Functional Safety with medini analyze
基于模型的安全评估过程

ANSYS SBU

议程

- 航空系统安全性评估的要求和挑战
- ANASYS medini 与 安全性评估
- medini应用案例： 机轮刹车系统
- 小结

相关标准

民用飞机

SAE ARP-4754A Guidelines for Development of Civil Aircraft and Systems

SAE ARP-4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

系统安全性

软件安全性

FPGA安全性

DO-178C Software Considerations in Airborne Systems and Equipment Certification

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

认证机构

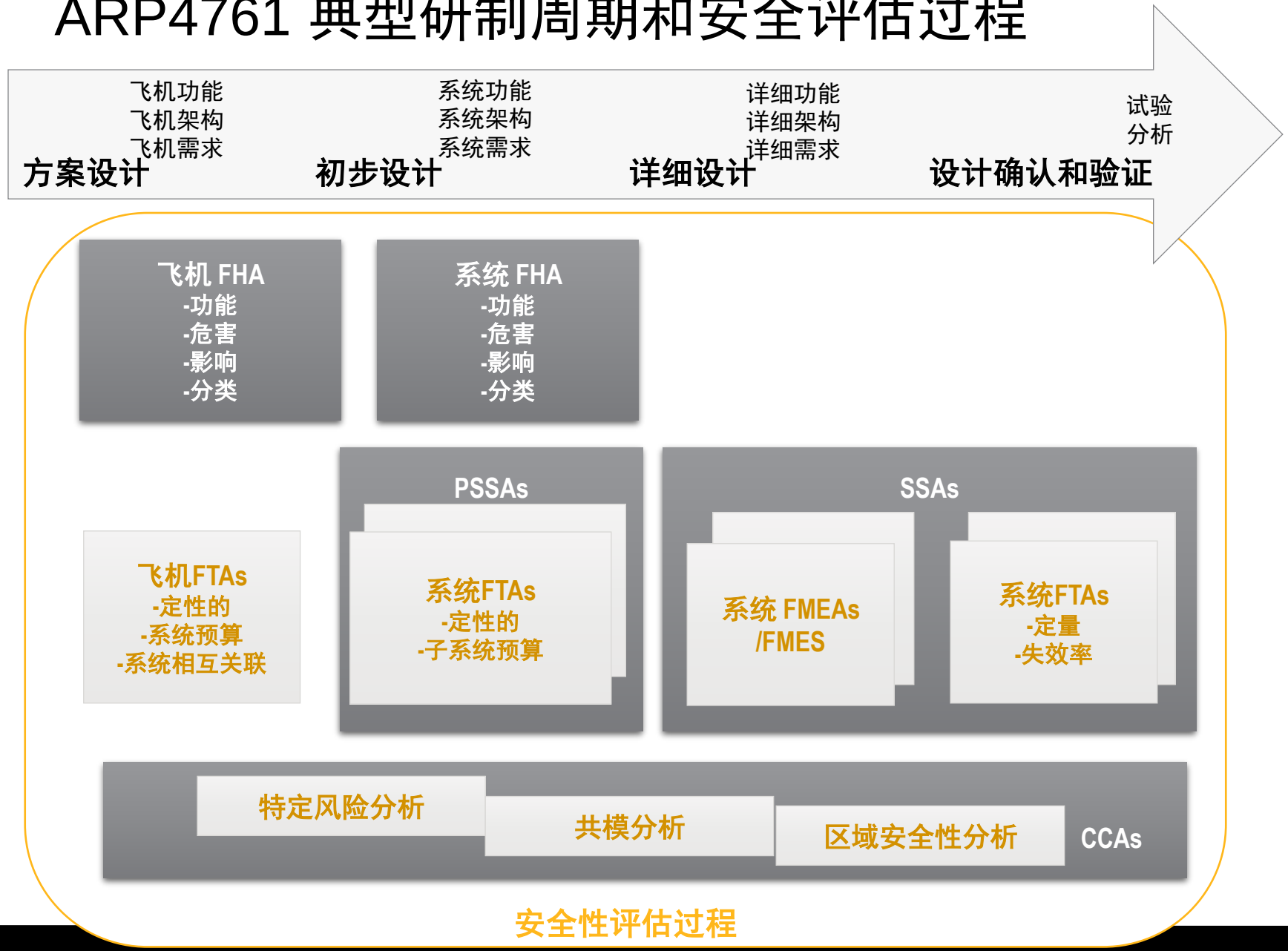
FAA 美国联邦航空管理局

EASA 欧洲航空安全管理局

CAAC 中国民用航空局

ARP4761：“描述对民用航空器认证中进行安全性评估的指南和方法”[SAE 1996]

ARP4761 典型研制周期和安全评估过程



工程中有哪些功能安全活动?

分析验证

- 功能危险性评估（安全性评估）– 飞机级\系统级FHA
- 故障树分析– FTA (定性&定量)
- 识别失效状态 – HAZOP
- 危害分级及分配 - FDAL、IDAL
- 系统安全评估- PASA/PSSA/SSA
- 失效模式和影响分析– FMEA 、FMES
- 共因分析 - CCA

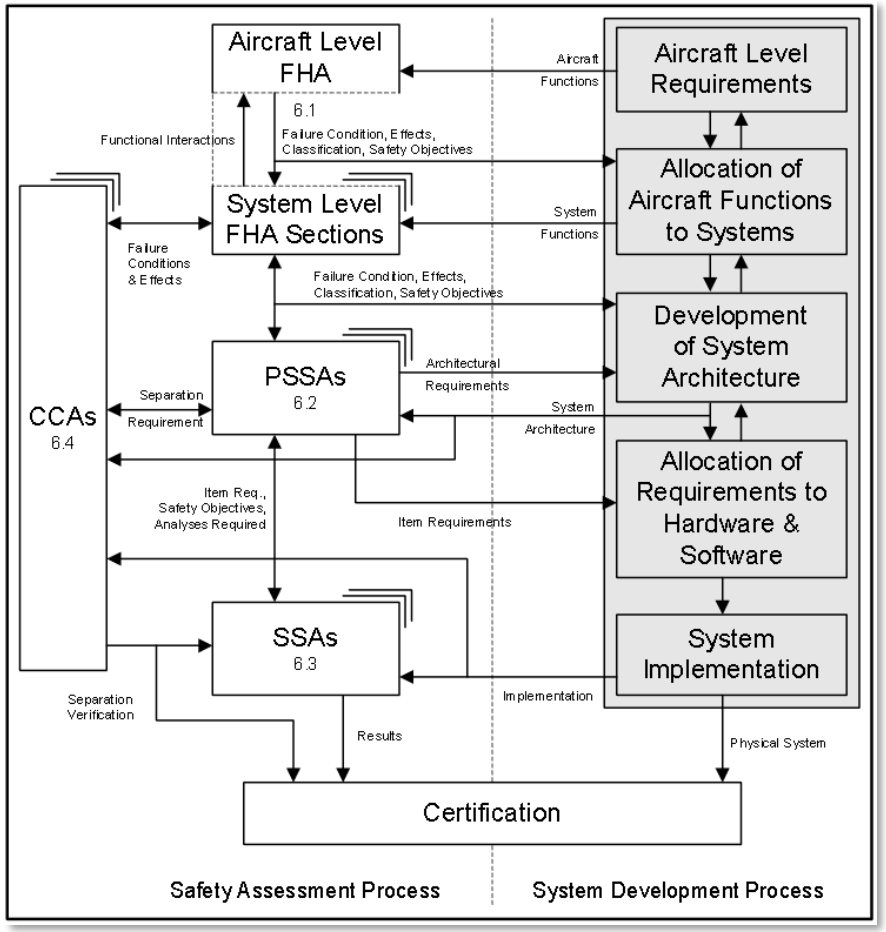
方案设计、架构

- 安全目标和安全需求定义及管理
- 架构设计： 从初始系统架构（SysML）到软硬件架构
- 可追溯性和分配

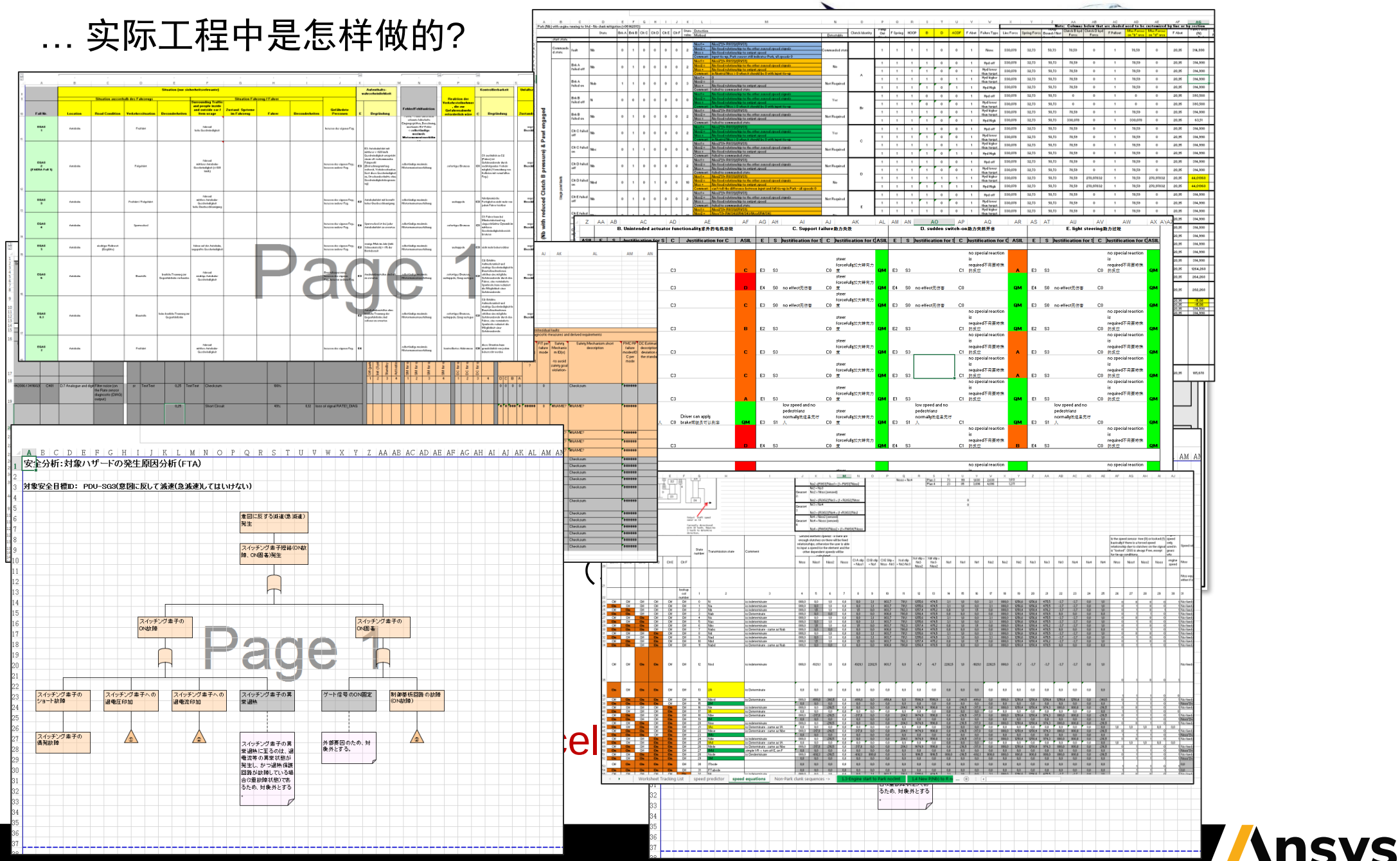
安全计划与项目管理

- 项目管理、报告
- 安全案例

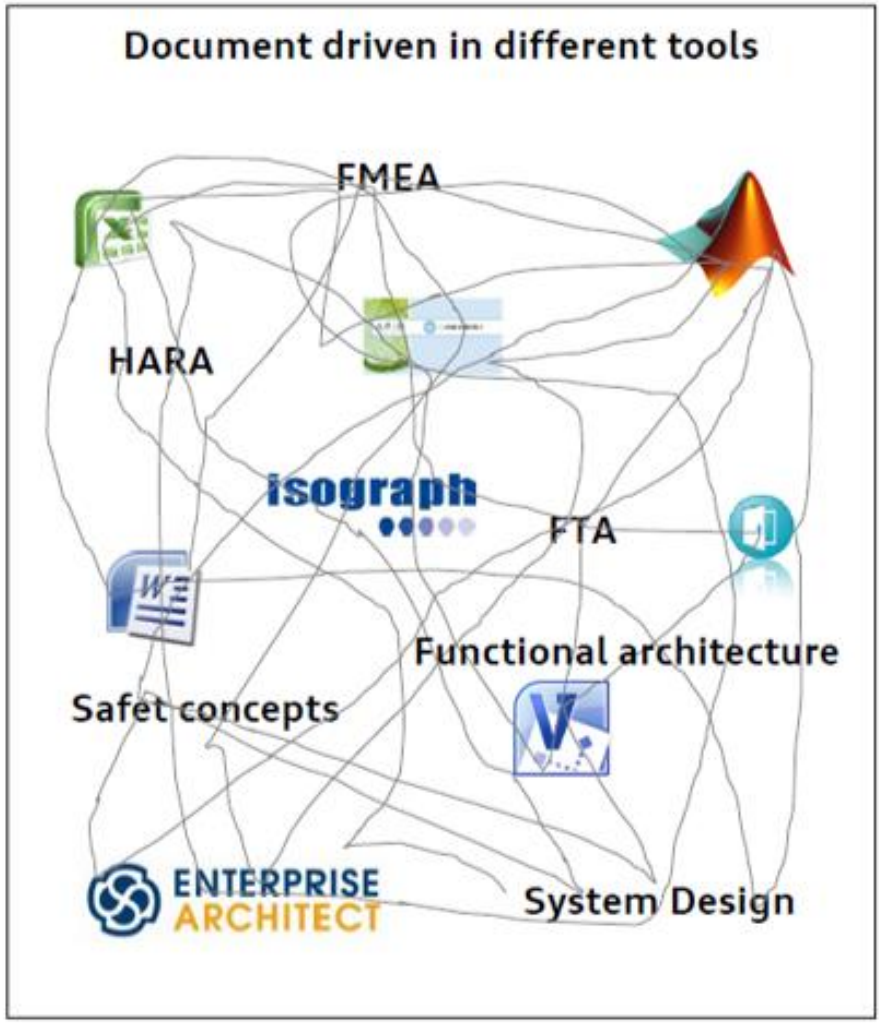
…目前大多采用的手段是excel 及单任务工具 …



… 实际工程中是怎样做的?


安全分析:対象ハザードの発生原因分析(FTA)
対象安全目標ID: PDU-SG3(意図に反して減速(急減速)してはいけない)
意図に反する減速(急減速)発生
スイッチング素子短絡(ON故障、ON固着)発生
スイッチング素子のON故障
スイッチング素子のON固着
スイッチング素子のショート故障
スイッチング素子への過電圧印加
スイッチング素子への過電流印加
スイッチング素子の異常過熱
ゲート信号のON固定
制御基板回路の故障(ON故障)
スイッチング素子の偶発故障
スイッチング素子の異常過熱に至るのは、過電流等の異常状態が発生し、かつ過熱保護回路が故障している場合(2重故障状態)であるため、対象外とする
外部要因のため、対象外とする。
Page 1
Page 1

传统方式： 容易出错、耗时费力



- 各种文档、工具间难以追溯
- 重复工作、冗余数据
- 设计与安全分析交互不畅
- 难以保证一致性
- 大量人工确认、无法自动化

议程

- 航空系统安全性评估的要求和挑战
- ANASYS medini 与 安全性评估
- medini应用案例： 机轮刹车系统
- 小结

ANSYS medini: 综合安全分析解决方案

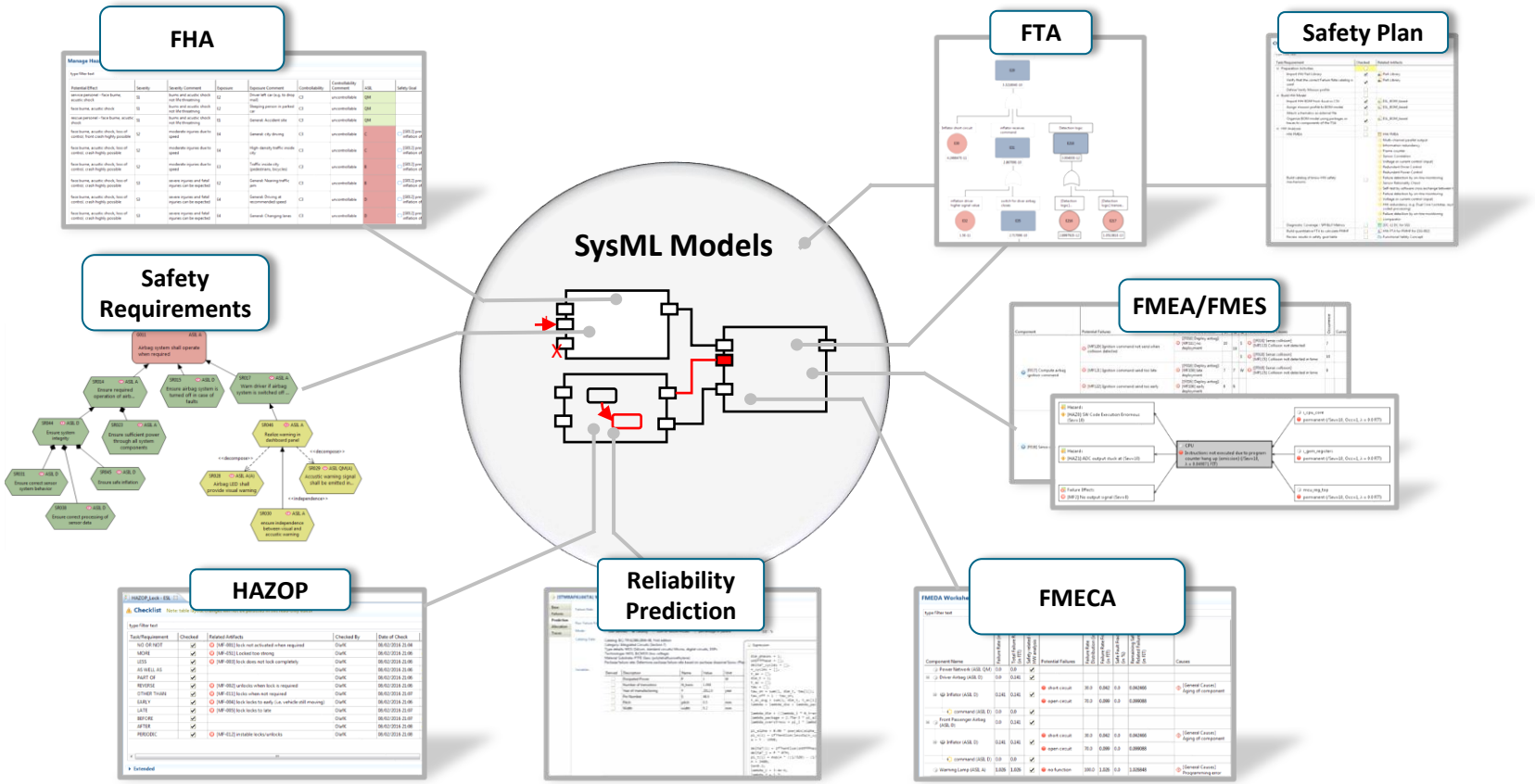
- 安全性分析与可靠性工程的综合解决方案
- 基于模型的方法，覆盖全生命周期，高效连接安全要求、安全评估、架构设计，确保追踪性和一致性
- 符合功能安全标准的最佳实践：ARP4761/ARP4754A，IEC 61508，EN50126/50128/50129 , ISO 26262
- 内置大量高效的工程模板、检查单和手册，SN 29500，IEC 62380，MIL HDBK 217F/217+，GJB299C, FIDES Guide 2009 支持复用和自动化，大大减少成本和上市时间
- 适用于航空航天、汽车、轨道交通、核能等安全应用领域

全球250+ 客户

DAIMLER, Audi, TOYOTA, TRW, GM, MAGNA, Volkswagen, FCA, Ford, NISSAN, FOTON, NXP, DENSO, Continental, BOSCH, Valeo, DELPHI, nexteer AUTOMOTIVE, MANDO, daedong, DAESUNG, Panasonic, McLaren, ANALOG DEVICES, TESLA, SANYO, Allegro MicroSystems Europe Ltd, 航空工业光电所 AVIC Optronics, CASC, COMAC, 航空工业成都飞机设计研究所 AVIC CHENGDU AIRCRAFT DESIGN & RESEARCH INSTITUTE, MBDA MISSILE SYSTEMS

