基于模型的
功能安全和可靠性工程解决方案

杨瑾婧 高级咨询

ANSYS

议程

- ANASYS Medini 与 功能安全
- ANSYS Medini 安全分析在全生命周期中的应用
- 小结

什么是功能安全？

任何技术系统的采用都可能对人类造成危害

直接-- 燃烧，电击，物理伤害等

间接-- 污染环境

- **安全 safety**

  没有不可接受/不合理的风险

- **功能安全functional safety**
  - 不存在“由于系统功能失效行为引起的危险”而引起的不可接受的风险

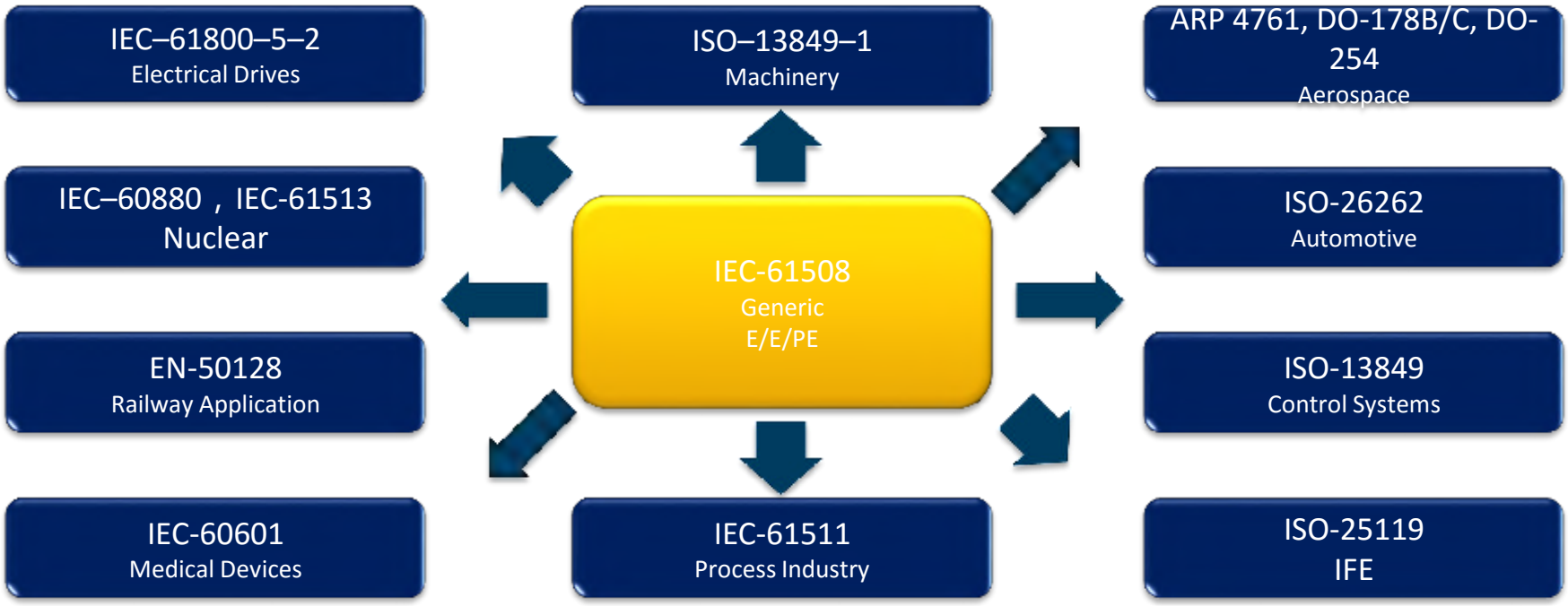
    示例1：汽车制动系统的潜在不可用性导致之后的碰撞是功能安全性的问题

    示例2：有害（例如有毒）材料的使用，不是功能安全的问题

- **风险risk**

  伤害发生的概率和危害的严重程度的组合

功能安全标准


IEC–61800–5–2
Electrical Drives
IEC–60880，IEC-61513
Nuclear
EN-50128
Railway Application
IEC-60601
Medical Devices
ISO–13849–1
Machinery
IEC-61508
Generic
E/E/PE
IEC-61511
Process Industry
ARP 4761, DO-178B/C, DO-254
Aerospace
ISO-26262
Automotive
ISO-13849
Control Systems
ISO-25119
IFE

工程中有哪些功能安全活动?

分析

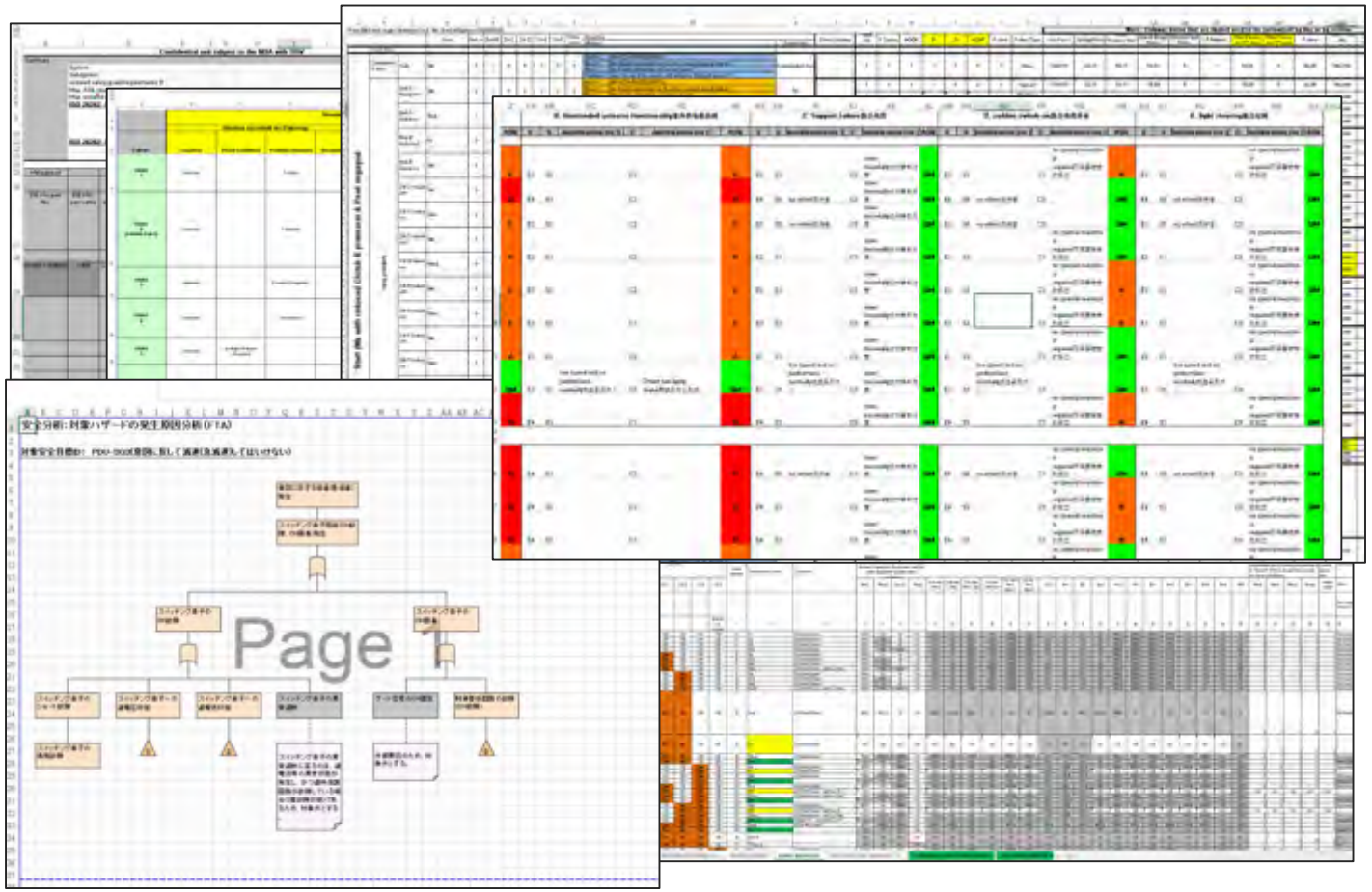
- 危害和可操作性分析– HAZOP
- 危害分析和风险评估– HARA
- 故障模式和影响分析– FMEA (定性)
- 故障模式，影响和诊断分析– FMEDA (定量)/FMECA
- 故障树分析– FTA (定性&定量)
- 事件树分析– ETA (定性&定量)
- 数学计算（可靠性和概率计算）或派生数据库

概念定义

- 安全目标和安全需求定义
- 架构设计： 从初步的系统级到HW / SW架构
- 可追溯性和分配

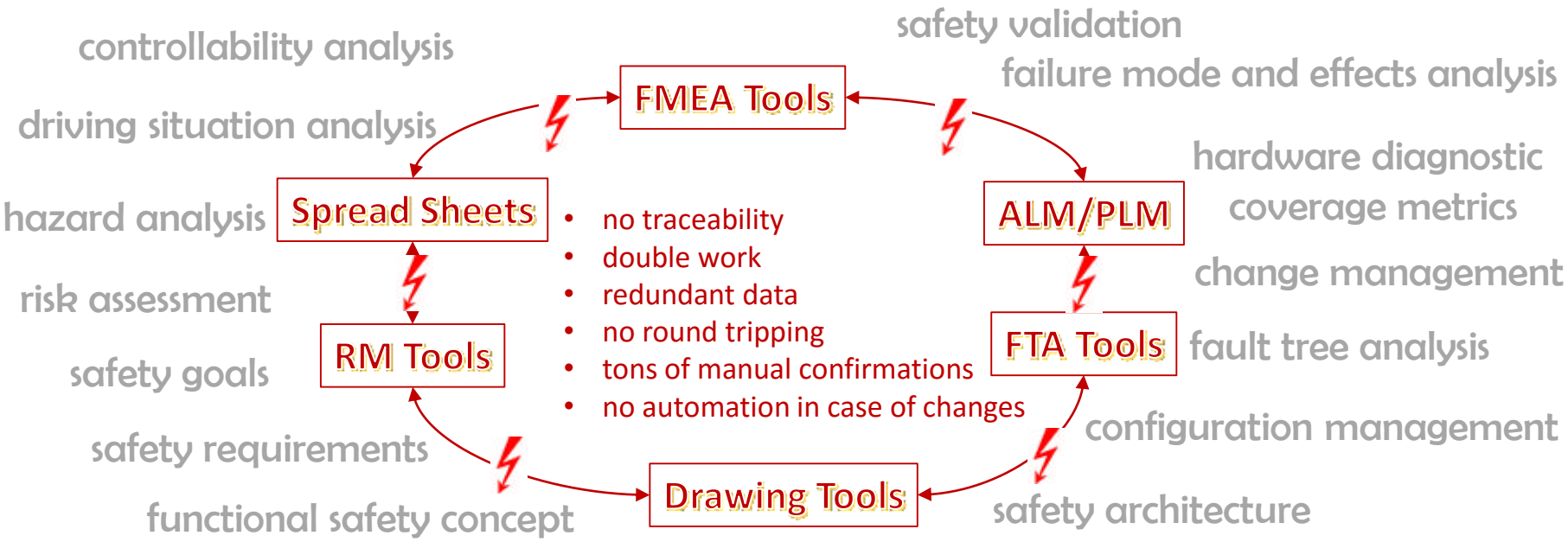
…目前大多采用的手段是excel …

… 实际工程中是怎样做的?



