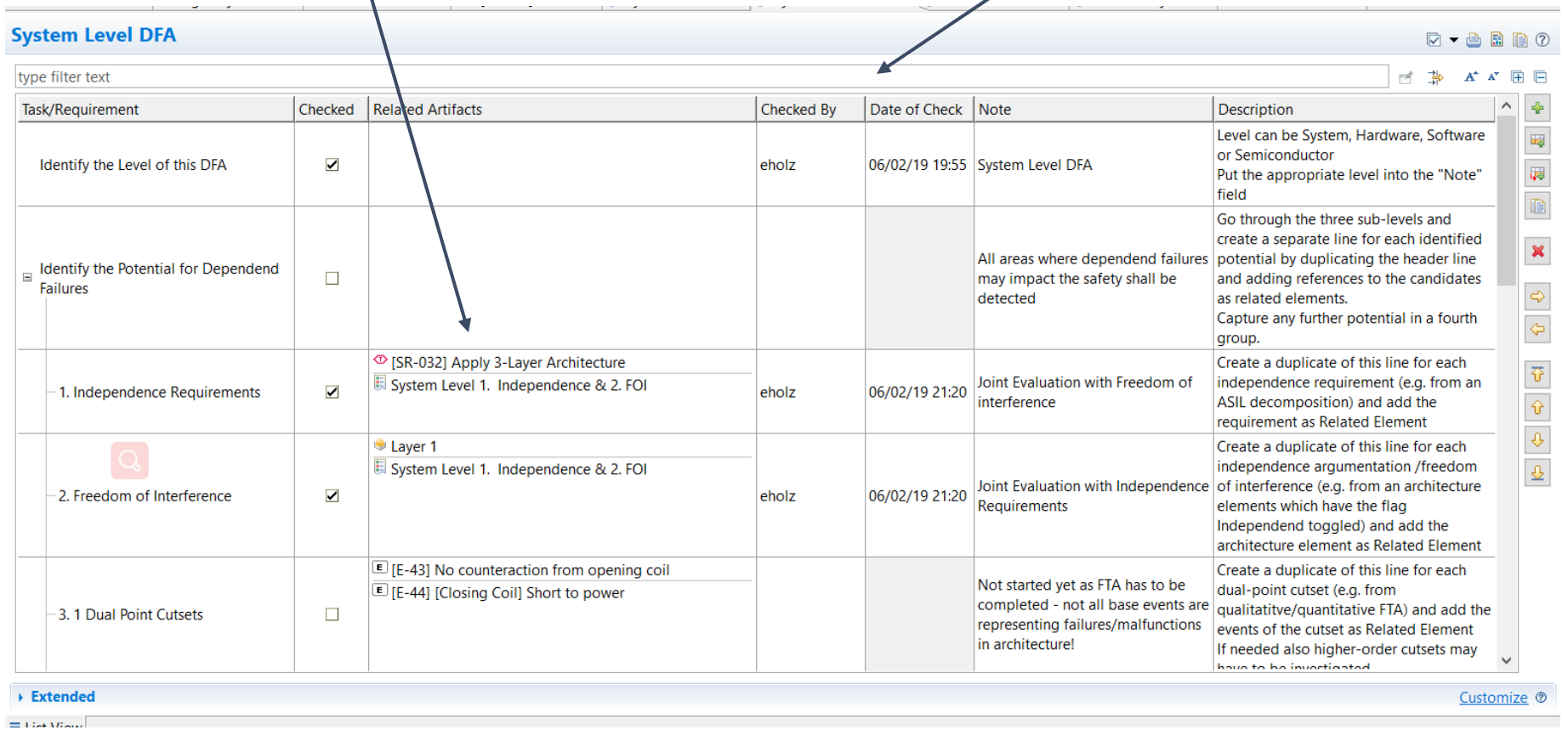


#	Events of Cut Set
1	E238
2	E239
3	E240
4	E228, E229
5	E230, E231
6	E235, E236

设计阶段（系统）

每项分析可直接链接到建模元素（将证据链接到检查项目）

基于检查单的形式实现系统、软件、硬件级别的DFA分析



设计阶段（硬件）

Medini支持的硬件失效率预计的工作流程

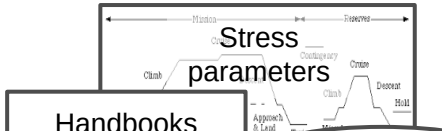
PCB (*Printed Circuit Board)*

BOM (*Bill of Material*):
accurate data, in sync with purchasing, e.g. from SAP, CAD tools

Part Number = *Unique ID for type and manufacturer of components*

C123
C124
Res12
IC42
…

BOM
(Excel, CSV)



Handbooks
(SN29500, IEC62380, etc.)

Part library

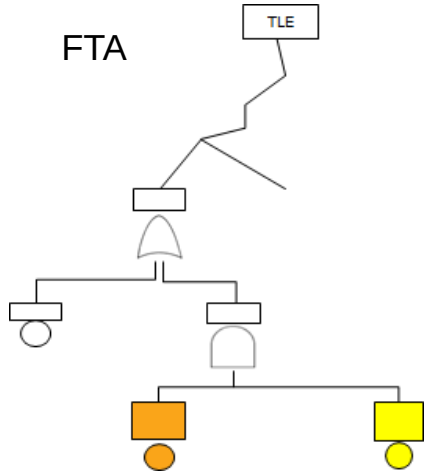
C123	
λ(stress)	open [90%] short [10%]
C124	
λ(stress)	open [90%] short [10%]
Res123	
λ(stress)	open [40%] drift [60%]
IC42	
λ(stress)	FM1 [X1%] FM2 [X2%] …
…	

Basis for FMEDA/FTA

Name	Failure Mode	%	FIT	Critical?	SM	DC	SPF

FMEDA

FTA



medini analyze中建议的可靠性分析方法

跨项目的通用准备 | 指定项目准备 | 分析 | 评估硬件指标

创建硬件库
Create Part Library
- Often imported from EXCEL
- Can be imported from previous projects

Edit Part Data
- E.g. manufacturer

Arrange into folders
- E.g. resistors, capacitors…

Assign to each part type
- Failure Rates
- Adaptation Models for Failure Rates
- Failure Modes
- Probability Distribution of Failure Modes

(taken from diverse industry standards like IEC 62380, SN29500. MIL-HDBK 217 etc.)

确定工作场景并导入BOM
Specify Mission Profile
- Ambient Temperature
- On/Off Cycles

Import Bill-of-Material (BOM)
- Match HW Parts to Types in Library
- Append missing parts to library

Link BOM-based HW Arch. to Higher Level Architecture
- Assign Parts to Components
- Understand relations to hazards

Adjust part type specific load parameters for current project
- Different parameters needed depending on used industry standard (e.g. rated current)
- Scaling formulas can be modified

For each part:
- Is it safety related at all?

For each failure mode*):
- Can it directly cause violation of current safety goal?
- Are there mechanisms to prevent this?
- With which Diagnostic Coverage?
- Can it cause violation of current safety goal in combination with other failures?
- Are there mechanisms to prevent this failure mode from being latent?
- With which Diagnostic Coverage?

Perform quantitative FTA (including part failure rates and Safety Mechanisms)

What is the SPFM?
- Target met?

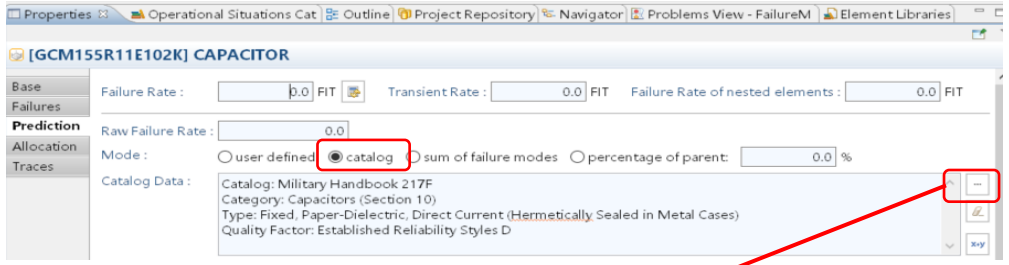
What is the LFM?
- Target met?

What is the PMHF? **)
- Target met?