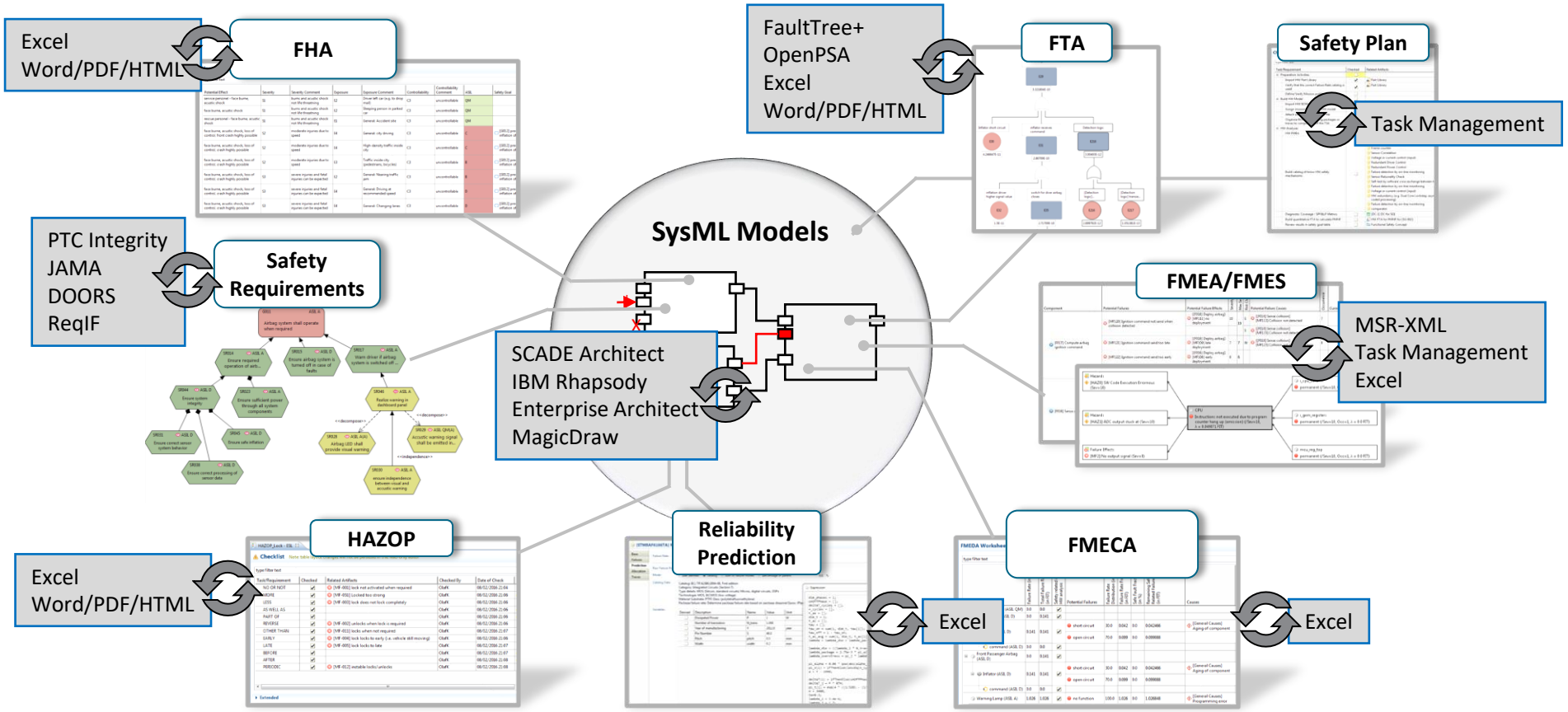
medini: 基于模型的安全分析

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



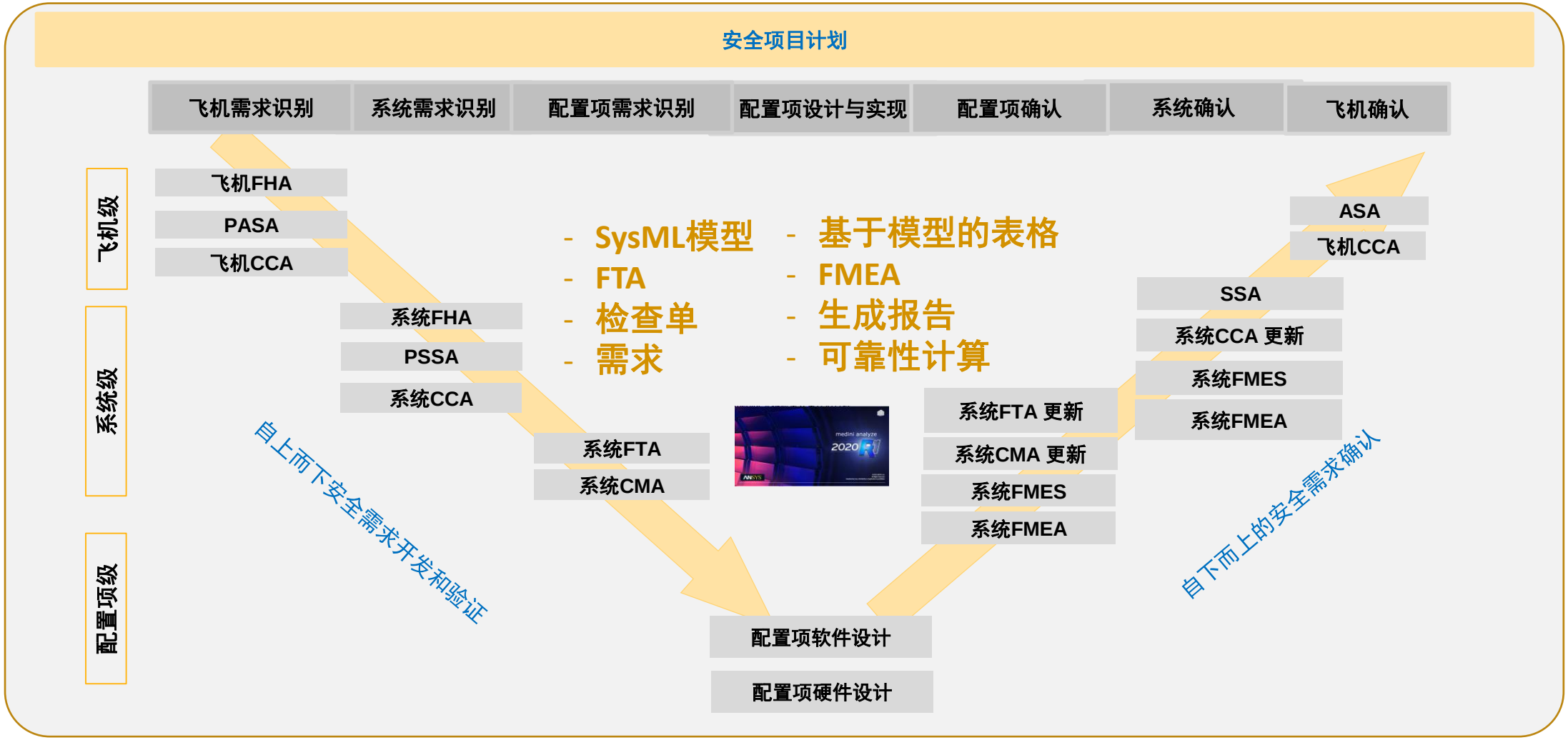
基于模型的方法确保一致性、可跟踪性和高效率

medini: 丰富的工具接口



开放的接口，保证工作的无缝衔接

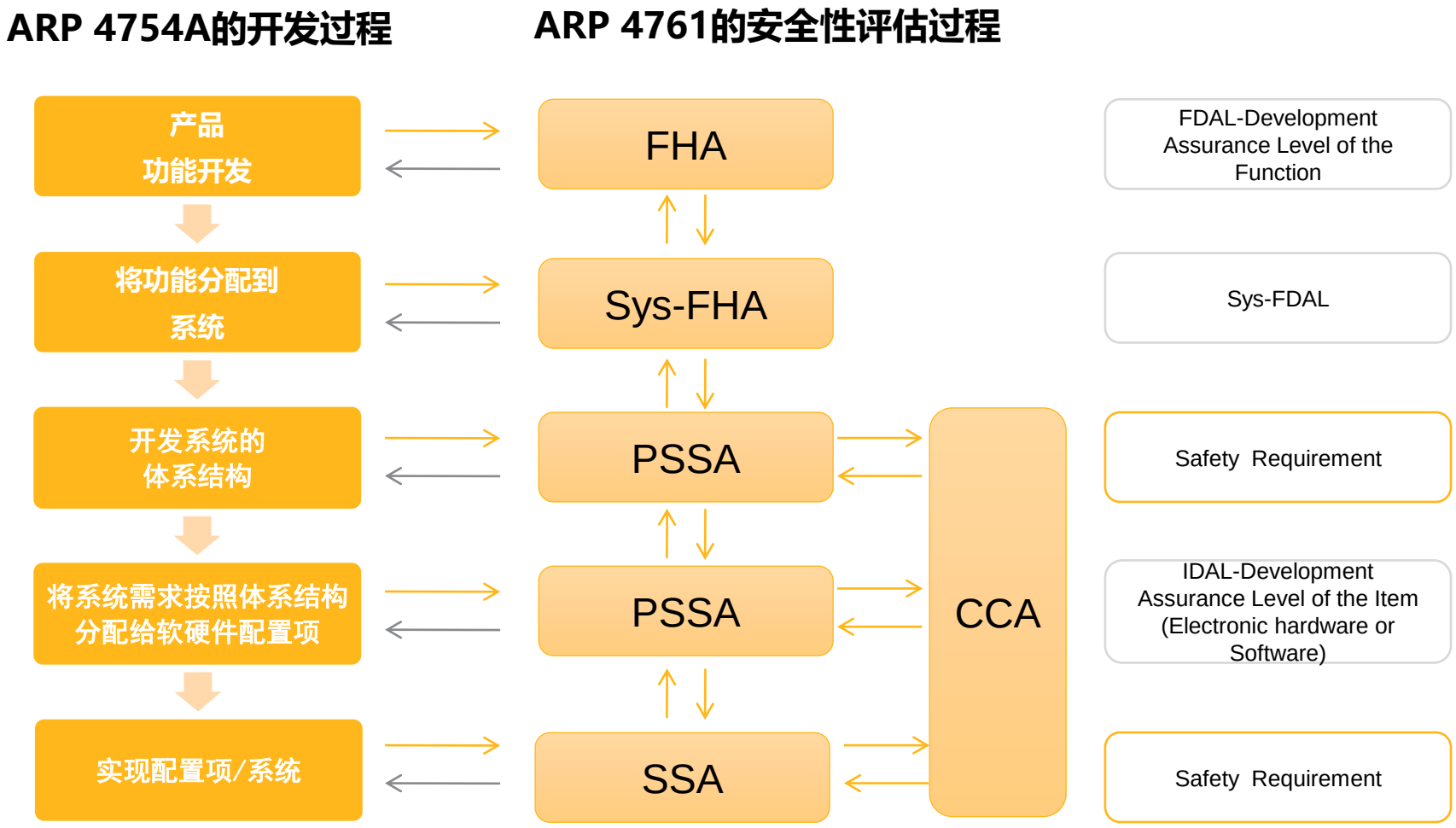
medini 支持航空安全评估过程



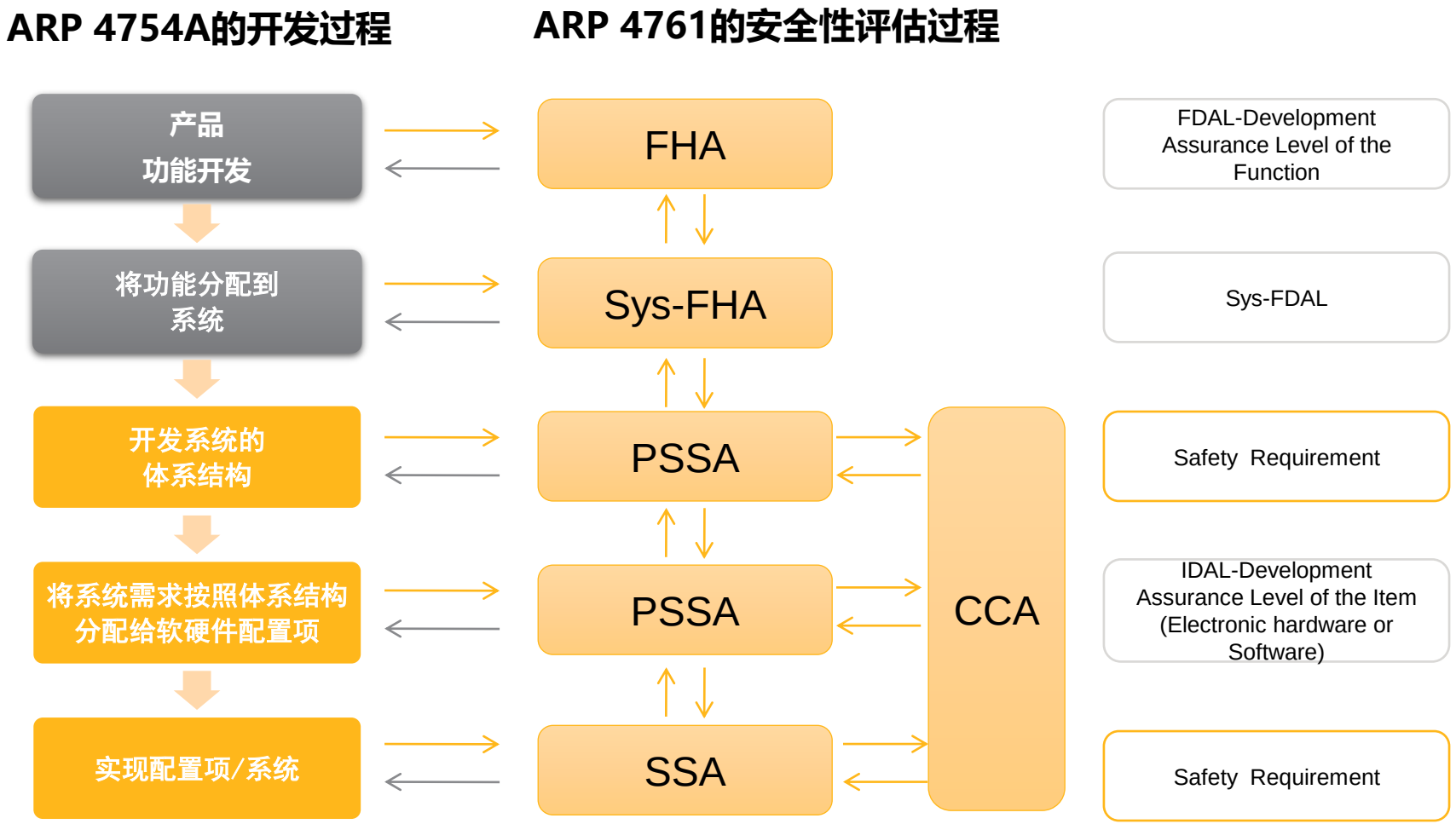
议程

- 航空系统安全性评估的要求和挑战
- ANASYS medini 与 安全性评估
- medini应用案例： 机轮刹车系统
- 小结

安全生命周期：

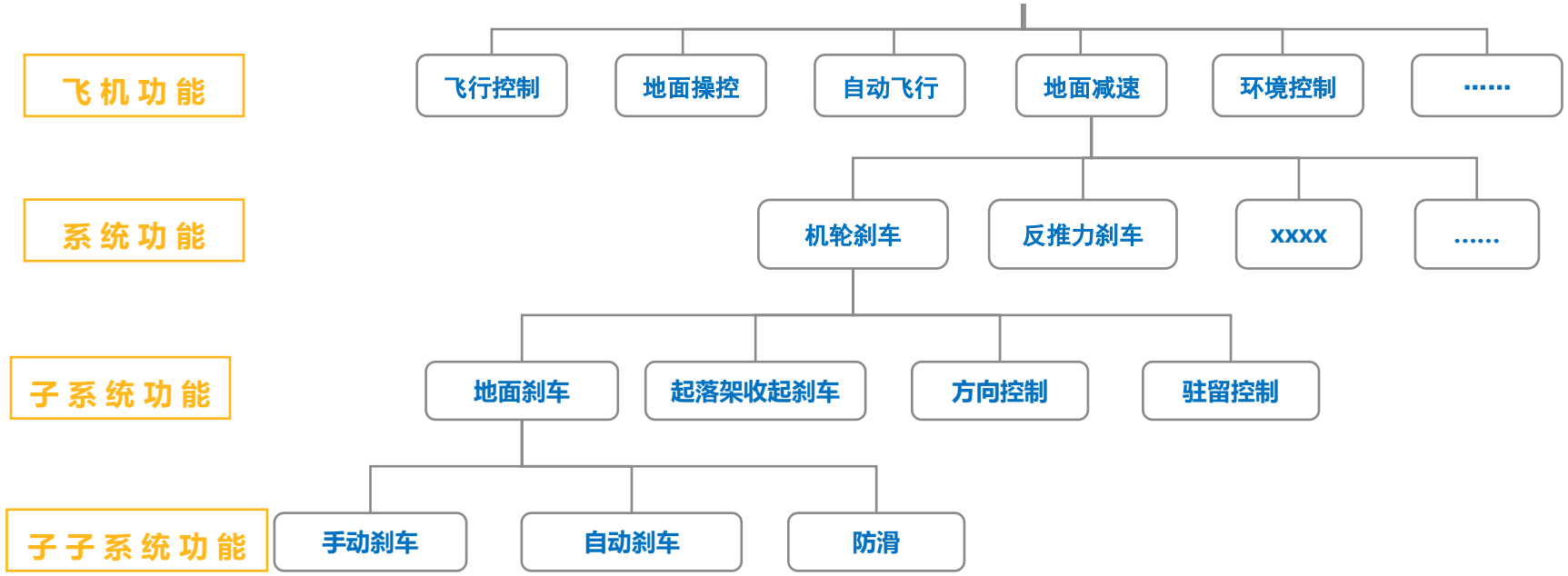

ARP 4754A的开发过程
ARP 4761的安全性评估过程
产品
功能开发
将功能分配到
系统
开发系统的
体系结构
将系统需求按照体系结构
分配给软硬件配置项
实现配置项/系统
FHA
Sys-FHA
PSSA
PSSA
SSA
CCA
FDAL-Development Assurance Level of the Function
Sys-FDAL
Safety Requirement
IDAL-Development Assurance Level of the Item (Electronic hardware or Software)
Safety Requirement