功能安全的传统方法：单个任务的点工具

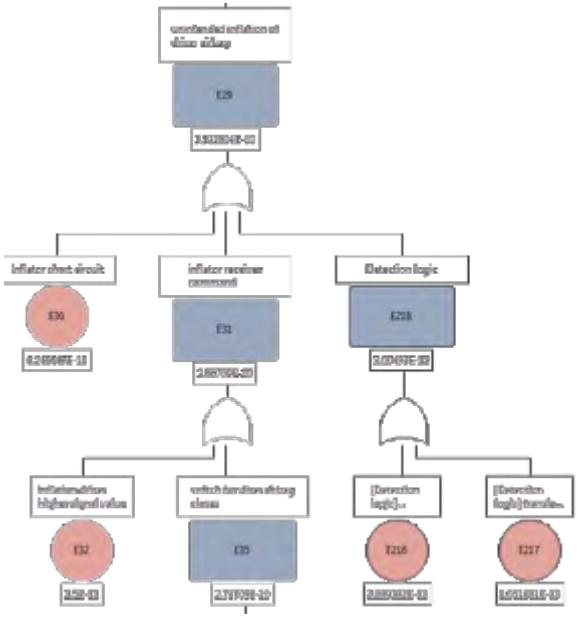
工程与安全分析之间没有整合



使用点工具的传统方法容易出错，耗时且浪费人力

ANSYS medini: 综合安全分析解决方案

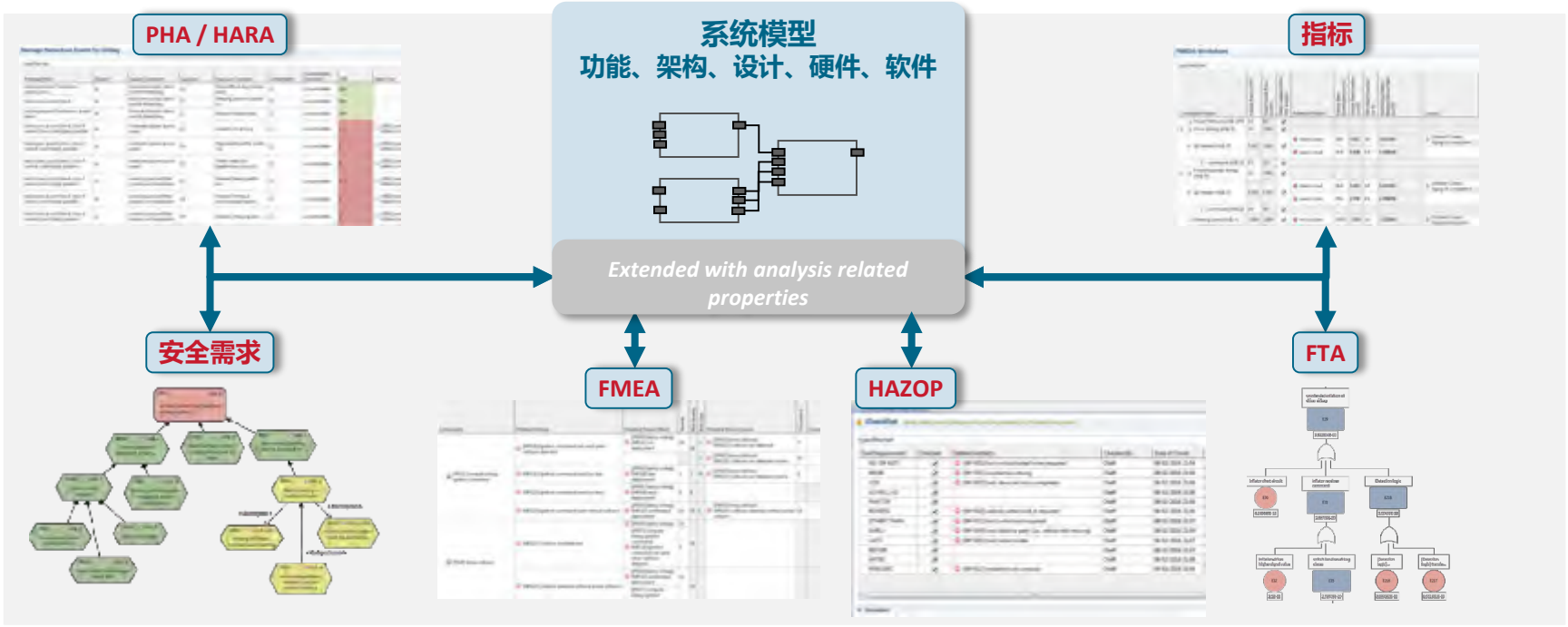
- 功能安全与可靠性工程的综合解决方案
- 符合最先进的标准IEC 61508，ISO 26262，VDA-Band 4，SAE J1739，SN 29500，IEC 62380，MIL HDBK 217F，FIDES，ARP 4761和DO-254（开发中）
- 结合基于模型的方法，在概念、系统、软件和硬件层面有效应用安全可靠性工程方法
- 减少高达50%的成本和上市时间，保证安全和可靠性