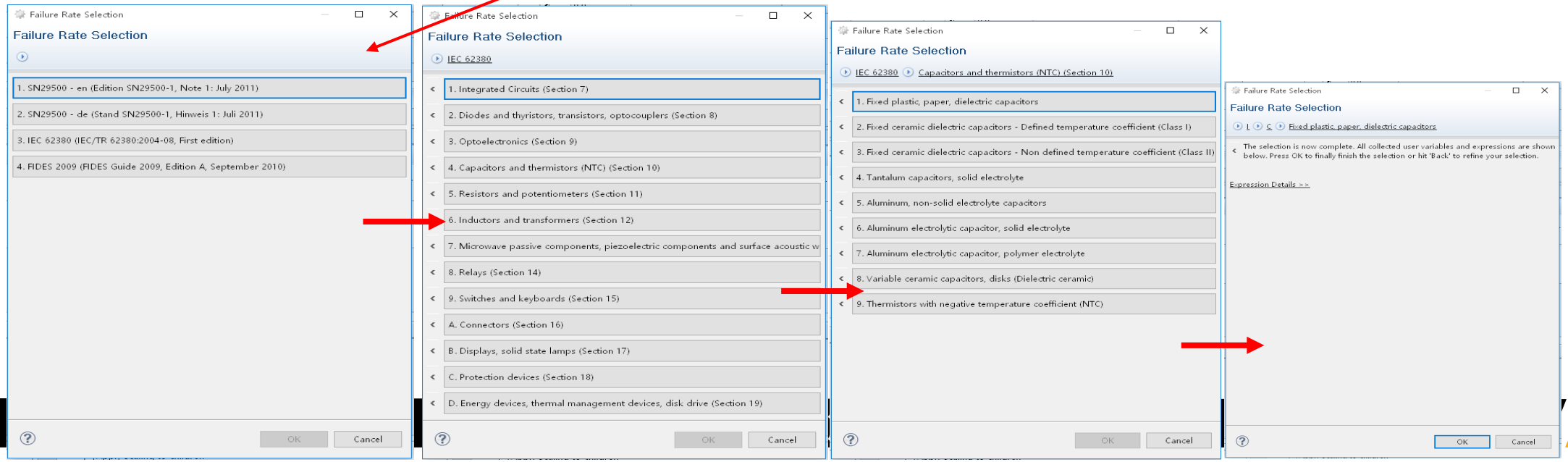
Generate Report

硬件失效率预计: 根据手册自动计算失效率

- 用户可根据项目需求，选择失效率参考手册，工具内置了以下手册：
  - Military Handbook 217F (MIL-HDBK-217F, Notice 2)
  - Siemens Norm 29500 (SN 29500, Editions 1996 and 2011 in German and English)
  - IEC 62380 (IEC TR 62380, 2004)
  - IEC 61709（Edition 3.0, 2017)
  - FIDES Guide 2009 (Edition A, September 2010)
  - GJB/Z 299C - 2006

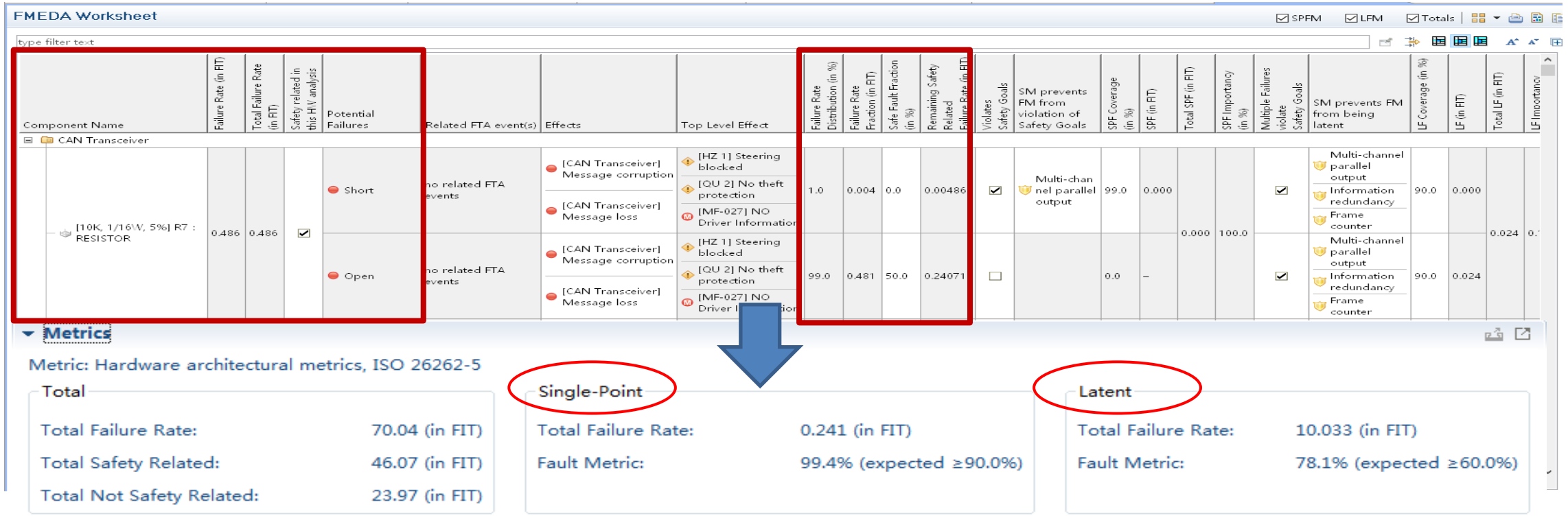


点击，指定具体使用的失效率手册、类别



安全验证: 硬件指标验证（单点、潜在故障指标计算）

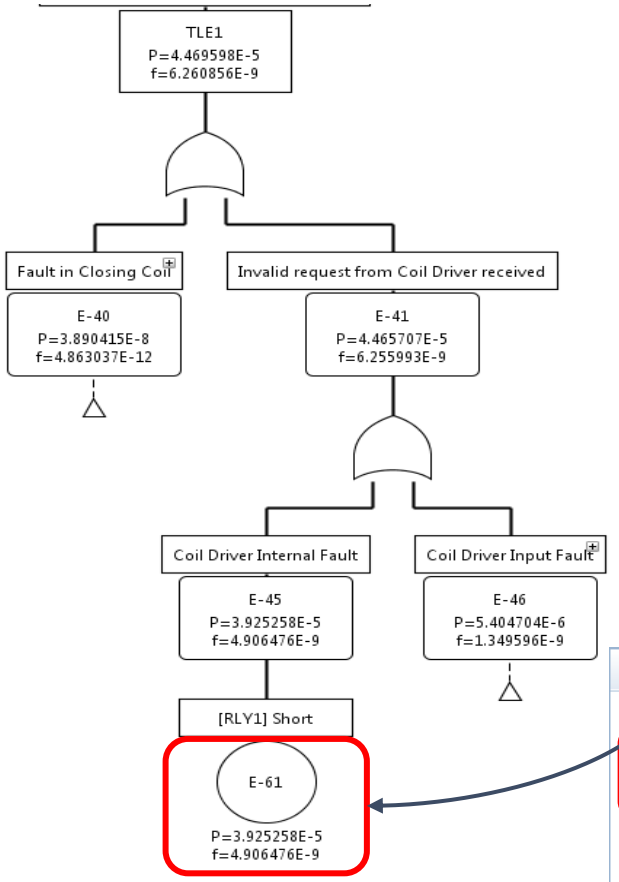
- 硬件诊断覆盖度分析（DC分析）
  - ✓ 支持基于架构自动生成FMEDA/FMECA，并自动填入元器件失效率、失效模式等指标
  - ✓ 基于完整的架构模型，自动计算SPF & LF并提供目标值验证
  - ✓ 支持创建安全机制库