安全生命周期 – 方案设计阶段：



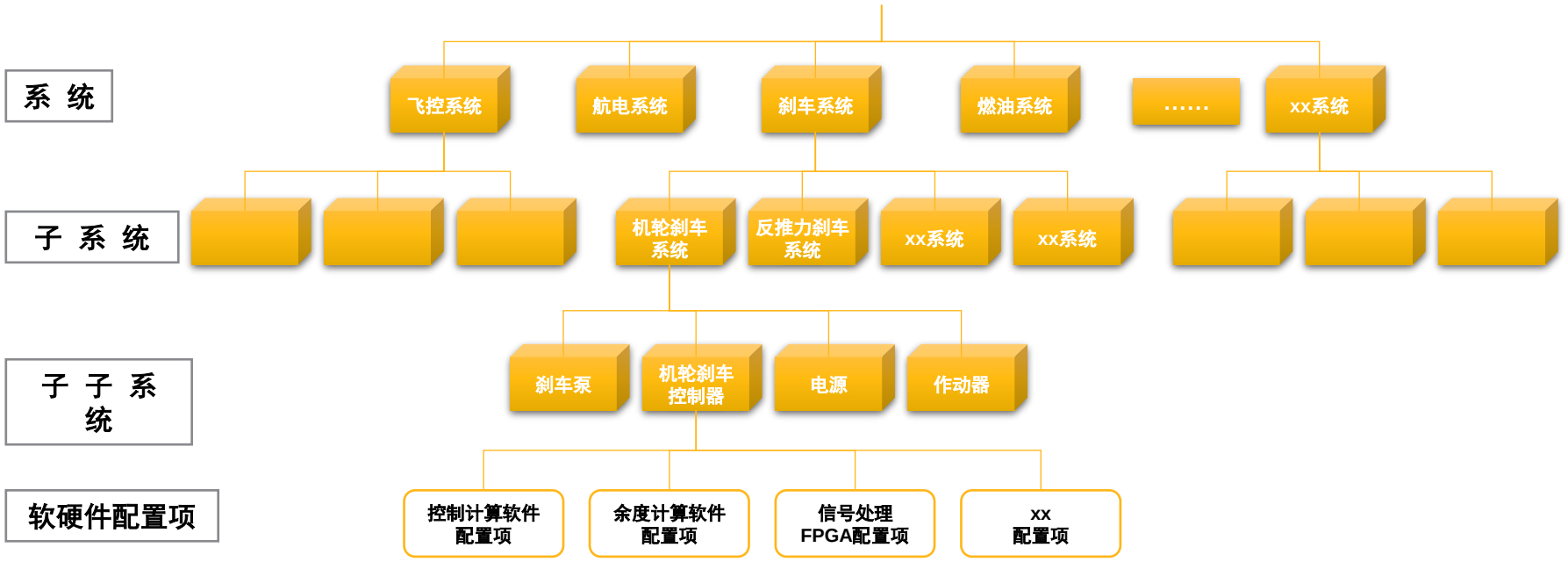
安全生命周期 – 方案设计阶段：

功 能 视 图



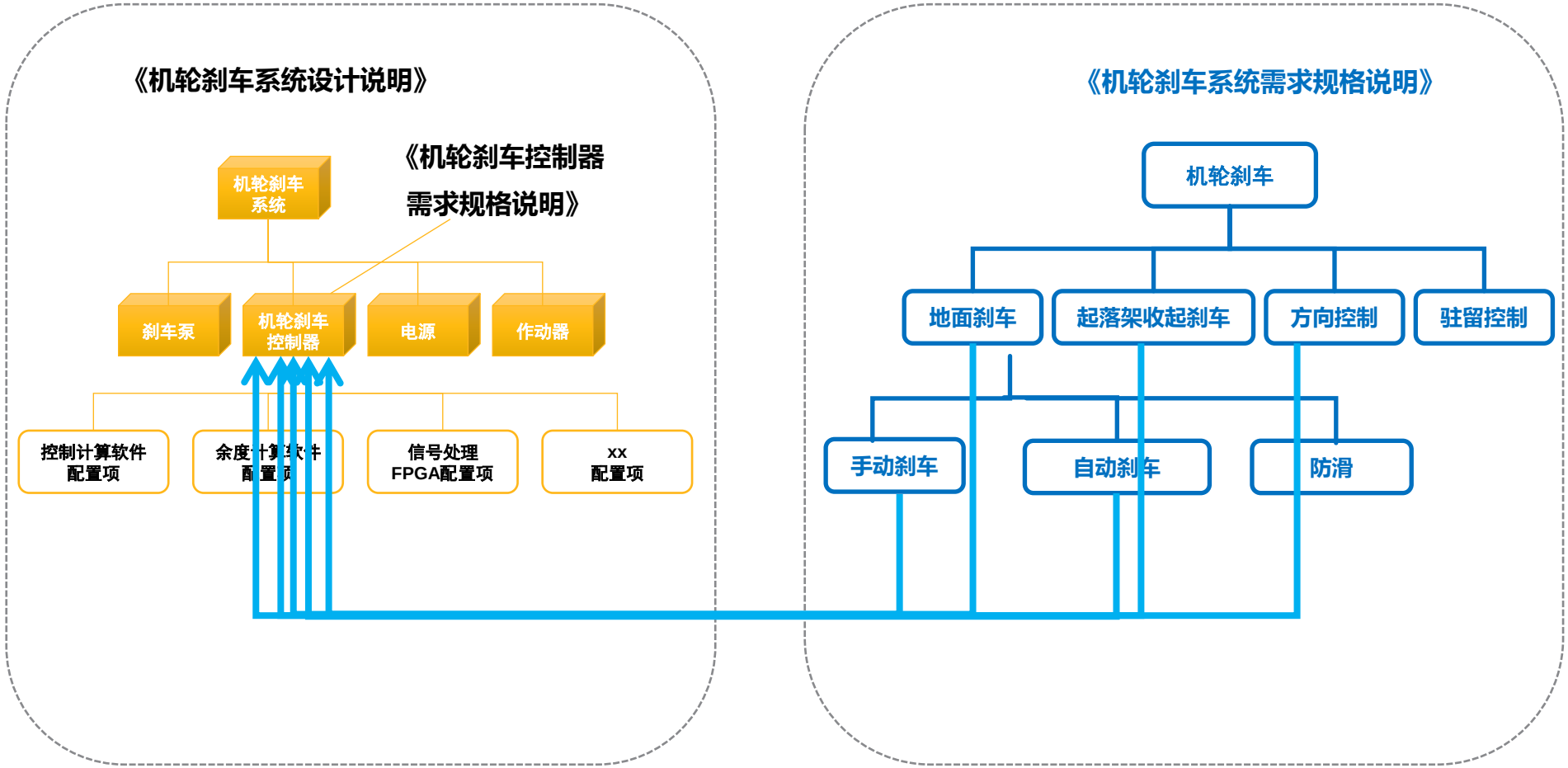
安全生命周期 – 方案设计阶段：

架 构 视 图



安全生命周期 – 方案设计阶段：

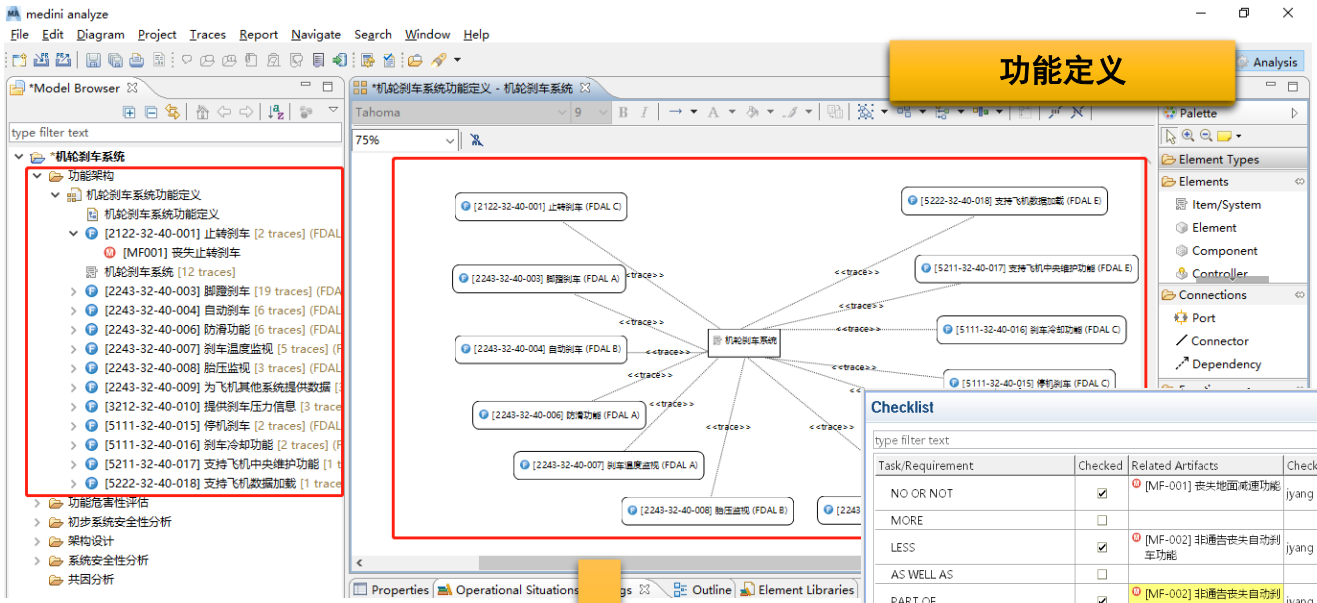
例子： 机轮刹车功能分配给机轮刹车系统的架构



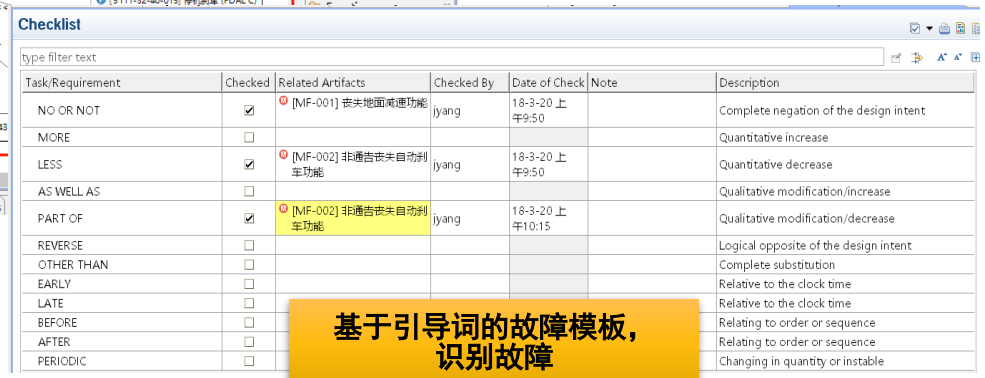
方案设计阶段：

产品
功能开发

将功能分配到
系统

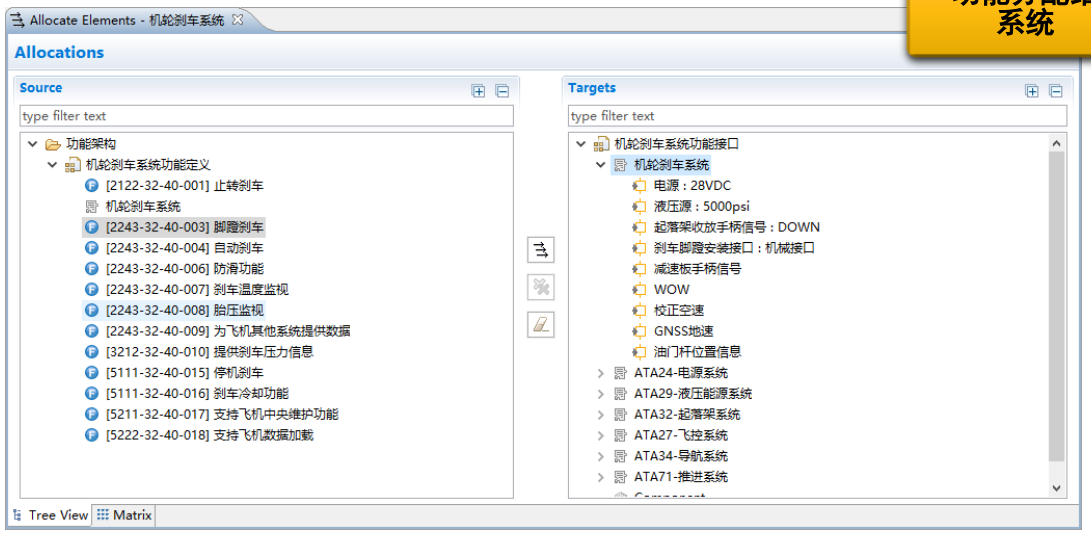


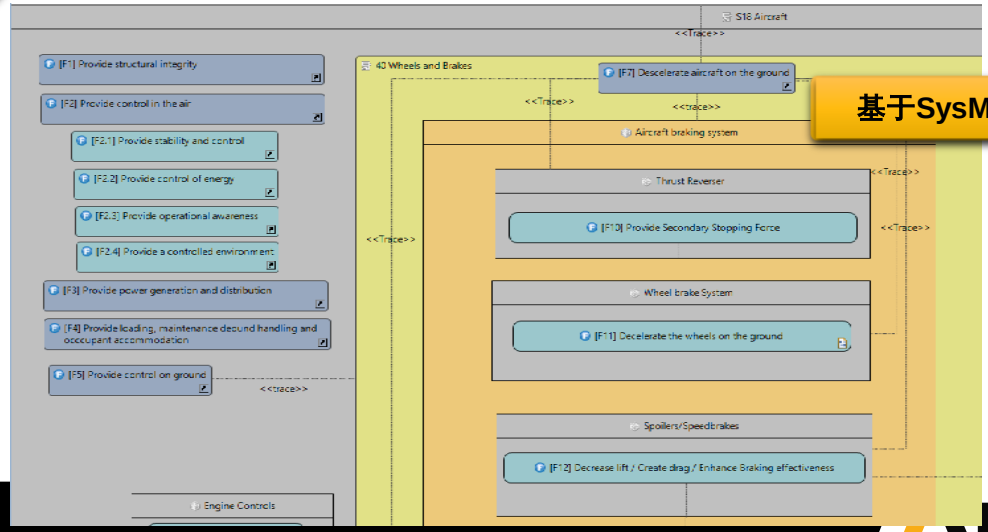
功能定义



基于引导词的故障模板，
识别故障

功能分配给
系统

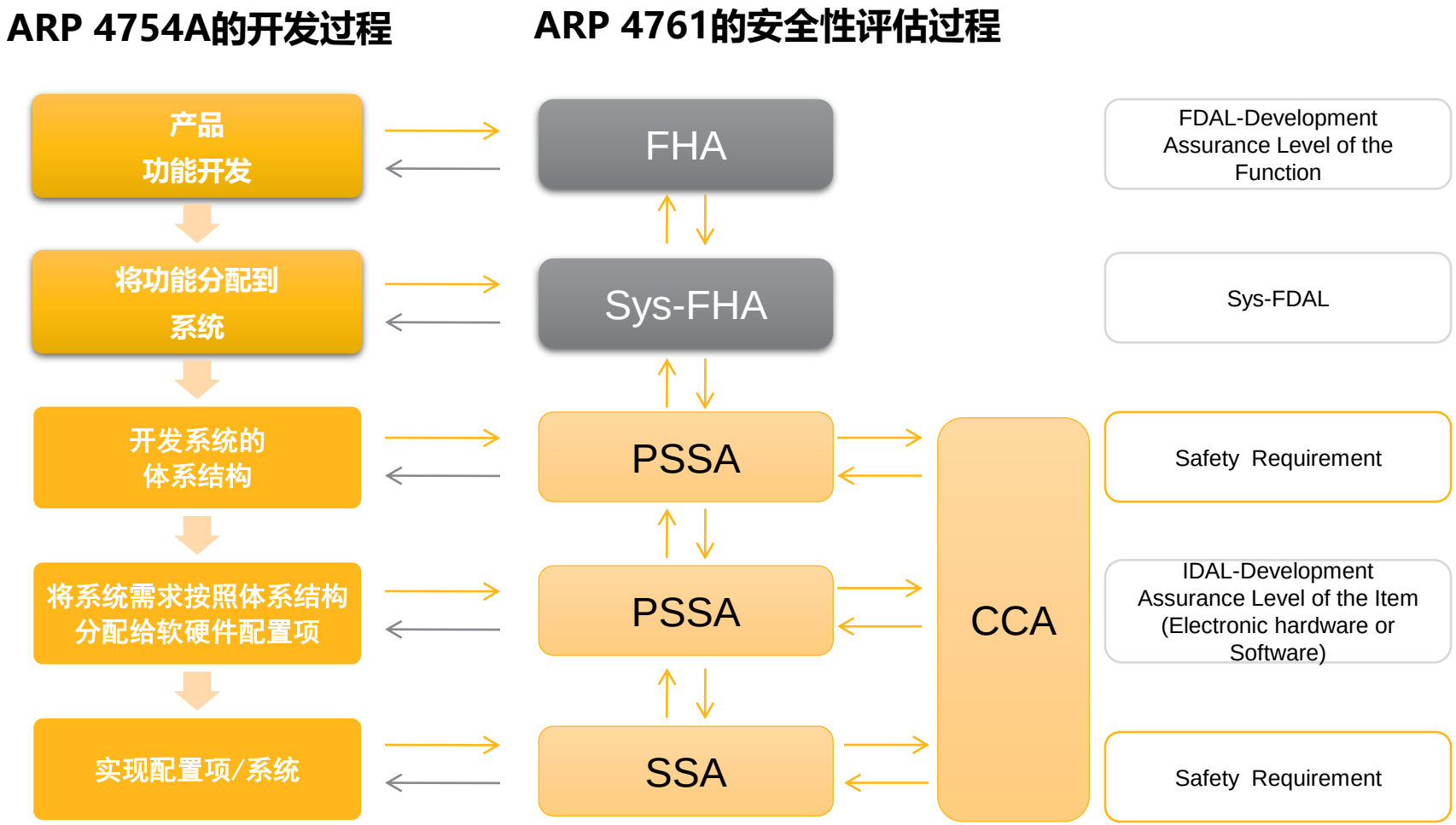




基于SysML的系统设计

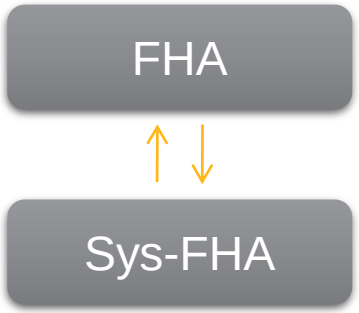
Ansys

安全生命周期 – 飞机级/系统级FHA （功能危险评估）



安全生命周期 – 飞机级/系统级FHA （功能危险评估）

对功能进行系统、全面的检查，以鉴别这些功能的失效状态并按严重性进行分类。
FHA是一种预测技术，试图探索系统部分功能失效的影响。



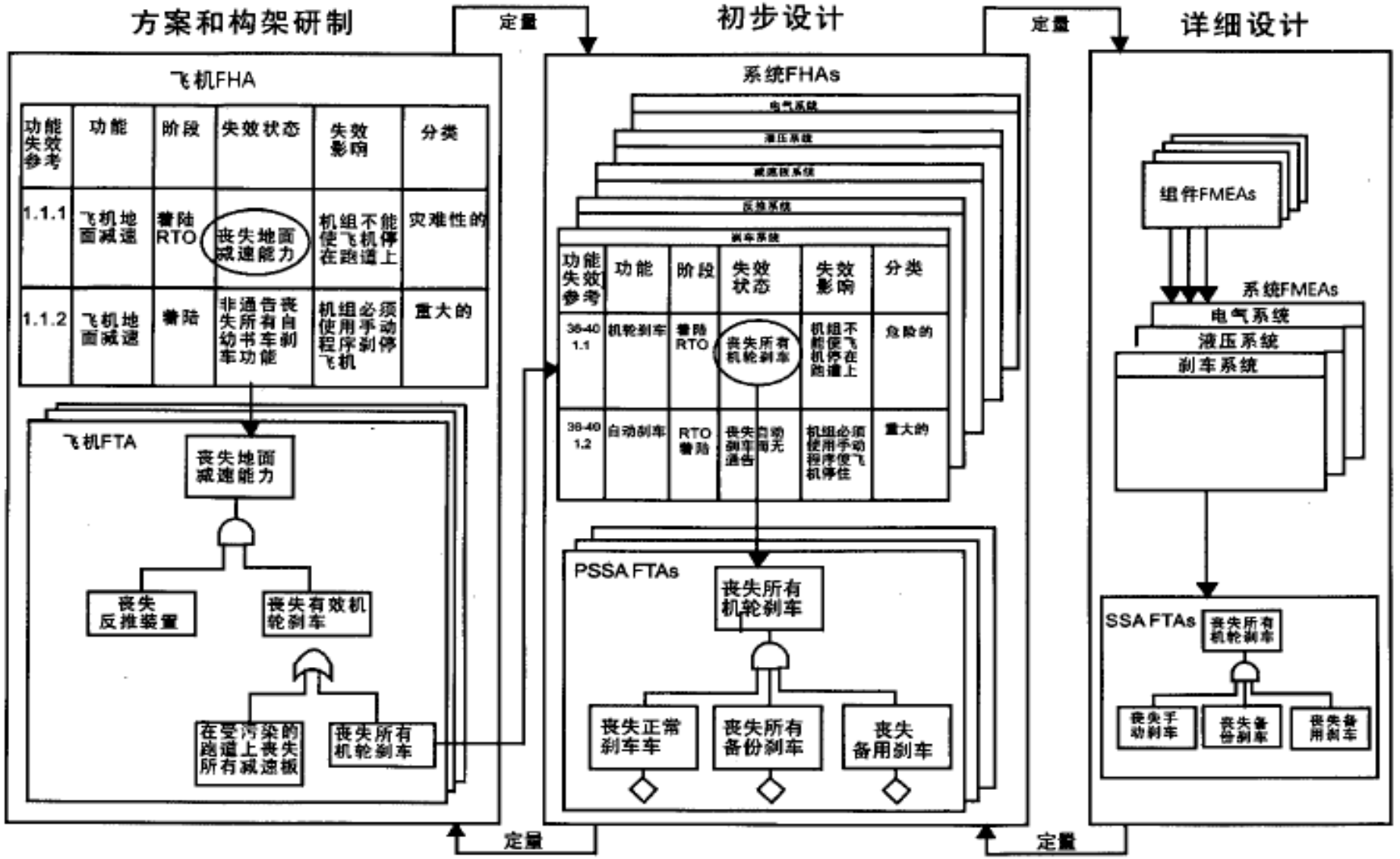
飞机级FHA: 针对飞机级功能进行的高层次定性评估

Function	Failure Condition	Flight phase	Failure effect	Classification	……
地面减速	所有刹车无法制动	Takeoff；Landing	Boom…Bang！	Catastrophic	
	主刹车无法制动，副刹车可以制动	Takeoff；Landing	刹车性能下降，可能造成冲出跑道…	Hazardous	
	主刹车可以制动，副刹车无法制动	Takeoff；Landing		Hazardous	
	刹车滞后制动	Takeoff；Landing	给机组带来操纵不利…	Major	
	刹车提前制动	Takeoff；Landing		Major	
	刹车制动温度过高	Takeoff；Landing	可能爆胎…	……	
	……				

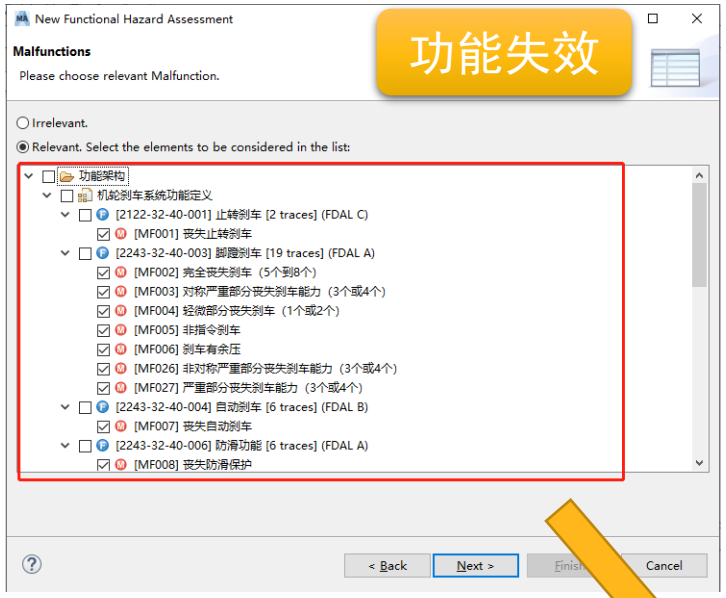
系统级FHA：飞机功能被分配到系统后，进行迭代的定性评估

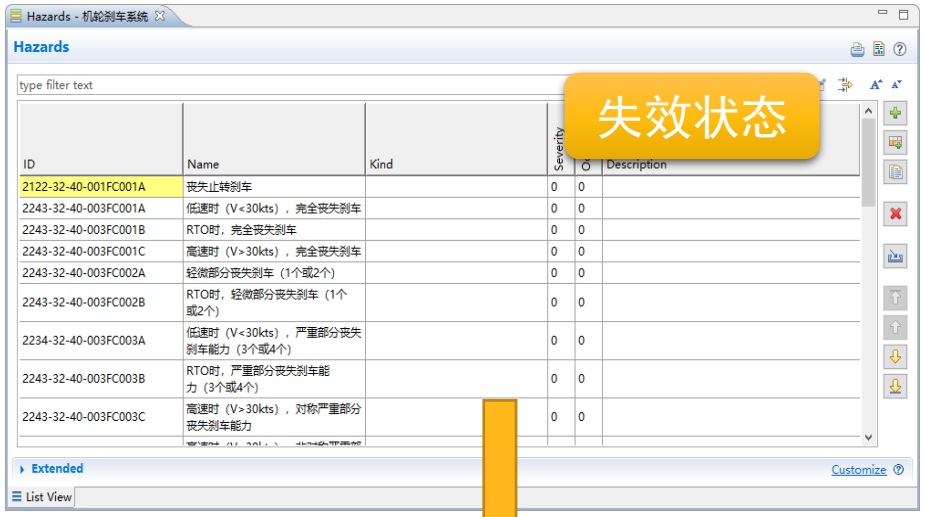
Function	Failure Condition	Flight phase	Failure effect	Classification	……
地面减速子功能1（接通制动阀）	FC1：无法接通制动阀			Catastrophic	
	……				