Fault Tree Analysis

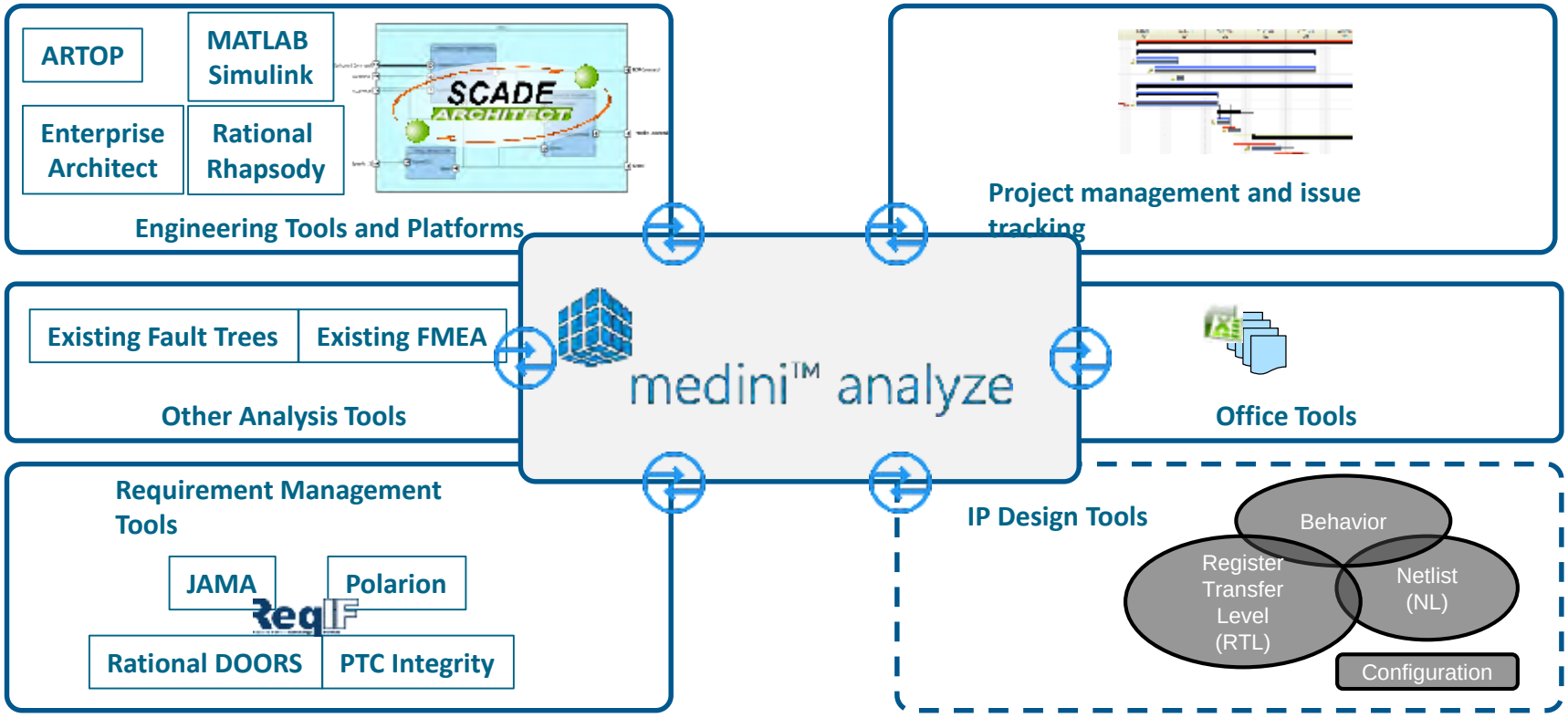
medini: 基于模型的安全分析

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



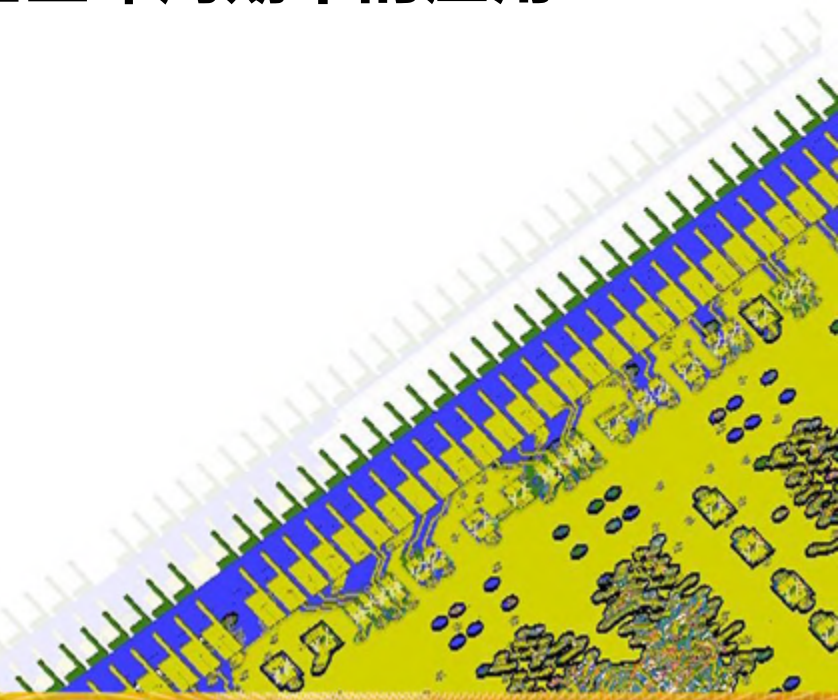
基于模型的方法确保无与伦比的一致性、可跟踪性和高效率

与其他工程工具集成

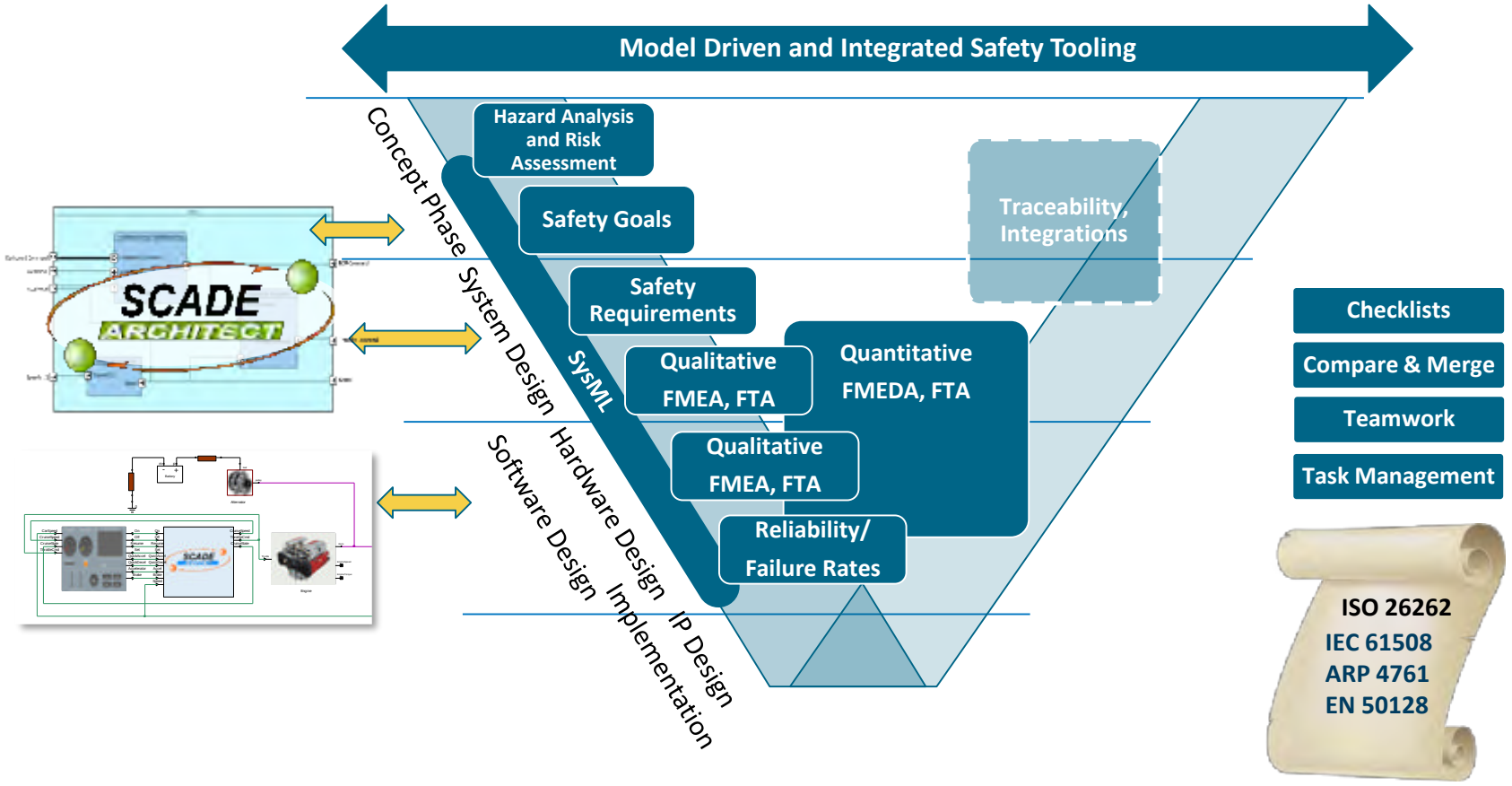


Safe Time and ensure Consistency in Case of Design Iterations

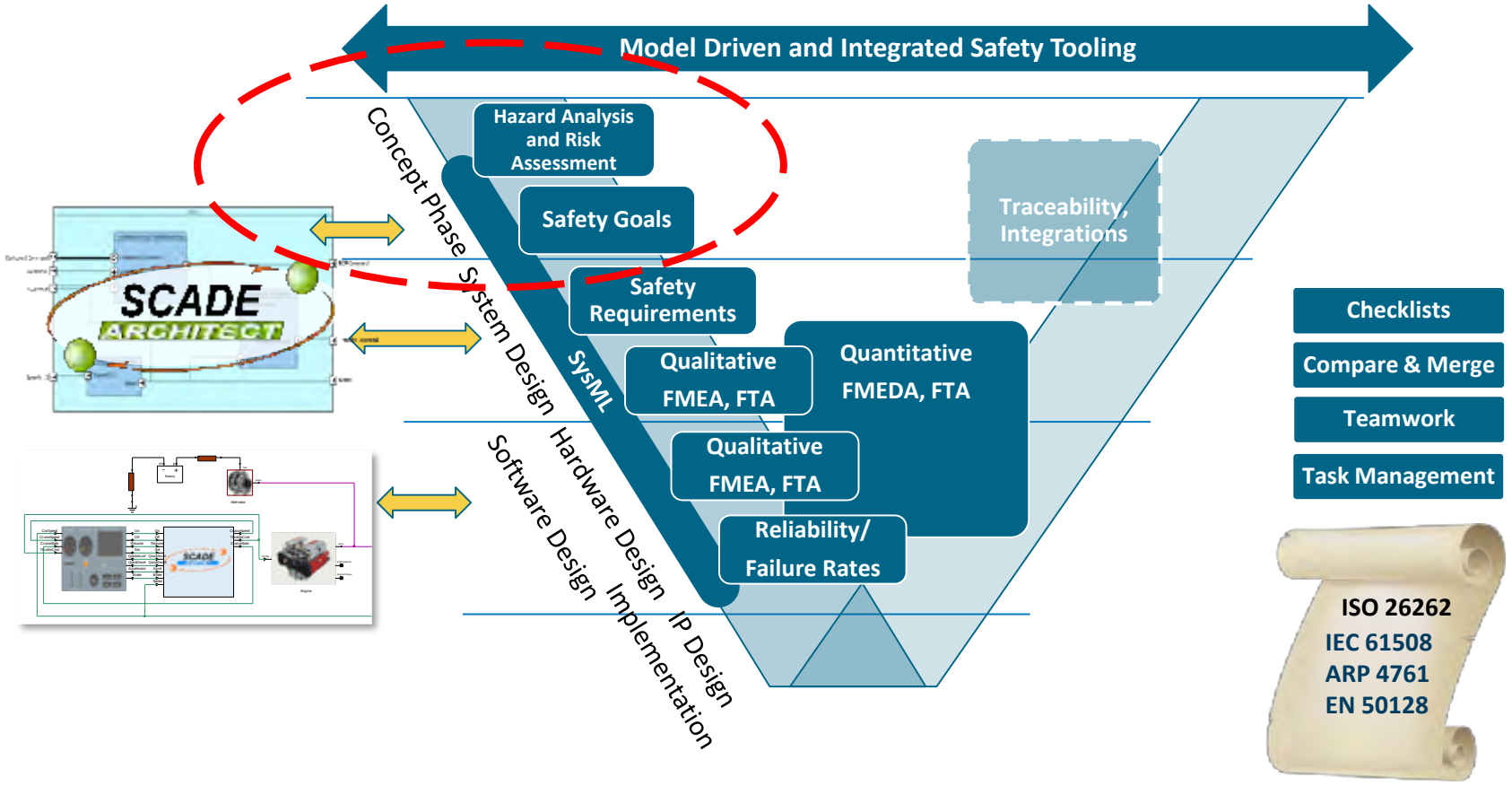
medini 安全分析在全生命周期中的应用



medini覆盖整个安全生命周期



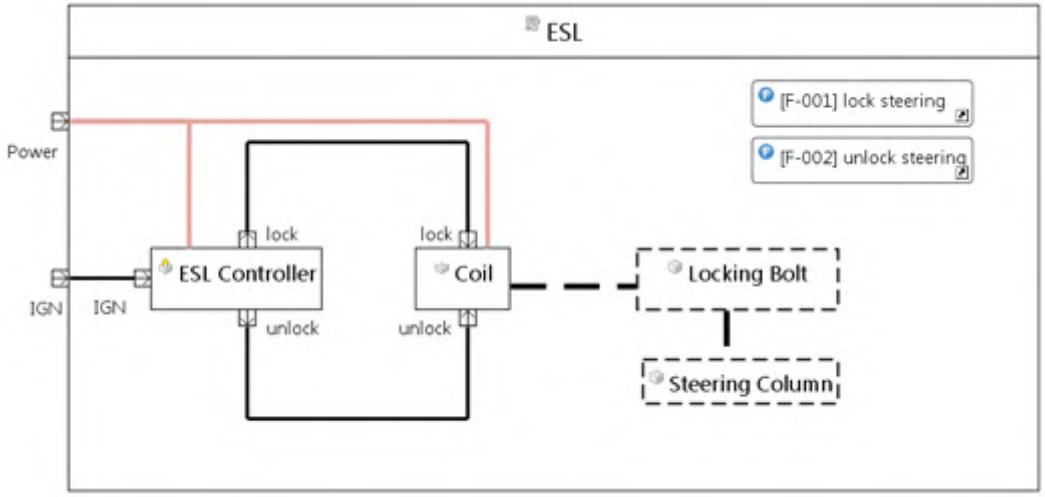
概念阶段：基于模型的PHA/HARA



概念阶段：基于模型的PHA/HARA

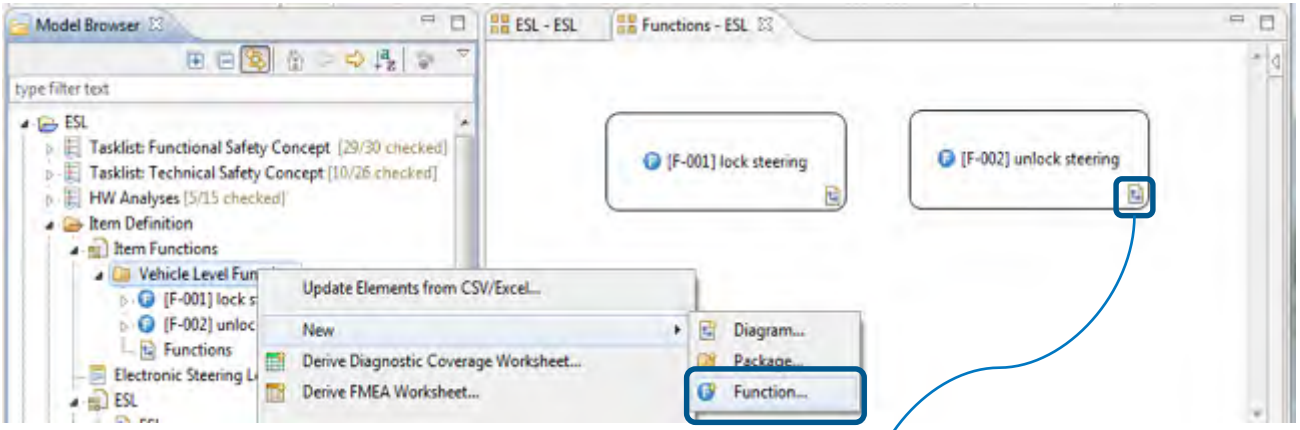
典型活动

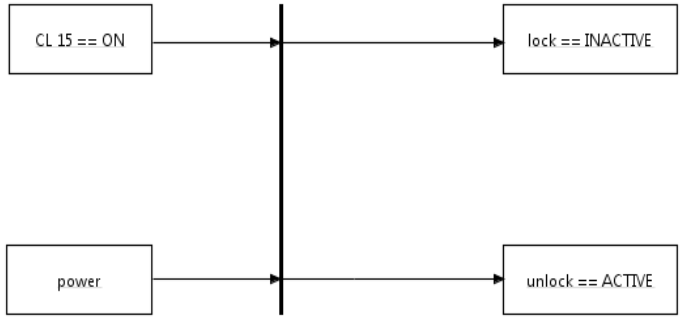
- ➢ 项目定义
  - ✓ 项目定义、描述
  - ✓ 功能建模、故障识别
  - ✓ 初始架构建模
- ➢ 危害分析和风险评估（PHA/HARA）
  - ✓ 危害分析
  - ✓ 确定安全目标
  - ✓ 推导功能安全需求及规范



项目定义

一切从一个好的功能模型开始

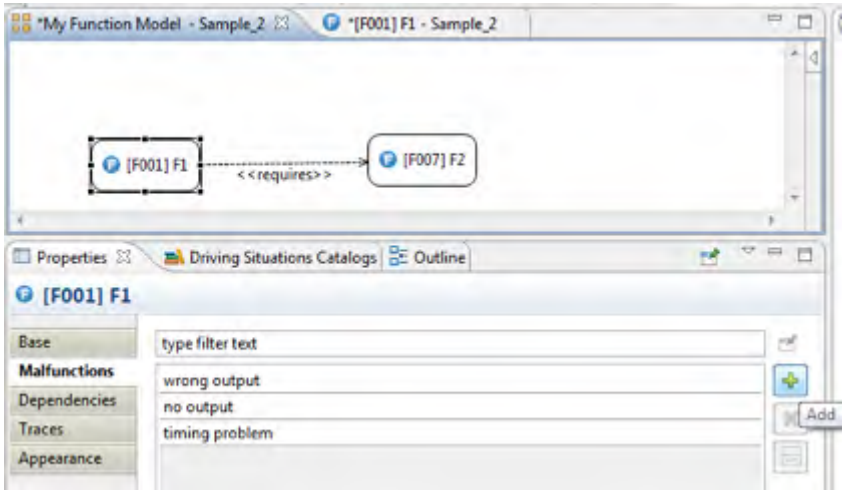




工具中，可以便捷地设定功能与功能间、故障间的关系。

项目定义
– 故障识别和建模

- 通常在一个“功能”内部创建
- 故障识别(HAZOP) ：工具预定义了丰富的清单模板
- 可以对因果关系建模



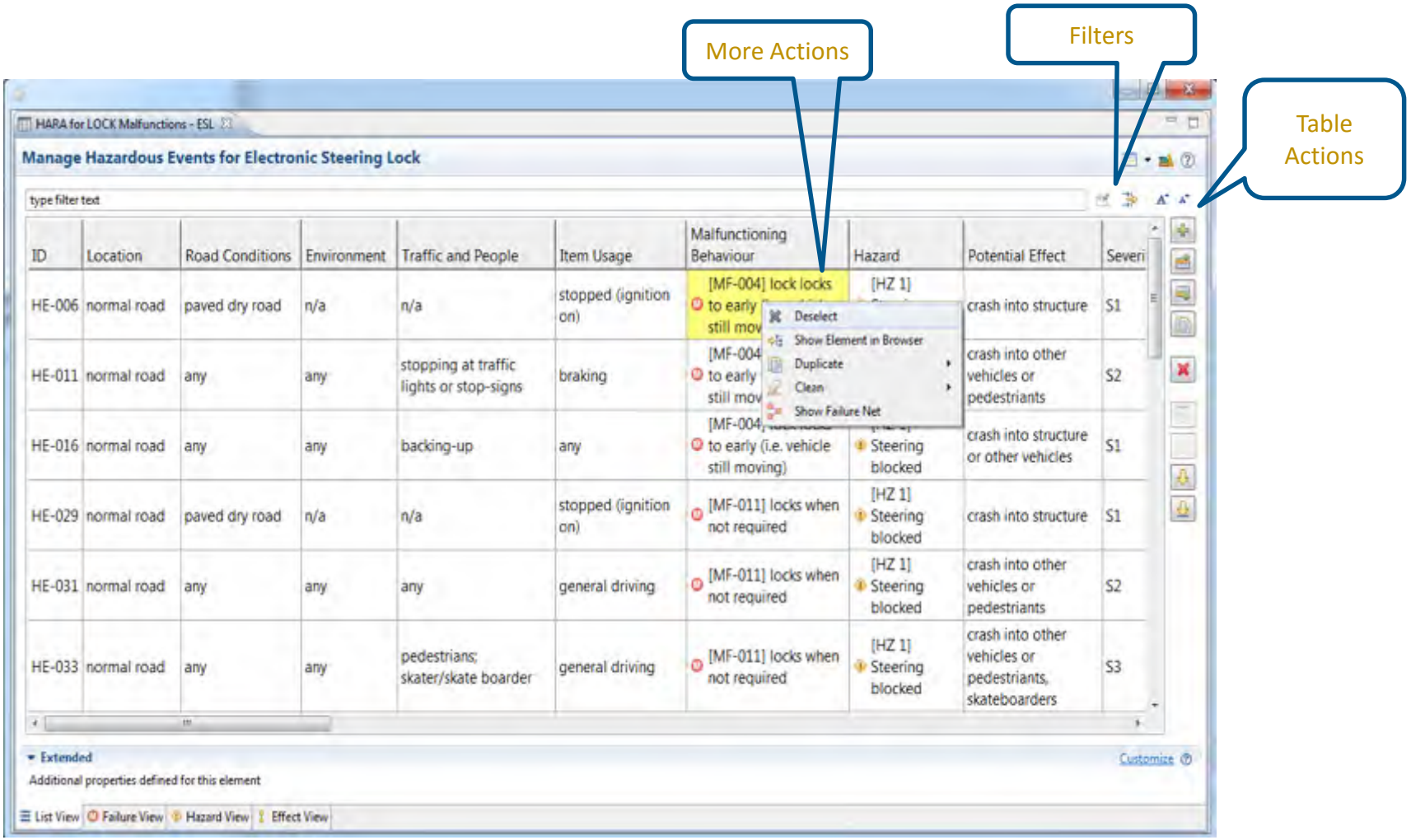
Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note	Description
NO OR NOT	☑	[MF-001] lock not activated when required	OlafK	08/02/2016 21:04		Complete negation of the design intent
MORE	☑	[MF-051] Locked too strong	OlafK	08/02/2016 21:06	n.a. wrt. FuSa, but to product safety/quality	Quantitative increase
LESS	☑	[MF-003] lock does not lock completely	OlafK	08/02/2016 21:06		Quantitative decrease
AS WELL AS	☑		OlafK	08/02/2016 21:06	n.a.	Qualitative modification/increase
PART OF	☑		OlafK	08/02/2016 21:06	n.a.	Qualitative modification/decrease
REVERSE	☑	[MF-002] unlocks when lock is required	OlafK	08/02/2016 21:06		Logical opposite of the design intent
OTHER THAN	☑	[MF-011] locks when not required	OlafK	08/02/2016 21:07		Complete substitution
EARLY	☑	[MF-004] lock locks to early (i.e. vehicle still moving)	OlafK	08/02/2016 21:06		Relative to the clock time
LATE	☑	[MF-005] lock locks to late	OlafK	08/02/2016 21:07		Relative to the clock time
BEFORE	☑		OlafK	08/02/2016 21:07	n.a.	Relating to order or sequence
AFTER	☑		OlafK	08/02/2016 21:08	n.a.	Relating to order or sequence
PERIODIC	☑	[MF-012] instable locks/unlocks	OlafK	08/02/2016 21:08		Changing in quantity or instable