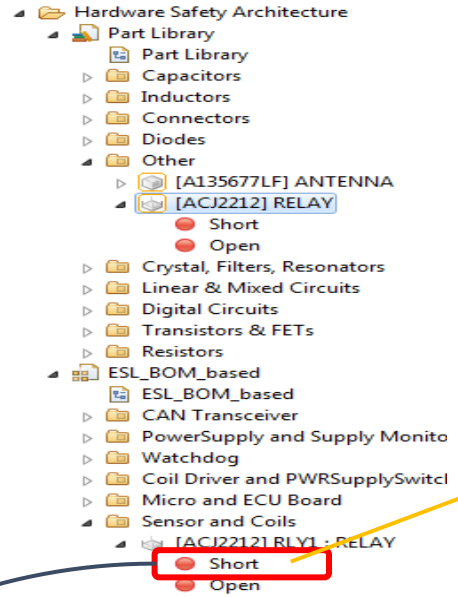


安全验证: 硬件指标验证（随机硬件失效率指标计算）

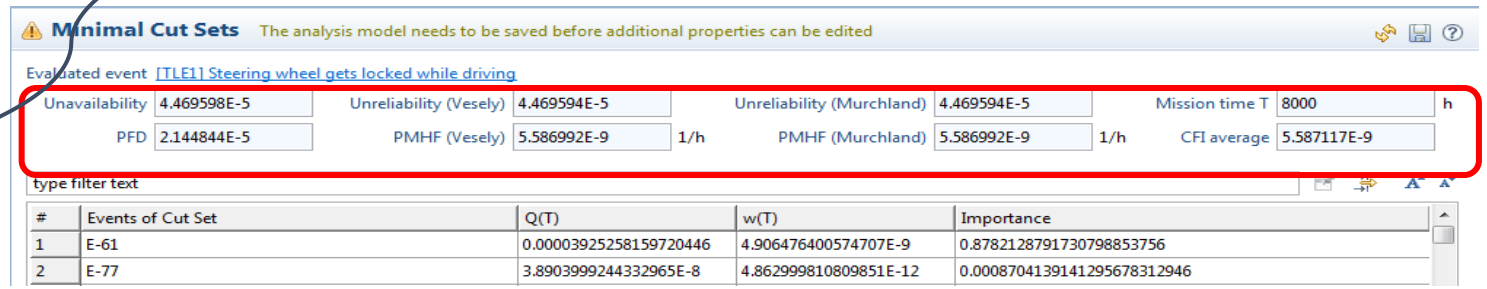
定量故障树分析（Quantitative FTA）

✓ 支持基于FTA计算PMHF

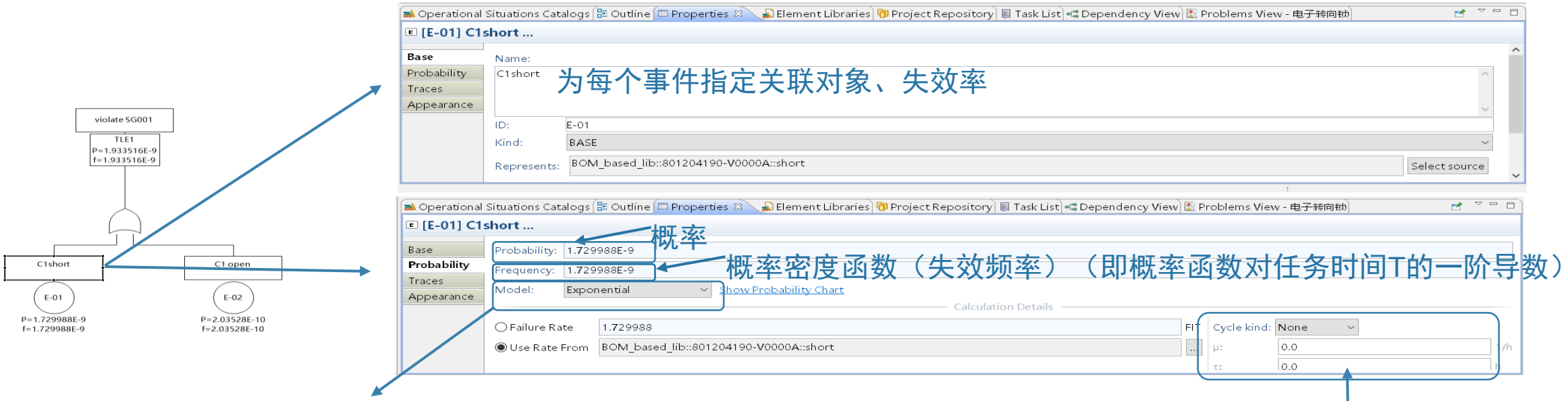




硬件架构(SysML)
元素的
失效模式
自动在FTA中呈现



安全验证: 硬件指标验证（随机硬件失效率指标计算）



medini analyze支持七种不同的概率模型

- 固定概率：[0..1]之间的常数值，不随时间变化。
- 与时间无关的派生概率：其值是从对应的模型元素派生的：
- 指数分布：$P(E) = 1- e^{-\lambda t}$， 其中λ是事件的失效率和t 为任务时间（以小时为单位）。
- 具有恒定修复率的指数分布（即“可修复事件”）：如果组件的故障可以在恒定的修复时间内修复，则：
  $P(E) = \lambda/(\lambda+\mu) * (1- e^{-(\lambda + \mu)t})$，其中λ是组件的故障率（以小时为单位），μ是修复率（每小时），t是任务时间（以小时为单位）。
- 具有测试/监视间隔的指数分布（即“监视事件”）：如果定期监视组件并且更换/修复组件故障，则： $P€ = 1- e^{-\lambda(t \bmod tau)}$
- Weibull分布：$P(E) = 1- e^{-(\max\{t - g, 0\} / a)beta}$
- 自定义：允许用户提供几乎任何数学表达式或脚本来计算概率P（E）