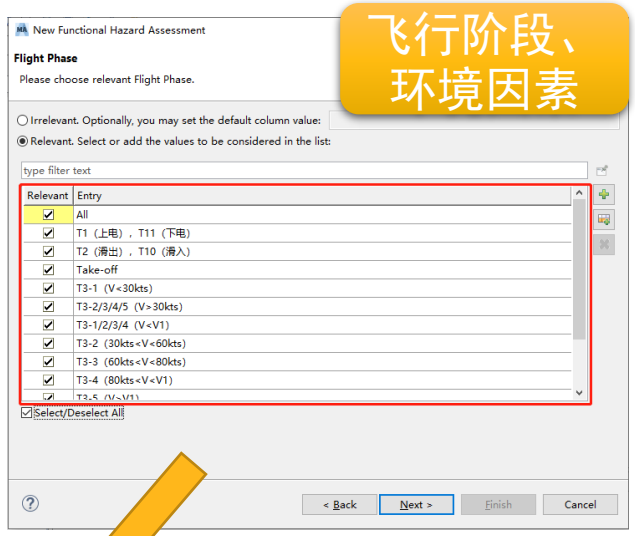
例子：FHA 与 FTA/FMEA 之间的关系



medini 用于FHA







自动生成FHA表格

机轮刹车系统功能危害性评估表

type filter text

功能定义	失效状态编号	飞行阶段	功能失效行为	飞行员感知	运行环境	应急构型	失效状态	对飞机的影响	对机组的影响	对乘客的影响	失效状态影响等级	FDAL	支撑材料
[2243-32-40-003] 脚蹬刹车	SC220	Take-off	[MF027] 严重部分丧失刹车能力(3个或4个)	• 告知的 • 未告知的	正常	RTO	[2243-32-40-003FC003B] RTO时，严重部分丧失刹车能力(3个或4个)	丧失有效的减速功能，可能造成飞机冲出跑道，飞机结构受损，甚至彻底损毁	可能由于飞机的损毁而死亡	可能由于飞机的损毁而绝大部分或者全部死亡	Catastrophic	A	工模试验
[2243-32-40-007] 刹车温度监视	SC187	Take-off	[MF011] 错误的刹车温度信息	• 告知的 • 未告知的	正常	RTO	[2243-32-40-007FC002C] RTO时，错误的刹车低温信息(伴...刹车过热)	起落架可能会在刹车时起火，导致飞机不能有效减速，冲出跑道而完全损毁	可能由于飞机的损毁而死亡	可能由于飞机的损毁而绝大部分或者全部死亡	Catastrophic	A	工模试验
[2243-32-40-006] 防滑功能	SC159	Take-off	[MF008] 丧失防滑保护	• 未告知的	正常	正常	[2243-32-40-006FC001B] 未告知的丧失防滑保护	防滑功能失效可能导致拖胎、爆胎，损坏飞机结构	机组工作负荷极大增加，完成任务的能力极大降低	可能导致部分乘客严重受伤	Catastrophic	A	工模试验
[2243-32-40-003] 脚蹬刹车	SC131	Take-off	[MF006] 刹车有余...	• 未告知的	正常	正常	[2243-32-40-003FC005C] 未告知的刹车有余压	可能导致刹车过热起飞，如...起起落架，过热刹车造成轮...其他设备不安全影响，如起飞后发现刹车温度过热，不收...起落架，带起落架爬升，如碰上越障情况，造成潜在危险。	极大的增加驾驶员的工作负担,可能受伤	可能导致部分乘客受伤或死亡	Hazardous	B	工模试验
[2243-32-40-004] 自动刹车	SC108	Take-off	[MF007] 丧失自动刹车	• 告知的	正常	正常	[2243-32-40-004FC001C] RTO时，告知的丧失自动刹车	可以通过人工刹车实现飞机减速，降低性能或安全余度	机组采用脚蹬刹车实现飞机减速，RTO情况下，严重增加工作负荷	无	Major	C	飞行试验
[2243-32-40-003] 脚蹬刹车	SC081	Take-off	[MF006] 刹车有余...	• 未告知的	正常	RTO	[2243-32-40-003FC005B] 未告知的刹车有余压同时RTO	可能因为前期刹车一直使用，而导致RTO时，刹车没有足够能力吸收RTO刹车能量，导致飞机冲出跑道	极大的增加驾驶员的工作负担,造成伤亡	可能导致大部分部分乘客受伤或死亡	Catastrophic	A	工模试验
[2243-32-40-003] 脚蹬刹车	SC203	Take-off	[MF002] 完全丧失刹车（5个到8个）	• 告知的 • 未告知的	正常	RTO	[2243-32-40-003FC001B] RTO时，完全丧失刹车	丧失有效的减速功能，可能造成飞机冲出跑道，飞机结构受	驾驶员不能通过刹车系统刹	可能由于飞机的损毁而绝大部分	Catastrophic	A	工模试验

medini 用于PASA – FTA

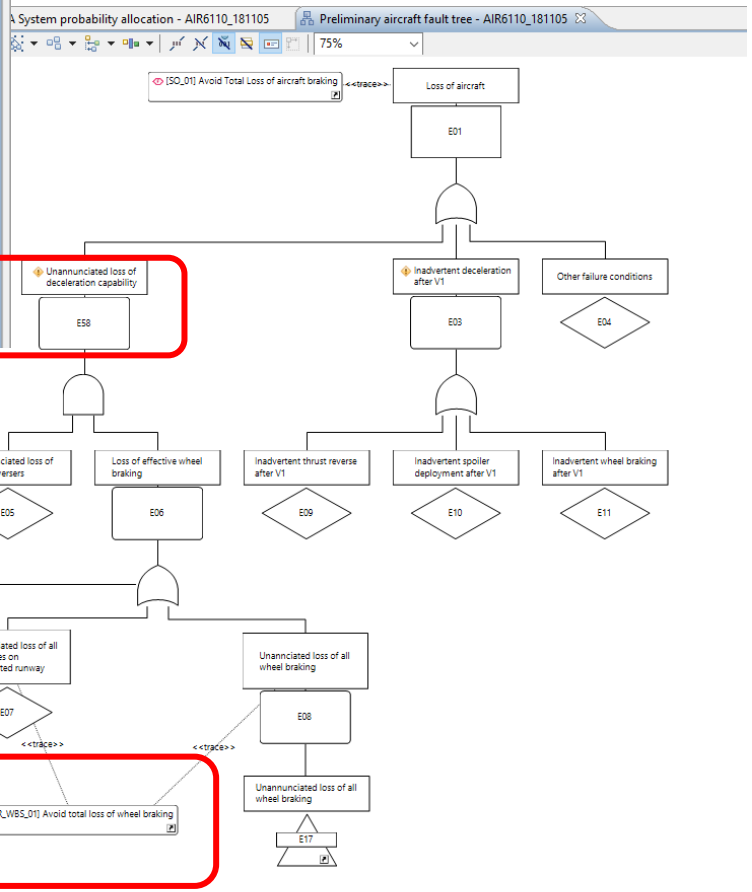
Safety program plan - AIR6110_181105 | AFHA - AIR6110_181105

Scenario Analysis

type filter text

ID	Function	Failure Condition (Hazard description)	Phase	Effect of failure condition on Aircraft/Crew	Failure Condition Classification
AFHA1	[F7] Descelerate aircraft on the ground	[AFHA_H1.1] Unannunciated loss of deceleration capability	Landing/RTO	Crew is unable to decelerate the aircraft,resulting in a high speed overrun	Catastrophic
AFHA2	[F7] Descelerate aircraft on the ground	[AFHA_H1.2] Annunciated loss of deceleration capability	Landing	Crew selcets a more suitable runway, notifies emergency grond support, and prepares occupants for runway overrun	Minor
AFHA3	[F7] Descelerate aircraft on the ground	[AFHA_H1.1] Unannunciated loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resultiing in low speed contact with terminal, aircraft, or vehicles.	Major
AFHA4	[F7] Descelerate aircraft on the ground	[AFHA_H1.2] Annunciated loss of deceleration capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No safety effects

System probability allocation - AIR6110_181105 | Preliminary aircraft fault tree - AIR6110_181105

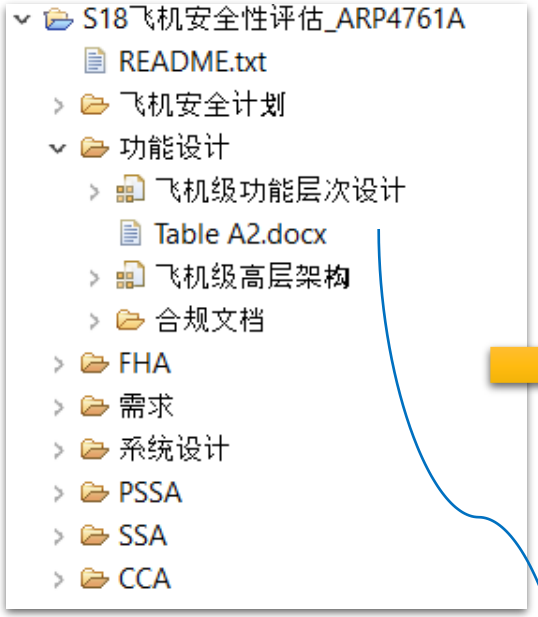


AFHA中的失效状态在 PASA 中进一步分析

- 派生并追溯至安全需求
- 分配资源

派生安全需求

medini 用于FHA



AFHA: 在方案设计阶段中定义的功能及其失效，自动出现在FHA表中，并且被评估以确定失效状态并导出FDAL

type filter text

ID	Function	Malfunctioning Behaviour	Flight Phase	crew awareness	Failure Condition	Aircraft Effect	Crew Effect	Occupants Effect	Potential Effect	Verification	Failure Condition Classification	FDAL
SC003	[F8.1.001] 飞机地面减速功能	[M力					Crew selects a overrun.		crash into structures		Hazardous	B
SC006	[F8.1.001] 飞机地面减速功能	[MF028] 丧失所有减速能力	Taxi	Annunciated	[AFHA_H1.2] 通告丧失所有减速能力	none	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs	none	no safety effect		No Safety Effect	E
SC005	[F8.1.001] 飞机地面减速功能	[MF028] 丧失所有减速能力	Taxi	No Indication	[AFHA_H1.1] 非通告丧失所有减速能力	low speed contact with terminal, aircraft, or vehicles	Crew is unable to stop the aircraft on the taxi way	minor injuries	crash into structures		Major	C
SC008	[F8.1.001] 飞机地面减速功能	[MF031] 意外减速	Take-Off before V1	Perceived	[AFHA_H1.4] v1前意外减速	high speed overrun, fire	Crew will stop the aircraft on runway by applying full brake.	none	loss of aircraft, crash into structures		Hazardous	B
SC007	[F8.1.001] 飞机地面减速功能	[MF031] 意外减速	Take-Off after V1	Perceived	[AFHA_H1.3] v1后意外减速	high speed overrun	Crew is unable to accelerate to takeoff	severe and fatal injuries	loss of aircraft, crash into structures	[E02] V1后意外减速	Catastrophic	A
SC002	[F8.1.001] 飞机地面减速功能	[MF028] 丧失所有减速能力	Rejected Take-Off (RTO)	No Indication	[AFHA_H1.1] 非通告丧失所有减速能力	high speed overrun	Crew is unable to decelerate the aircraft.	severe and fatal injuries	loss of aircraft, crash into structures		Catastrophic	A
SC001	[F8.1.001] 飞机地面减速功能	[MF028] 丧失所有减速能力	Landing	No Indication	[AFHA_H1.1] 非通告丧失所有减速能力	high speed overrun	Crew is unable to decelerate the	severe and fatal injuries	loss of aircraft, crash into	[E01] 非通告丧失所有减速能	Catastrophic	A

支持在工作产品之间导航。

飞机级FTA（定性）：将来自AFHA的已识别失效状态与故障树事件相连；或者，直接从失效状态派生故障树事件。

Sys-FHA: 功能分配给系统后，评估系统功能及其失效

Aircraft FHA - A | Functional archit | AFHA failure con | Emergency landin | Aircraft Level FT | Preliminary aircr | System FHA Wheel

Scenario Analysis

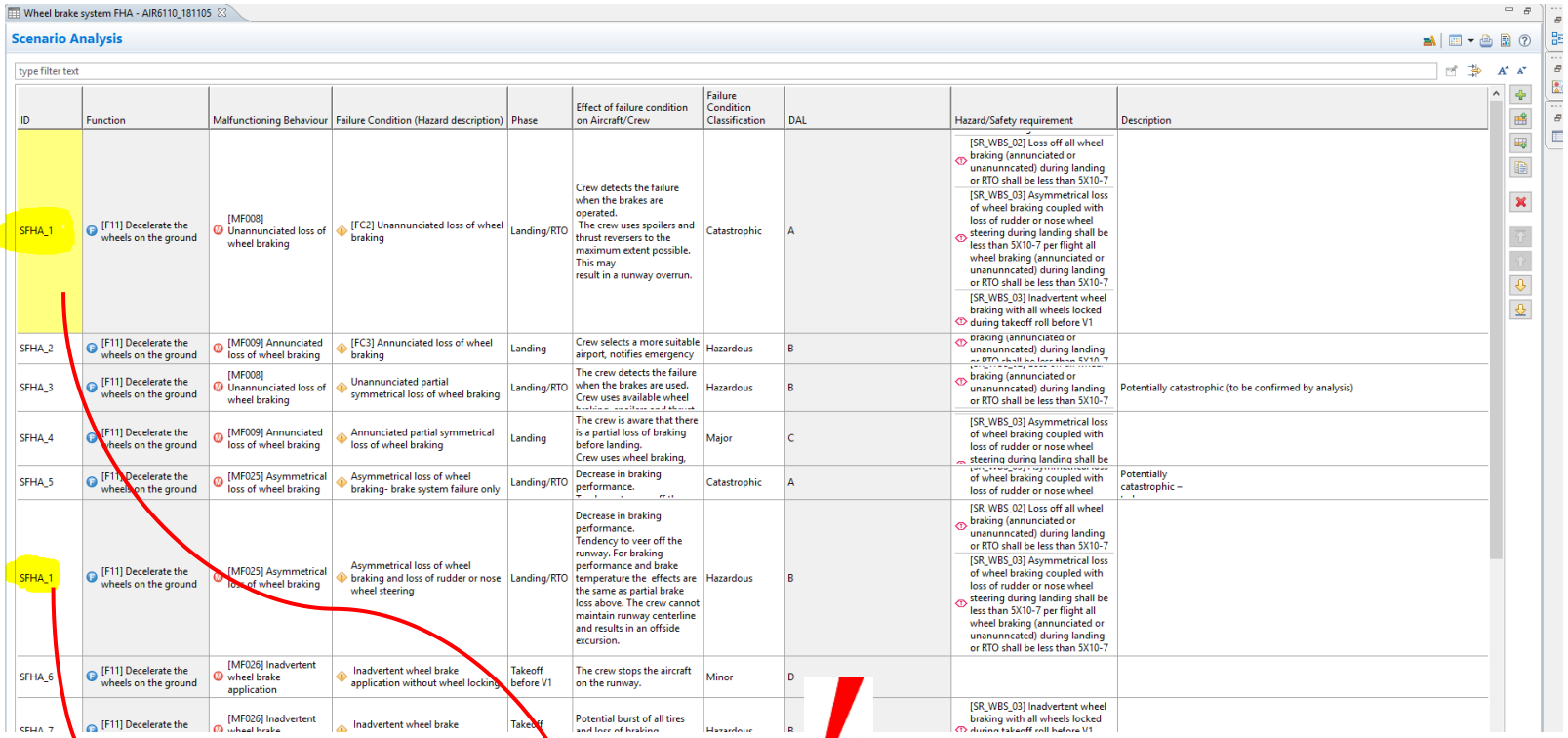
type filter text

ID	Function	HAZOP Guide Word	Failure Condition (Hazard description)	Effect of Aircraft/(				
1	[F009] Decelerate the wheels on the ground	NOT	[FC1] Loss of all wheel braking	The crew when the The crew thrust re extent possible. This may result in a runway overrun				ciated or ll be less than 5X10-7
2	[F009] Decelerate the wheels on the ound	NOT	[FC2] Unannunciated loss of wheel braking	The crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers maximum extent possible. This may result in a runway overrun	Hazardous	B	[SO_01] Avoid total loss of wheel braking	[SR027] Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5X10-7 per flight all wheel braking (annunciated or unannunciated) during landing or RTO shall be less than 5X10-7
3	[F009] Decelerate the wheels on the ground	NOT	[FC3] Annunciated loss of wheel braking	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun. Crew uses spoilers and thrust reversers to the maximum extent possible	Hazardous	B	[SO_01] Avoid total loss of wheel braking	[SR028] Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5X10-7 per flight