危害分析和风险评估（PHA/HARA）

medini支持：

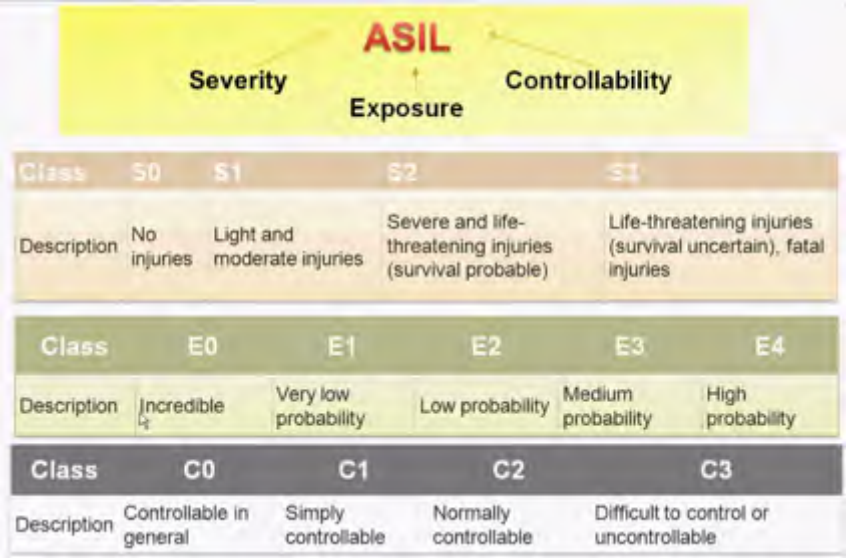
- 对系统提供的**每个功能**进行危害分析和风险评估。
- 识别在**不同情景下**系统的潜在故障，通过风险评估，识别危害的**严重度、暴露概率和可控性**。
- 危害**分级（SIL，ASIL）**
- 预防措施

medini - 支持 Hazard Log (HARA table) 自由定义



medini – 自动计算安全完整性等级

- 选择每个危害事件的合理参数（E，C，S），并对每个参数给出相应的证明。
- 以ASIL为例，确定好严重度、暴露率和可控性三个参数之后，medini工具会自动计算出ASIL等级



Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Operational Situation | Malfunction | Hazard/Effect | Risk Estimation | ASIL

Location	Road Conditions	Environment	Traffic and People	Item Usage	Malfunctioning Behaviour	Hazard	Potential Effect	Severity	Severity Comment	Exposure	Exposure Comment	Controllability	Controllability Comment	ASIL
normal road	any	any	pedestrians; skater/skate boarder	general driving	[MF-011] locks when not required	[HZ 1] Steering blocked	crash into other vehicles or pedestrians, skateboarders	S3	medium speed	E3	Traffic inside city (pedestrians, bicycles)	C2	distance to other vehicles or pedestrians	B
normal road	any	any	stopping at traffic lights or stop-signs	braking	[MF-011] locks when not required	[HZ 1] Steering blocked	crash into other vehicles or pedestrians	S2	medium speed	E4	Stopping at traffic lights etc in cities	C2	distance to other vehicles or pedestrians	B
normal road	any	any	turning right	general driving	[MF-011] locks when not required	[HZ 1] Steering blocked	crash into other vehicles or pedestrians	S2	medium speed	E3	Turning into side-road; crossing bike-road	C2	distance to other vehicles or pedestrians	A
normal road	any	any	changing lanes	general driving	[MF-011] locks when not required	[HZ 1] Steering blocked	crash into other vehicles	S2	medium speed	E4	Changing lanes in city traffic	C3	distance to other vehicles	C

medini – 安全目标和安全需求

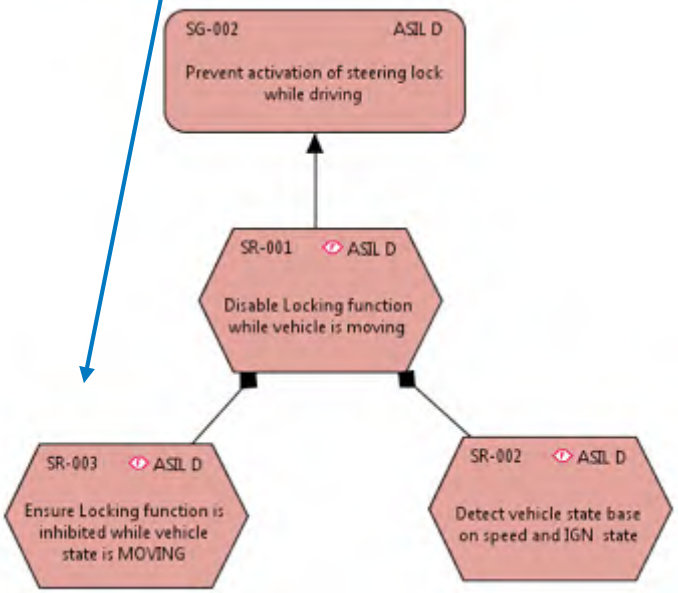
- 安全目标 + 功能安全需求
- 功能安全架构 (SysML)
- 安全需求分配

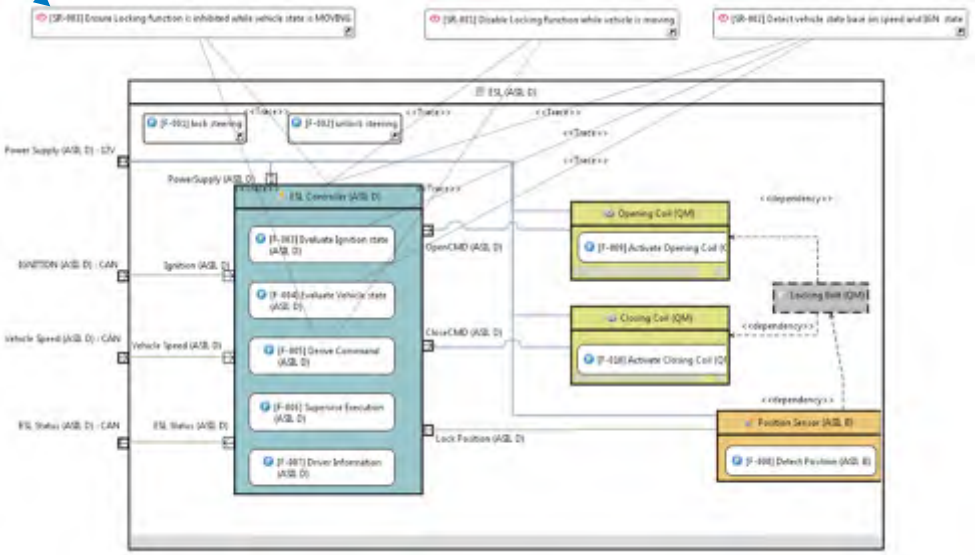
Safety Requirements Editor

ID	Name	Description	Kind
SR001	Prevent the ignition without reason		FUNCTIONAL
SR006	Provide reliable communication		TECHNICAL
SR007	Provide duplication of sensors		TECHNICAL
SR005	Provide SW Diagnostics for ACU	Self-check using redundant communication	TECHNICAL
SR002	After a crash is detected and airbags are fired once, switch OFF airbag system.	handle this in the algorithms	TECHNICAL
SR011	ensure that fire command is issued only once		FUNCTIONAL
SR008	Provide Acceleration Sensor		HARDWARE

Add | Add After | Insert | Duplicate | Edit | Remove

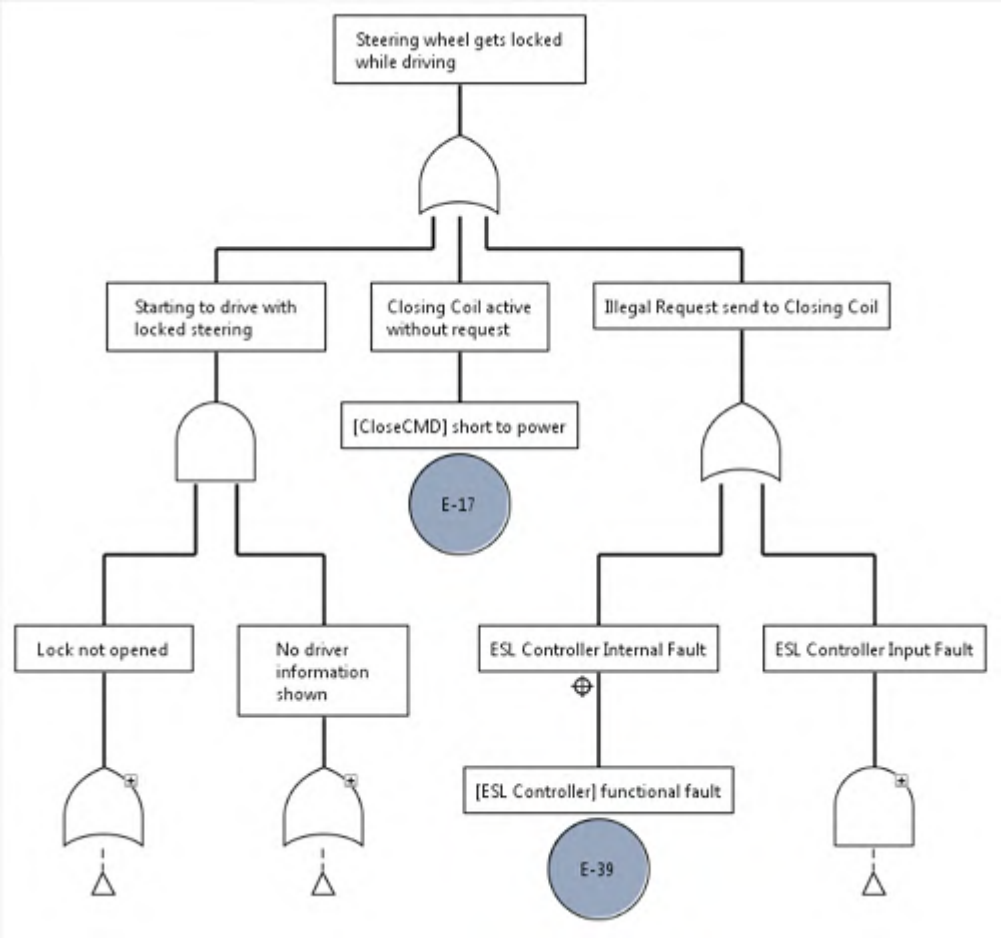
Safety Goal = Top level Safety Objective





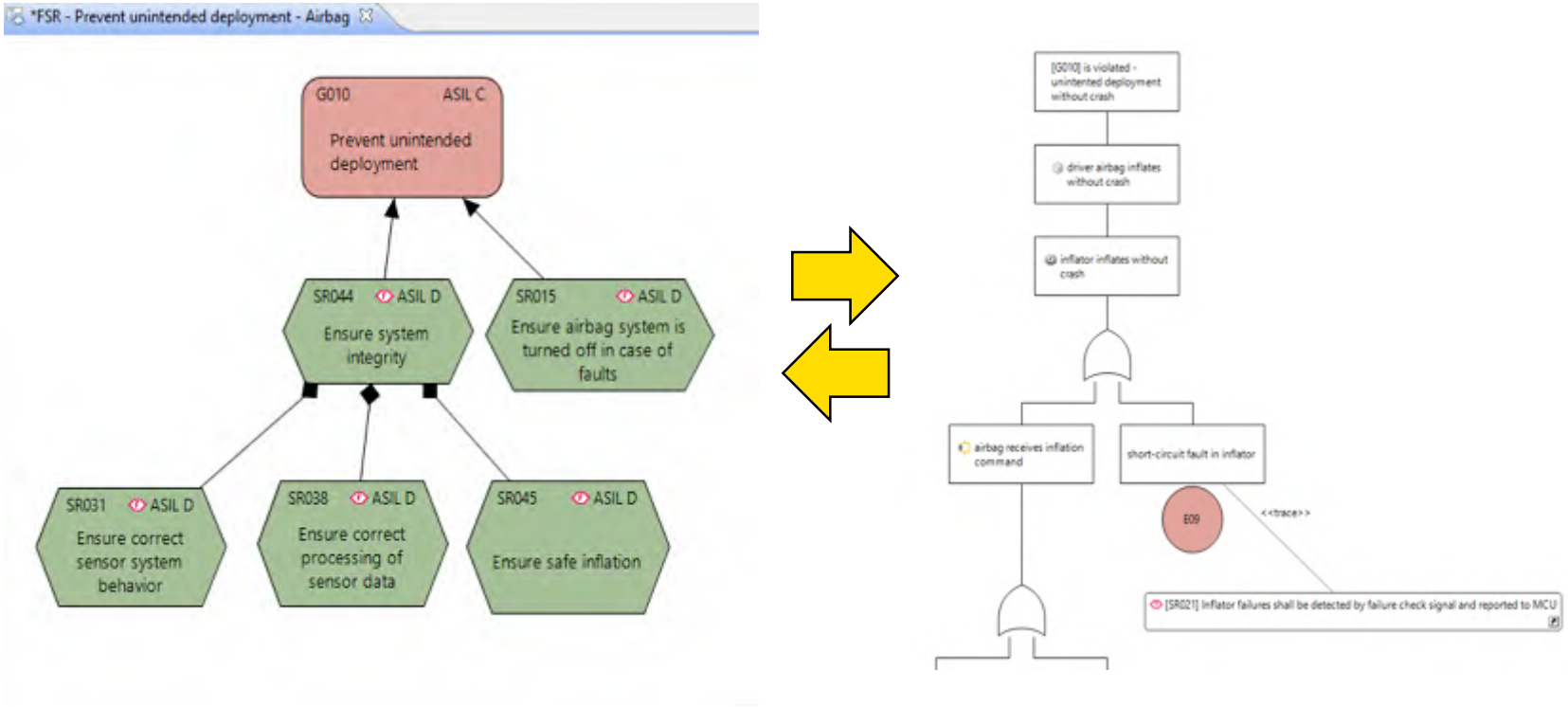
medini – 定性FTA

- **定性FTA (分析初始架构: 什么将导致安全目标违例?)**
  - 自顶向下的安全分析
  - 从不良事件开始
  - 发生下一级事件的条件是什么（使用AND, OR, n out of m,..)
- **可以在各个阶段、各个层次进行FTA**