安全验证: 硬件指标验证（随机硬件失效率指标计算）

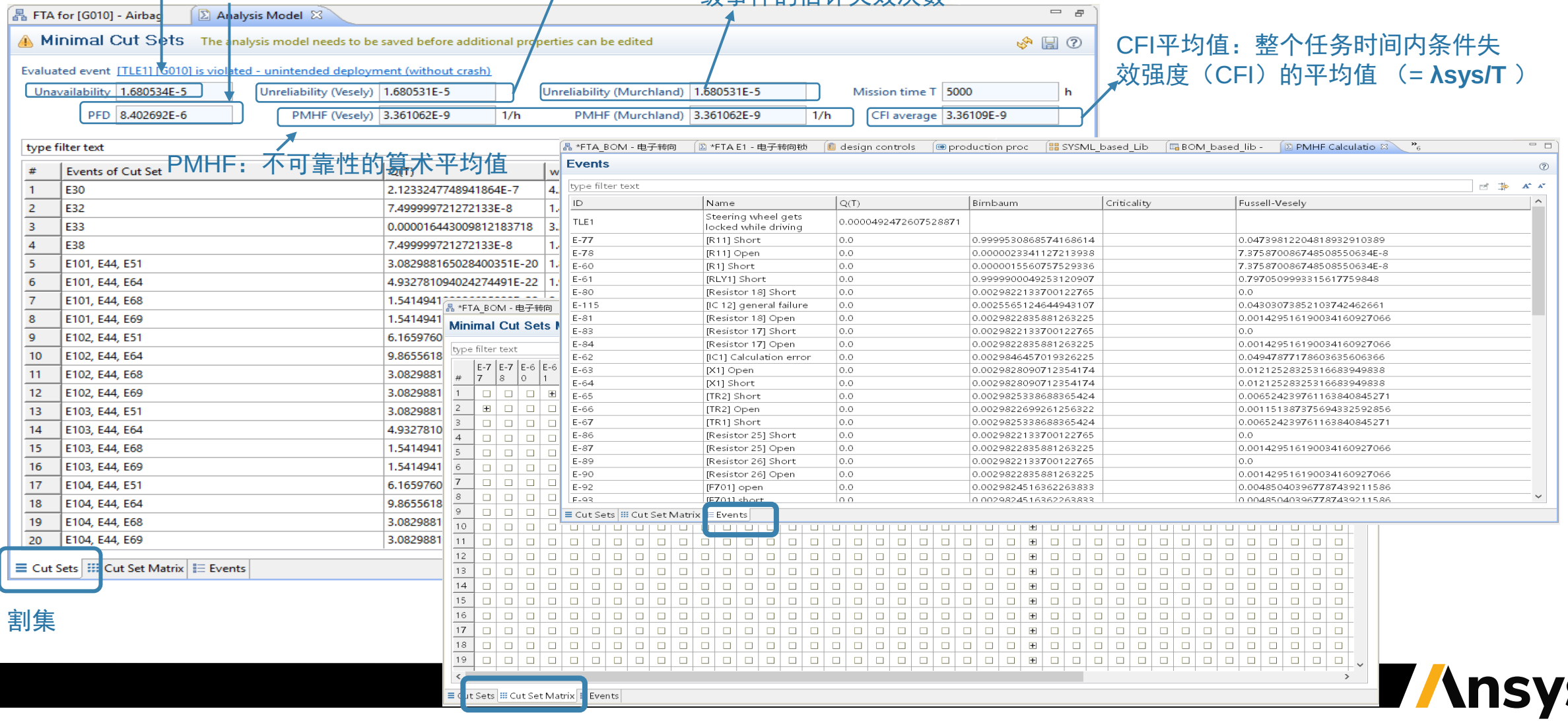
不可用性：顶级事件在任务时间T发生的概率

PFD：不可用性的算术平均值

不可靠性（Vesely）：在[0..T]区间内发生顶级事件的概率

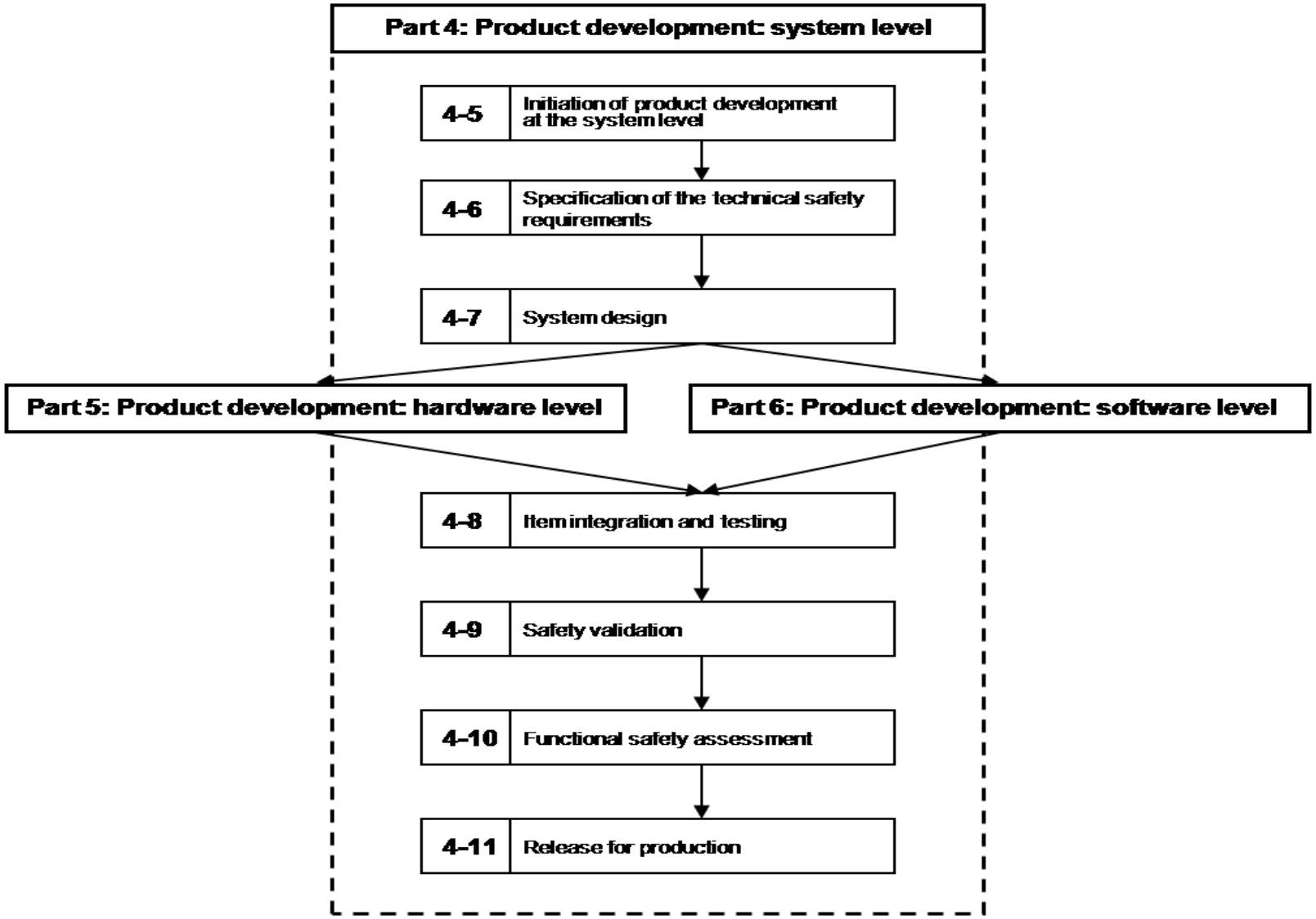
不可靠性（Murchland）：顶级事件的估计失效次数

CFI平均值：整个任务时间内条件失效强度（CFI）的平均值 （= **λsys/T** ）



割集

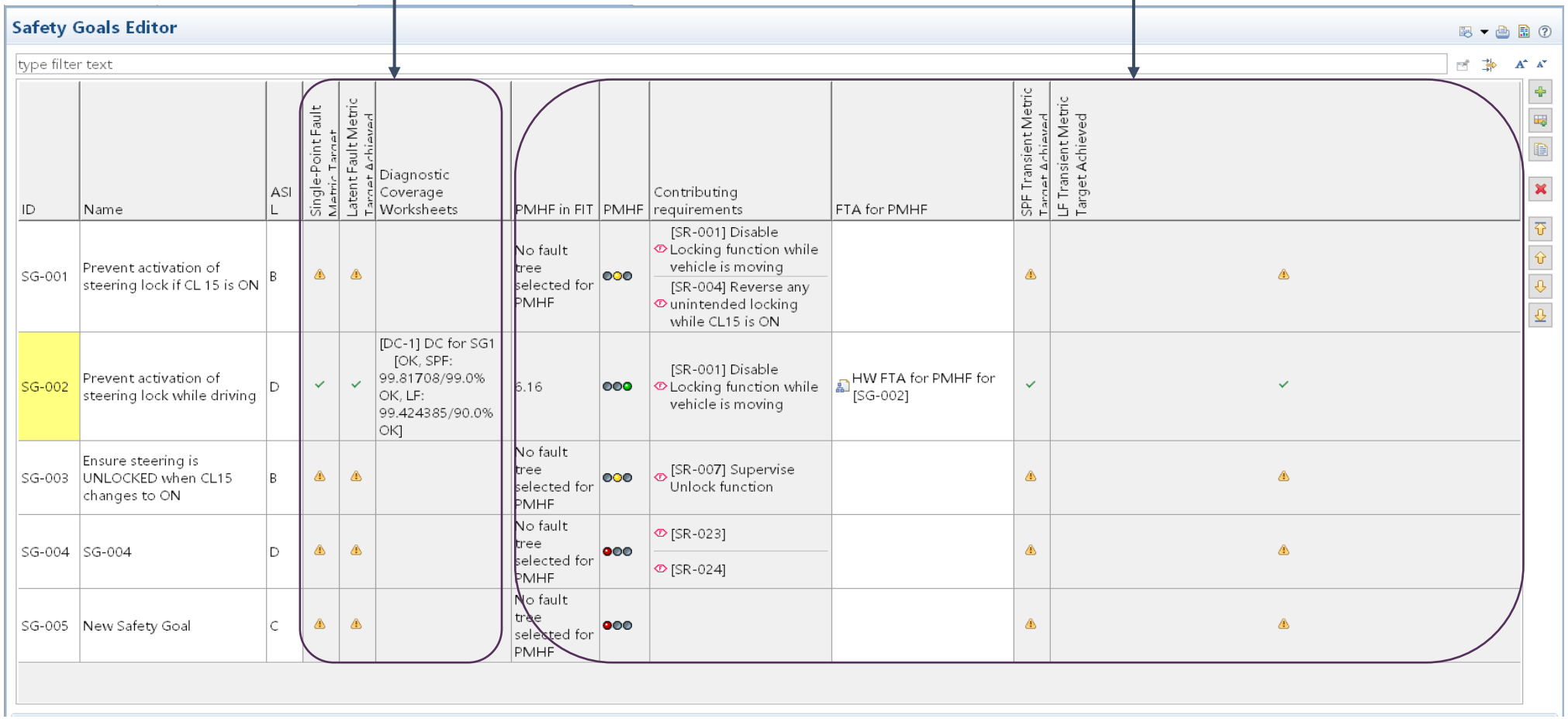
安全验证与评审


Part 4: Product development: system level
4-5
Initiation of product development at the system level
4-6
Specification of the technical safety requirements
4-7
System design
Part 5: Product development: hardware level
Part 6: Product development: software level
4-8
Item integration and testing
4-9
Safety validation
4-10
Functional safety assessment
4-11
Release for production

