

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





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

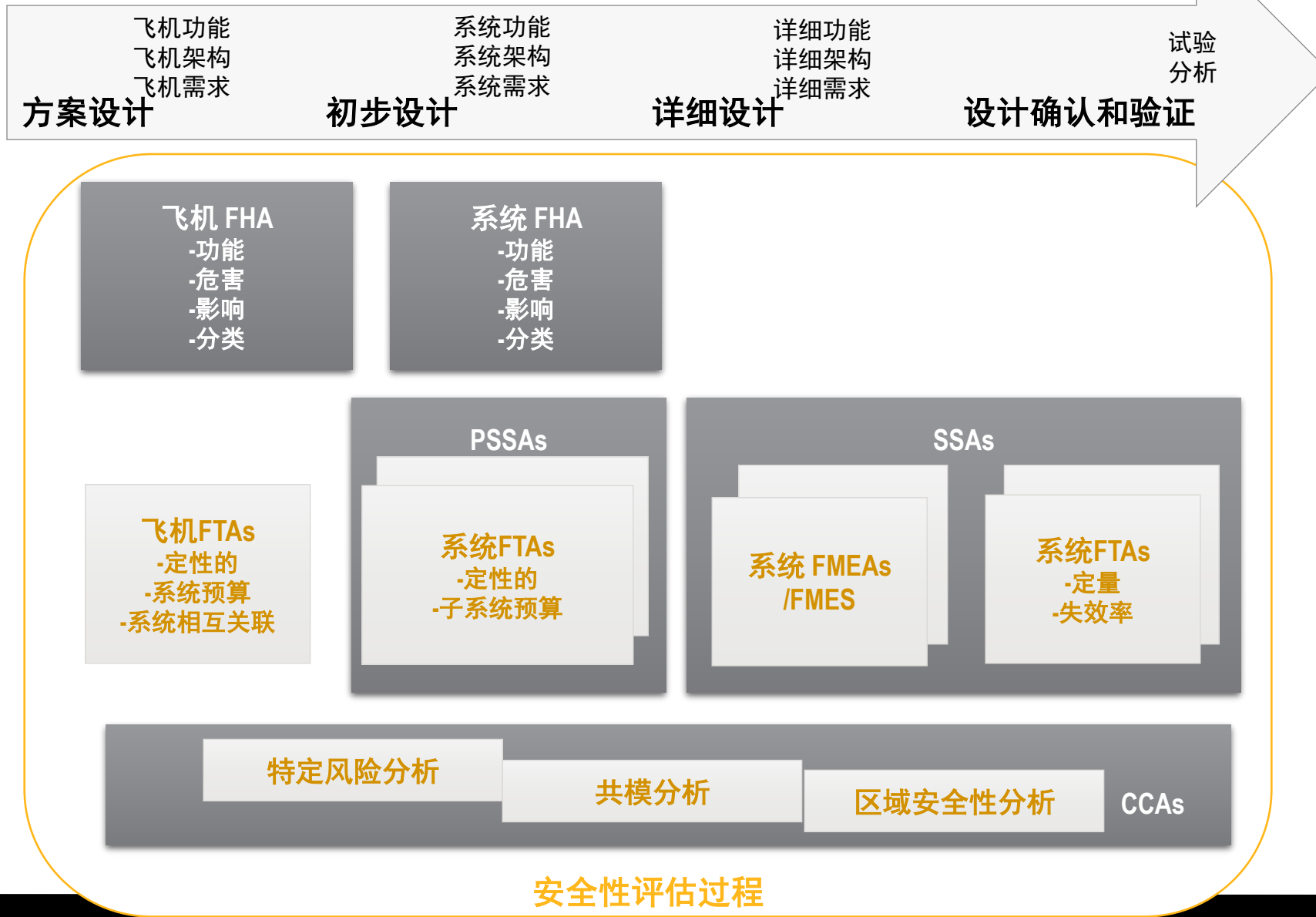
EASA 欧洲航空安全管理局

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

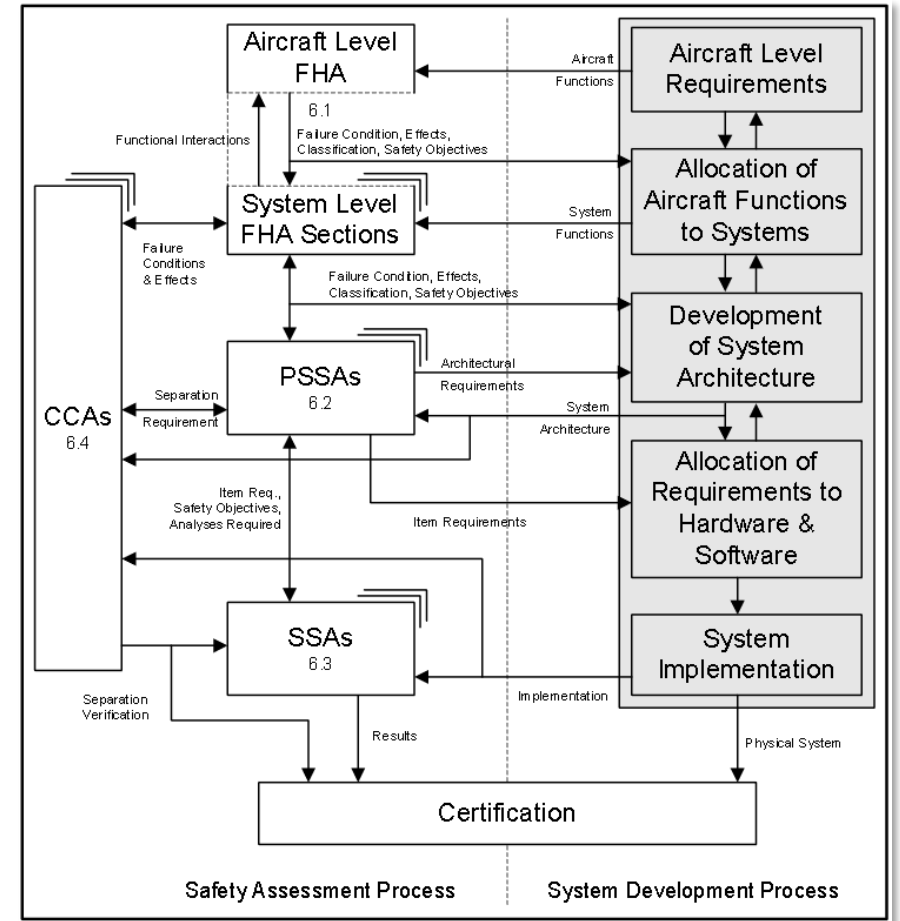
方案设计、架构

- 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

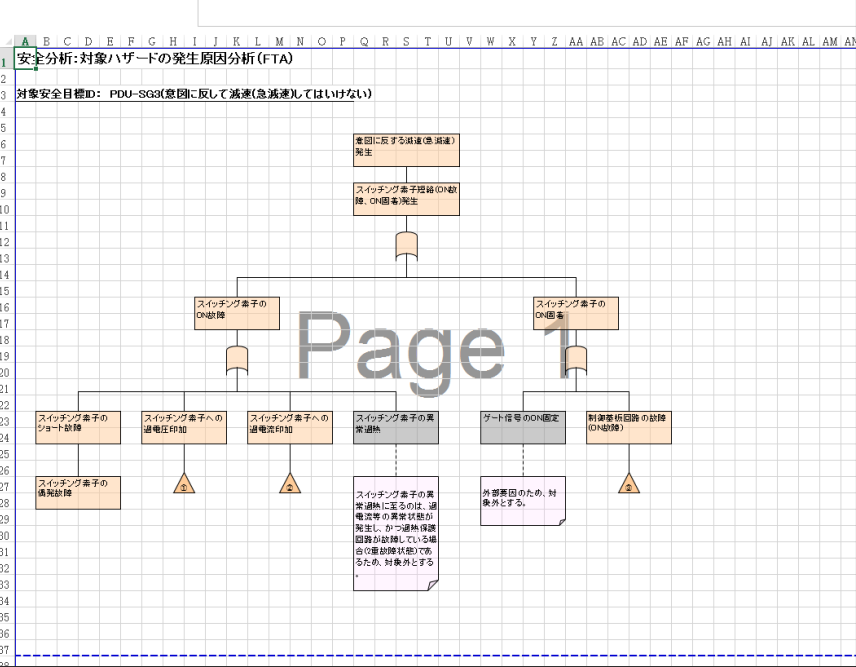
...目前大多采用的手段是excel 及单任务工具 ...



... 实际工程中是怎样做的?