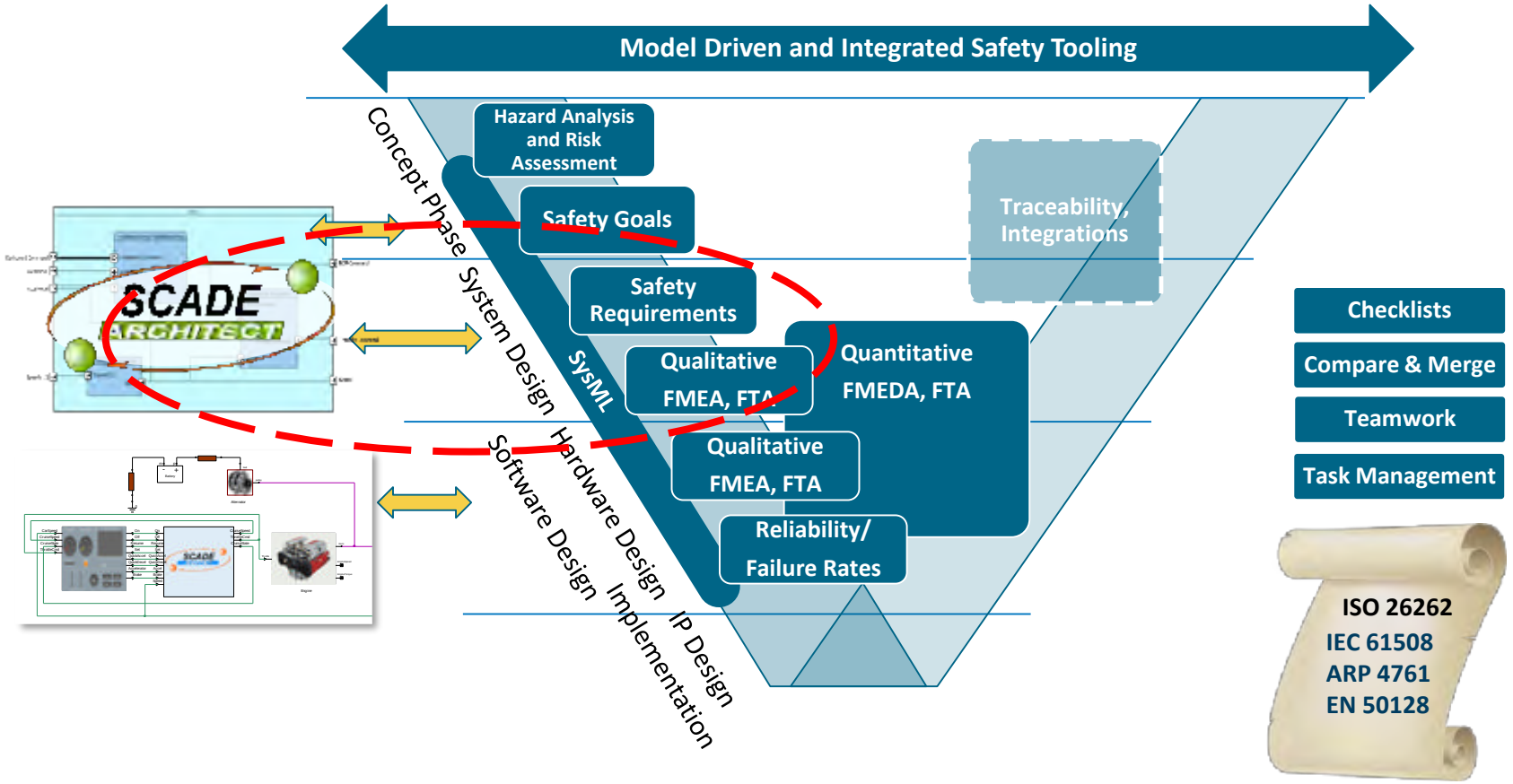


medini – 安全目标、需求模型与FTA集成

- **与定性FTA集成**
  在FTA活动中创建需求
  通过脚本将（A）SIL调整到目标的（A）SIL



系统设计阶段：安全目标、安全需求与系统设计模型集成



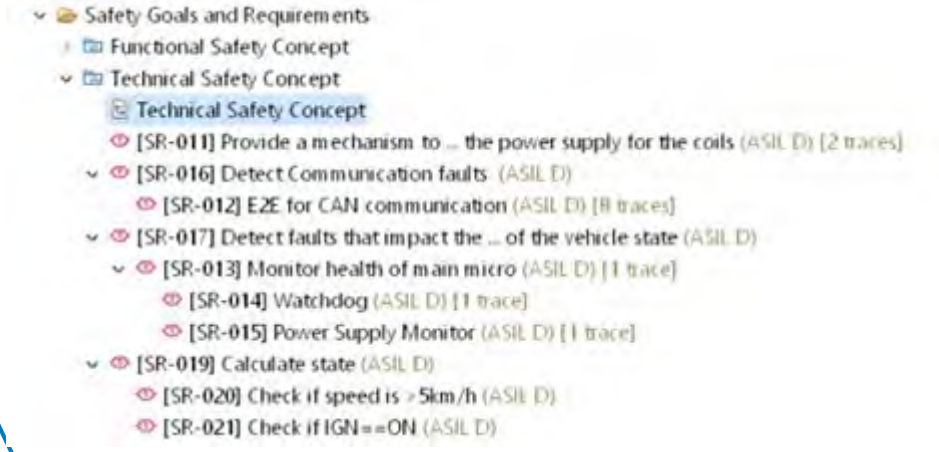
系统设计阶段：安全目标、安全需求与系统设计模型集成

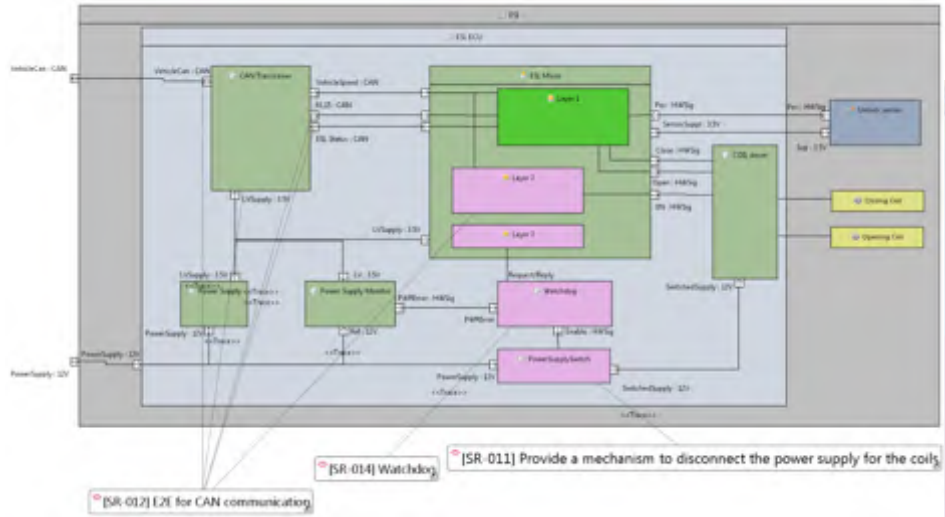
- **要完成的任务：**
  - 应按照功能安全概念规定技术安全需求
  - 应对技术安全需求规定必要的安全机制
  - 技术安全需求应分配给系统设计元素，应直接分配或进一步细化为给硬件、软件或两者

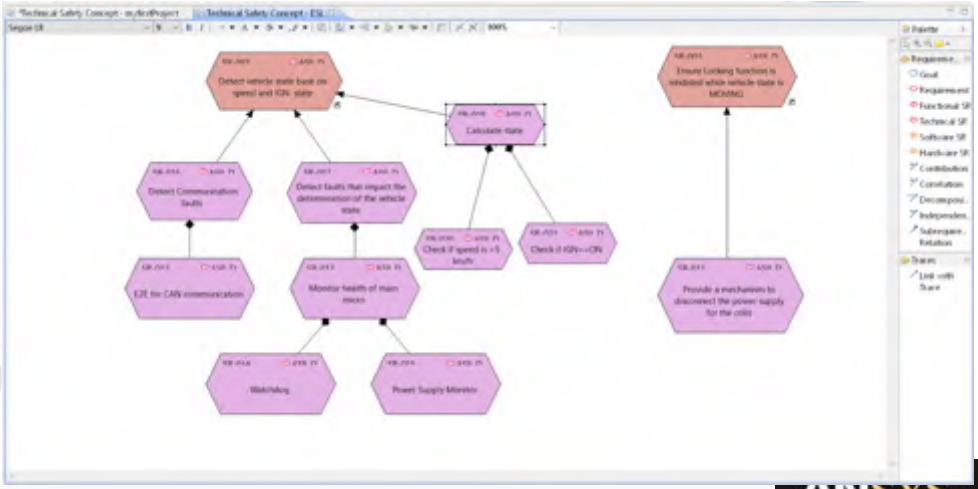
- **典型活动：**
  - 推导技术安全需求
  - 建立技术安全架构（SysML）
  - 分配安全需求
  - 安全分析: FMEA
    - ✓ 从元件故障模式开始，发现潜在的影响
    - ✓ 分析因果链
    - ✓ 规划对策

medini – 技术安全需求与技术安全架构

- 从功能安全需求推导技术安全需求
- 技术安全架构（SysML）
- 分配安全需求



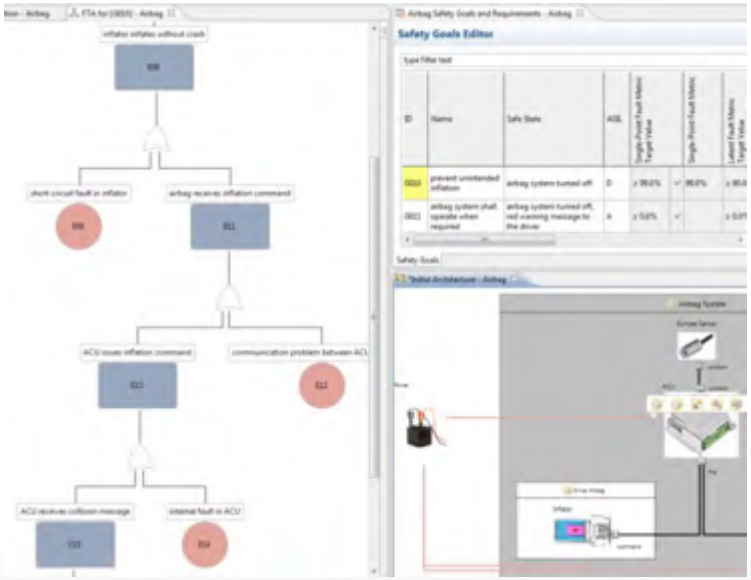


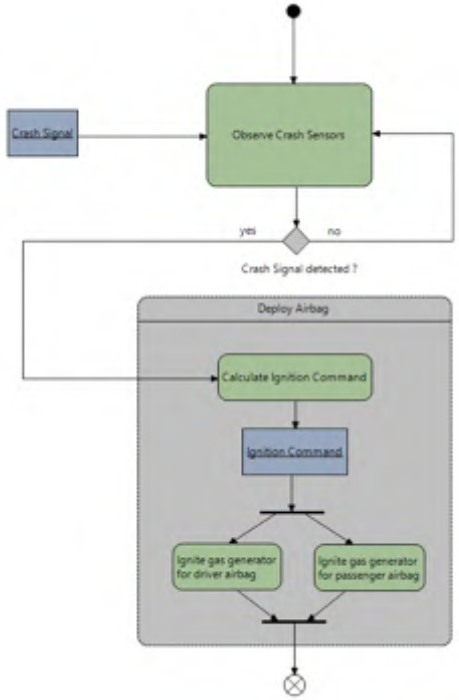


medini– 系统设计建模

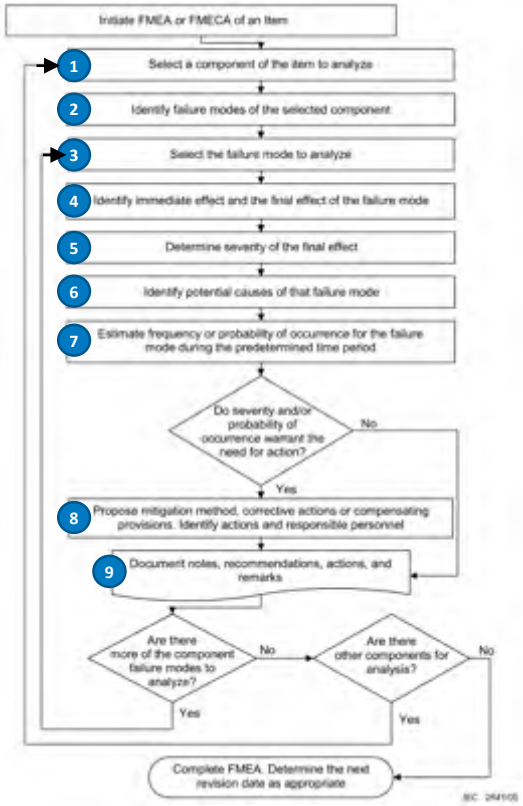
Medini支持基于SysML 进行系统架构、设计和行为建模，集成了基于功能安全分析方法的架构/功能设计