验证每个安全目标的要求都满足

FMEDA 验证SPFM& LFM

FTA 验证 PMHF



Safety Goals Editor

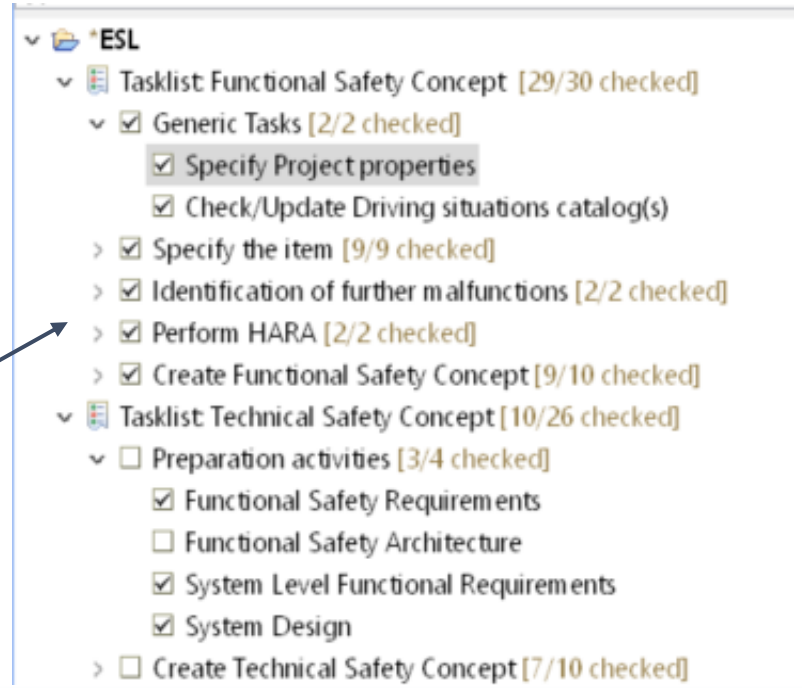
type filter text

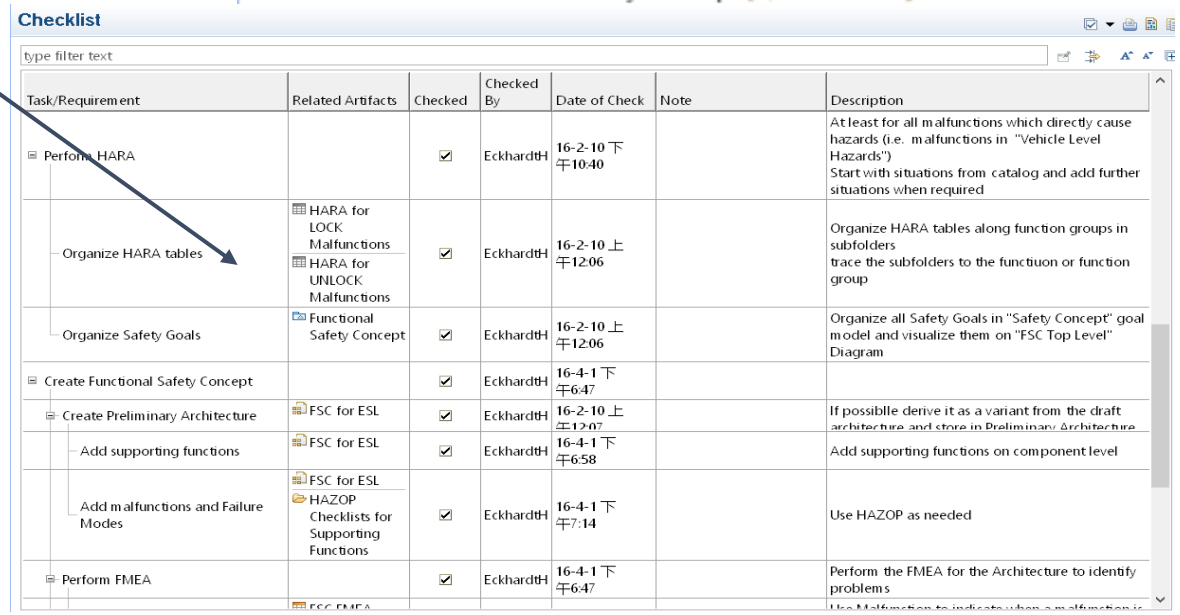
ID	Name	ASIL	Single-Point Fault Metric Target	Latent Fault Metric Target Achieved	Diagnostic Coverage Worksheets	PMHF in FIT	PMHF	Contributing requirements	FTA for PMHF	SPF Transient Metric Target Achieved	LF Transient Metric Target Achieved
SG-001	Prevent activation of steering lock if CL 15 is ON	B	⚠	⚠		No fault tree selected for PMHF		[SR-001] Disable Locking function while vehicle is moving [SR-004] Reverse any unintended locking while CL15 is ON		⚠	⚠
SG-002	Prevent activation of steering lock while driving	D	✓	✓	[DC-1] DC for SG1 [OK, SPF: 99.81708/99.0% OK, LF: 99.424385/90.0% OK]	6.16		[SR-001] Disable Locking function while vehicle is moving	HW FTA for PMHF for [SG-002]	✓	✓
SG-003	Ensure steering is UNLOCKED when CL15 changes to ON	B	⚠	⚠		No fault tree selected for PMHF		[SR-007] Supervise Unlock function		⚠	⚠
SG-004	SG-004	D	⚠	⚠		No fault tree selected for PMHF		[SR-023] [SR-024]		⚠	⚠
SG-005	New Safety Goal	C	⚠	⚠		No fault tree selected for PMHF				⚠	⚠

安全计划- 任务检查表

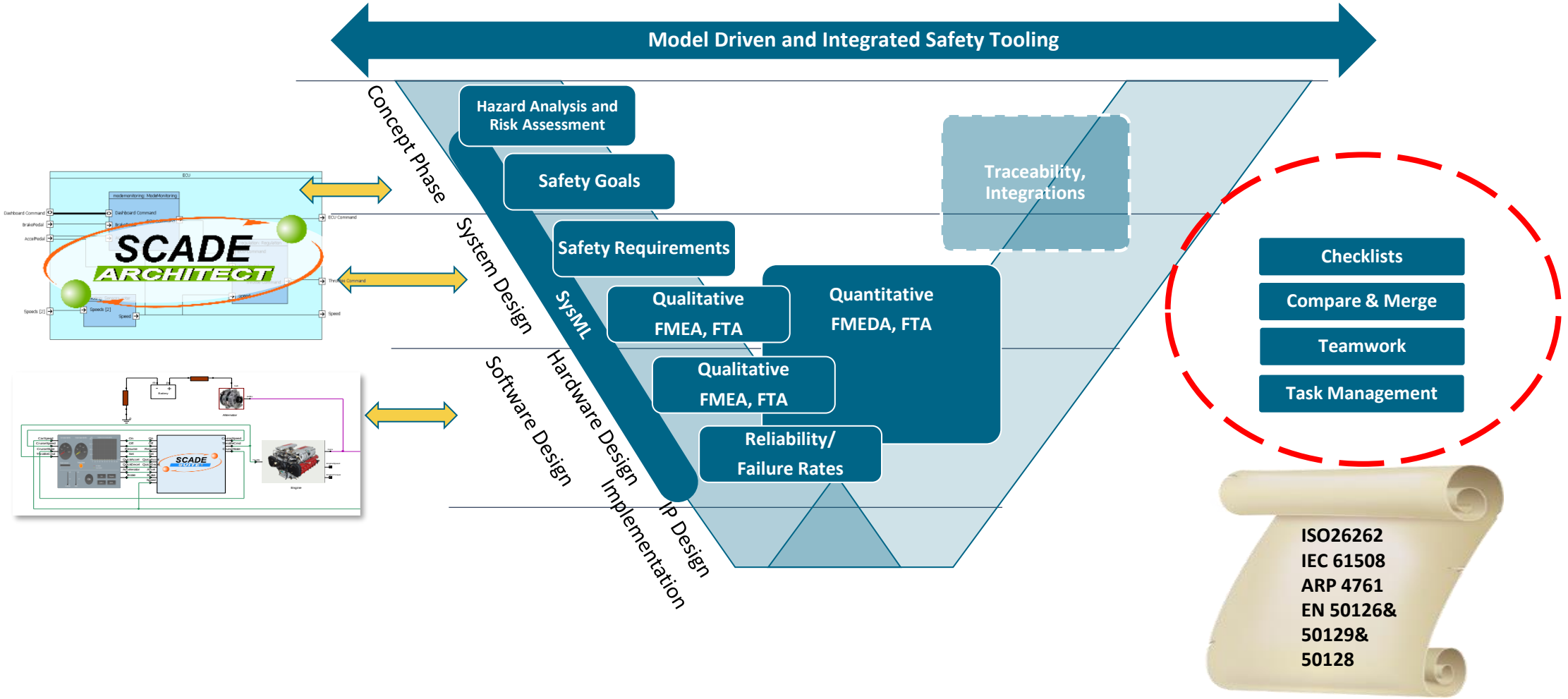
- **任务检查表（Checklist）可用于验证和确认活动、安全计划和进度跟踪。工具支持：**