Item No.	Location	Road Condition	Vehicle Condition	Environment	Driver Condition	Vehicle State	Vehicle Function	Vehicle Parameter	Vehicle Component	Vehicle Material	Vehicle Structure	Vehicle Detail	Vehicle Assembly	Vehicle Test	Vehicle Result
0001	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass	
0002	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0003	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0004	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0005	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		

Page 1

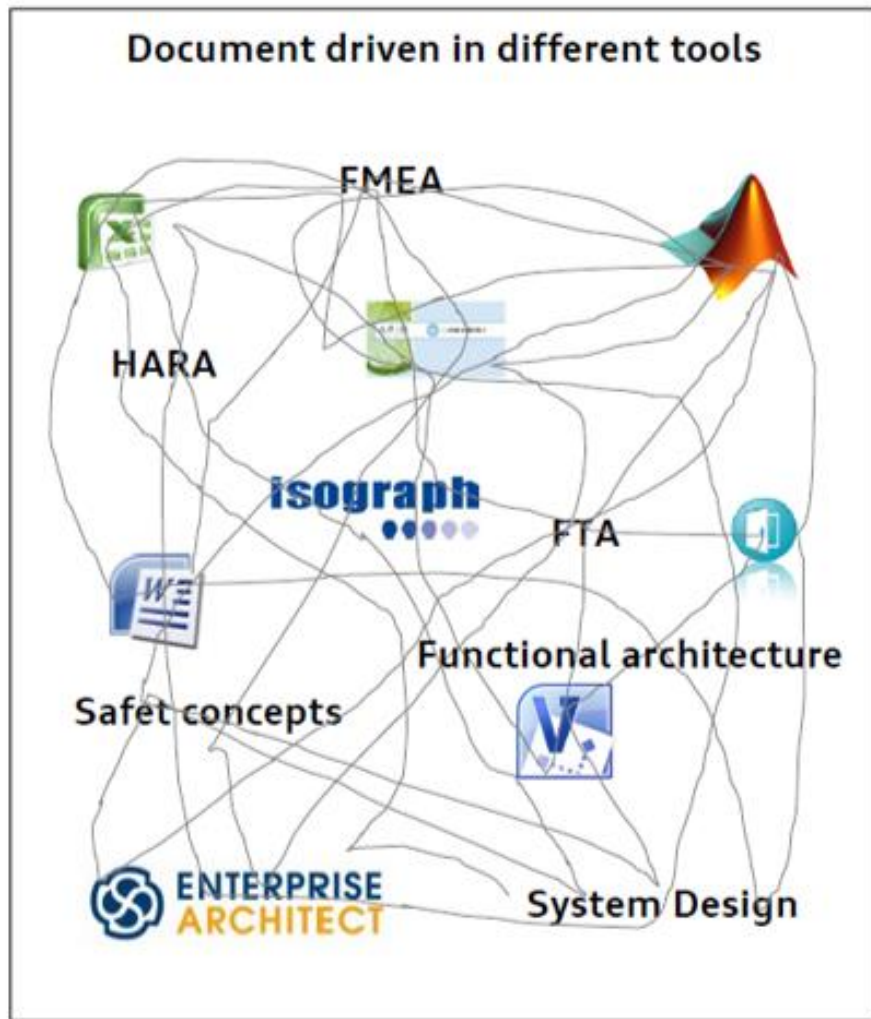


Page

Item No.	Location	Road Condition	Vehicle Condition	Environment	Driver Condition	Vehicle State	Vehicle Function	Vehicle Parameter	Vehicle Component	Vehicle Material	Vehicle Structure	Vehicle Detail	Vehicle Assembly	Vehicle Test	Vehicle Result
0001	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass	
0002	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0003	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0004	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0005	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0006	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0007	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0008	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0009	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0010	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0011	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0012	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0013	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0014	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0015	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0016	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0017	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0018	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0019	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0020	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0021	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0022	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0023	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0024	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0025	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0026	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0027	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0028	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0029	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0030	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0031	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0032	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0033	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0034	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0035	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0036	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		
0037	Front	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Pass		



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

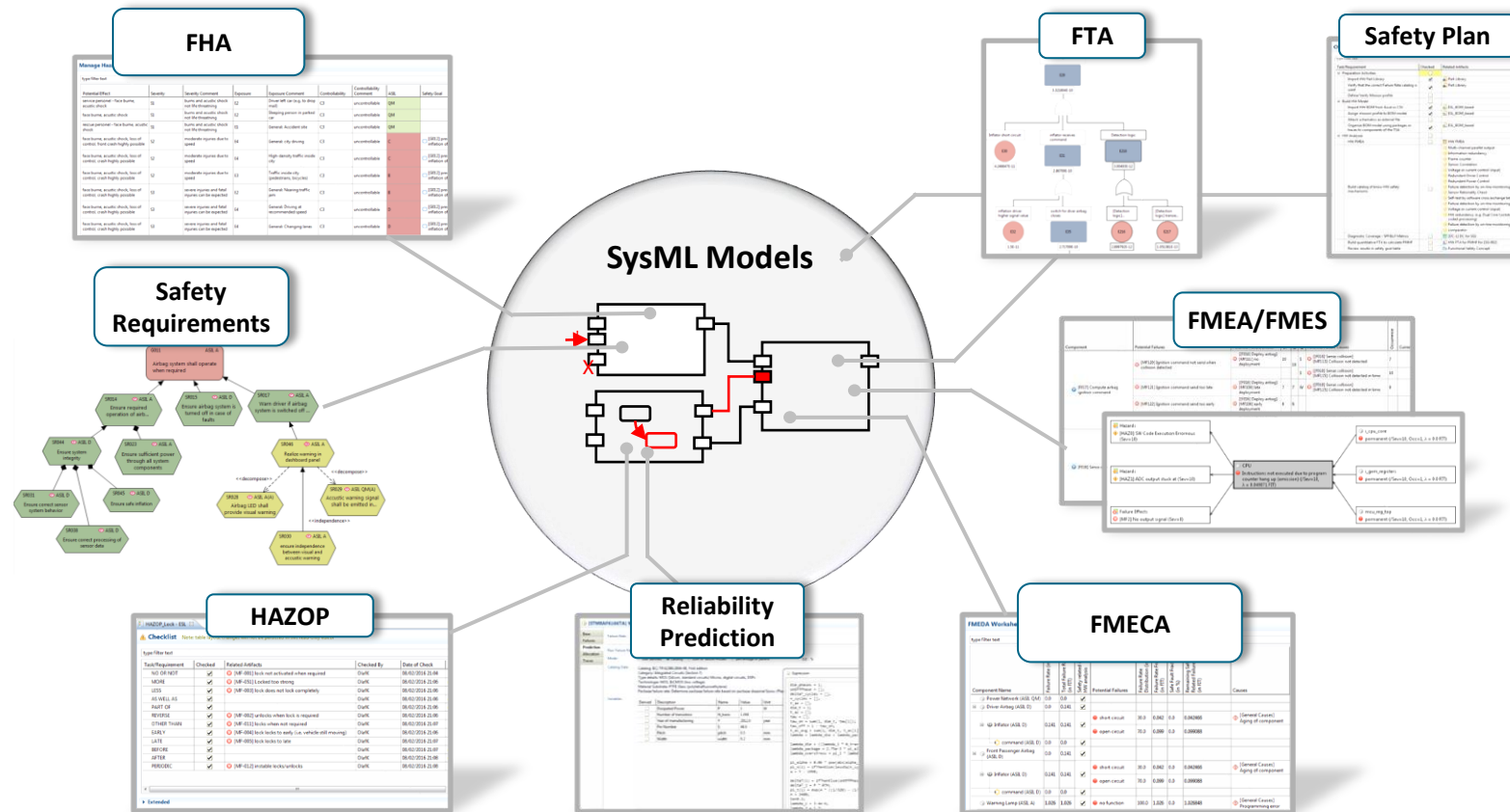
- 安全性分析与可靠性工程的综合解决方案
- 基于模型的方法，覆盖全生命周期，高效连接安全要求、安全评估、架构设计，确保追踪性和一致性
- 符合功能安全标准的最佳实践：ARP4761/ARP4754A, IEC 61508, EN50126/50128/50129, ISO 26262
- 内置大量高效的工程模板、检查单和手册，SN 29500, IEC 62380, MIL HDBK 217F/217+, GJB299C, FIDES Guide 2009 支持复用和自动化，大大减少成本和上市时间
- 适用于航空航天、汽车、轨道交通、核能等安全应用领域