- 通过图形和表格编辑器进行SysML建模
- 使用块定义图和内部框图对功能依赖性和故障的功能架构进行图形化建模
- 使用活动图对功能和过程的行为建模





medini – FMEA安全分析



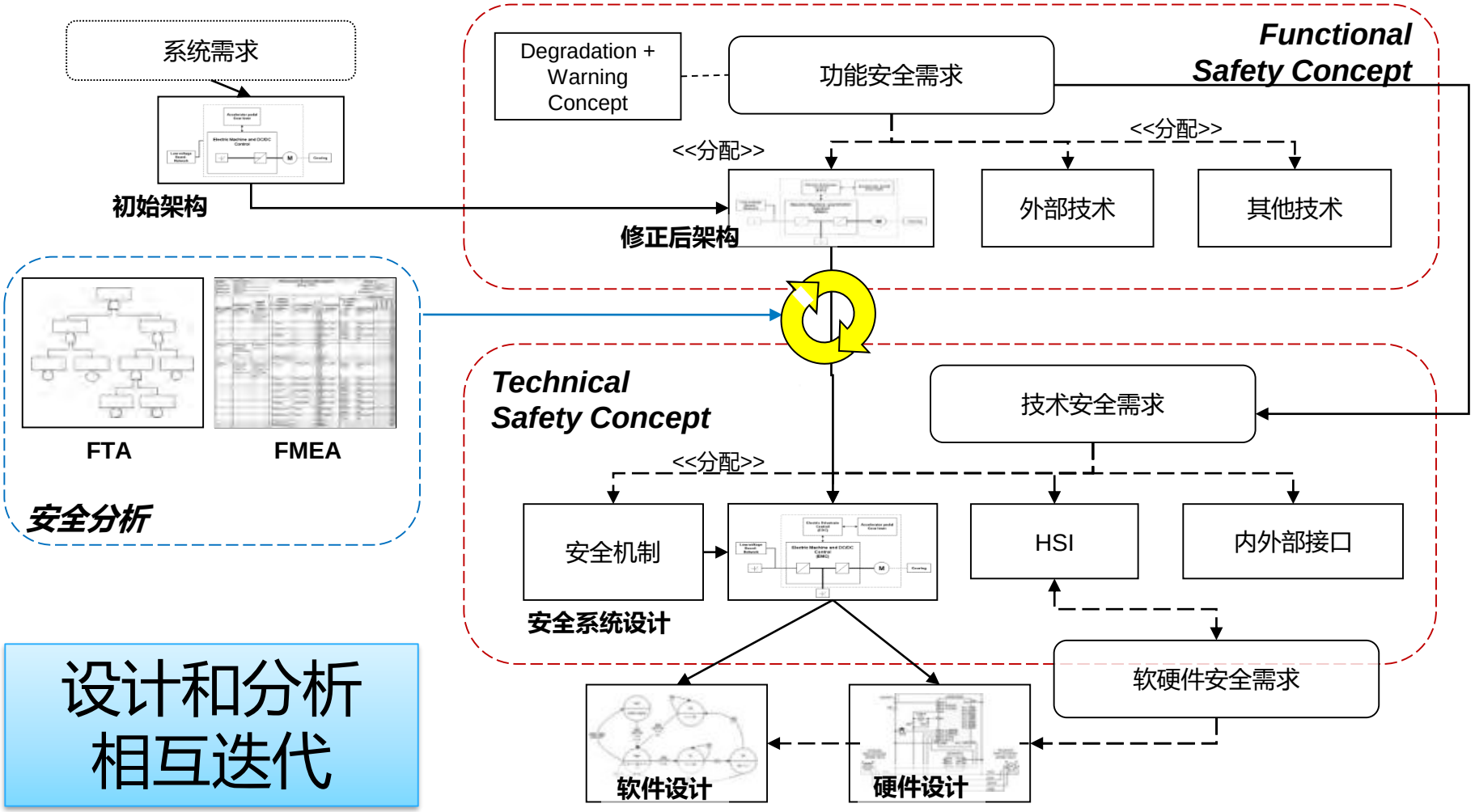
IEC 60812的 FMEA流程

FMEA工作表列各不相同，但基本结构和（风险）评估通常类似：

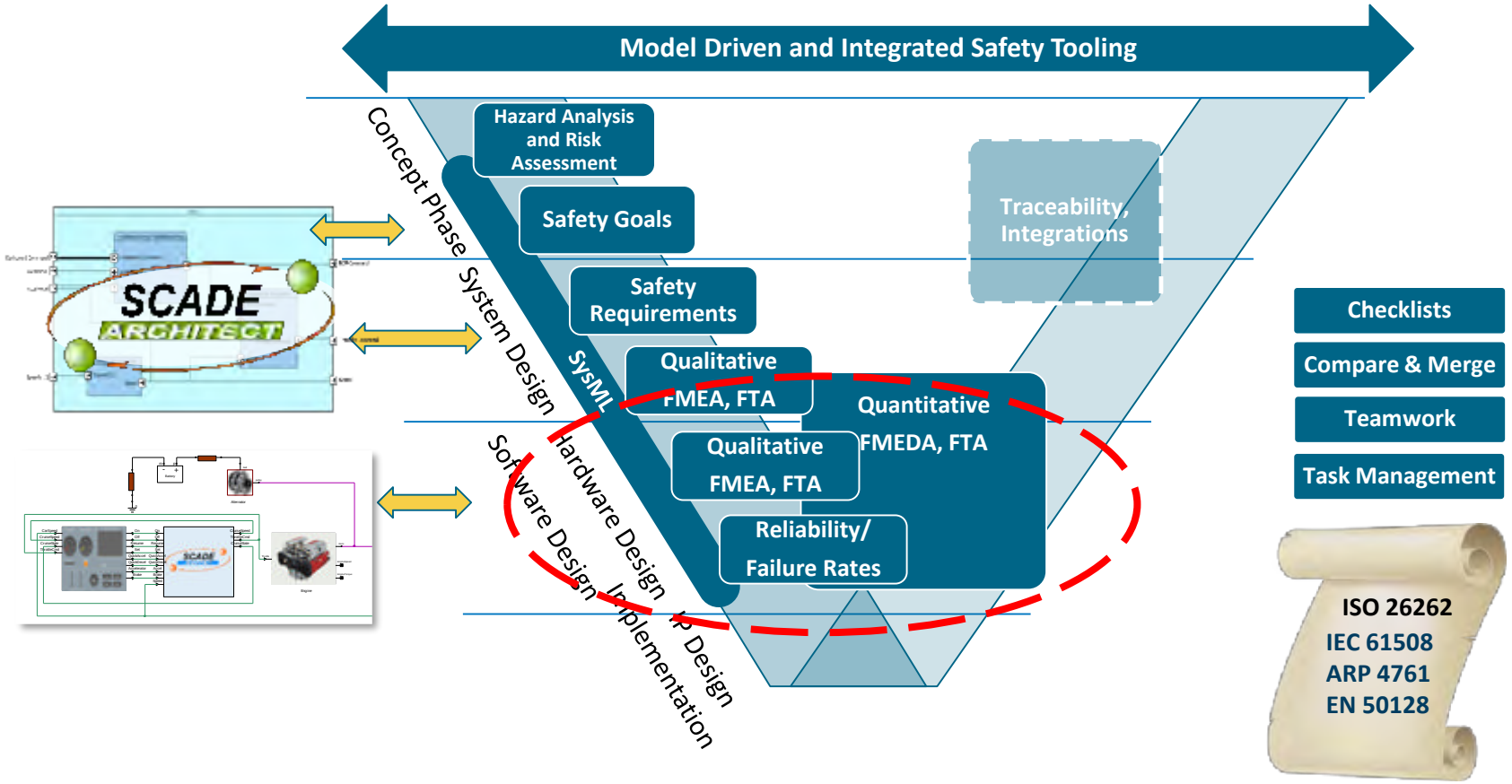
- ✓ **组件→故障模式 →影响效果;**
- ✓ 识别**原因、现有措施、行动**
- ✓ **风险优先级编号（RPN）**作为产品 ---"严重性x发生率x检测"

1	2	4	4	5		6	7		8			RPN	9					
	Potential failure mode	Potential effect(s) of failure		SEV	CLASS	Potential cause(s)/ mechanism(s) of failure	Detail cause(s)/ mechanism(s) of failure	Occur	Current design controls prevention	Current design controls detection	Det		Recommended action(s)	Responsibility and target completion date	Action results			
															Actions taken	SEV	Occur	Det	RPN
D1	Short	Battery voltage + shorts to ground -	Battery drain, walk home	10		Inherent defect of the component	Material breakdown	3	Selection of higher quality and rating	Evaluation and reliability validation testing	1	30						
D1	Open	No reverse voltage protection	Not noticeable	2		Inherent defect of the component	Bonding or semiconductor crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	2	12						
C9	Short	Battery voltage + shorts to ground	Battery drain – walk home;	10		Inherent defect of the component	Dielectric breakdown or crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	1	30						
C9	Open	No EMI filtering	Item operation out of specification	2		Inherent defect of the component	Dielectric open, leak, void, or crack	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	4						
L1	Open	No V1 –	Item inoperable No warning display	9		Inherent defect of the component	Material breakdown	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	18						
R91	Open	No voltage for the item switching circuit	Item inoperable No warning display	9		Inherent defect of the component	Bonding or material crack	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	18						