  - 具有层次结构检查项和可自定义属性的检查单定义
  - 直接链接到建模元素（例如用于将证据链接到检查项目）
  - 提供大量预定义检查单模板





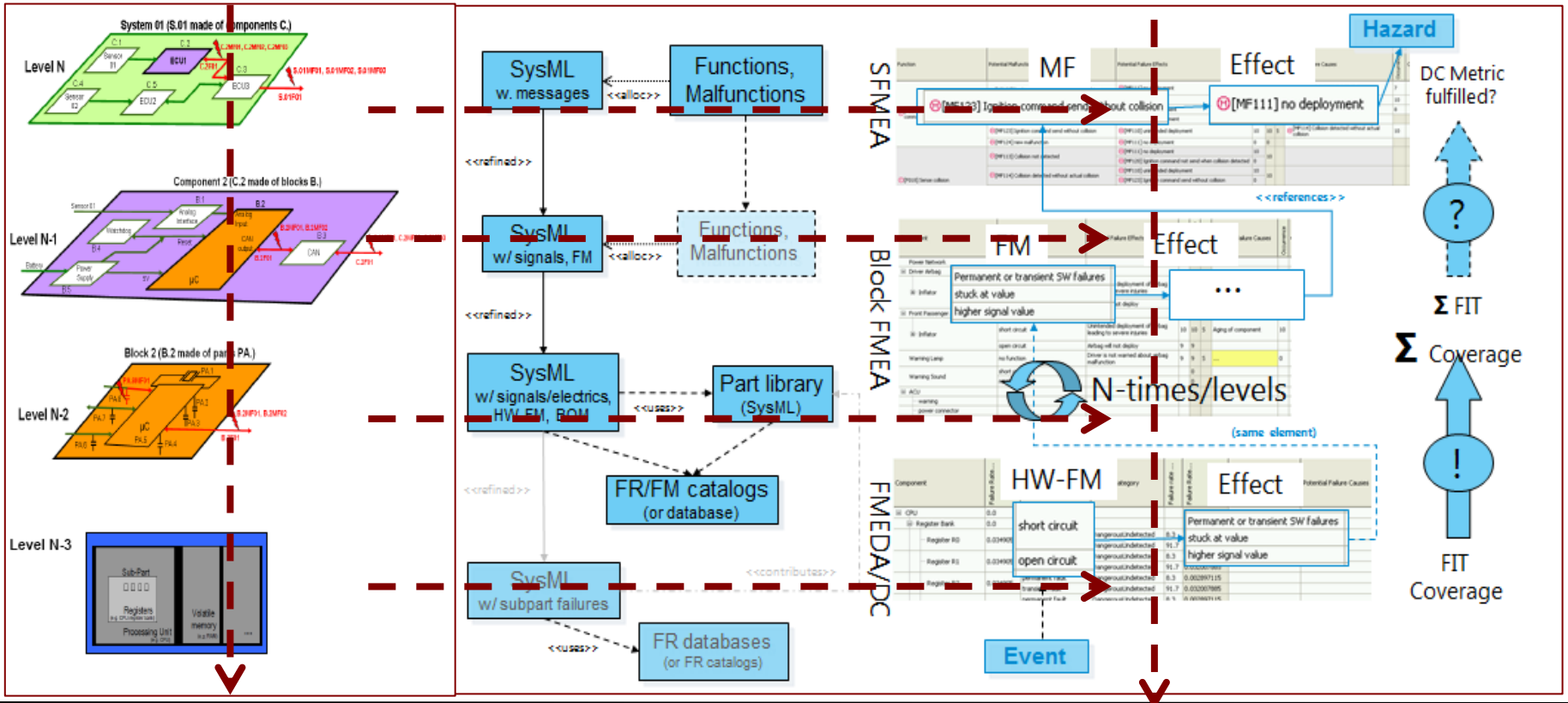
项目管理：一致性、可跟踪性和高效率



项目管理：成熟的跟踪功能

任何信息元素之间可以定义追踪关系

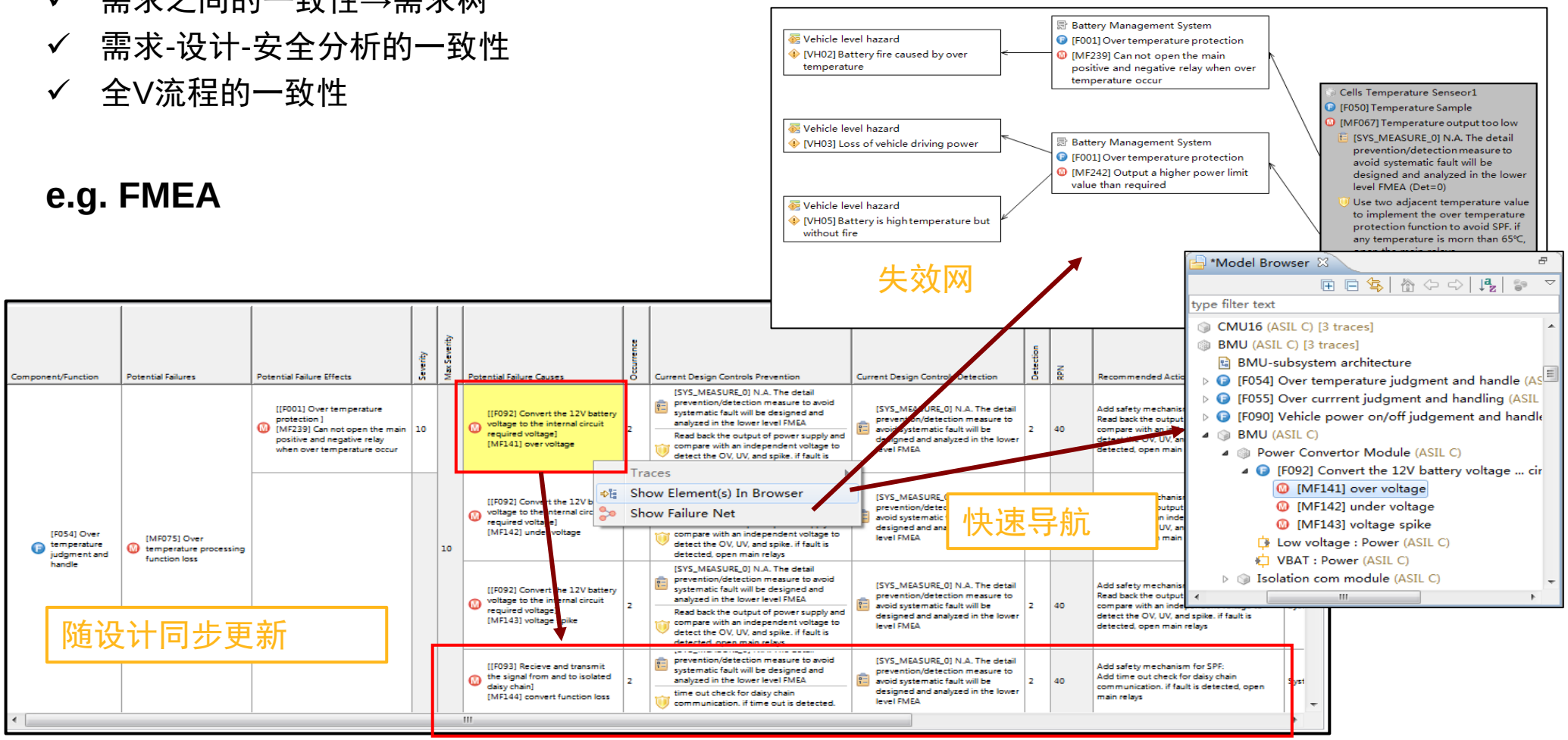
- ✓ 需求和架构之间的跟踪（Allocation of SRs）
- ✓ 架构（系统/硬件/软件）之间的跟踪、变更管理（结构化、分层设计）
- ✓ 不同层级之间证据链的跟踪（一致性）
- ✓ 失效模式、效应之间的跟踪（Failure Net）



项目管理：全流程的一致性

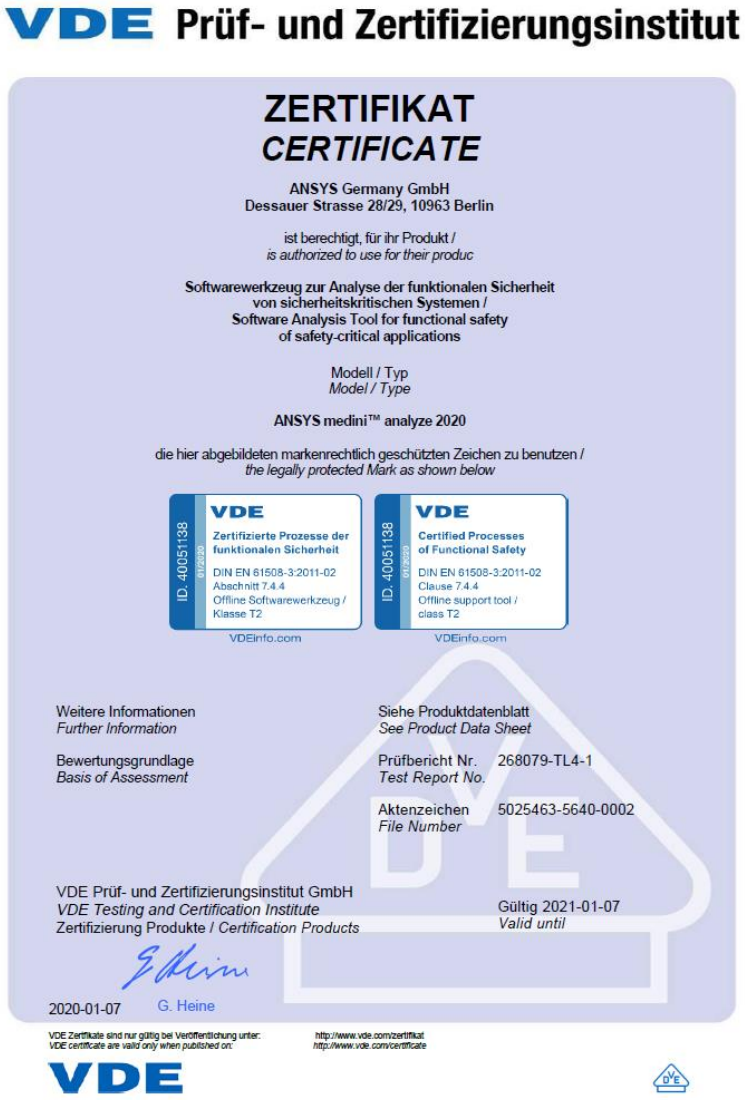
- ✓ 需求之间的一致性→需求树
- ✓ 需求-设计-安全分析的一致性
- ✓ 全V流程的一致性

e.g. FMEA



工具认证(IEC 61508)

- IEC 61508将“离线支持工具”分类为T1-T3
- Medini目前拿到了T2类别的工具认证证书
- T2类别：工具“支持对设计或可执行代码的测试或验证”
- medini可以支持SIL4**或**ASILD**级别的安全分析活动，**通过将medini的工具鉴定包在客户的环境运行，可以将工具鉴定为TCL3级别的工具



VDE Prüf- und Zertifizierungsinstitut

ZERTIFIKAT
CERTIFICATE

ANSYS Germany GmbH
Dessauer Strasse 28/29, 10963 Berlin

ist berechtigt, für ihr Produkt /
is authorized to use for their produc

Softwarewerkzeug zur Analyse der funktionalen Sicherheit
von sicherheitskritischen Systemen /
Software Analysis Tool for functional safety
of safety-critical applications

Modell / Typ
Model / Type

ANSYS medini™ analyze 2020

die hier abgebildeten markenrechtlich geschützten Zeichen zu benutzen /
the legally protected Mark as shown below

VDE
Zertifizierte Prozesse der funktionalen Sicherheit
DIN EN 61508-3:2011-02
Abschnitt 7.4.4
Offline Softwarewerkzeug / Klasse T2
ID. 40051138
VDEinfo.com

VDE
Certified Processes of Functional Safety
DIN EN 61508-3:2011-02
Clause 7.4.4
Offline support tool / class T2
ID. 40051138
VDEinfo.com

Weitere Informationen
Further Information

Siehe Produktdatenblatt
See Product Data Sheet

Bewertungsgrundlage
Basis of Assessment

Prüfbericht Nr. 268079-TL4-1
Test Report No.