全球250+ 客户



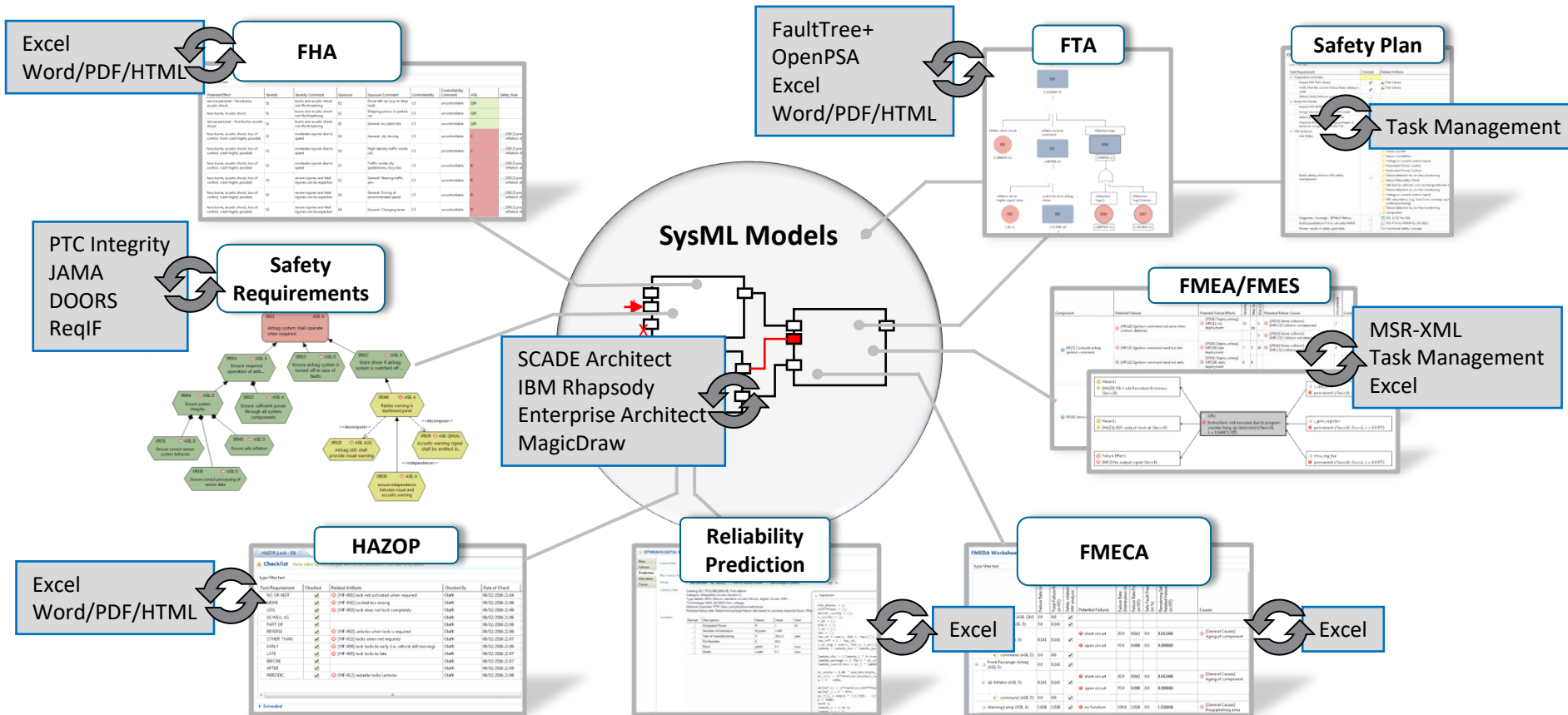
medini: 基于模型的安全分析

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



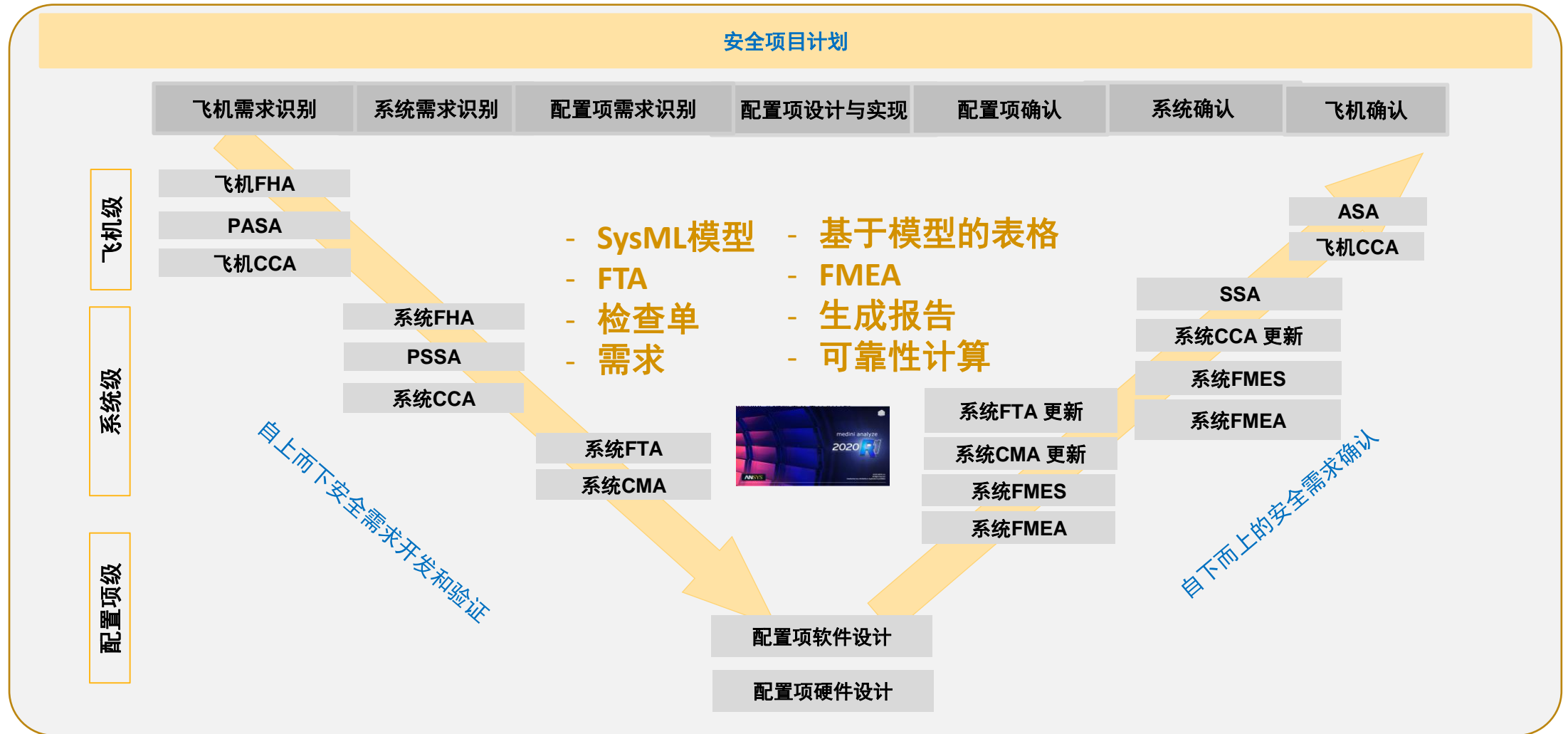
基于模型的方法确保一致性、可跟踪性和高效率

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



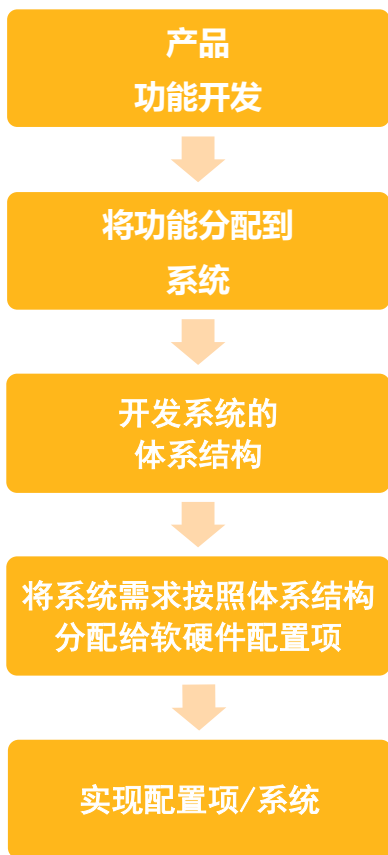
议程

- 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

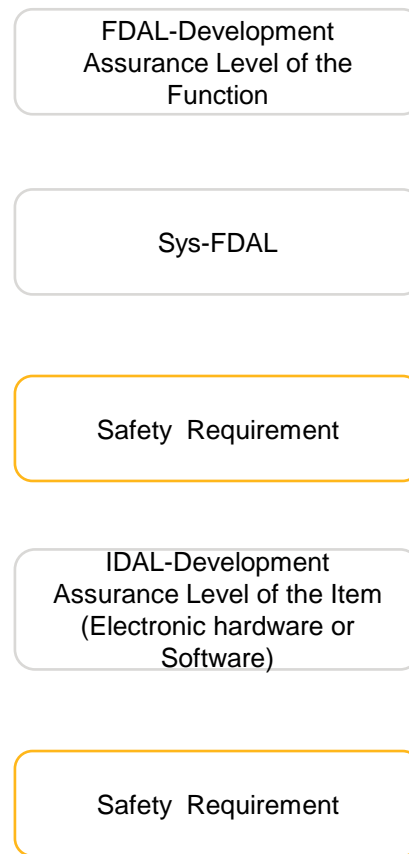
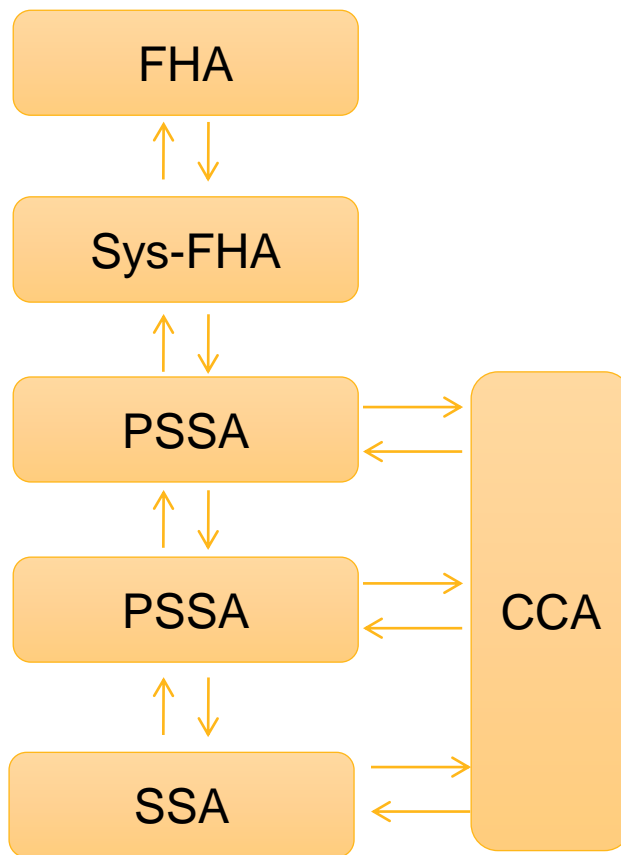