子系统继续分析

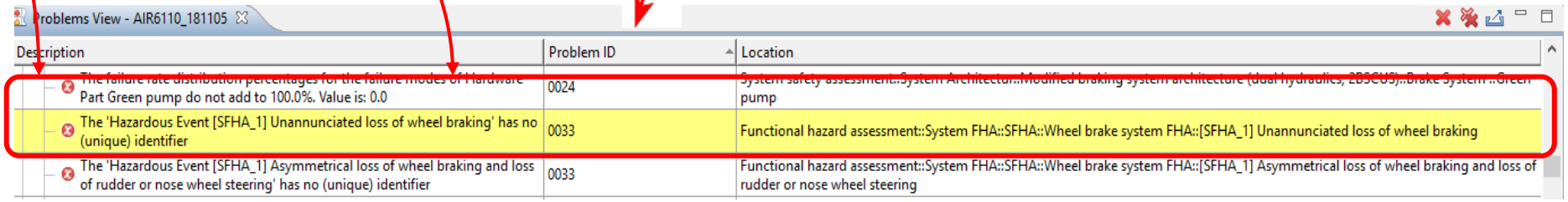
Ansys

内置规则检查 Validation Rules

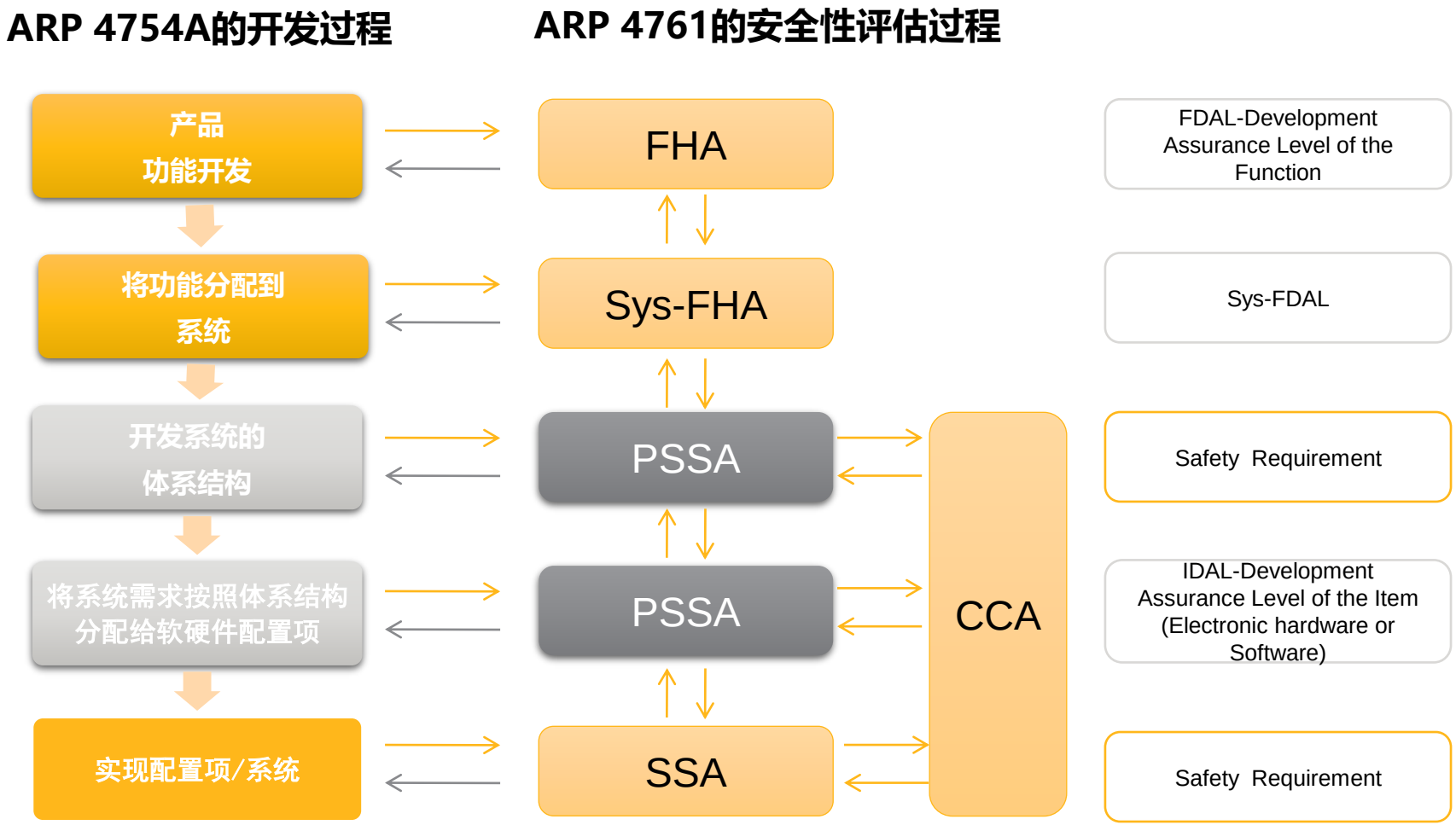


- 验证规则用于早期发现问题和不一致性
- 规则集可定制

比如： 检查SFHA的条目是否具有唯一的ID



安全生命周期 – 初步系统安全评估
Preliminary System Safety Assessment

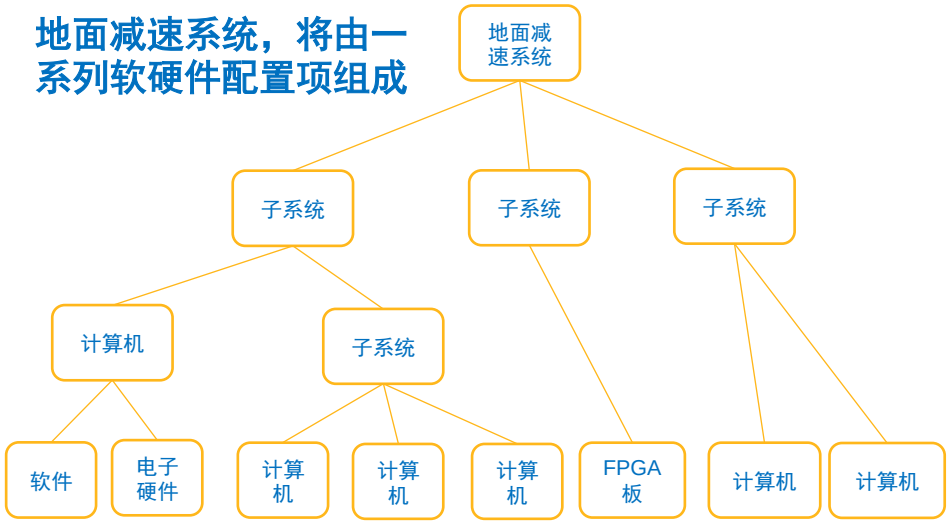


安全生命周期 – 初步飞机/系统安全评估
Preliminary Aircraft/System safety assessment

开发系统的
体系结构

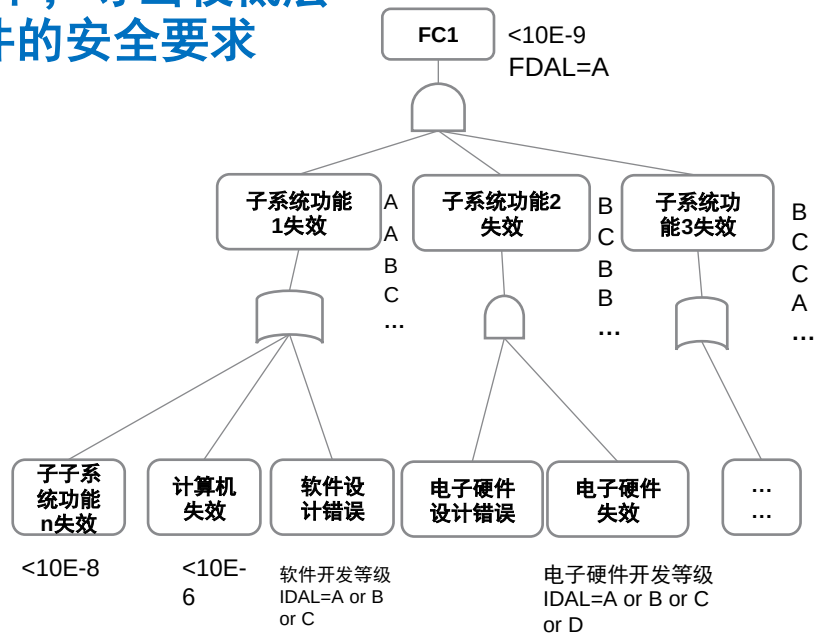
定义“地面减速”系统

地面减速系统，将由一系列软硬件配置项组成

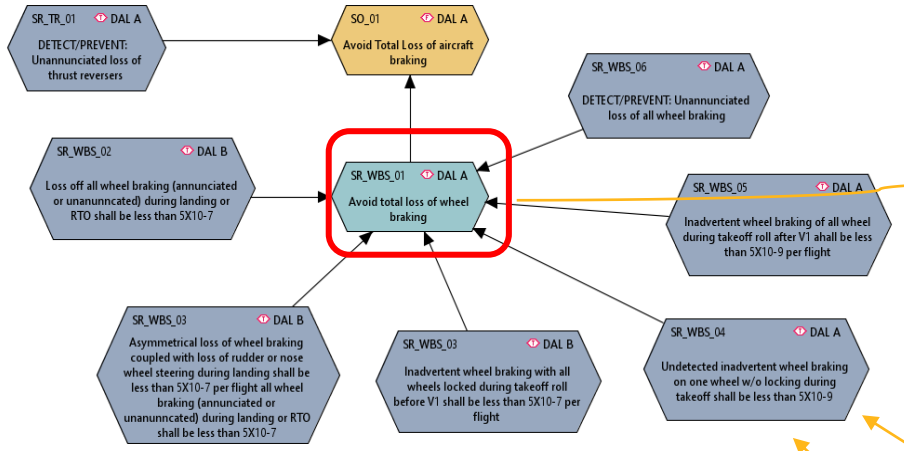


PSSA (FTA)

自上而下，导出较低层组件的安全要求

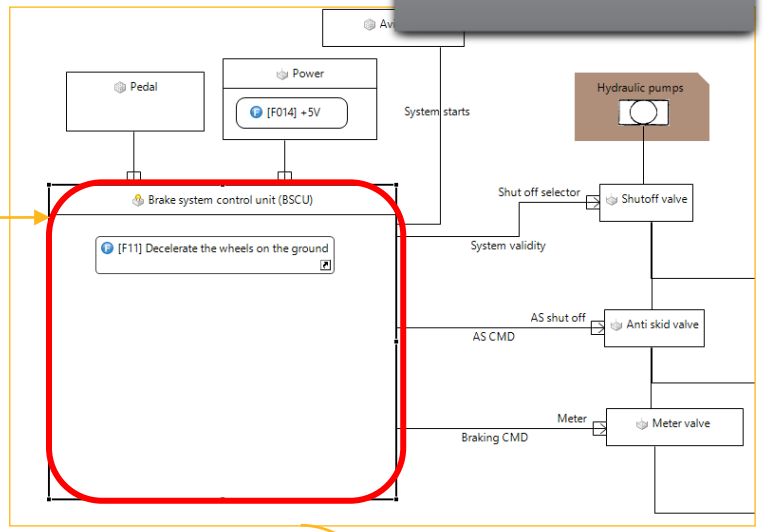


medini 用于PSSA



安全需求分配给架构

建立系统架构 (SysML)



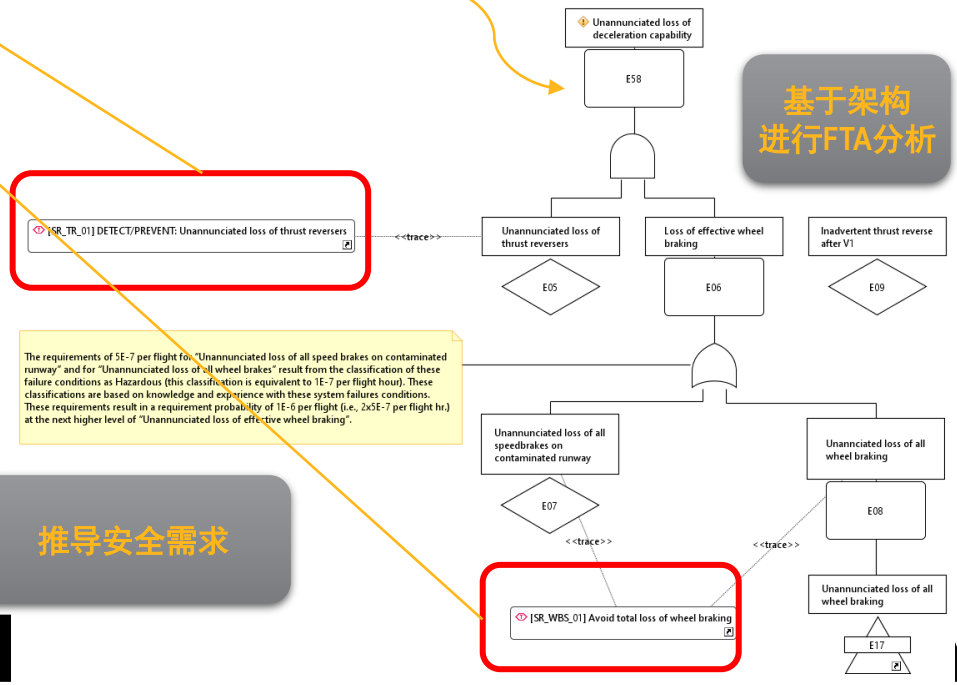
多种视图管理安全需求

Safety Requirements Editor

type filter text

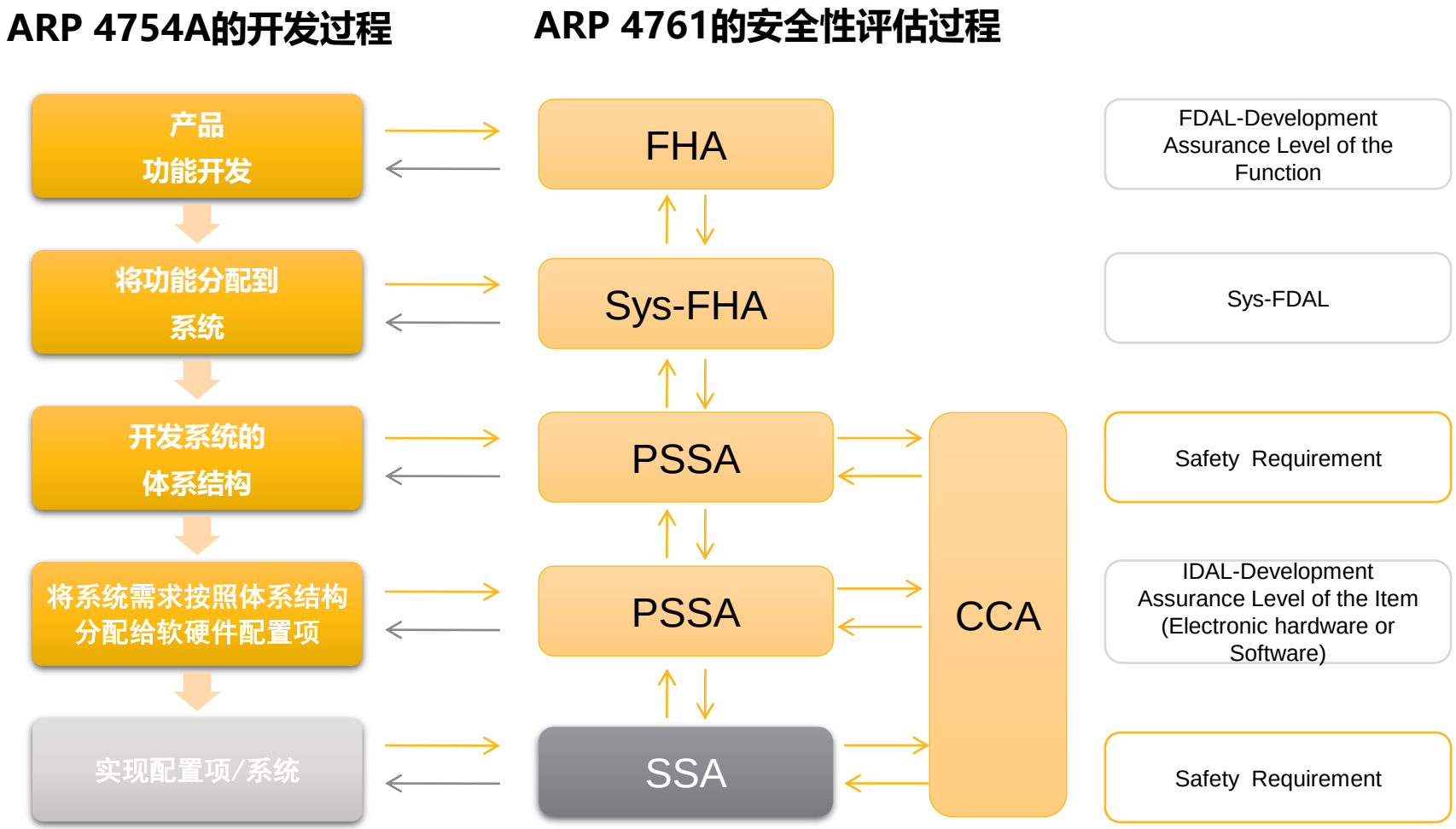
N°	ID	Name	Kind	DAL	Status	All
1	SO_01	Avoid Total Loss of aircraft braking	FUNCTIONAL	A	PROPOSED	[F7] Descelerate aircraft on the ground (FDAL A) S18 aircraft (IDAL A)
2	SR_WBS_06	DETECT/PREVENT: Unannunciated loss of all wheel braking	TECHNICAL	A	PROPOSED	Brake system control unit (BSCU) (IDAL B) Brake System Aircraft braking system (IDAL A) [F5] Provide control on ground (FDAL A) [F7] Descelerate aircraft on the ground (FDAL A)
3	SR_WBS_01	Avoid total loss of wheel braking	TECHNICAL	A	PROPOSED	Brake System Brake system control unit (BSCU) (IDAL B) Normal Brake System Alternate brake system Emergency brake system Aircraft braking system (IDAL A) Wheel brake System (IDAL B) [F11] Decelerate the wheels on the ground (FDAL A) [F5] Provide control on ground (FDAL A) [F7] Descelerate aircraft on the ground (FDAL A)
4	SR_WBS_02	Loss off all wheel braking (annunciated or unanunncated) during landing or RTO shall be less than 5X10-7	TECHNICAL	B	PROPOSED	Brake system control unit (BSCU) (IDAL B) Normal Brake System Brake system control unit (BSCU) (IDAL A) Aircraft braking system (IDAL A) Wheel brake System (IDAL B) [F11] Decelerate the wheels on the ground (FDAL A) [F5] Provide control on ground (FDAL A) [F7] Descelerate aircraft on the ground (FDAL A)
5	SR_WBS_03	Asymmetrical loss of wheel braking coupled with loss of	TECHNICAL	B	PROPOSED	Aircraft braking system (IDAL A) Wheel brake System (IDAL B) [F11] Decelerate the wheels on the ground (FDAL A)

基于架构进行FTA分析



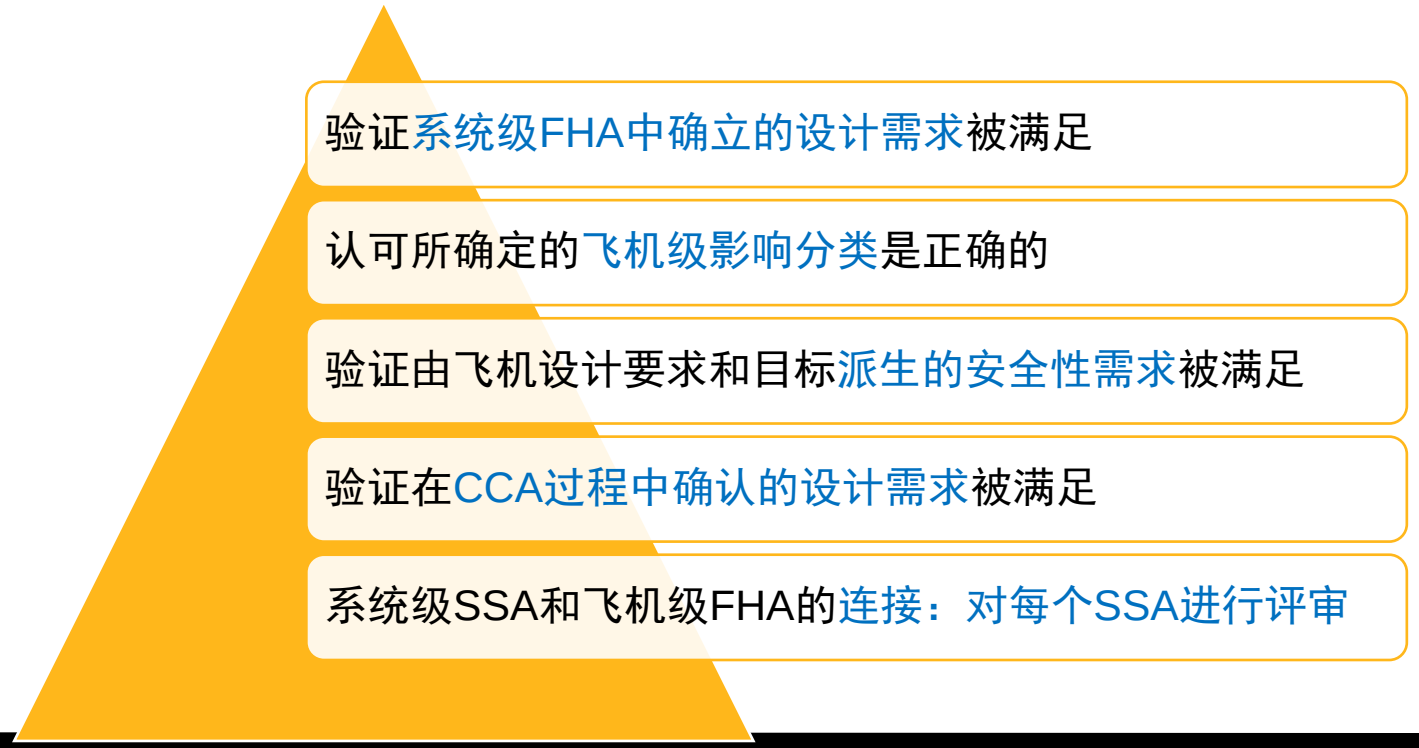
推导安全需求

安全生命周期 – 系统安全评估
System Safety Assessment



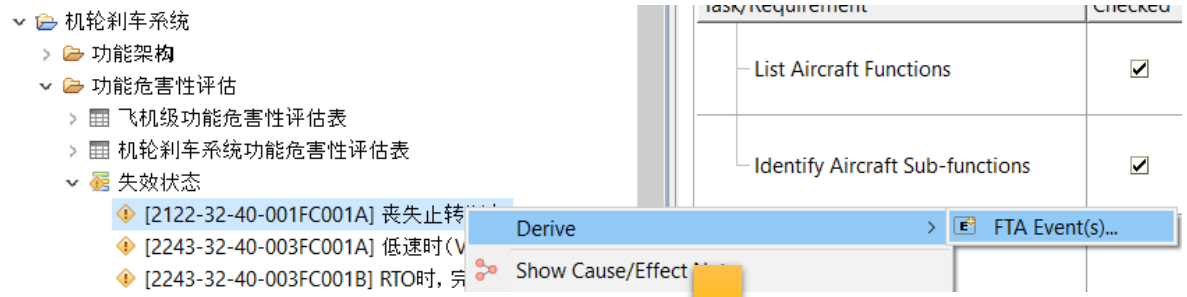
SSA- 系统安全性评估

- SSA： 对系统、系统架构以及系统安装进行系统性核查，以表明其符合安全性要求。
- 可以是定性的，也可是定量的。
- SAA过程是作为验证设计的安全需求和安全目标已被满足的自上而下的方法