Aktenzeichen 5025463-5640-0002
File Number

VDE Prüf- und Zertifizierungsinstitut GmbH
VDE Testing and Certification Institute
Zertifizierung Produkte / *Certification Products*

Gültig 2021-01-07
Valid until

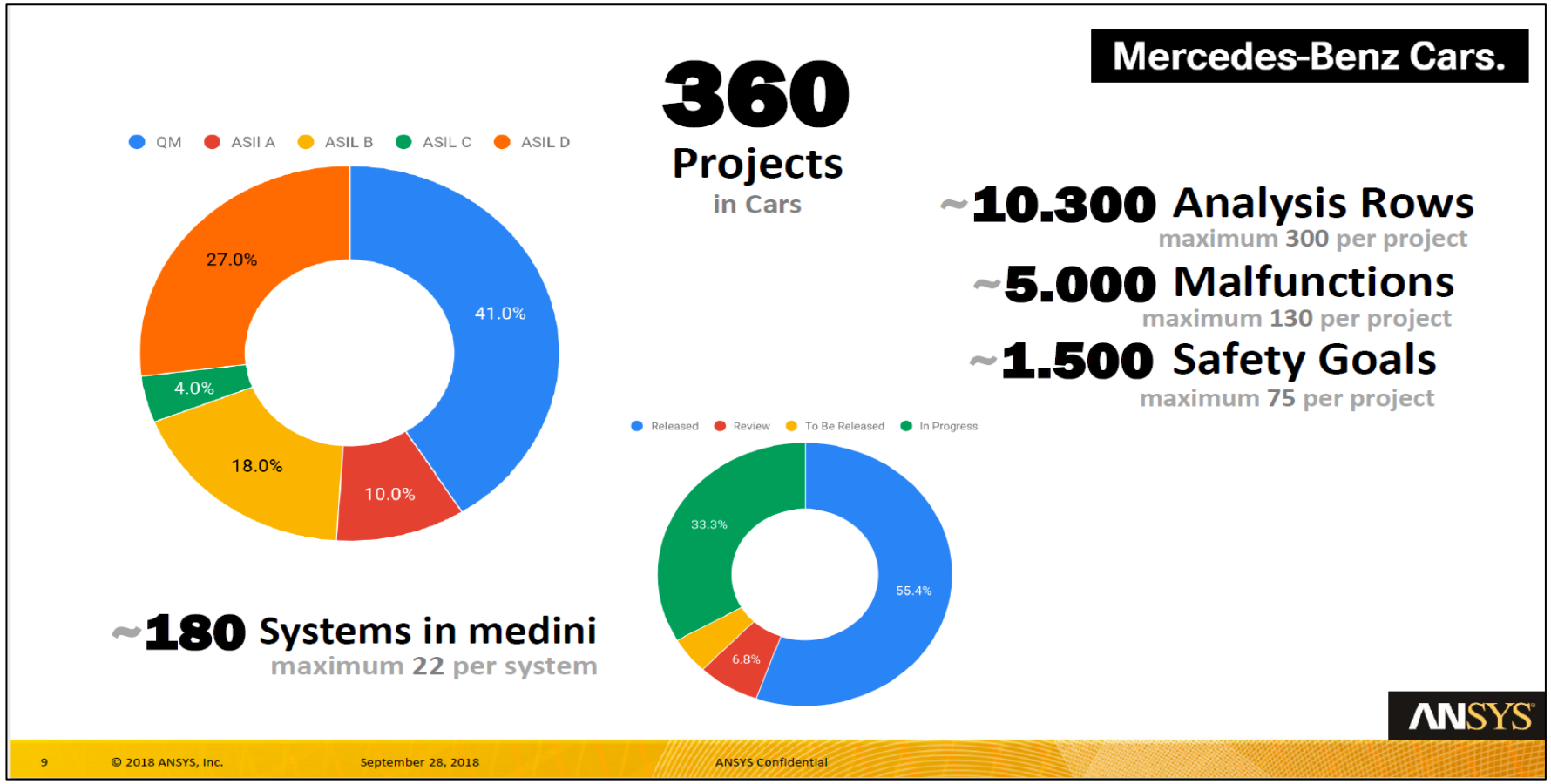
2020-01-07 G. Heine

VDE Zertifikate sind nur gültig bei Veröffentlichung unter:
VDE certificate are valid only when published on:
http://www.vde.com/zertifikat
http://www.vde.com/certificate

VDE

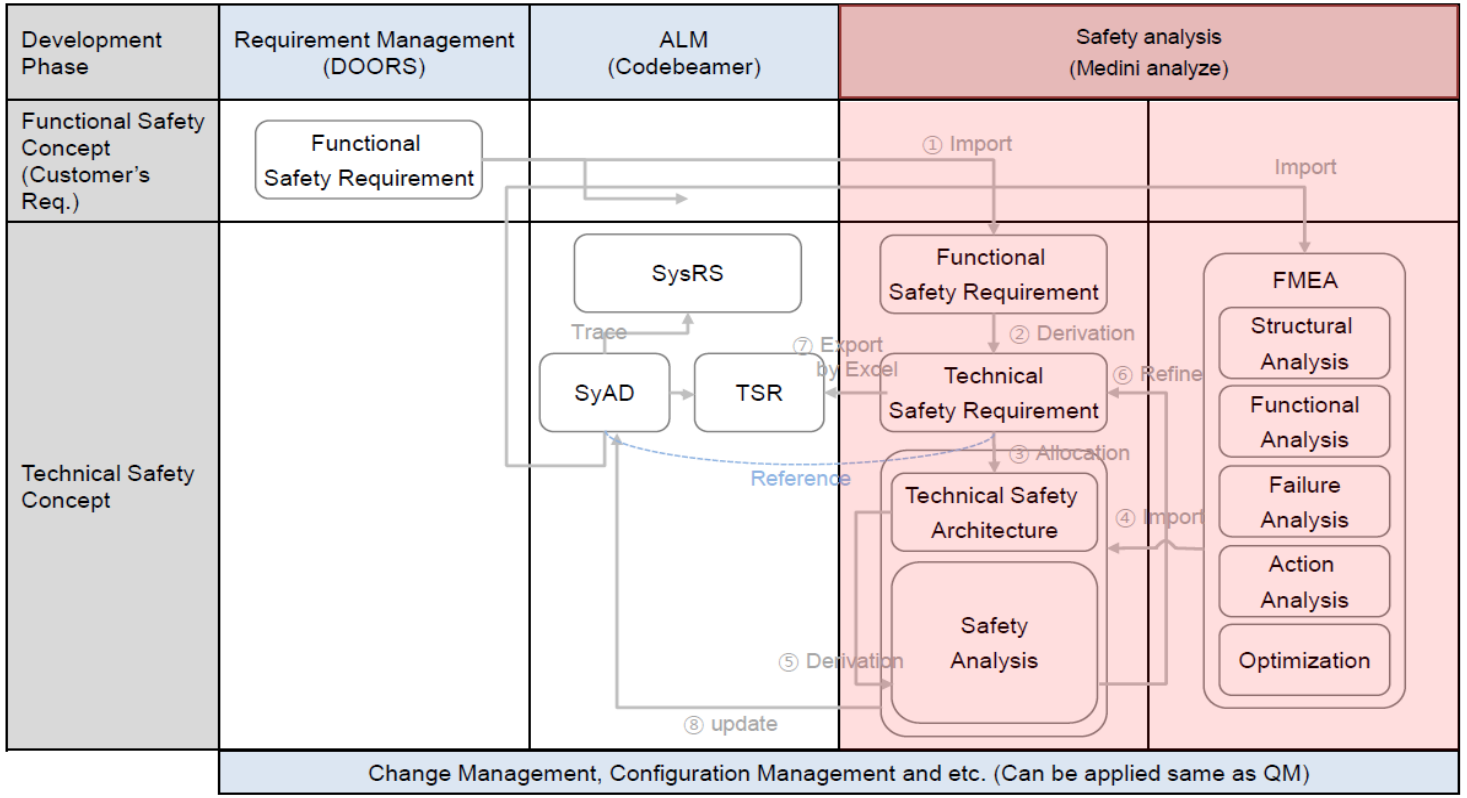
客户案例-戴姆勒

DAIMLER

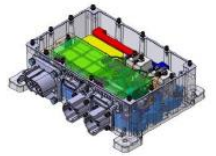


- 戴姆勒集团目前有大约**360个项目**在medini上进行安全分析，使用用户约**300人**
- medini确保了所有项目数据，安全目标和分析工作产品都是**一致且可追溯的**
- 几乎所有的手动检查工作现在都由**medini自动完成**

客户案例-LG



✓ DC Charging box (ASIL-C)
- DC fast charging controller for PHEV and EV
- OEM : Classified
- Project Period : 2015 ~



✓ BMS (ASIL-C)
- Battery management system for EV
- OEM : Classified
- Project Period : 2015 ~

✓ Telematics (ASIL-B)
- In-Vehicle safety and security service
- OEM : Classified
- Project Period : 2015 ~