安全生命周期 :

ARP 4754A的开发过程

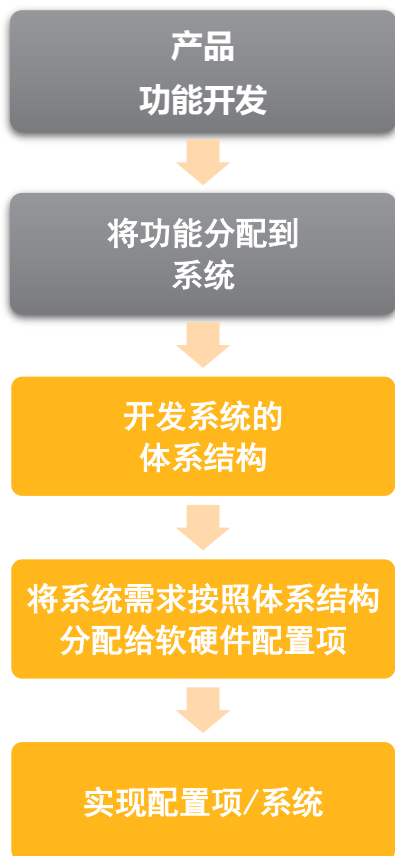


ARP 4761的安全性评估过程

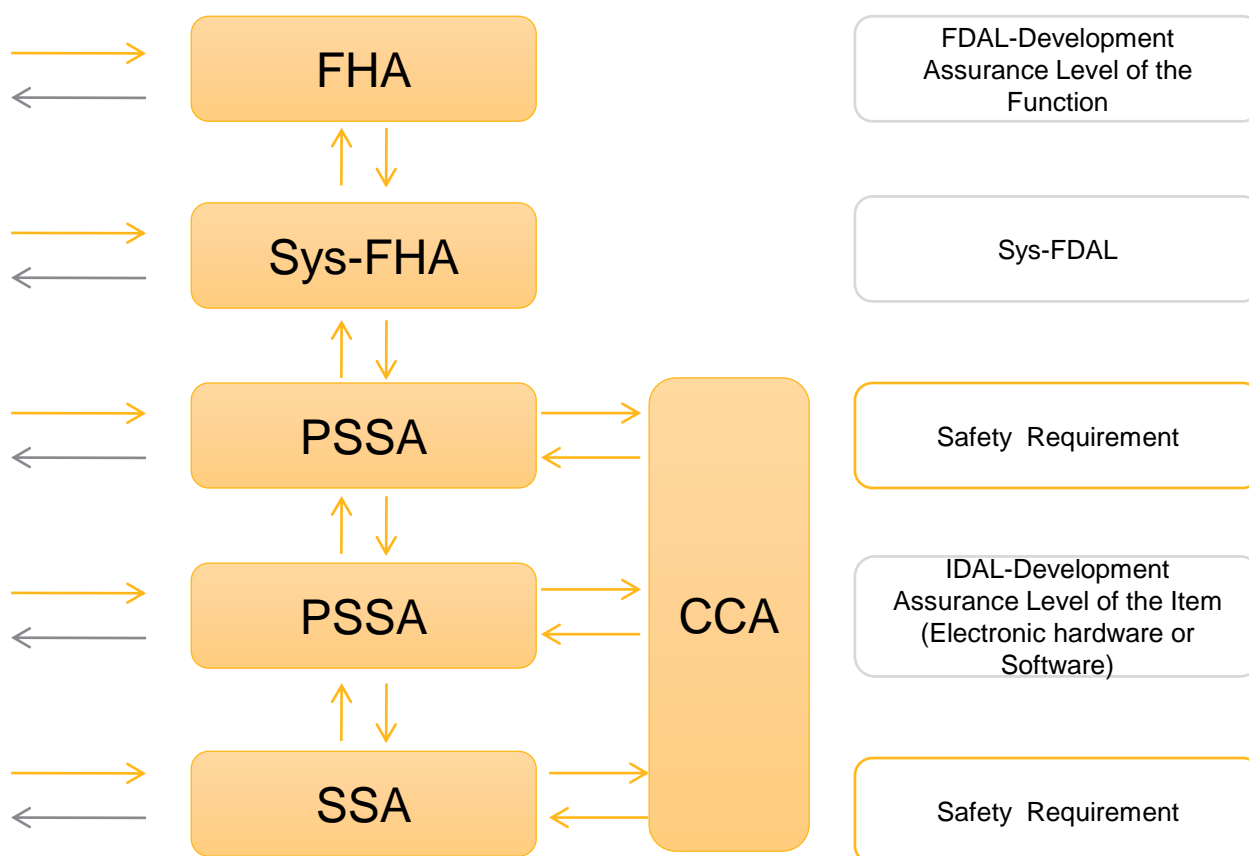


安全生命周期 - 方案设计阶段:

ARP 4754A的开发过程

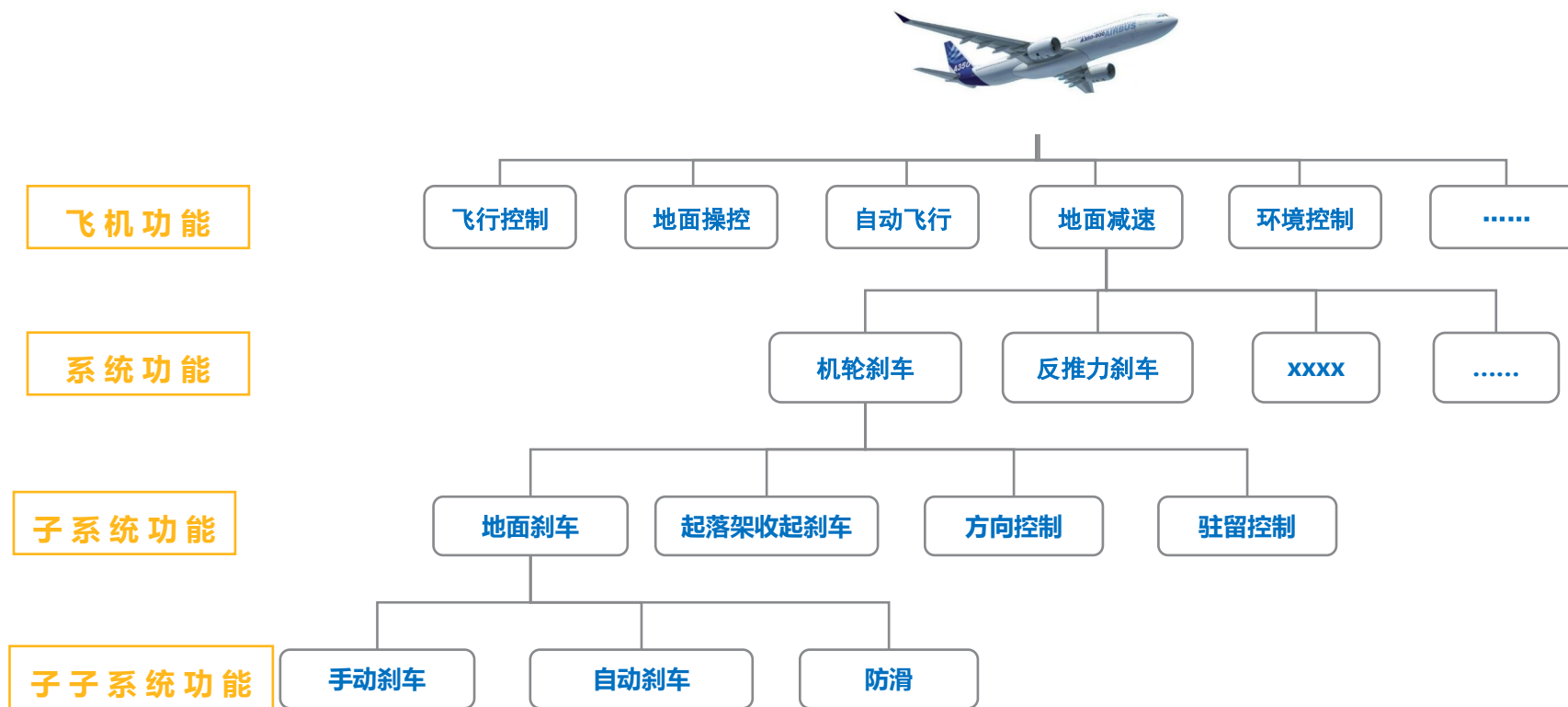


ARP 4761的安全性评估过程



安全生命周期 - 方案设计阶段:

功能视图



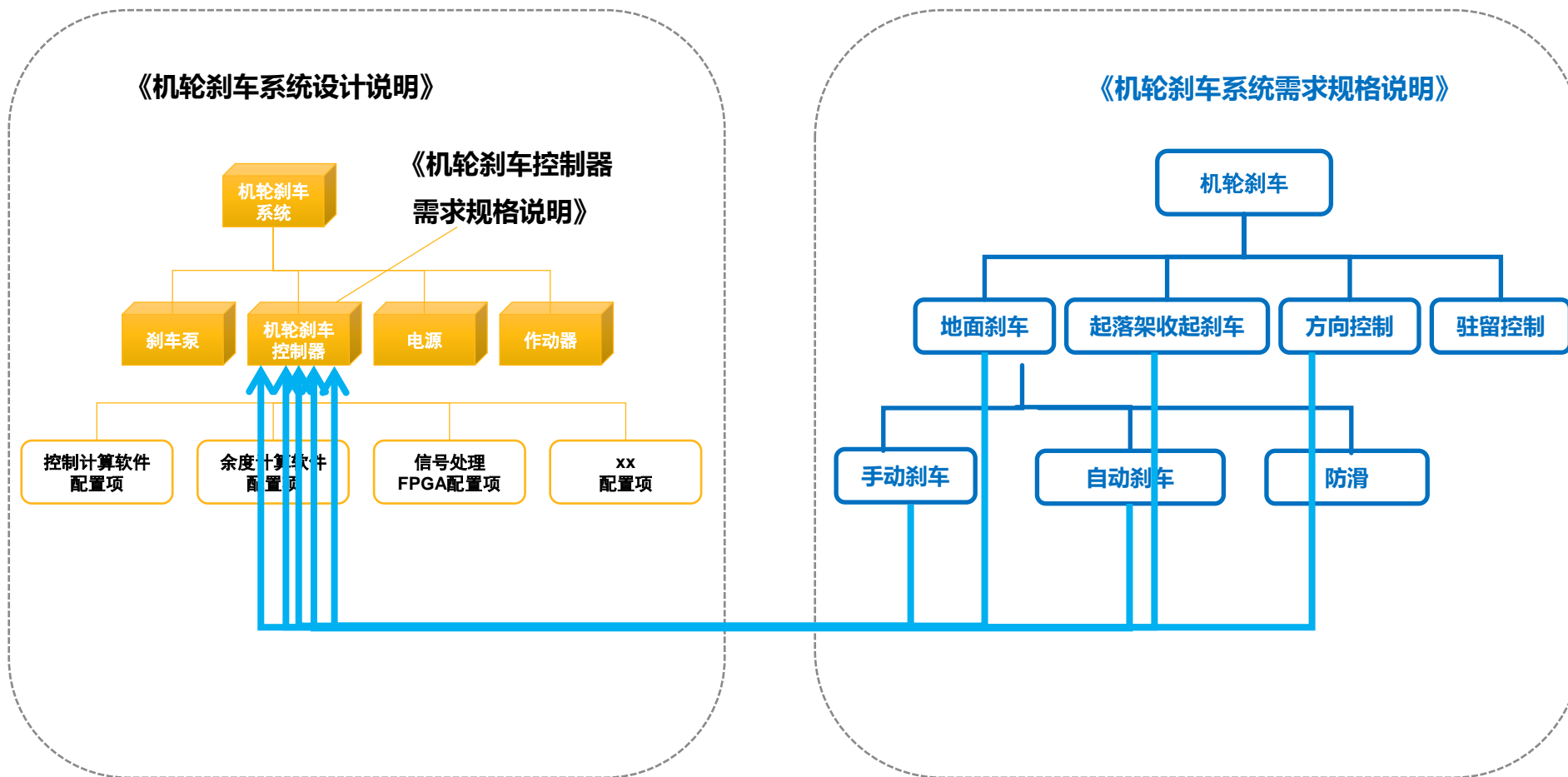
安全生命周期 - 方案设计阶段:

架构视图



安全生命周期 – 方案设计阶段：

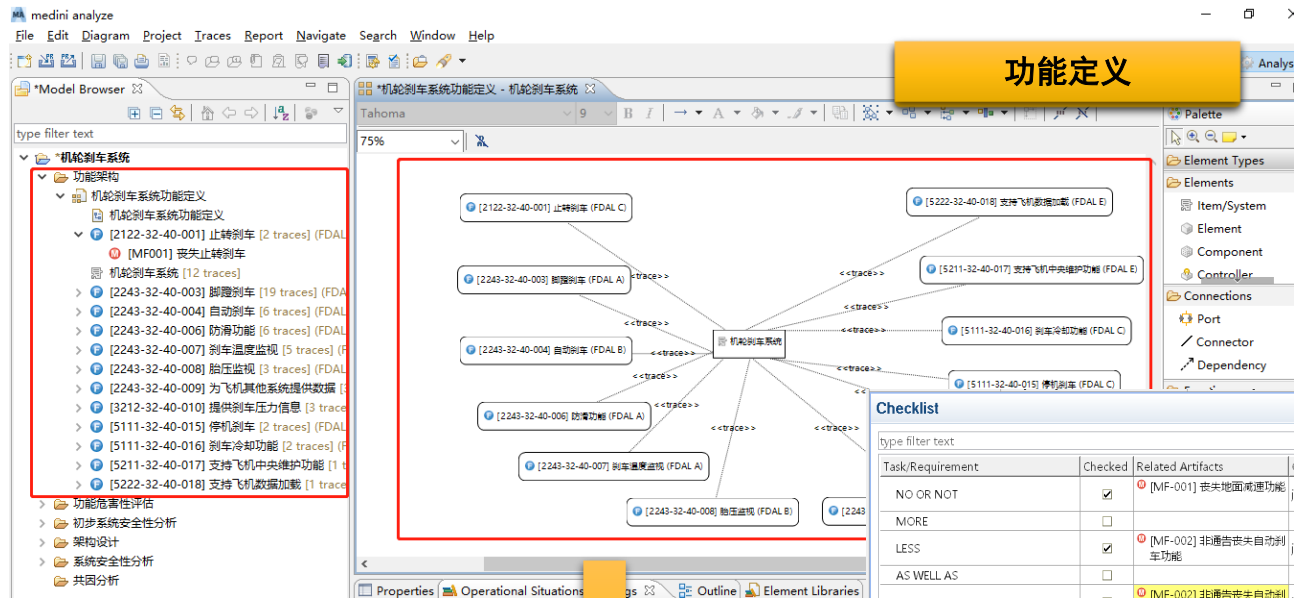
例子：机轮刹车功能分配给机轮刹车系统的架构



方案设计阶段:

产品
功能开发

将功能分配到
系统

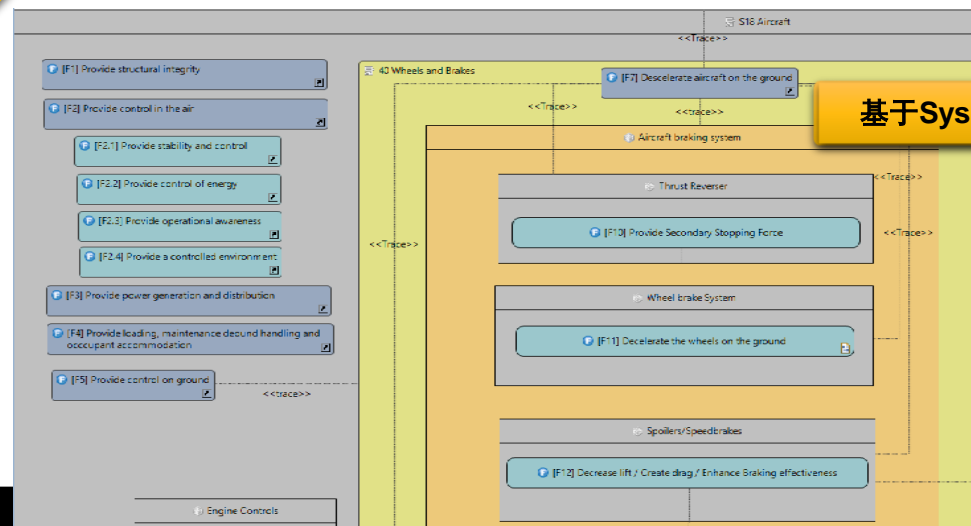
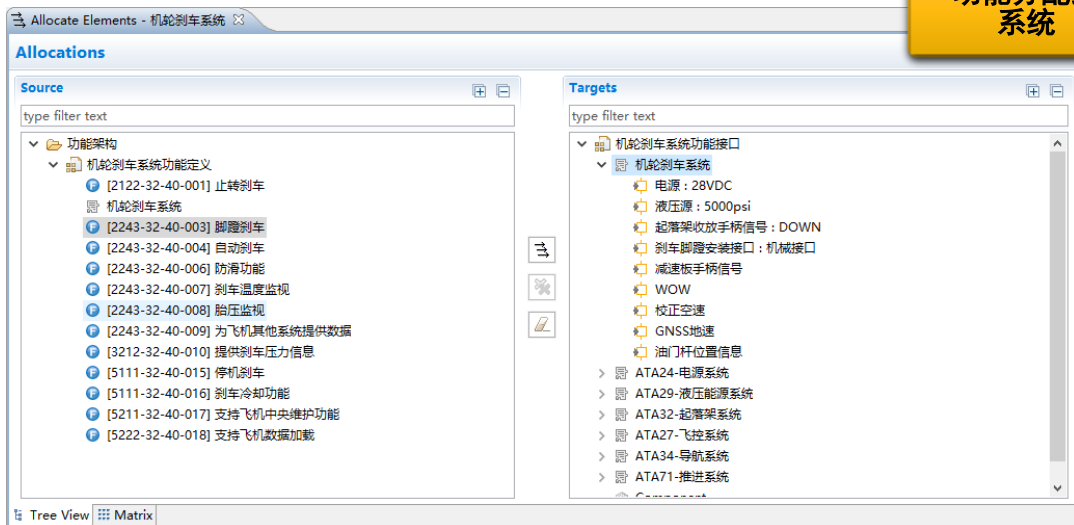