medini基于模型的安全性分析: 设计/分析工作流程



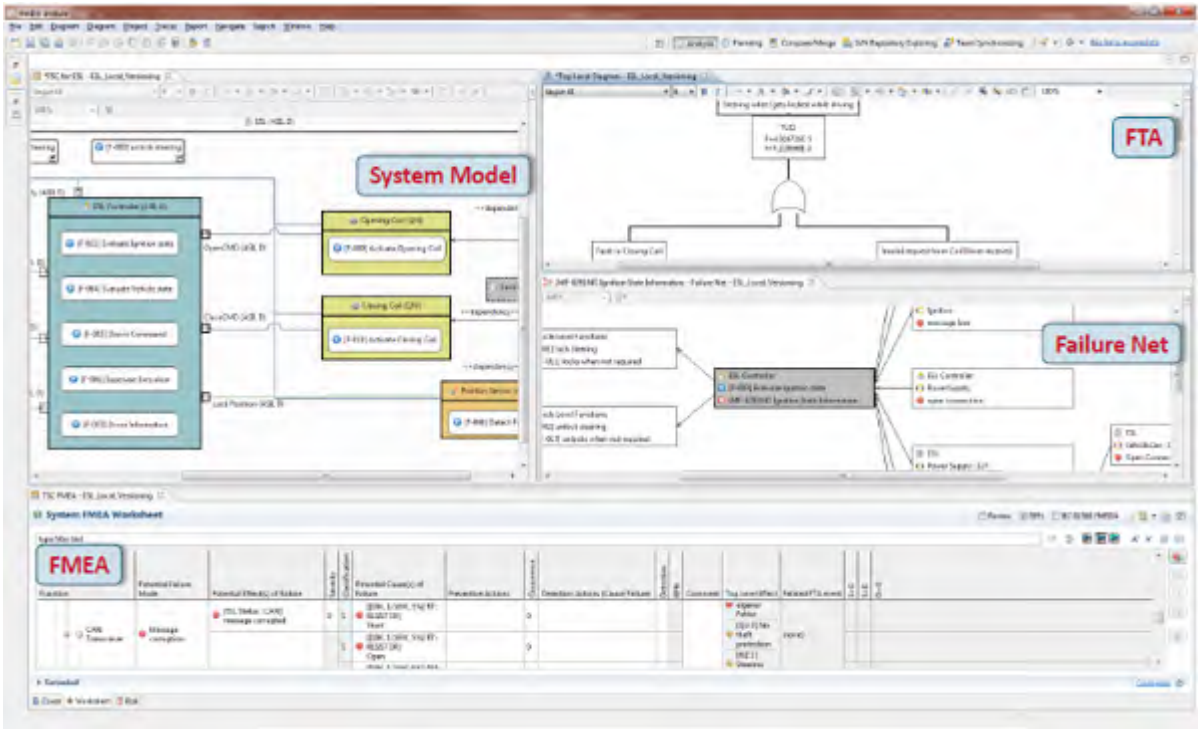
安全验证：基于模型的不同层次安全分析和可靠性预测



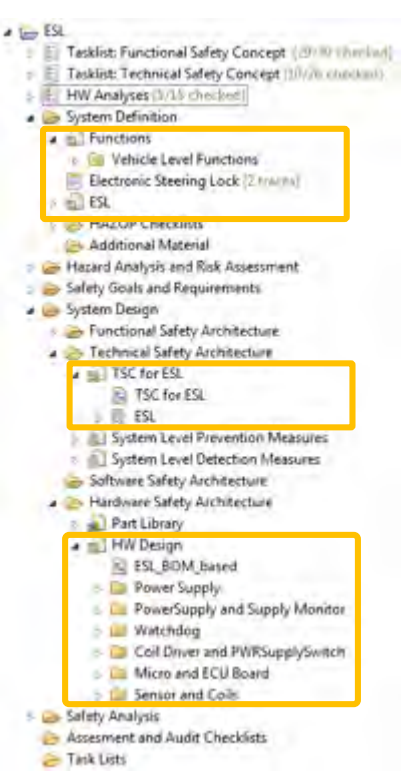
安全验证：基于模型的不同层次安全验证和可靠性预测

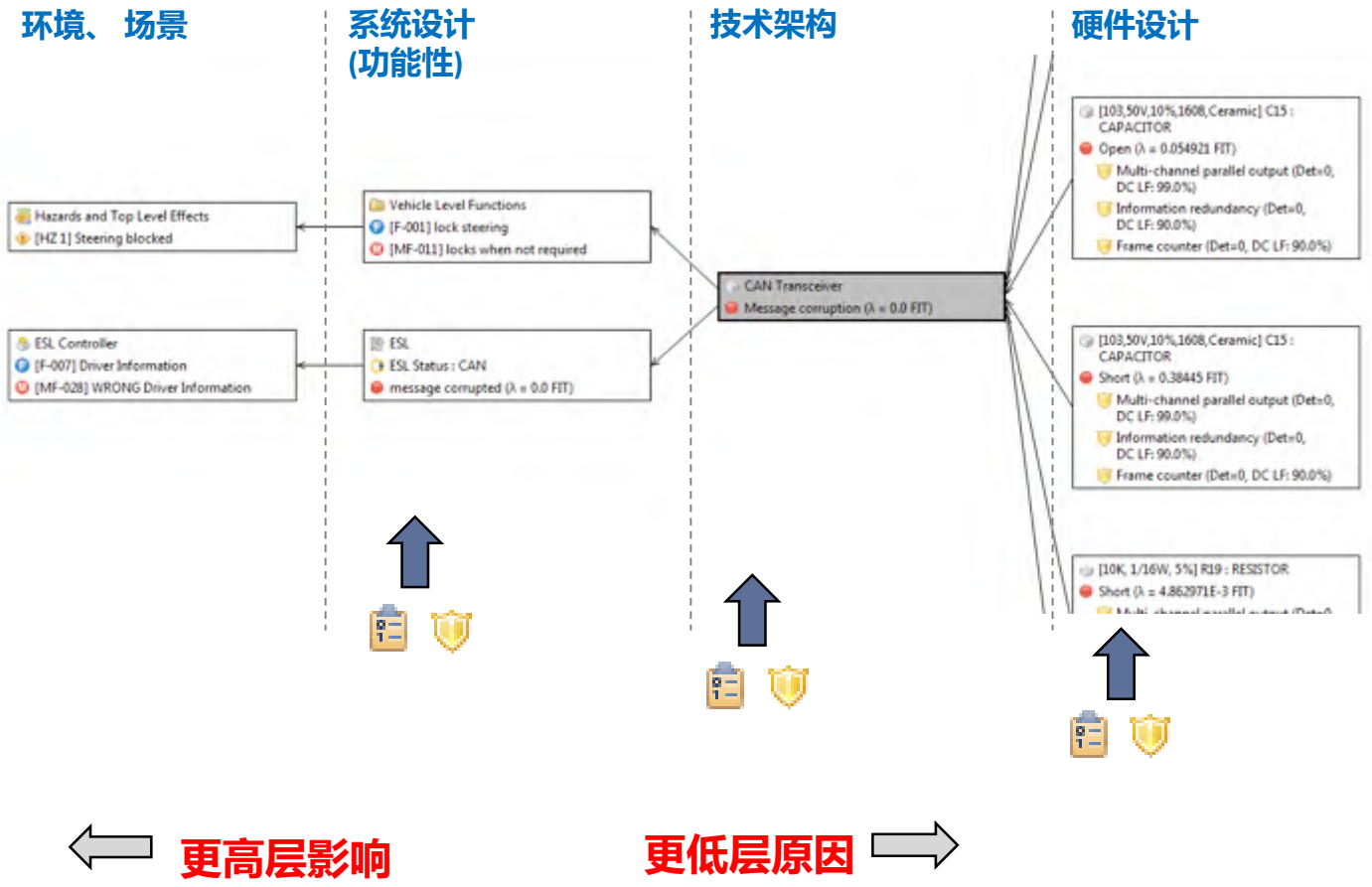
典型活动

- 定性/定量 FTA、FMEA 、诊断覆盖率
- 硬件安全需求规范
- 硬件结构指标
- 硬件随机失效评估、验证



medini - 将故障层次结构集成到系统设计模型中



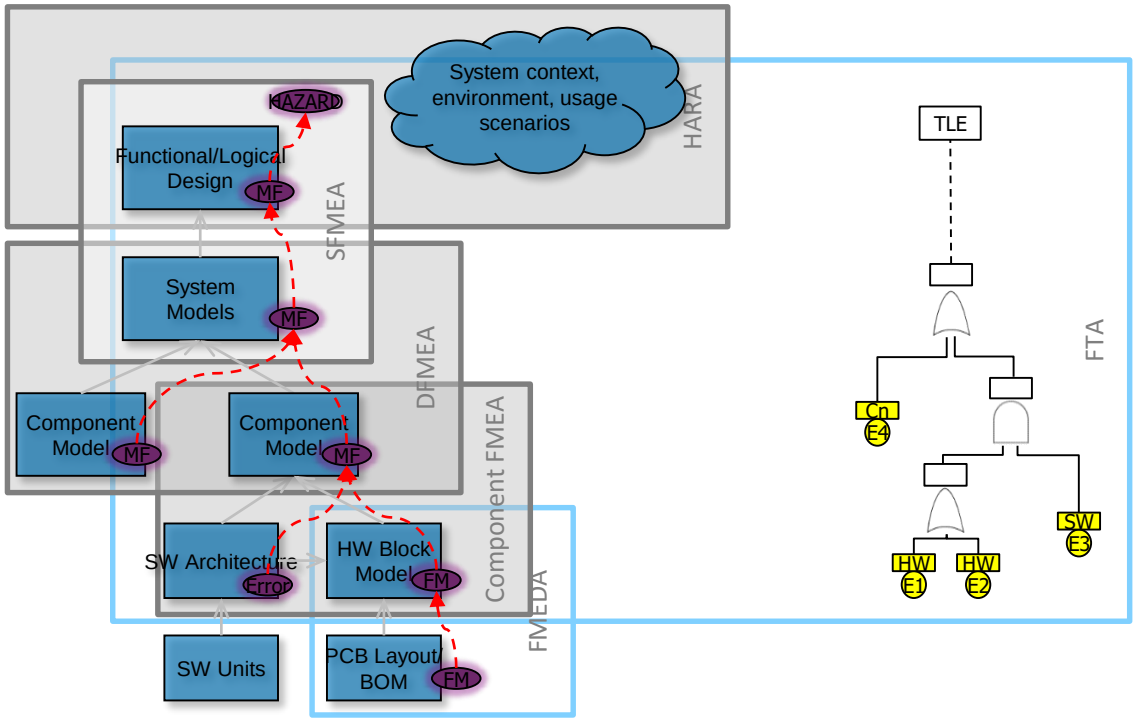


medini - 支持在不同设计层次应用 FMEA

- 提供FMEA的标准模板
- 自由定制的FMEA表布局

- 自动计算风险优先级编号（RPN）
- 自动填充表，并保持与SysML模型元素的一致性

- 支持Excel和MSR-FMEA导入



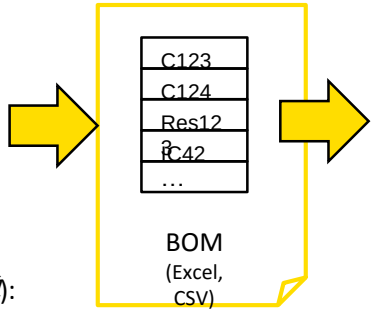
Note: the hierarchy of FMEA as "failure net" ("failure cause → higher level effect") is only partly overlapping with a fault tree analysis ("immediate failure cause → effect").

medini - 硬件级安全分析

对于硬件级的安全分析，主要是处理随机硬件故障。medini可用于

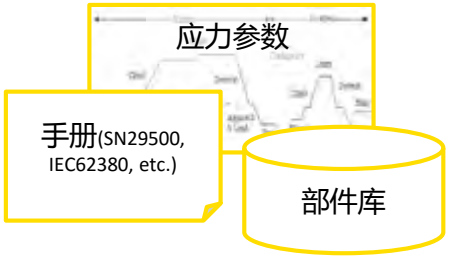
- **基于HW元件特性导出其基本故障率**
- **进一步将基本故障率分布在故障模式或复杂硬件元素的部分**
- **进而完成根据安全标准所要求的硬件指标和PMHF的计算。**

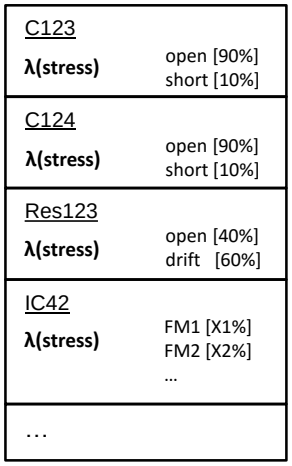
PCB (*Printed Circuit Board)*



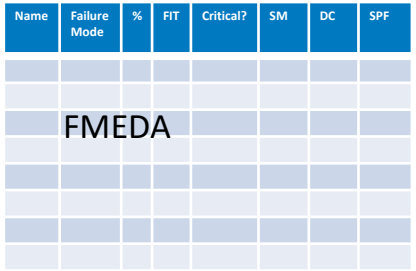
BOM (*物料清单*): accurate data, in sync with purchasing, e.g. from SAP, CAD tools

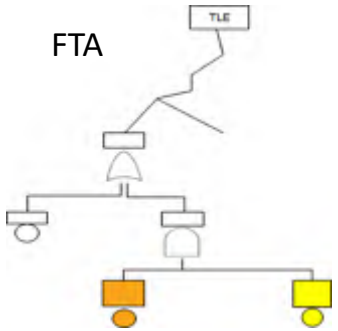
Part Number = *Unique ID for type and manufacturer of components*



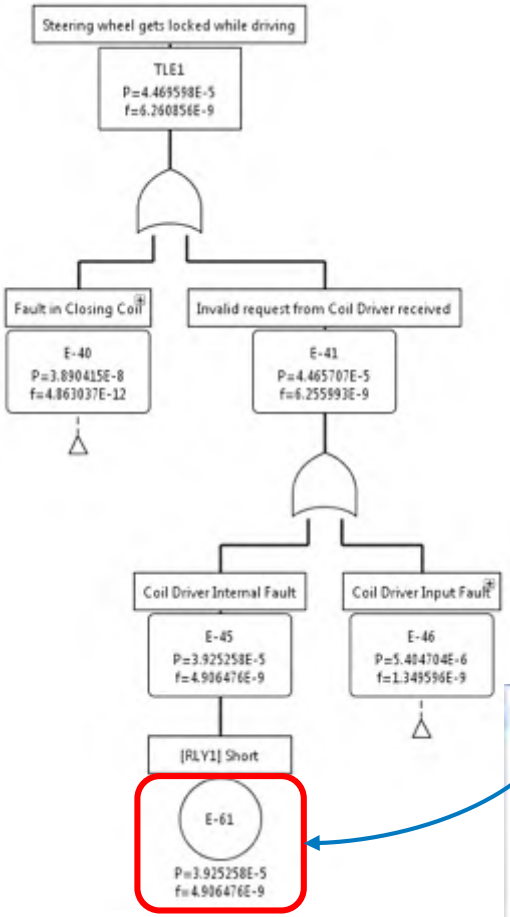


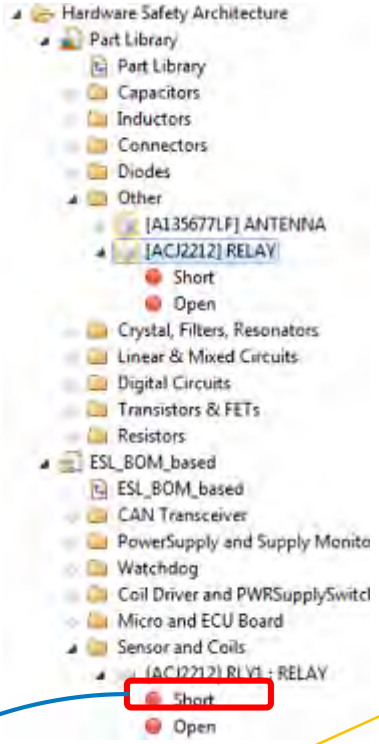
FMEDA/FTA的基础





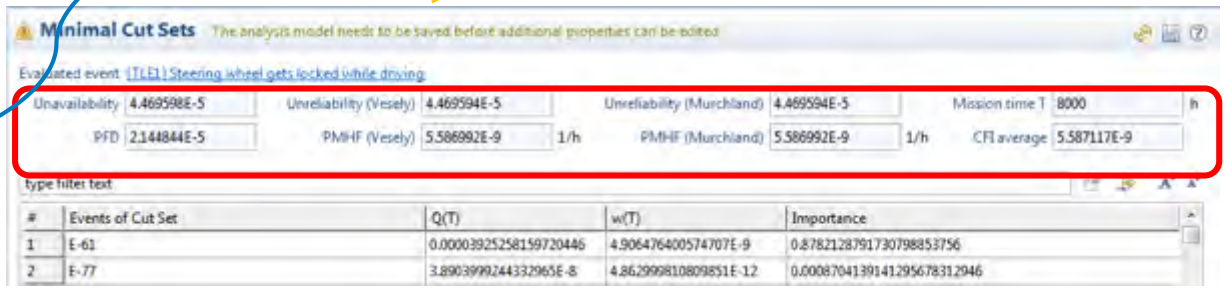
medini - 随机HW故障的概率指标（PMHF）





- 通常通过定量FTA

硬件架构(SysML)
元素的
失效模式
在FTA中呈现



medini - 计算完整的基于SysML的架构模型的指标（FMEDA/FMECA）

FMEDA Worksheet

SPFM LFM

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Related FTA event(s)	Effects	Top Level Effect	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of Safety Goals	SPF Coverage (in %)	SPF (in FIT)
Power Supply															
[10K, 1/16W, 5%] R7 : RESISTOR	0.486	0.486	☑	Short	no related FTA events	[CAN Transceiver] Message corruption [CAN Transceiver] Message loss	[HZ 1] Steering blocked [QU 2] No theft protection [MF-027] NO Driver Information	1.0	0.0	0.0	0.0	☑	Multi-channel parallel output	99.0	0.0
				Open	no related FTA events	[CAN Transceiver] Message corruption [CAN Transceiver] Message loss	[HZ 1] Steering blocked [QU 2] No theft protection [MF-027] NO Driver Information	99.0	0.0	50.0	0.0	☑	Multi-channel parallel output	99.0	0.0
[10K, 1/16W, 5%] R19 : RESISTOR	0.486	0.486	☑	Short	no related FTA events	[CAN Transceiver] Message corruption [CAN Transceiver] Message loss	[HZ 1] Steering blocked [QU 2] No theft protection [MF-027] NO Driver Information	1.0	0.0	50.0	0.0	☐		0.0	-