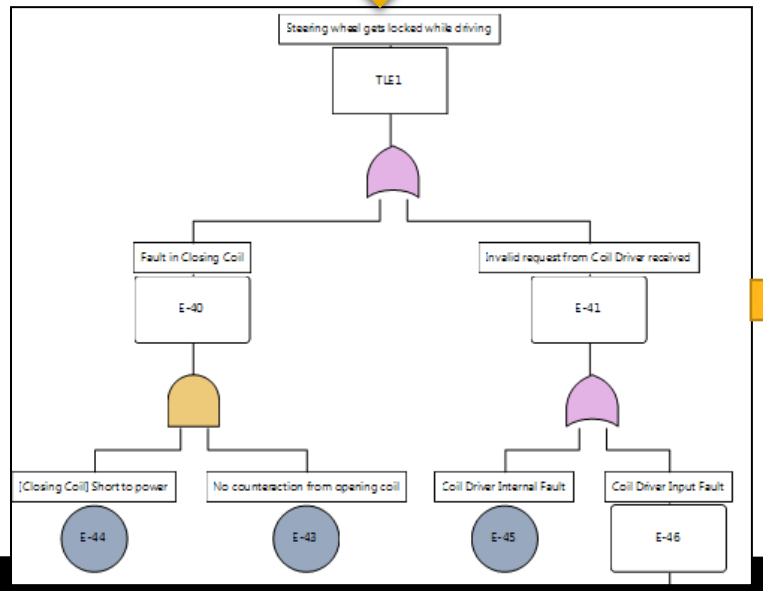


medini 用于SSA - FTA

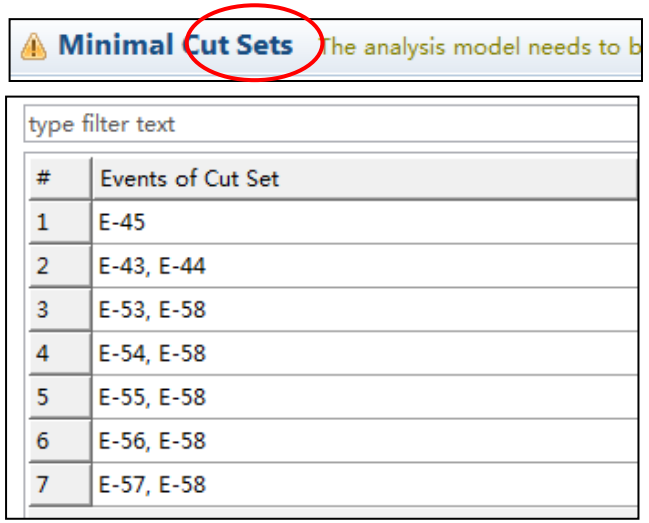
- **定性故障树分析（Qualitative FTA）**



基于失效状态/功能失效/
失效模式自动生成FTA事件



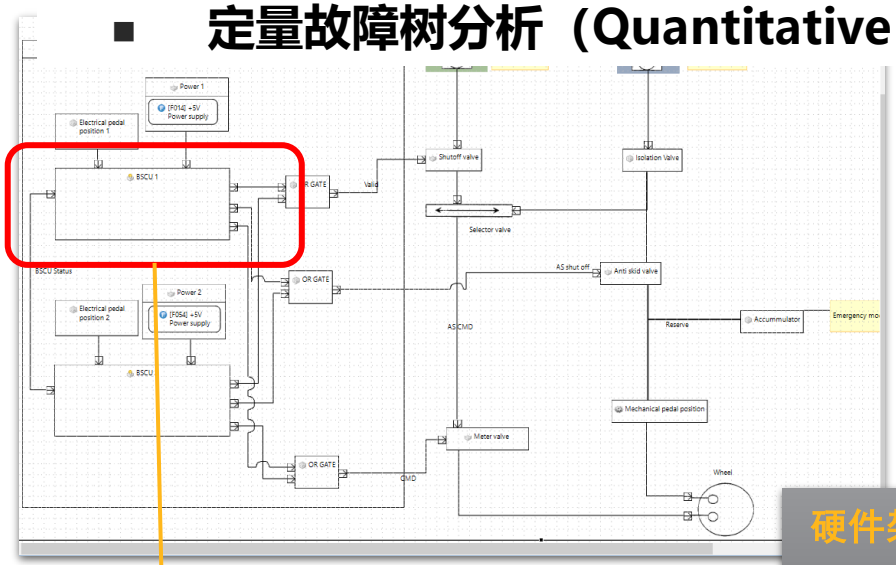
自动计算最小割集，
识别单点故障、多点故障



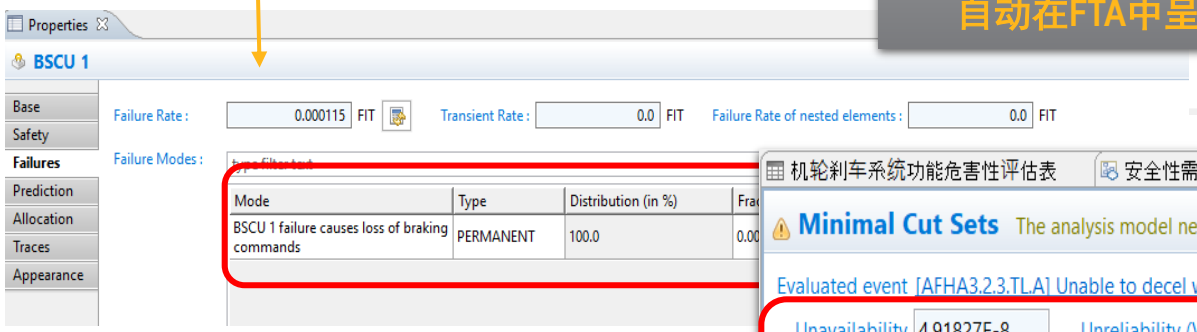
#	Events of Cut Set
1	E-45
2	E-43, E-44
3	E-53, E-58
4	E-54, E-58
5	E-55, E-58
6	E-56, E-58
7	E-57, E-58

medini 用于SSA - FTA

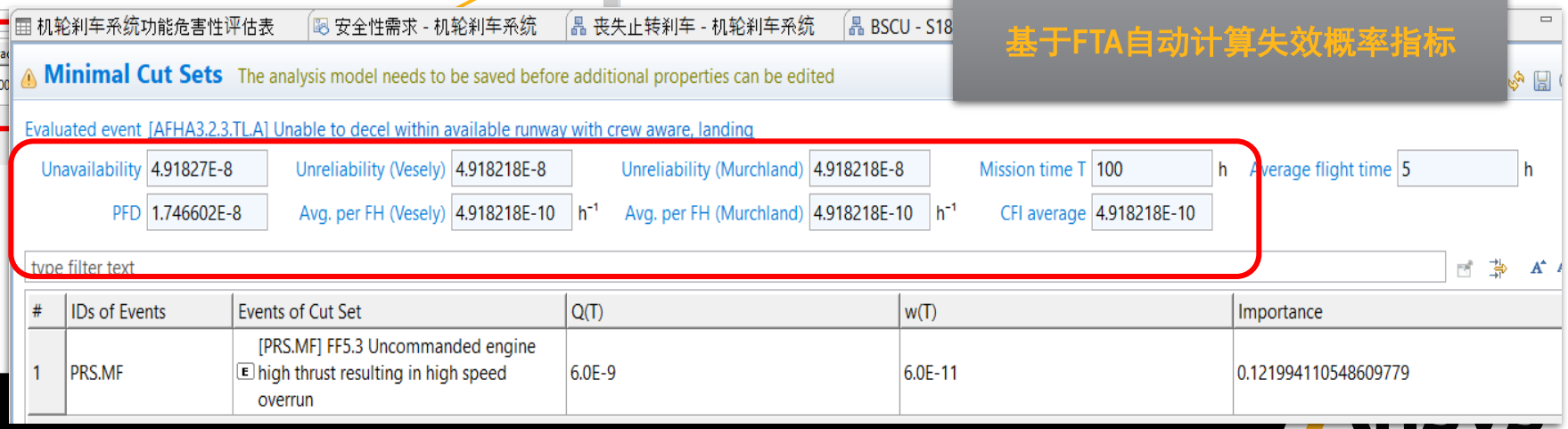
- **定量故障树分析（Quantitative FTA）**



硬件架构(SysML)元素的
失效概率
自动在FTA中呈现



基于FTA自动计算失效概率指标



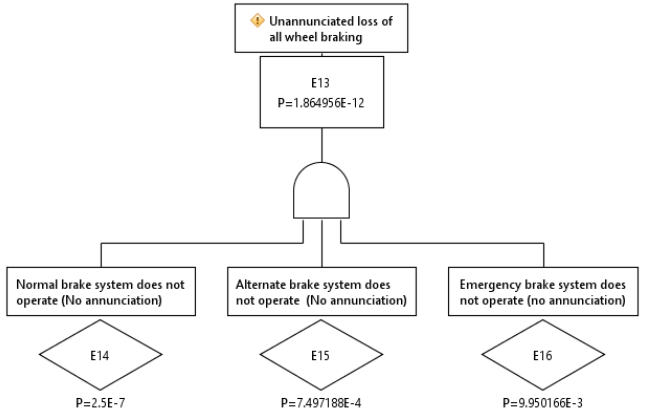
FTA – 考虑飞行阶段

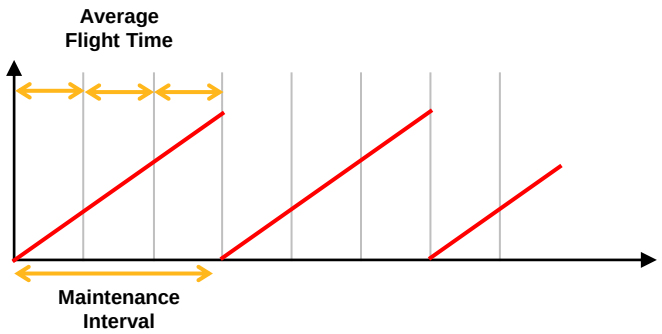
通过定量故障树确定故障概率

- 定量目标通常是“每个飞行小时的平均故障概率（FH）”
- 延迟、维护间隔和事件暴露率，决定了最大的“有风险时间”和整体故障概率
- “平均飞行时间”，将评估划分到每次飞行

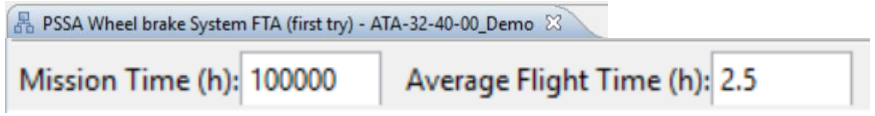
2019 R1推出第一套针对航空航天的特定FTA扩展

- 任务时间和平均飞行时间之间的区别
- 基本事件的“风险时间模型”

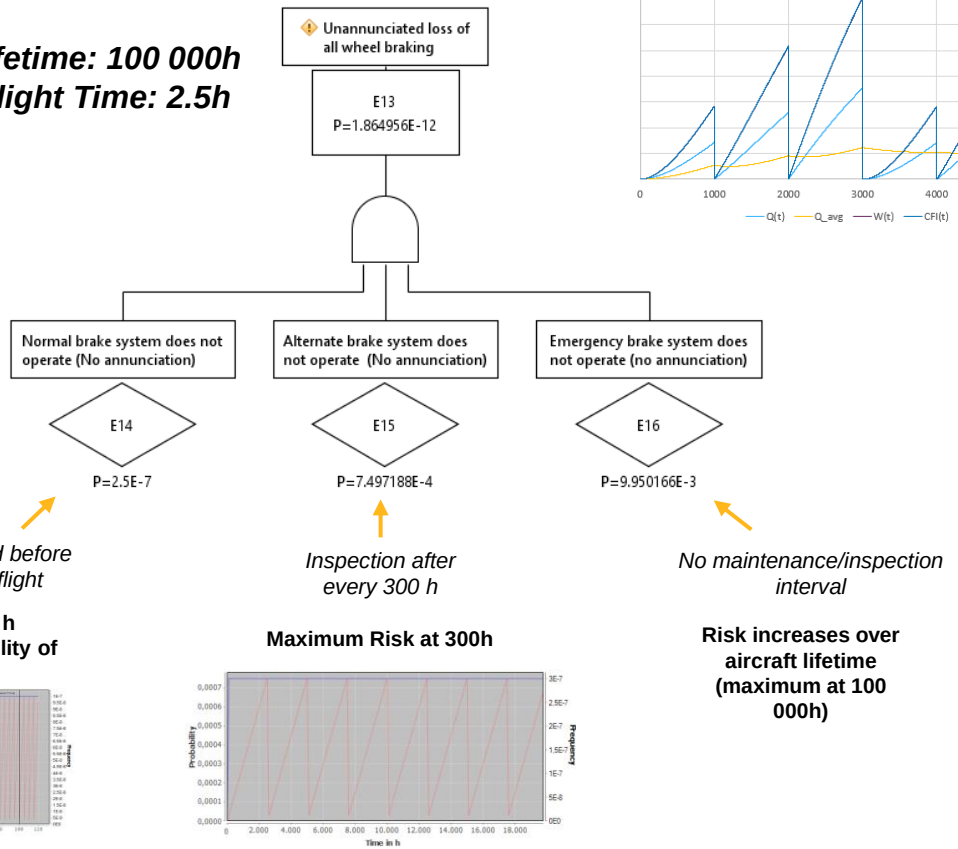




例子： Risk Times

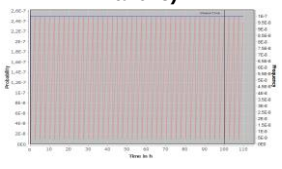


Aircraft Lifetime: 100 000h
Average Flight Time: 2.5h



Inspected before every flight

Risk Time: 2.5 h (Maximum Probability of Failure)



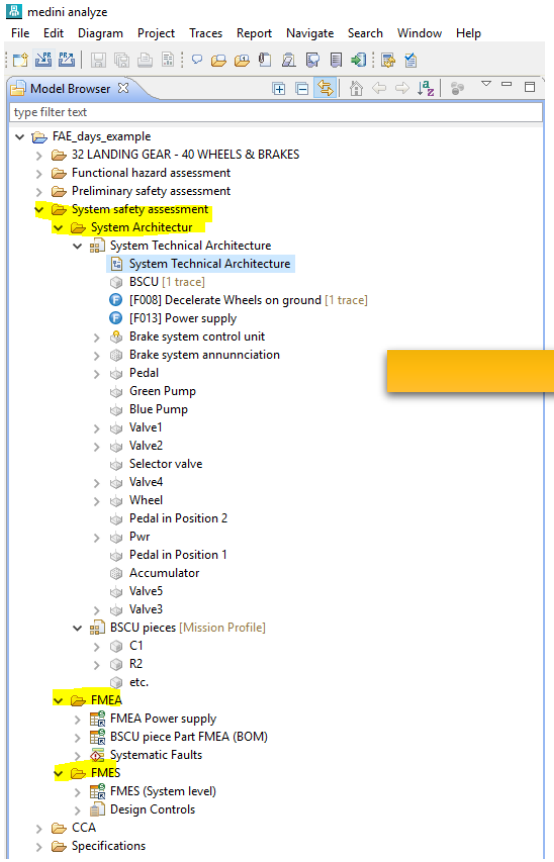
Inspection after every 300 h

Maximum Risk at 300h

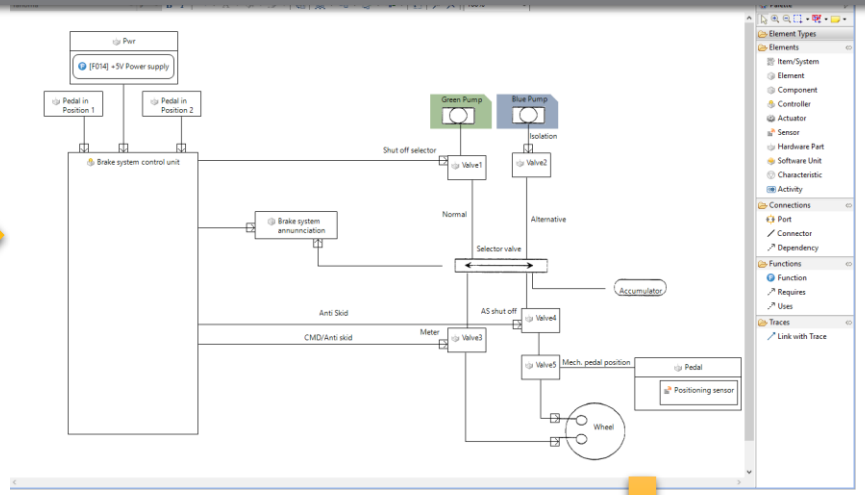
No maintenance/inspection interval

Risk increases over aircraft lifetime (maximum at 100 000h)

medini 用于SSA - FMEA



定义技术架构 - 创建零部件库或从外部数据导入零部件库（例如BOM列表），为您的SysML模型中的组件提供规格（失效率，温度间隔等）。



基于架构自动生成FMEA

System FMEA Worksheet

Review RPN IEC 61508 FMEDA

type filter text

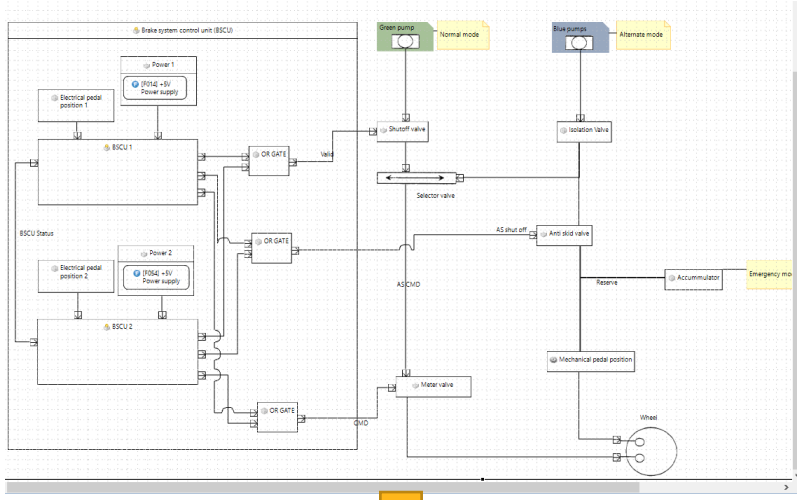
Component	Potential Failures	Potential Failure Effects	Top Level Effect	Severity	Max Severity	Risk Class	Potential Failure Causes	Occurrence	Detection	RPN	S×O	S×D	D×O
Power Supply : 12V	open connection	[[F-003] Evaluate Ignition state] [MF-029] NO Ignition State Information	[QU 2] No theft protection	9	9	S	[[PUMT1] TR8 : TRANSISTOR] Short	3	2	54			
		[[F-004] Evaluate Vehicle state] [MF-033] NO Vehicle State Information	[HZ 1] Steering blocked	8		S	[[PUMT1] TR8 : TRANSISTOR] Open	3	2	54			
		[[F-005] Derive Command] [MF-037] NO Command issued		9		S	[[PUMT1] TR7 : TRANSISTOR] Short	3	2	54			
		[[F-006] Supervise Execution] [MF-044] NO Lock State Information	[MF-027] NO Driver Information	0		S	[[PUMT1] TR7 : TRANSISTOR] Open	0					

FMEA基于SysML体系结构设计中的功能/系统/组件，并且始终与该模型同步。

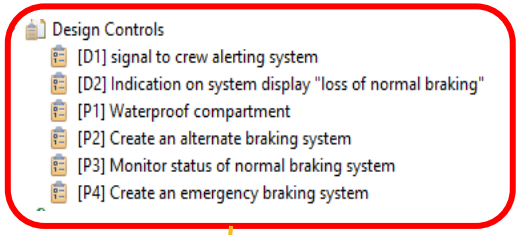
Ansys

medini 用于SSA – FMEA

- **基于系统模型自动派生FMEA**



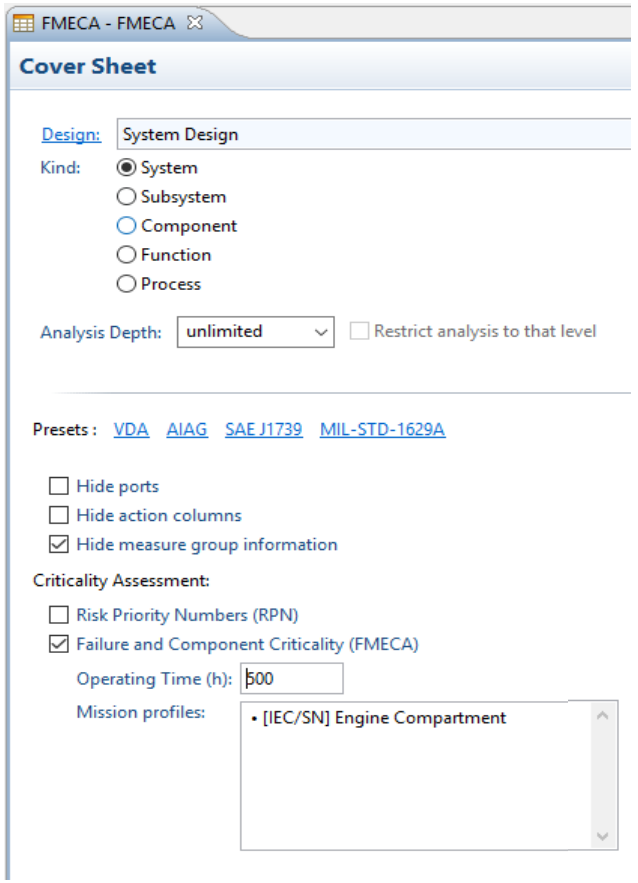
- **双击从预设的安全机制库选择**



- **直接用于FMEA分析**

BSCU 1	BSCU 1 failure causes loss of braking commands	[AFHA_H1.1] Unannunciated loss of deceleration capability	[BSCU1FAILS] [BSCU 1] BSCU 1 failure causes loss of braking commands	[Brake system control unit (BSCU)] BSCU fault causes loss of braking commands	10	10		[[F014] +5V Power supply] [MF010] +5V out of spec.			
								[[F014] +5V Power supply] [MF012] +5V open			
							S	[[F014] +5V Power supply] [MF059] Short to ground or other voltage	0	[P1] Waterproof compartment [P2] Create an alternate braking system [P4] Create an emergency braking system [P3] Monitor status of normal braking system	[D1] signal to crew alerting system [det: 10] [D2] Indication on system display "loss of normal braking" [det: 10]	10

medini 用于SSA - FMECA

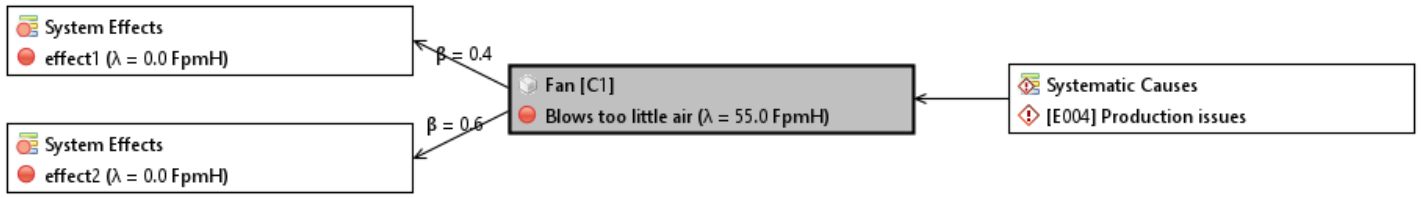


定义目录组件的基本故障率（基于可靠性手册）

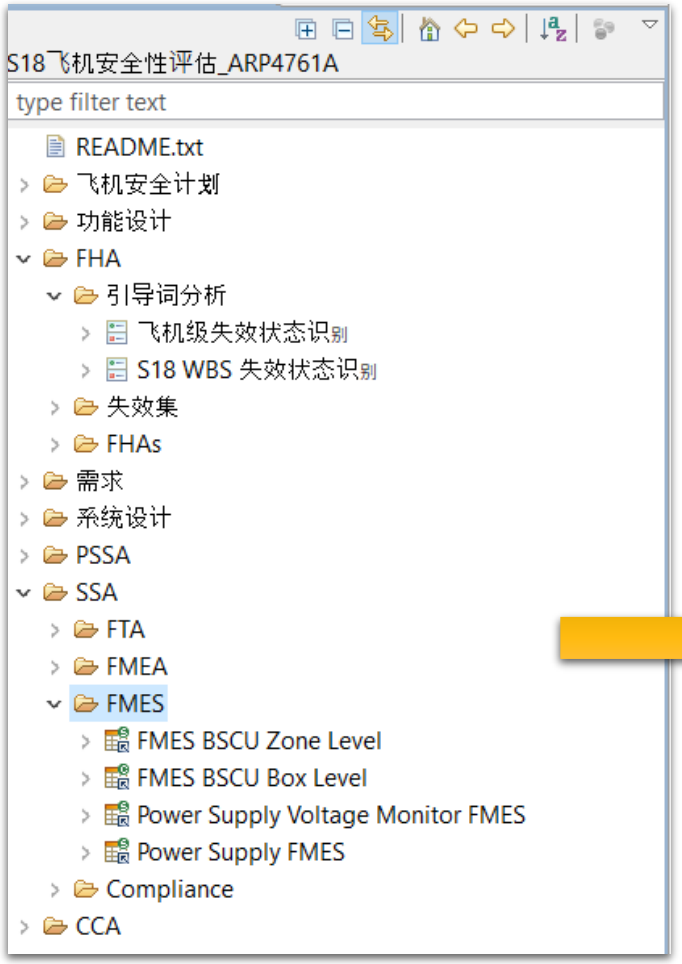
System FMEA Worksheet

type filter text

Component/Function	Failure Rate (in FpmH)	Operating Time (h)	Mission Phases	Component Criticality (in FpmH)	Potential Failures	Failure Rate Distribution (in %)	Failure Rate Fraction (in FpmH)	Potential Failure Effects	Conditional Probability (β)	Failure Mode Criticality (in FpmH)	Severity	Max Severity	Potential Failure Causes
Fan [C1]	100.0	500.0	(all phases)	C_9: 11000.0	Blows too little air	55.0	55.0	[System Effects] effect1	0.4	11000	9	10	[Systematic Causes] [E004] Production issues
								[System Effects] effect2	0.6	16500	10		
				C_10: 16500.0	Blows too much air	5.0	5.0					0	
					Blows no air	40.0	40.0					0	
Generator [C2]	12.058	500.0	Taxi	C_10: 6029.0	No output	29.0	3.496	[System Effects] effect3	1.0	1748	10	10	[Systematic Causes] [E004] Production issues
					Degraded	71.0	8.561	[System Effects] effect3	1.0	4280	10	10	[Systematic Causes] [E003] EMI