功能定义

功能分配给
系统

基于引导词的故障模板,
识别故障

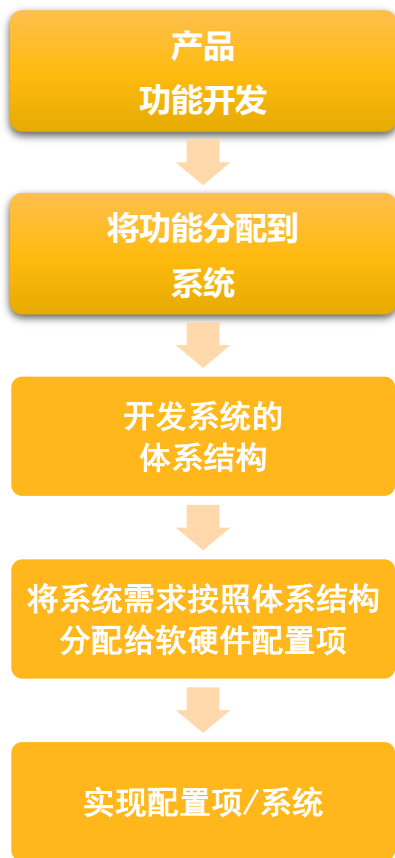
Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note	Description
NO OR NOT	<input checked="" type="checkbox"/>	[MF-001] 丧失地面减速功能	lyang	18-3-20 上午9:50		Complete negation of the design intent
MORE	<input type="checkbox"/>					Quantitative increase
LESS	<input checked="" type="checkbox"/>	[MF-002] 非通告丧失自动刹车功能	lyang	18-3-20 上午9:50		Quantitative decrease
AS WELL AS	<input type="checkbox"/>					Qualitative modification/increase
PART OF	<input checked="" type="checkbox"/>	[MF-002] 非通告丧失自动刹车功能	lyang	18-3-20 上午10:15		Qualitative modification/decrease
REVERSE	<input type="checkbox"/>					Logical opposite of the design intent
OTHER THAN	<input type="checkbox"/>					Complete substitution
EARLY	<input type="checkbox"/>					Relative to the clock time
LATE	<input type="checkbox"/>					Relative to the clock time
BEFORE	<input type="checkbox"/>					Relating to order or sequence
AFTER	<input type="checkbox"/>					Relating to order or sequence
PERIODIC	<input type="checkbox"/>					Changing in quantity or instable



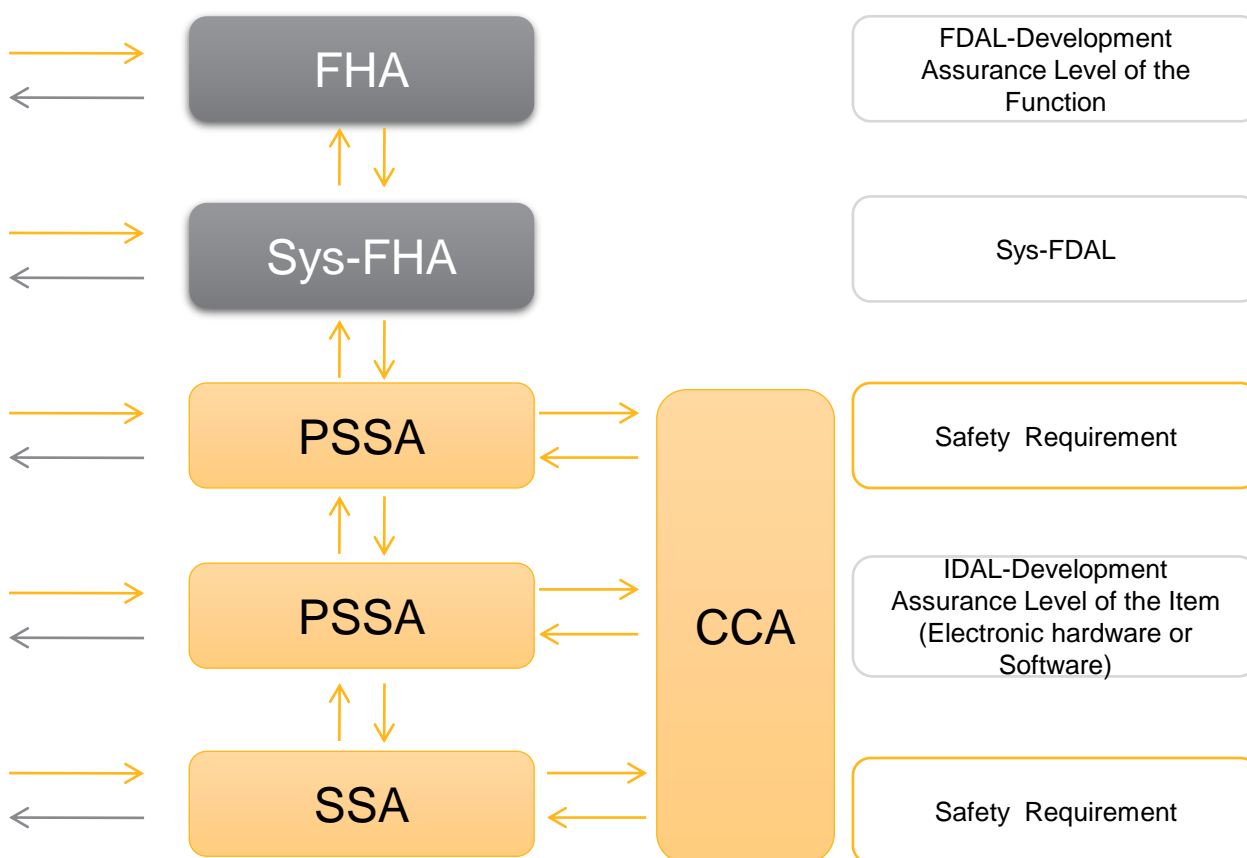
基于SysML的系统设计

安全生命周期 — 飞机级/系统级FHA (功能危险评估)