诊断覆盖率分析和确定安全失效分数

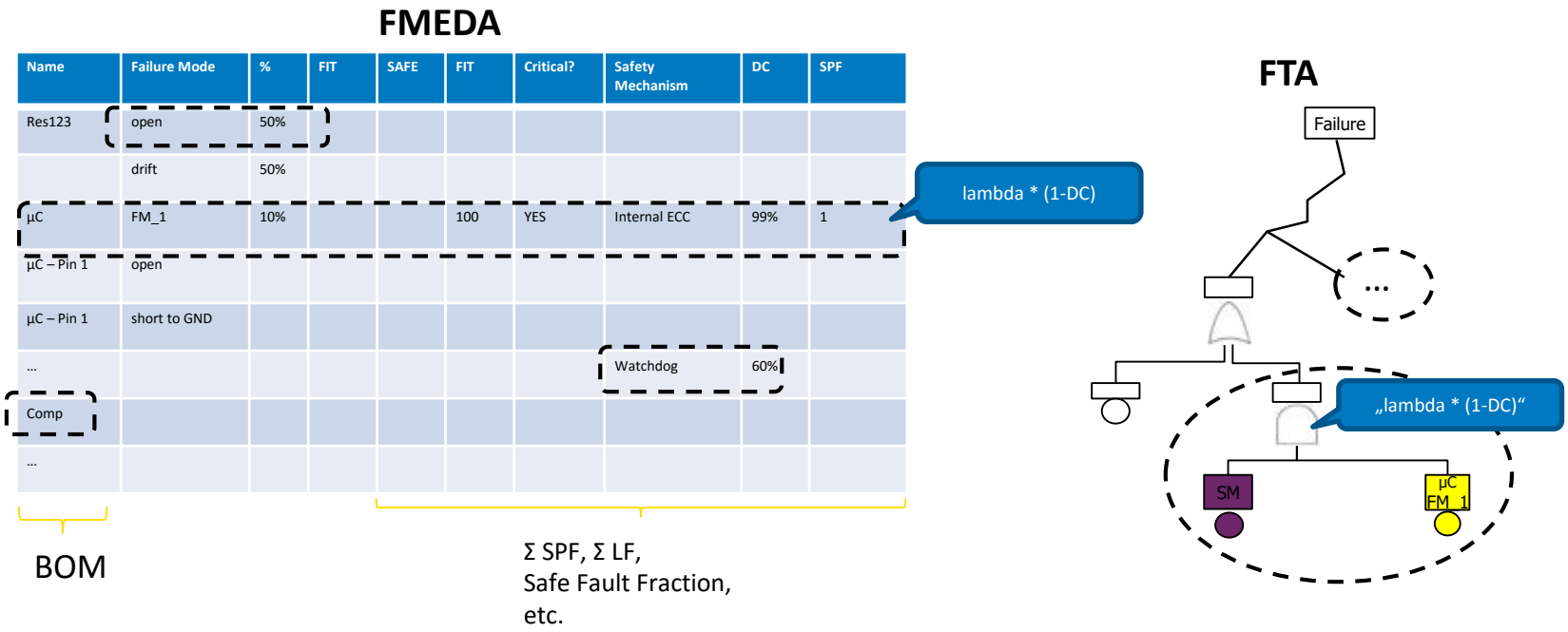
Metrics

Metric: Hardware architectural metrics, ISO 26262-5

Total		Single-Point	
Total Failure Rate:	3635.929 (in FIT)	Total Failure Rate:	17.455 (in FIT)
Total Safety Related:	3422.527 (in FIT)	Fault Metric:	99.4% (expected ≥99.0%)
Total Not Safety Related:	213.402 (in FIT)		

ISO 26262:
单点和潜在故障HW架构指标

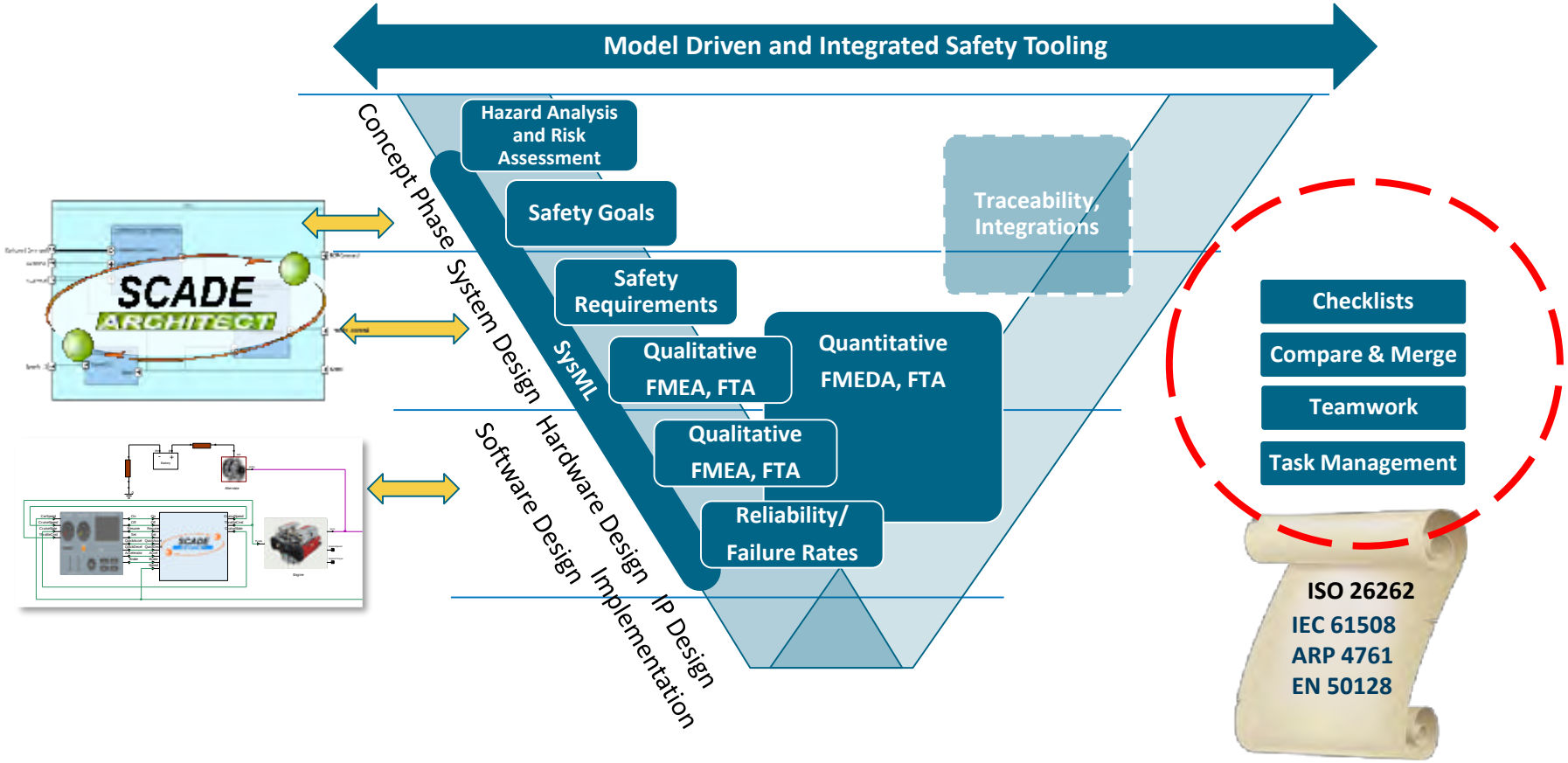
medini - FMEDA 与 FTA 的数据共享



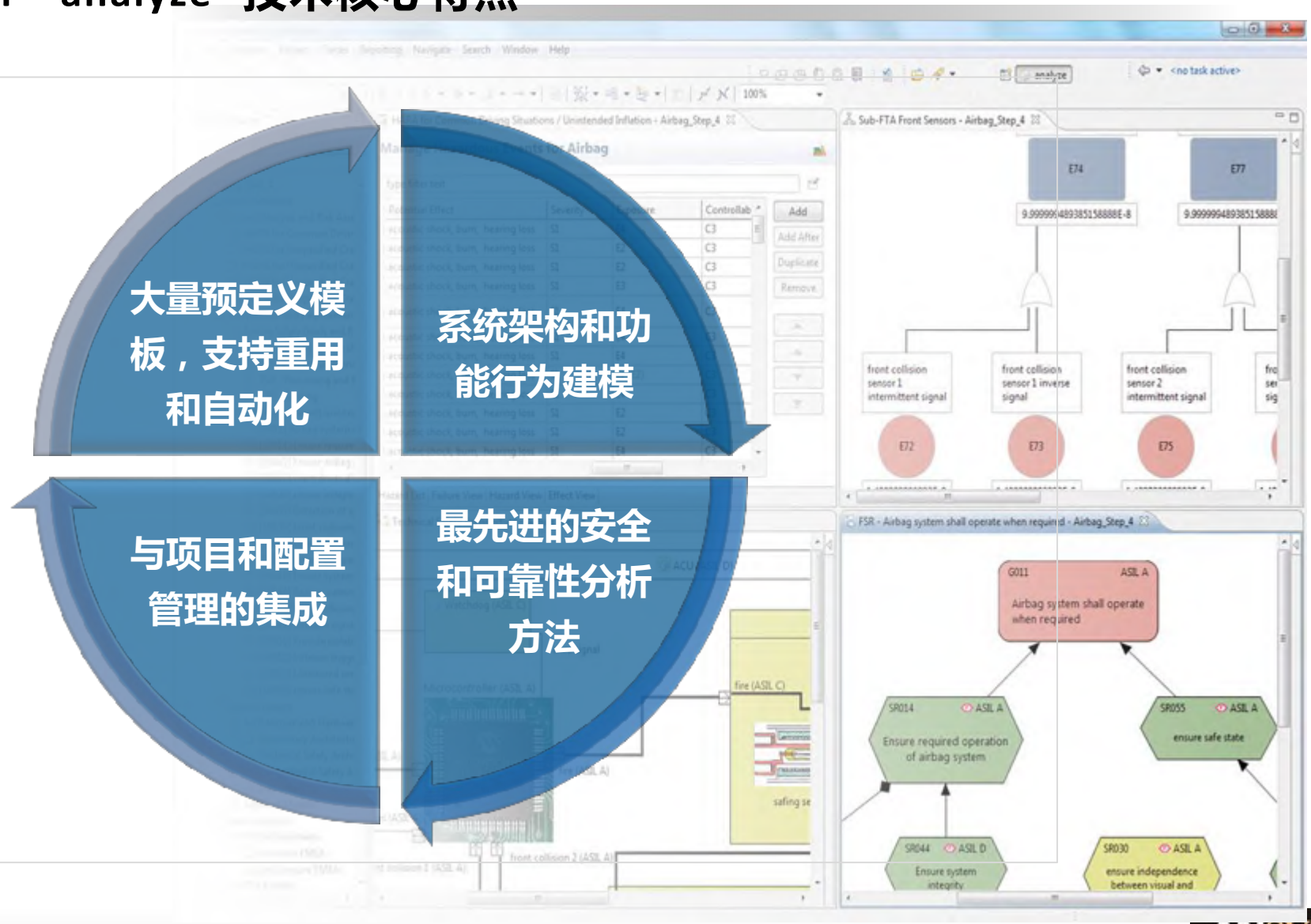
FMEDA和FTA共享**故障率、故障模式和诊断覆盖率**的相同信息

FMEDA和FTA 共享信息

项目管理：一致性、可跟踪性和高效率



medini™ analyze -技术核心特点



感谢聆听