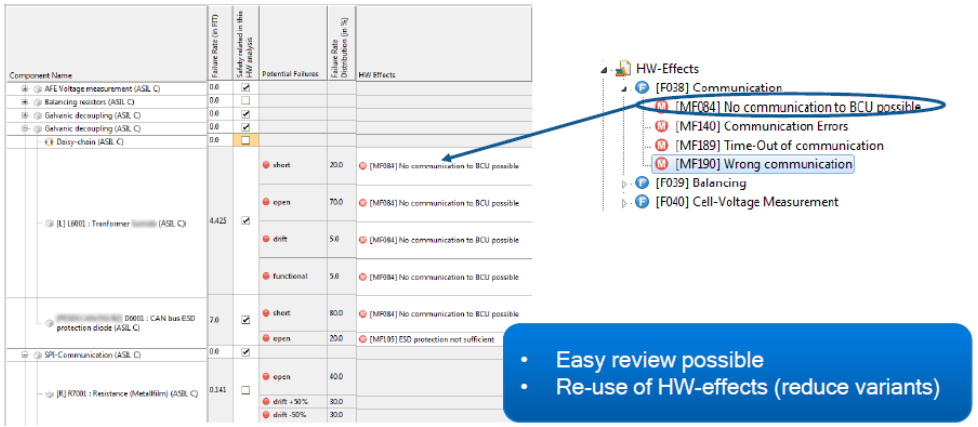
✓ ADAS (ASIL-B)
- Multi-purpose camera system for ADAS
- OEM : Classified
- Project Period : 2017 ~

- LG目前把medini作为整体工具链的重要一环去做安全分析
- 提高了工作效率，减少了不必要的工作
- 轻松的实现安全工作的一致性和可追溯性

客户案例-博世

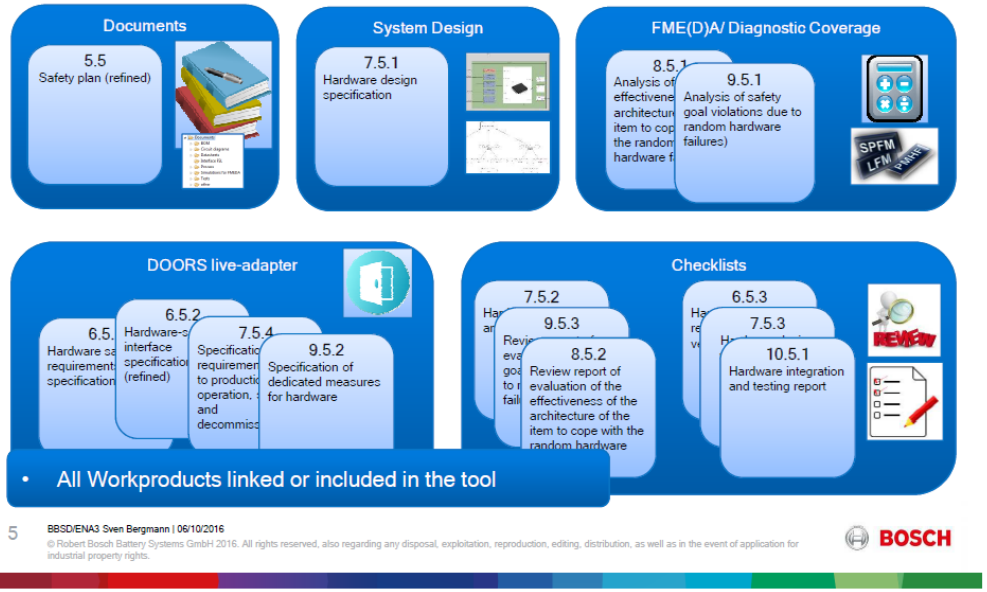
Safety-Analysis
HW-Effects

- Define HW-(mal)functions
- Drag and drop HW-Effects into FMEDA



- Easy review possible
- Re-use of HW-effects (reduce variants)

HW workproducts
ISO26262 Part 5 mapping to medini



- All Workproducts linked or included in the tool

- 博世把硬件部分的安全分析和定量计算放到medini中做分析
- 通过复用失效率手册，减少人工工作，节省了大量的时间
- 轻松的实现需求，分析，设计之间的交互，保证可追溯性和一致性

会议议程

- 汽车领域的安全要求及挑战
- ANSYS medini 基于模型的系统安全解决方案
- ANSYS medini 在完整的ISO 26262 安全生命周期中的应用
- 小结

medini: 优势总结

完整

遵循安全标准，支持全生命周期的开发验证

- 提供完整的功能安全综合解决方案，集成安全需求管理和系统架构设计
- 支持风险分析和风险评估，操作场景，安全目标和要求，SIL确定/分解，设计FMEA，过程FMEA，FMEDA，故障树分析，单点故障和潜在故障硬件度量，故障率等级，依据故障率手册的可靠性预测

高效

丰富的模板，支持重用和自动化

- 可定制的最佳实践模板；丰富的数据库；自动生成表格、自动评估故障树、自动硬件指标计算
- 大大节省人力和时间

管理

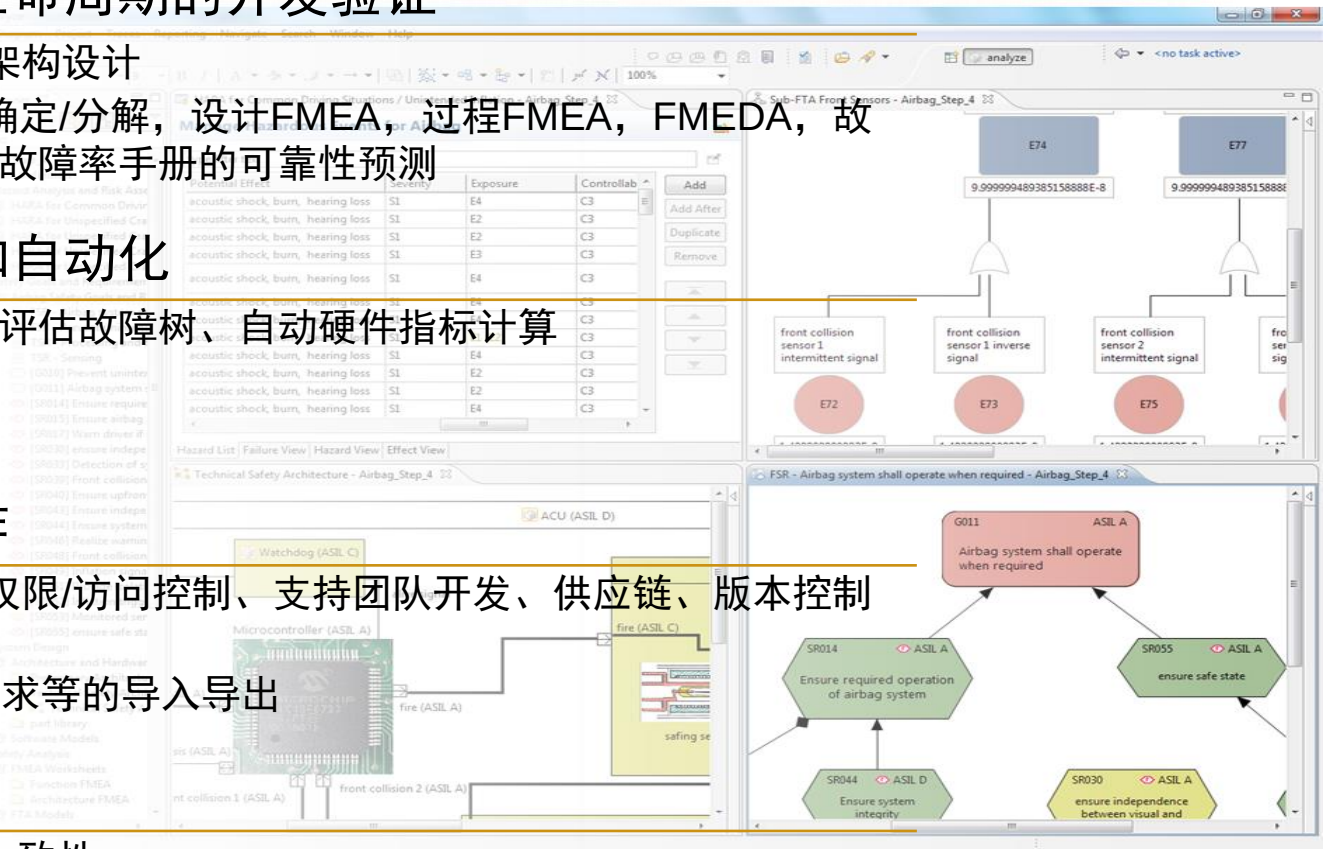
提升项目管理和团队协作

- 支持任务管理、可追溯性管理、变更管理和审查/评估、角色/权限/访问控制、支持团队开发、供应链、版本控制和PLM系统的集成，支持任意项目的差异分析和模型合并
- 支持与其他工具的桥接，支持FMEA、架构模型、BOM表、需求等的导入导出

一致

确保追踪性、一致性

基于SysML架构模型，提供完整清晰的证据链，确保追踪性、一致性



Q&A
欢迎您的提问