ARP 4754A的开发过程



ARP 4761的安全性评估过程

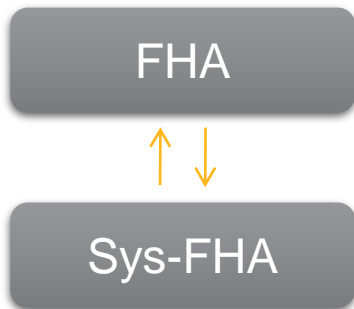


安全生命周期 — 飞机级/系统级FHA（功能危险评估）

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

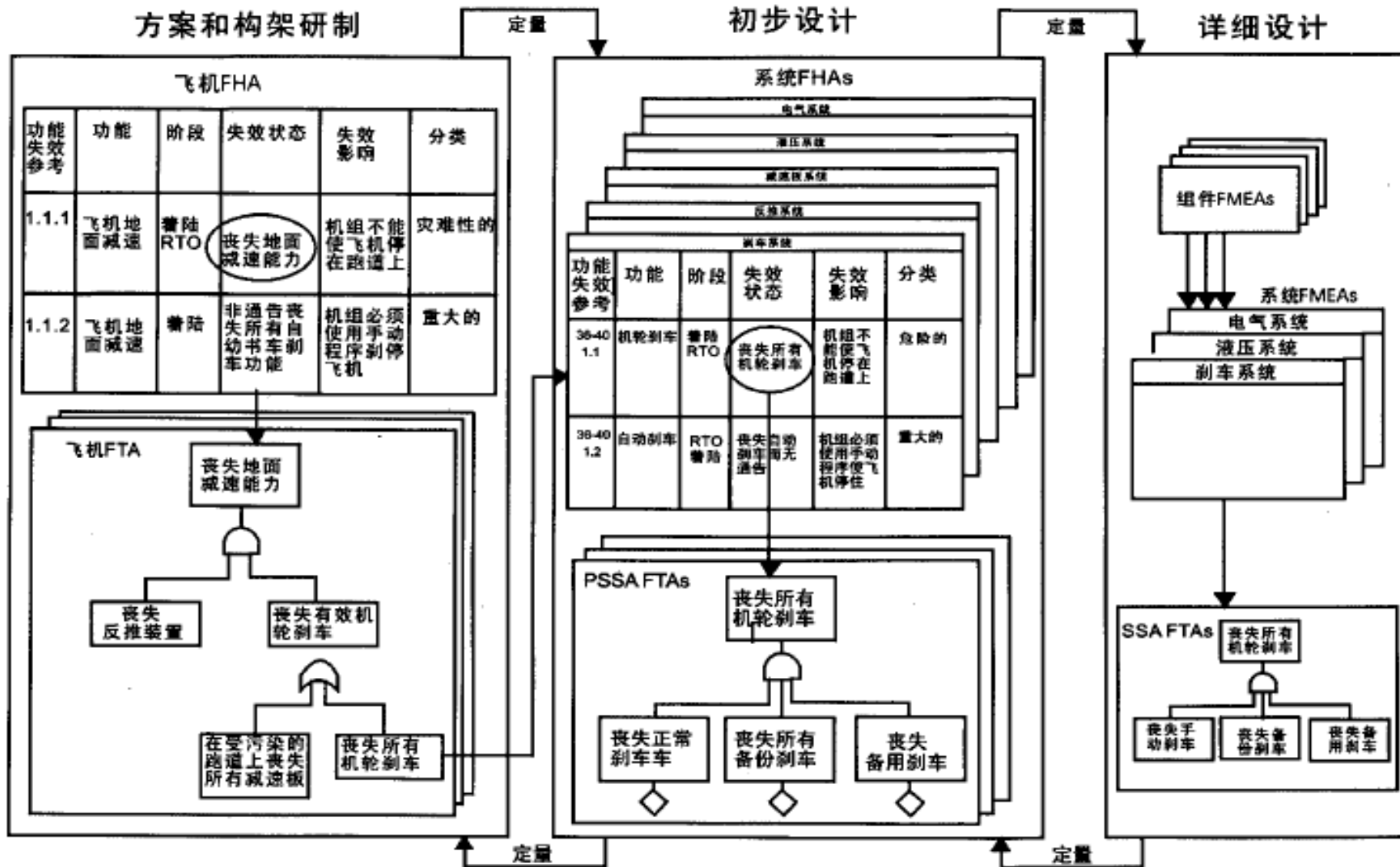
Function	Failure Condition	Flight phase	Failure effect	Classification
地面减速	所有刹车无法制动	Takeoff; Landing	Boom...Bang!	Catastrophic	
	主刹车无法制动, 副刹车可以制动	Takeoff; Landing	刹车性能下降, 可能造成冲出跑道...	Hazardous	
	主刹车可以制动, 副刹车无法制动	Takeoff; Landing		Hazardous	
	刹车滞后制动	Takeoff; Landing	给机组带来操纵不利...	Major	
	刹车提前制动	Takeoff;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

New Functional Hazard Assessment

Malfunctions
Please choose relevant Malfunction.

Irrelevant.
 Relevant. Select the elements to be considered in the list:

功能失效

- 功能架构
 - 机轮刹车系统功能定义
 - [2122-32-40-001] 止转刹车 [2 traces] (FDAL C)
 - [MF001] 丧失止转刹车
 - [2243-32-40-003] 脚蹬刹车 [19 traces] (FDAL A)
 - [MF002] 完全丧失刹车 (5个到8个)
 - [MF003] 对称严重部分丧失刹车能力 (3个或4个)
 - [MF004] 轻微部分丧失刹车 (1个或2个)
 - [MF005] 非指令刹车
 - [MF006] 刹车有余压
 - [MF026] 非对称严重部分丧失刹车能力 (3个或4个)
 - [MF027] 严重部分丧失刹车能力 (3个或4个)
 - [2243-32-40-004] 自动刹车 [6 traces] (FDAL B)
 - [MF007] 丧失自动刹车
 - [2243-32-40-006] 防滑功能 [6 traces] (FDAL A)
 - [MF008] 丧失防滑保护

< Back Next > Finish Cancel

Hazards - 机轮刹车系统

Hazards

type filter text

ID	Name	Kind	Severity	Description
2122-32-40-001FC001A	丧失止转刹车		0 0	
2243-32-40-003FC001A	低速时 (V<30kts), 完全丧失刹车		0 0	
2243-32-40-003FC001B	RTO时, 完全丧失刹车		0 0	
2243-32-40-003FC001C	高速时 (V>30kts), 完全丧失刹车		0 0	
2243-32-40-003FC002A	轻微部分丧失刹车 (1个或2个)		0 0	
2243-32-40-003FC002B	RTO时, 轻微部分丧失刹车 (1个或2个)		0 0	
2234-32-40-003FC003A	低速时 (V<30kts), 严重部分丧失刹车能力 (3个或4个)		0 0	
2243-32-40-003FC003B	RTO时, 严重部分丧失刹车能力 (3个或4个)		0 0	
2243-32-40-003FC003C	高速时 (V>30kts), 对称严重部分丧失刹车能力		0 0	

失效状态

Extended List View Customize

New Functional Hazard Assessment

Flight Phase
Please choose relevant Flight Phase.

Irrelevant. Optionally, you may set the default column value:
 Relevant. Select or add the values to be considered in the list:

飞行阶段、环境因素

type filter text

Relevant Entry

- All
- T1 (上电), T11 (下电)
- T2 (清出), T10 (清入)
- Take-off
- T3-1 (V<30kts)
- T3-2/3/4/5 (V>30kts)
- T3-1/2/3/4 (V<V1)
- T3-2 (30kts<V<60kts)
- T3-3 (60kts<V<80kts)
- T3-4 (80kts<V<V1)
- T3-5 (V<V1)

Select/Deselect All

< Back Next > Finish Cancel

机轮刹车系统功能危害性评估表

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(样-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] 刹车有余压	• 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] 刹车有余压	• 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	可能致大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] 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	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绝大部分	可能由于飞机的损毁而绝大部分	Catastrophic	A	工模试验

自动生成FHA表格

medini 用于PASA – FTA

Safety program plan - AIR6110_181105

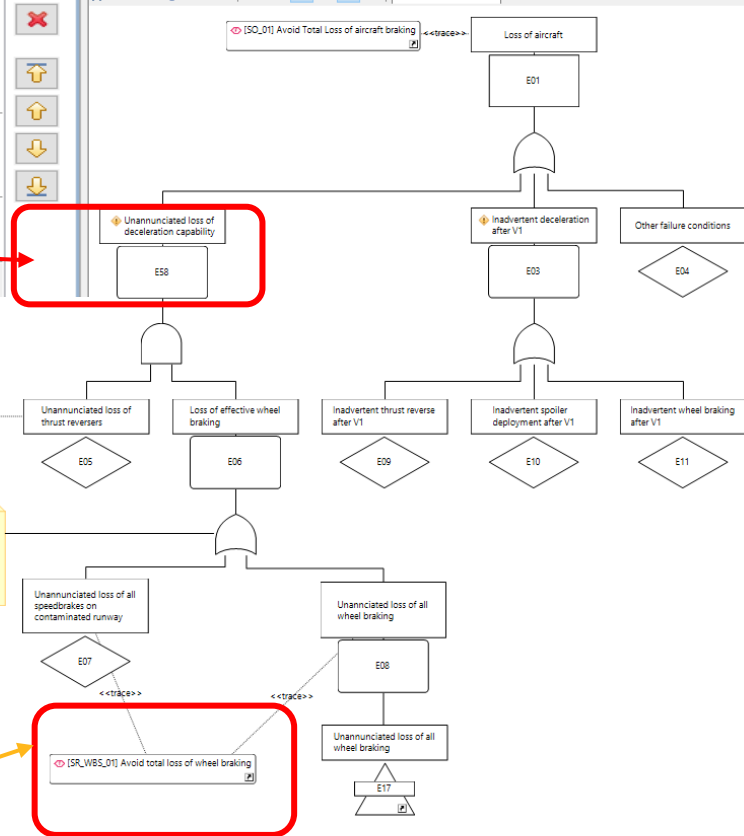
AFHA - AIR6110_181105

Scenario Analysis

type filter text

ID	Function	Failure Condition (Hazard description)	Phase	Effect of failure condition on Aircraft/Crew	Failure Condition Classification
AFHA1	[F7] Decelerate aircraft on the ground	[AFHA_H1.1] Unannounced loss of deceleration capability	Landing/RTO	Crew is unable to decelerate the aircraft, resulting in a high speed overrun	Catastrophic
AFHA2	[F7] Decelerate aircraft on the ground	[AFHA_H1.2] Announced loss of deceleration capability	Landing	Crew selects a more suitable runway, notifies emergency ground support, and prepares occupants for runway overrun	Minor
AFHA3	[F7] Decelerate aircraft on the ground	[AFHA_H1.1] Unannounced loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.	Major
AFHA4	[F7] Decelerate aircraft on the ground	[AFHA_H1.2] Announced 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

S18飞机安全性评估_ARP4761A
 README.txt
 飞机安全计划
 功能设计
 飞机级功能层次设计
 Table A2.docx
 飞机级高层架构
 合规文档
 FHA
 需求
 系统设计
 PSSA
 SSA
 CCA