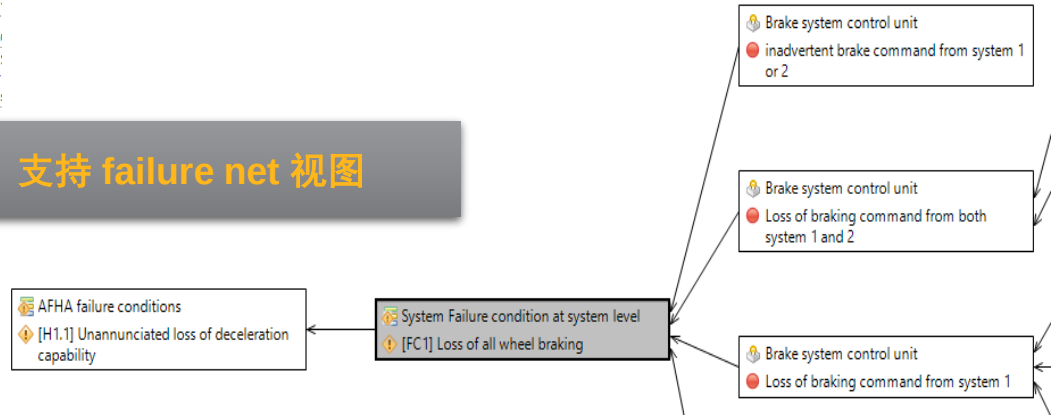
medini用于SSA - FMEA/FMES



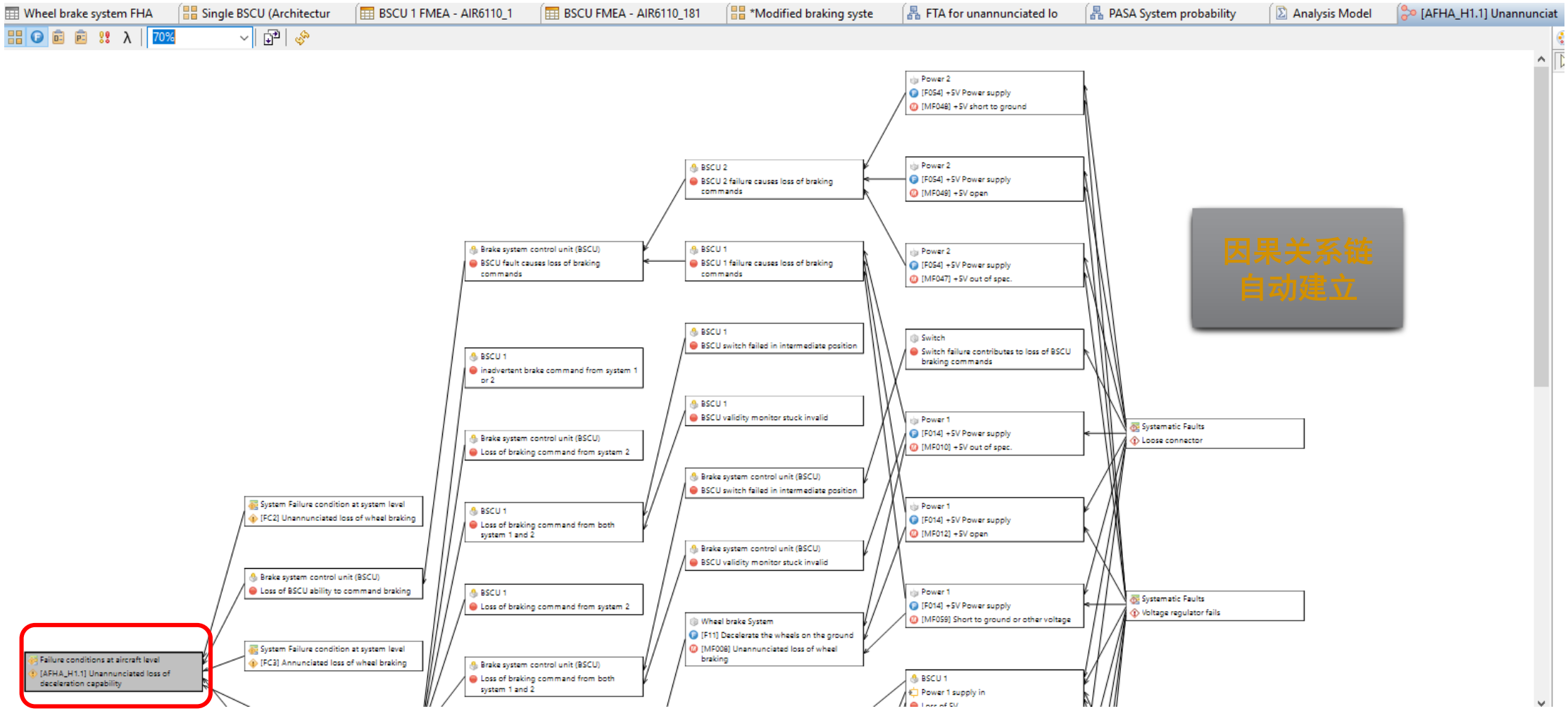
来自FMEA的相同失效影响在FMES中被归类为一种模式；
FMES总结了所有与FMEA具有相同效果的较低级失效模式。

FMES和FMEA表格视图可完全自定义、支持从第三方导入。

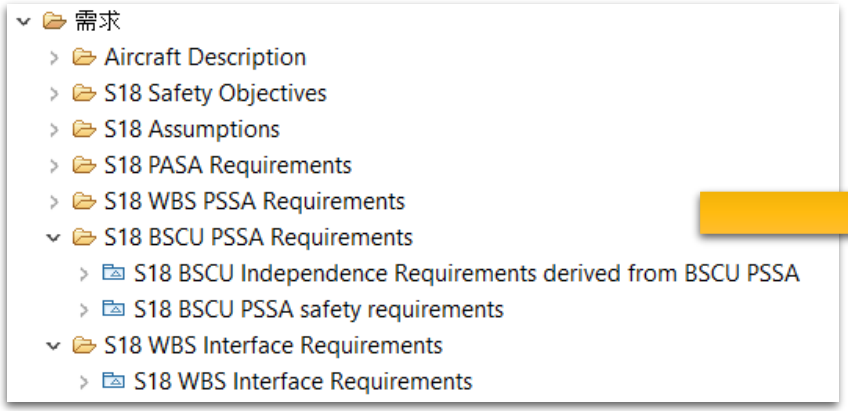
支持 failure net 视图



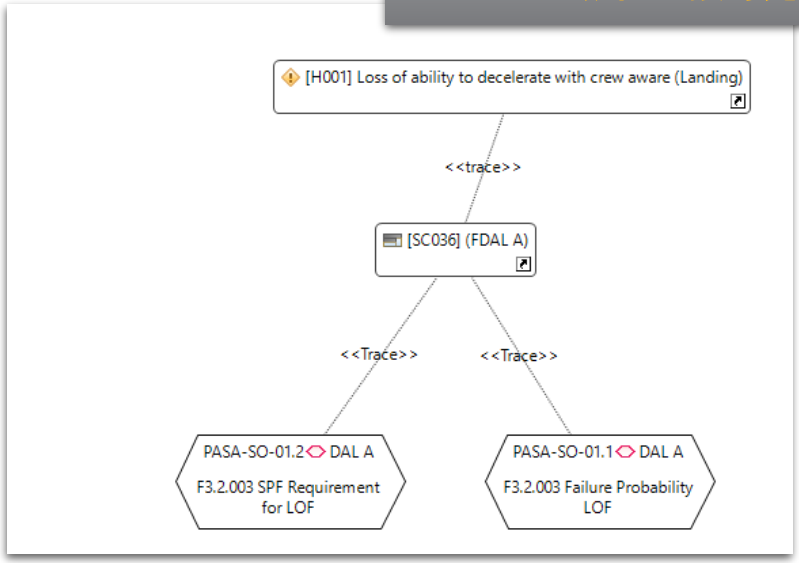
medini 用于SSA – FMES/Cause-effect net

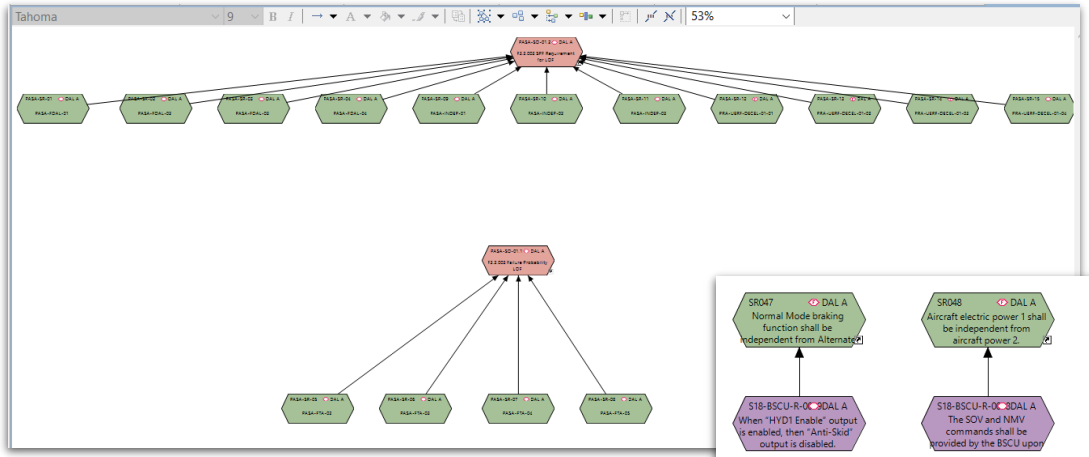


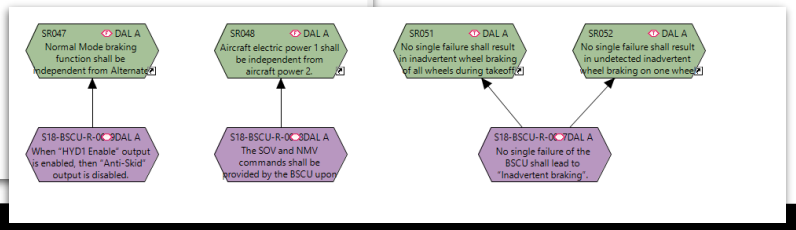
medini 用于SSA – 安全需求管理



追溯性直接可见，例如 追溯至失效状态

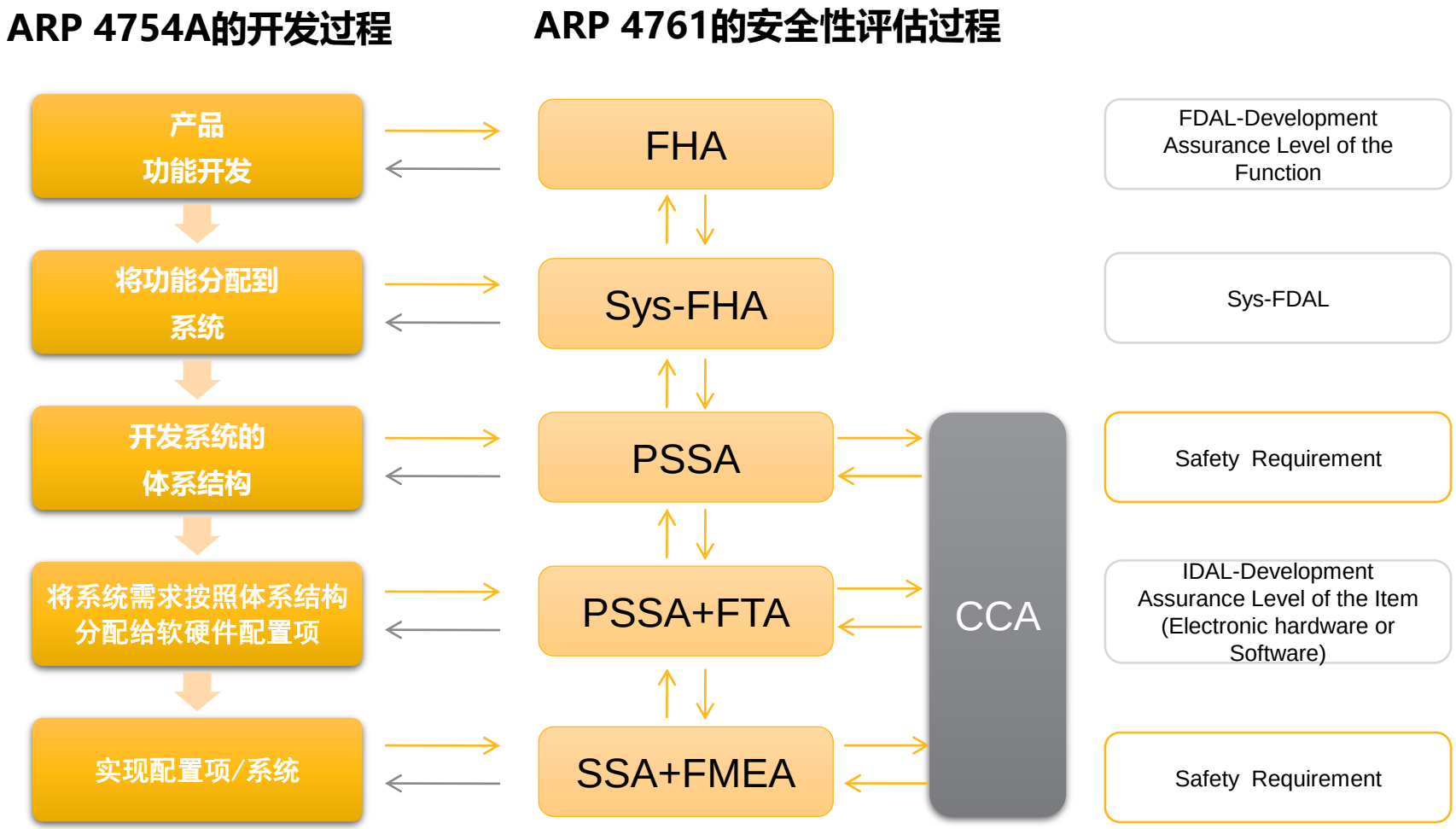






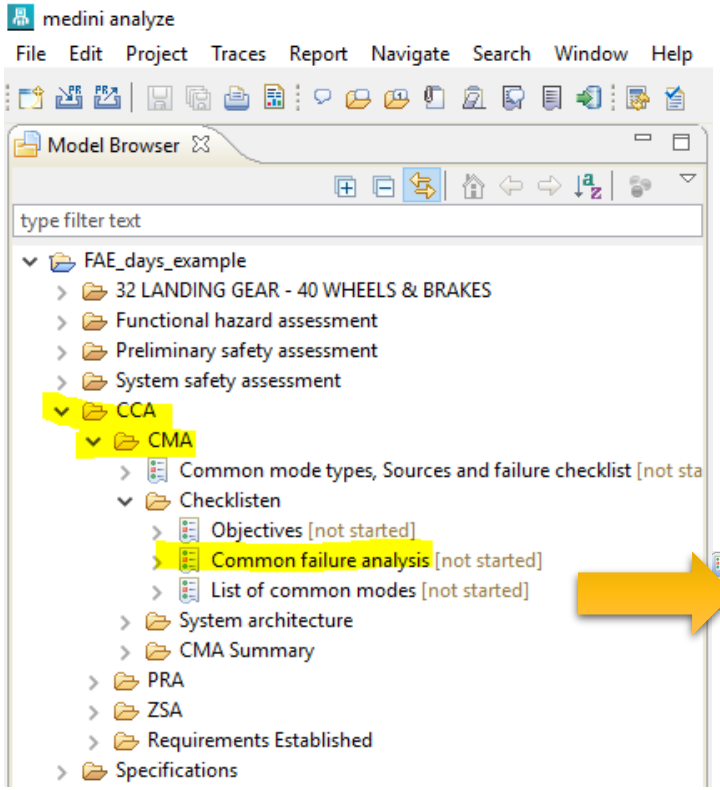
图形化需求编辑显示了所有分析方法产生的各个层次的安全需求之间的关系。

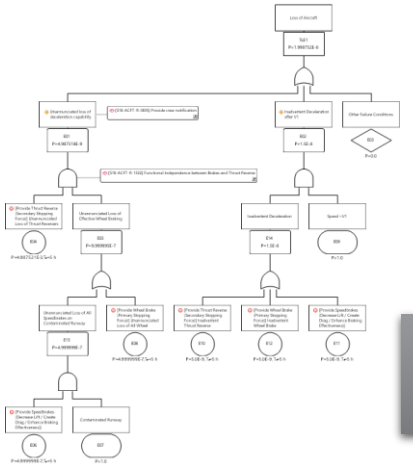
安全生命周期 – 共因分析 Common Cause Analysis



medini 用于共因分析 CCA

共因分析： 确保功能、系统、组件间的独立性，以及独立性相关的风险是可接受的。

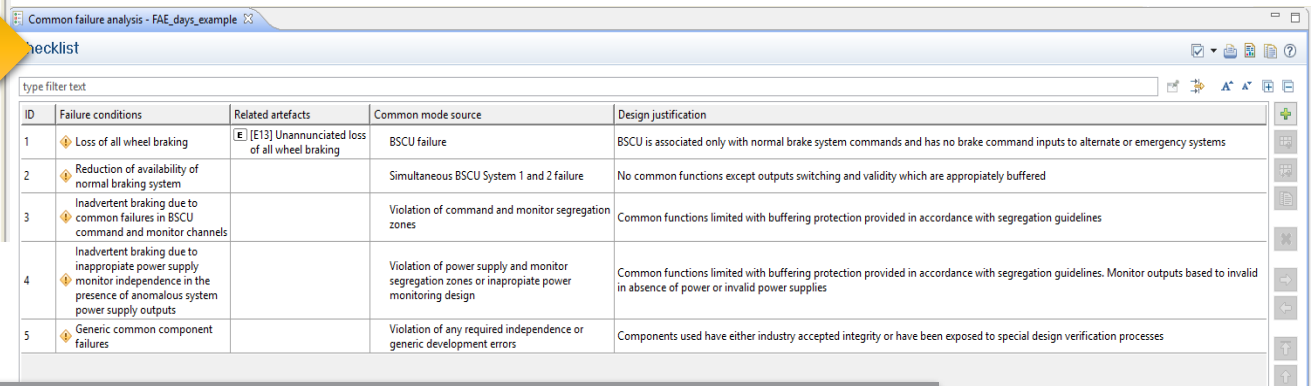




type filter text

#	Events of Cut Set
1	E-45
2	E-43, E-44
3	E-53, E-58
4	E-54, E-58
5	E-55, E-58
6	E-56, E-58
7	E-57, E-58

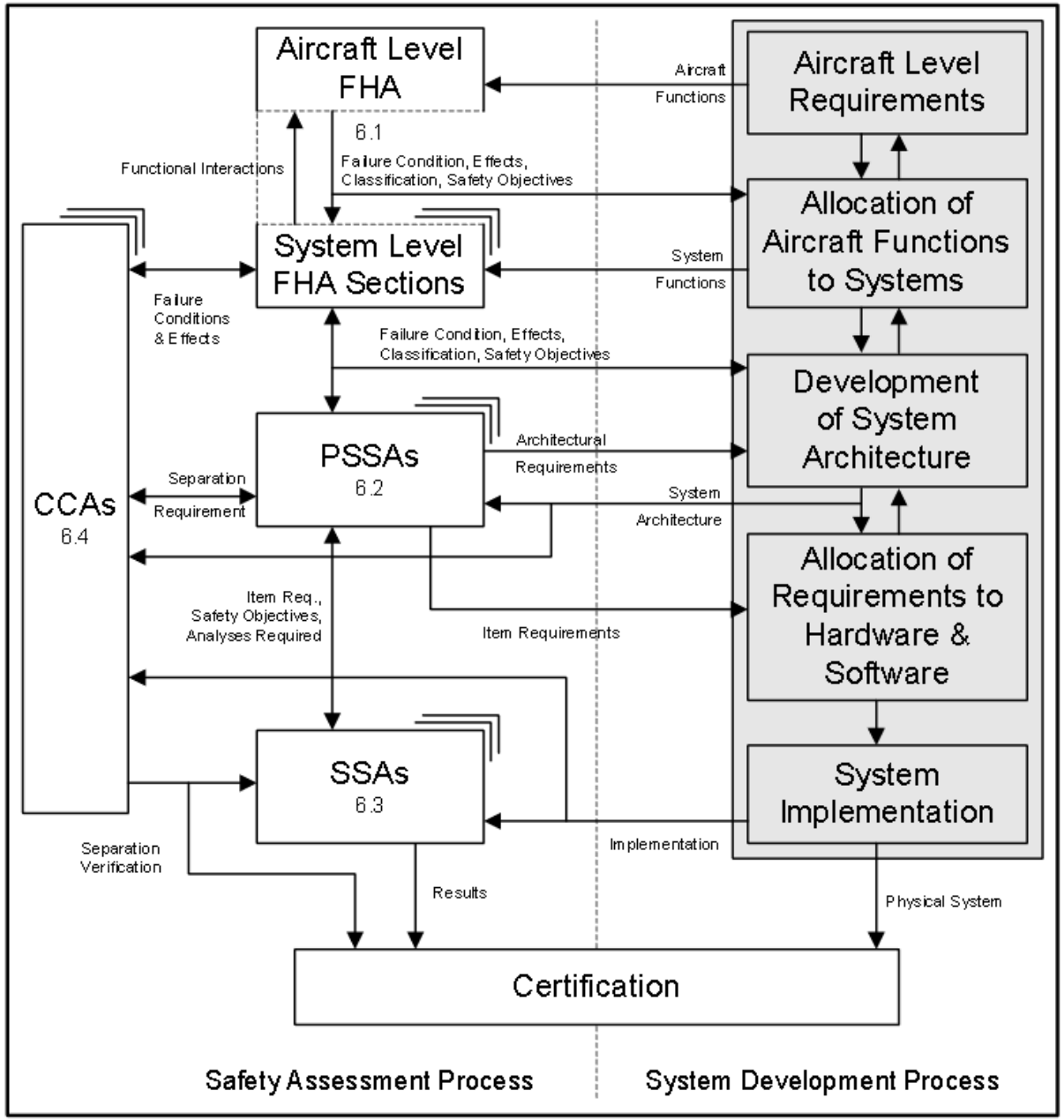
FTA分析（例如，通过最小割集）有助于识别常见模式。



ID	Failure conditions	Related artefacts	Common mode source	Design justification
1	Loss of all wheel braking	[E13] Unannunciated loss of all wheel braking	BSCU failure	BSCU is associated only with normal brake system commands and has no brake command inputs to alternate or emergency systems
2	Reduction of availability of normal braking system		Simultaneous BSCU System 1 and 2 failure	No common functions except outputs switching and validity which are appropiately buffered
3	Inadvertent braking due to common failures in BSCU command and monitor channels		Violation of command and monitor segregation zones	Common functions limited with buffering protection provided in accordance with segregation guidelines
4	Inadvertent braking due to inappropiate power supply monitor independence in the presence of anomalous system power supply outputs		Violation of power supply and monitor segregation zones or inapropiate power monitoring design	Common functions limited with buffering protection provided in accordance with segregation guidelines. Monitor outputs based to invalid in absence of power or invalid power supplies
5	Generic common component failures		Violation of any required independence or generic development errors	Components used have either industry accepted integrity or have been exposed to special design verification processes

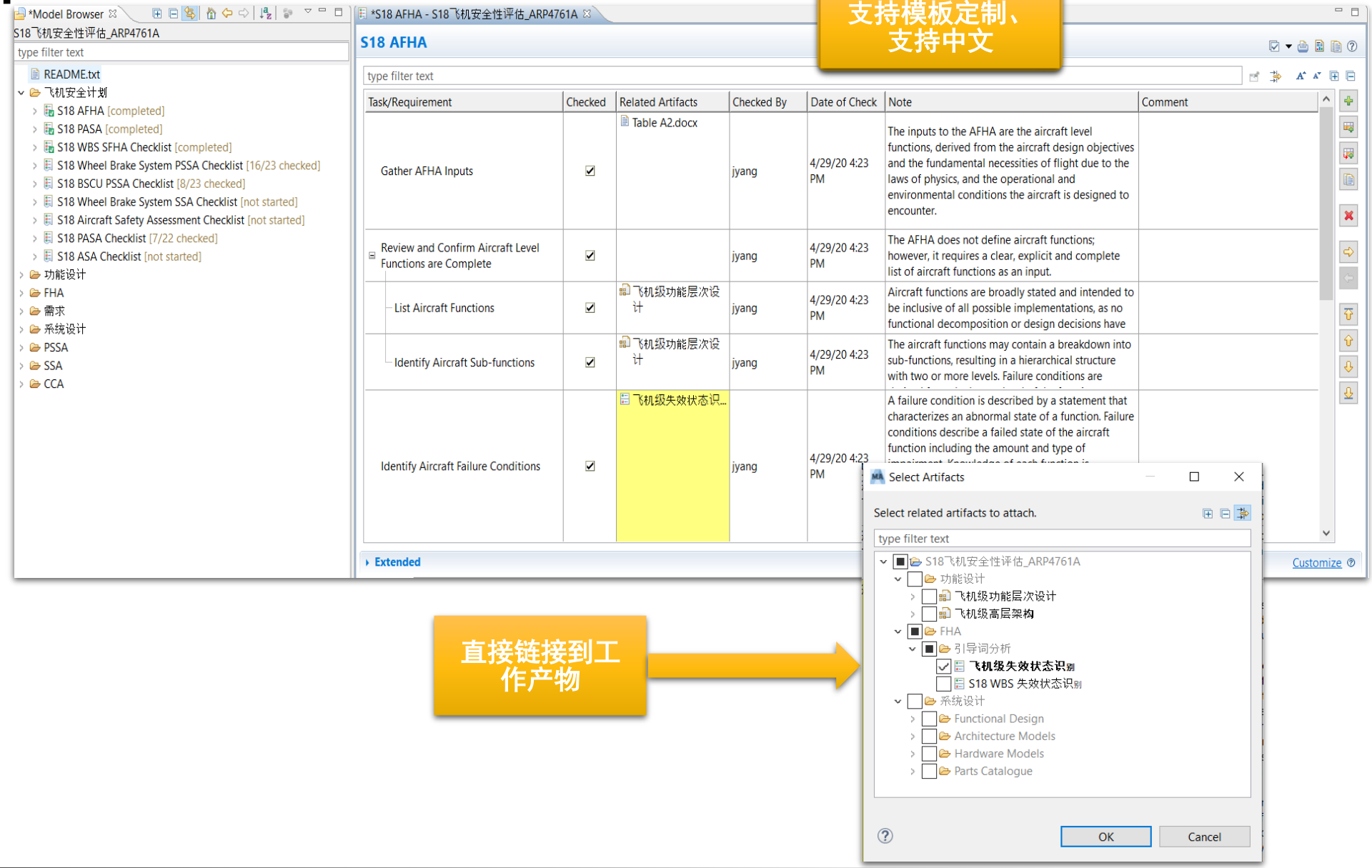
通过可定制检查单，工具可以显示潜在的共同模式列表以及确定的设计解决方案/措施以确保独立性。

安全生命周期 – 项目管理：一致性、可跟踪性和高效率



安全项目管理：

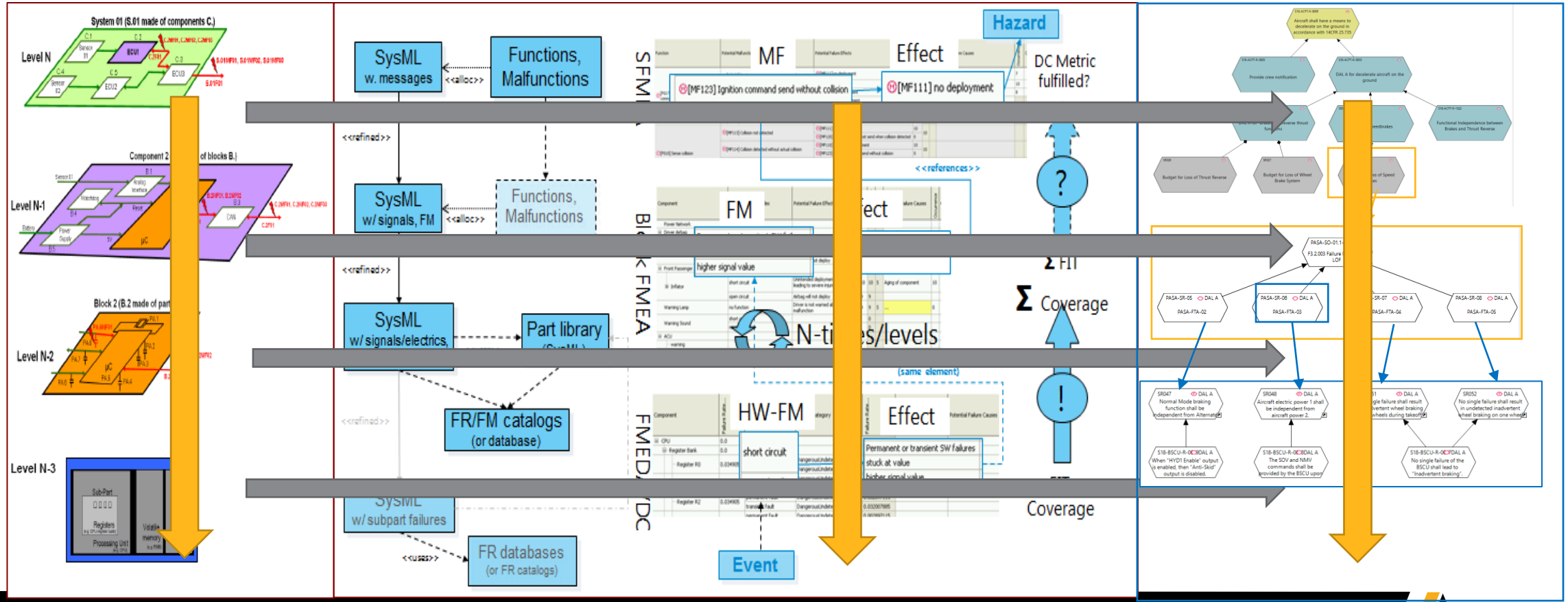
- 安全计划、任务检查表（Checklist）可用于验证和确认活动、安全计划和进度跟踪。
- 具有层次结构检查项
- 检查单可自定义属性
- 直接链接到建模元素
- 提供大量预定义模板



安全项目管理：成熟的跟踪功能，保证全流程的一致性

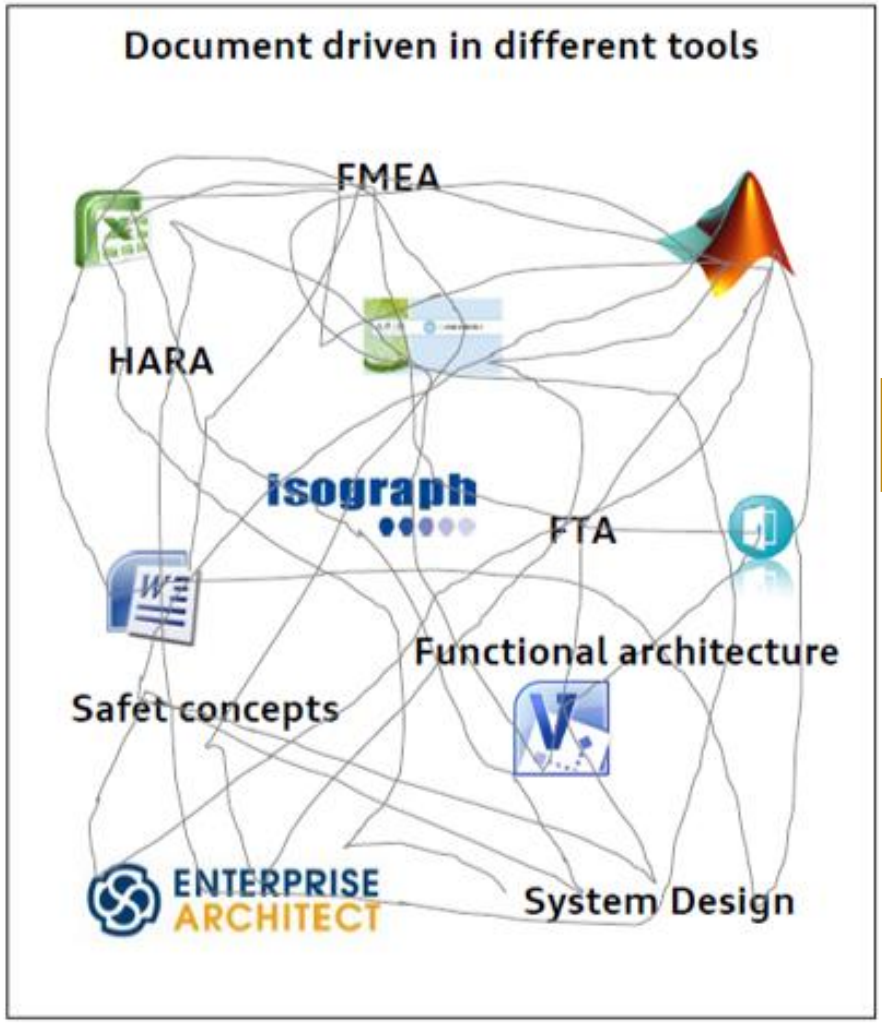
任何信息元素之间可以定义追踪关系

- ✓ 安全评估、安全需求和架构之间的跟踪和同步（Allocation of SRs）
- ✓ 架构（系统/子系统/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，因果效应的跟踪（一致性） （Failure Net）

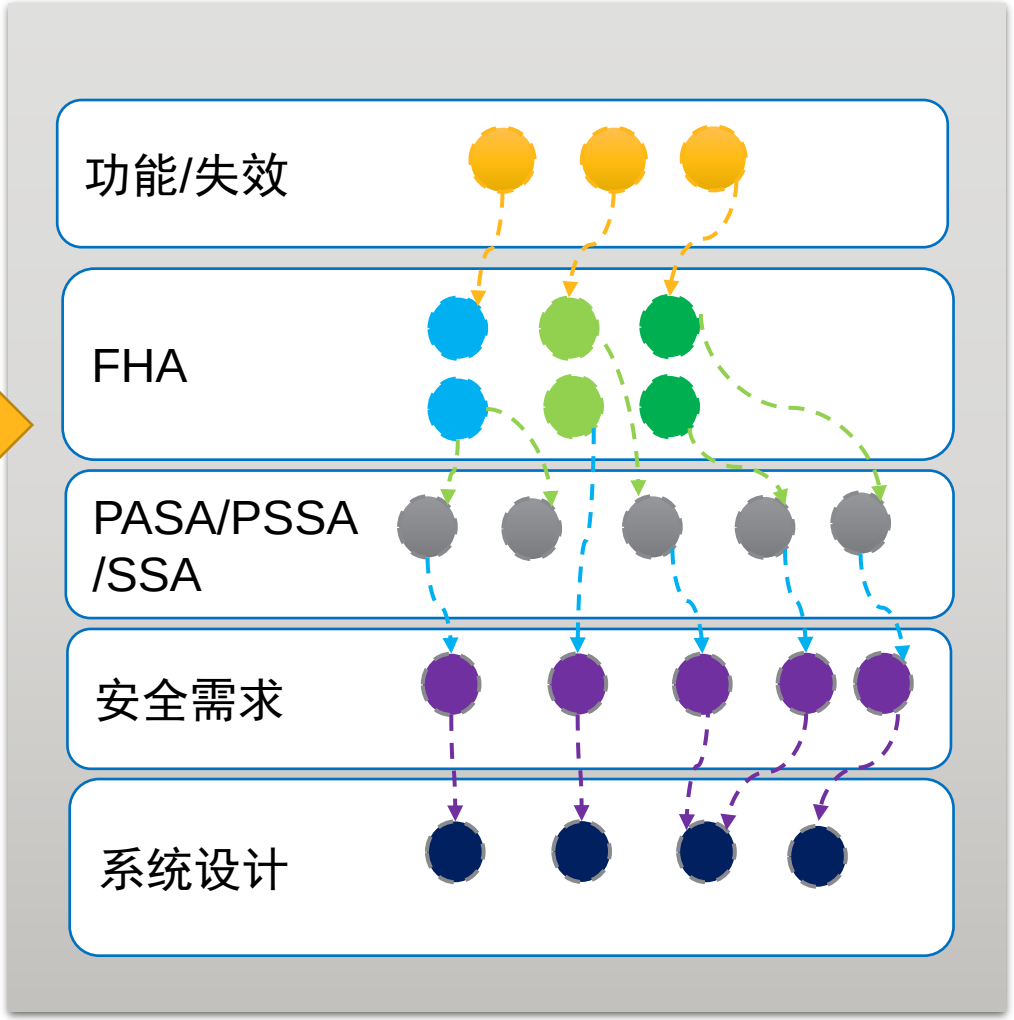


小结

基于模型的安全评估： 追踪性、一致性、高效率



集成的工具平台



medini 技术优势

完整 遵循ARP4761安全标准，支持全生命周期安全评估

- 提供完整的安全评估综合解决方案：支持FHA，PASA/PSSA，ASA/SSA，CCA，FTA，FMEA等评估阶段与方法
- 支持ARP4761/4761A全流程，并与ARP4754A飞机系统开发过程、需求管理过程相互交互

高效 丰富的模板，支持重用和自动化

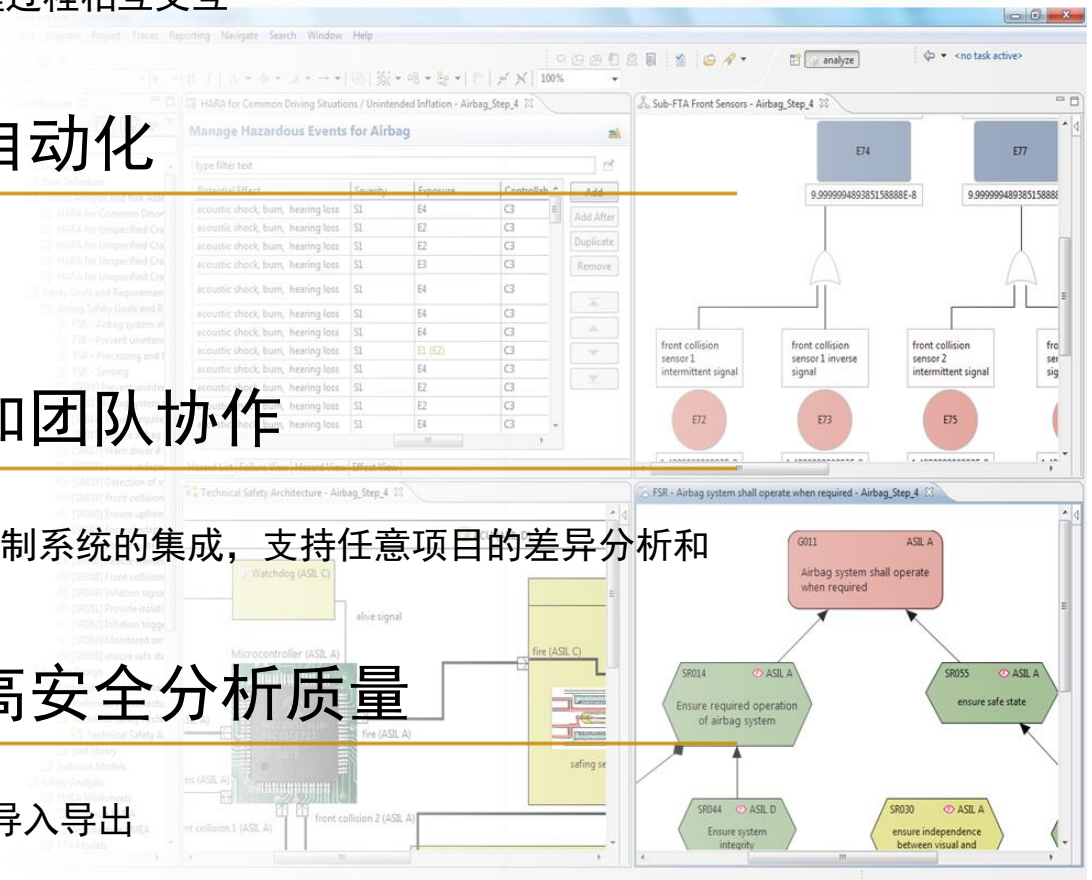
- 丰富的模板库；丰富的数据库；
- 自动生成分析表格、自动故障树评估、故障率计算

管理 支持项目管理、安全计划和团队协作

- 安全计划模板，便于整个安全项目的管理、评审
- 支持任务管理、可追溯性管理和审查/评估、支持团队开发、供应链、版本控制系统的集成，支持任意项目的差异分析和模型合并

一致 确保追踪性、一致性，提高安全分析质量

- 基于SysML架构模型，提供完整的证据链，确保追踪性、一致性
- 支持与其他工具的桥接，支持FMEA、FTA、架构模型、需求、BOM表等的导入导出



Q&A
欢迎您的提问