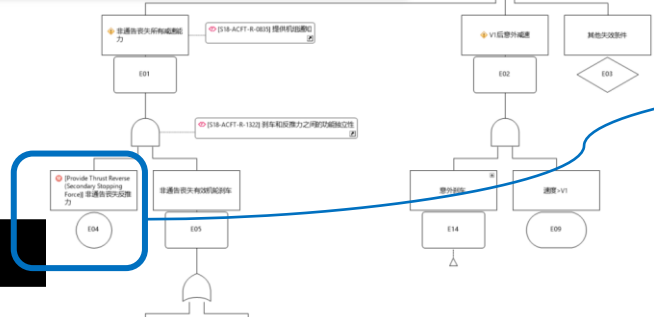
type filter text

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	[MF028] 丧失所有减速能力					Crew selects a		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	overrun. 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	[E02] V1后意外减速	Catastrophic	A

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

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。



子系统继续分析

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 reversers maximum extent possible. This may result in a runway overrun
2	[F009] Decelerate the wheels on the ground	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
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

Sys-FHA: 功能分配给系统后, 评估系统功能及其失效

内置规则检查 Validation Rules

Wheel brake system FHA - AIR6110_181105

Scenario Analysis

type filter text

ID	Function	Malfunctioning Behaviour	Failure Condition (Hazard description)	Phase	Effect of failure condition on Aircraft/Crew	Failure Condition Classification	DAL	Hazard/Safety requirement	Description
SFHA_1	[F11] Decelerate the wheels on the ground	[MF008] Unannunciated loss of wheel braking	[FC2] Unannunciated loss of wheel braking	Landing/RTO	Crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers to the maximum extent possible. This may result in a runway overrun.	Catastrophic	A	[SR_WBS_02] Loss off all wheel braking (annunciated or unannunciated) during landing or RTO shall be less than 5X10-7 [SR_WBS_03] 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 [SR_WBS_03] Inadvertent wheel braking with all wheels locked during takeoff roll before V1	
SFHA_2	[F11] Decelerate the wheels on the ground	[MF009] Annunciated loss of wheel braking	[FC3] Annunciated loss of wheel braking	Landing	Crew selects a more suitable airport, notifies emergency	Hazardous	B	[SR_WBS_03] Inadvertent wheel braking (annunciated or unannunciated) during landing or RTO shall be less than 5X10-7	
SFHA_3	[F11] Decelerate the wheels on the ground	[MF008] Unannunciated loss of wheel braking	Unannunciated partial symmetrical loss of wheel braking	Landing/RTO	The crew detects the failure when the brakes are used. Crew uses available wheel braking.	Hazardous	B	[SR_WBS_03] 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	Potentially catastrophic (to be confirmed by analysis)
SFHA_4	[F11] Decelerate the wheels on the ground	[MF009] Annunciated loss of wheel braking	Annunciated partial symmetrical loss of wheel braking	Landing	The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking.	Major	C	[SR_WBS_03] 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	Potentially catastrophic -
SFHA_5	[F11] Decelerate the wheels on the ground	[MF025] Asymmetrical loss of wheel braking	Asymmetrical loss of wheel braking- brake system failure only	Landing/RTO	Decrease in braking performance.	Catastrophic	A	[SR_WBS_02] Loss off all wheel braking (annunciated or unannunciated) during landing or RTO shall be less than 5X10-7 [SR_WBS_03] 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	
SFHA_1	[F11] Decelerate the wheels on the ground	[MF025] Asymmetrical loss of wheel braking	Asymmetrical loss of wheel braking and loss of rudder or nose wheel steering	Landing/RTO	Decrease in braking performance. Tendency to veer off the runway. For braking performance and brake temperature the effects are the same as partial brake loss above. The crew cannot maintain runway centerline and results in an offside excursion.	Hazardous	B	[SR_WBS_03] 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	
SFHA_6	[F11] Decelerate the wheels on the ground	[MF026] Inadvertent wheel brake application	Inadvertent wheel brake application without wheel locking	Takeoff before V1	The crew stops the aircraft on the runway.	Minor	D	[SR_WBS_03] Inadvertent wheel braking with all wheels locked during takeoff roll before V1	
SFHA_7	[F11] Decelerate the wheels on the ground	[MF026] Inadvertent wheel brake	Inadvertent wheel brake	Takeoff	Potential burst of all tires and loss of brakes.	Hazardous	A	[SR_WBS_03] Inadvertent wheel braking with all wheels locked during takeoff roll before V1	

- 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

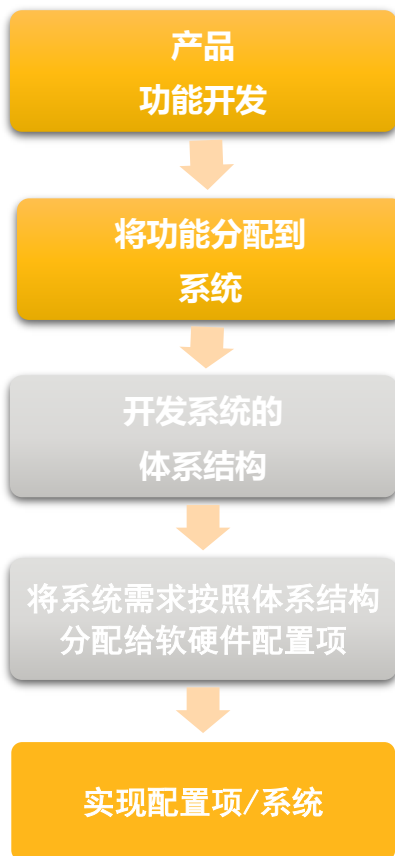
Problems View - AIR6110_181105

Description	Problem ID	Location
The failure rate distribution percentages for the failure modes of Hardware Part Green pump do not add to 100.0%. Value is: 0.0	0024	System safety assessment::System Architecton::Modified braking system architecture (dual hydraulics, 2BSCUS)::Brake System::Green pump
The 'Hazardous Event [SFHA_1] Unannunciated loss of wheel braking' has no (unique) identifier	0033	Functional hazard assessment::System FHA::SFHA::Wheel brake system FHA::[SFHA_1] Unannunciated loss of wheel braking
The 'Hazardous Event [SFHA_1] Asymmetrical loss of wheel braking and loss of rudder or nose wheel steering' has no (unique) identifier	0033	Functional hazard assessment::System FHA::SFHA::Wheel brake system FHA::[SFHA_1] Asymmetrical loss of wheel braking and loss of rudder or nose wheel steering

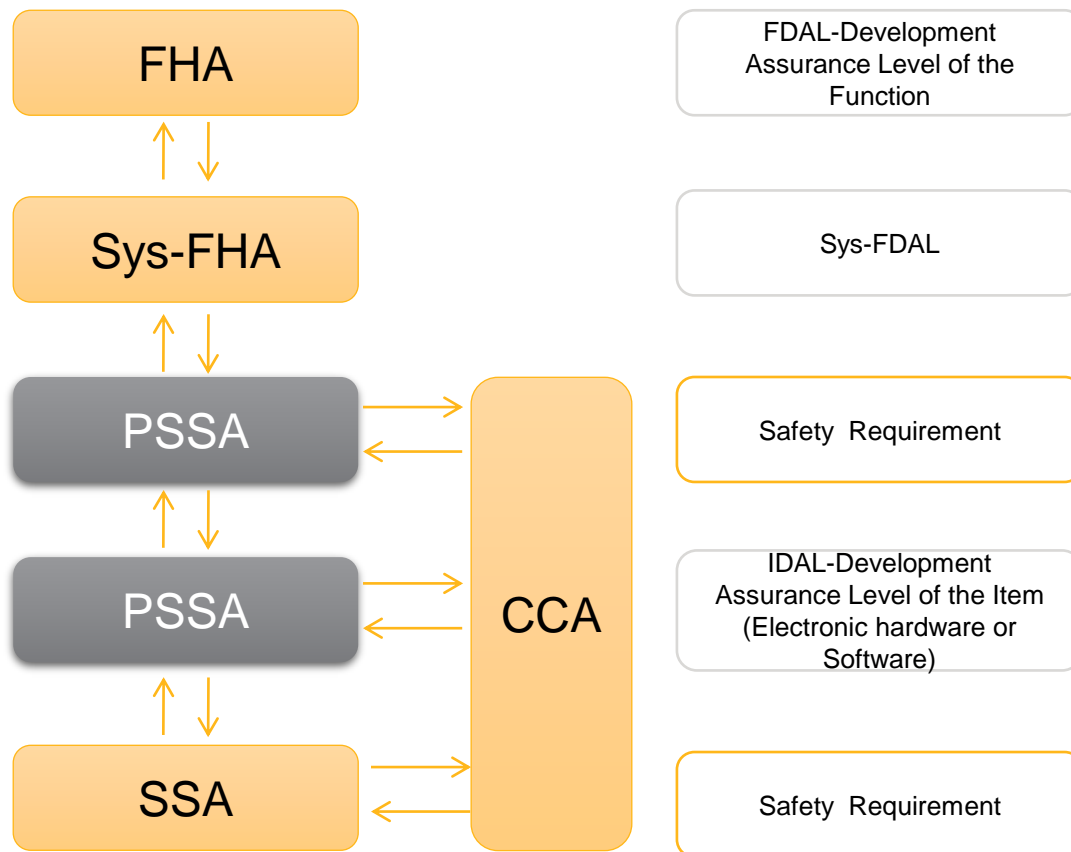
安全生命周期 — 初步系统安全评估

Preliminary System Safety Assessment

ARP 4754A的开发过程



ARP 4761的安全性评估过程



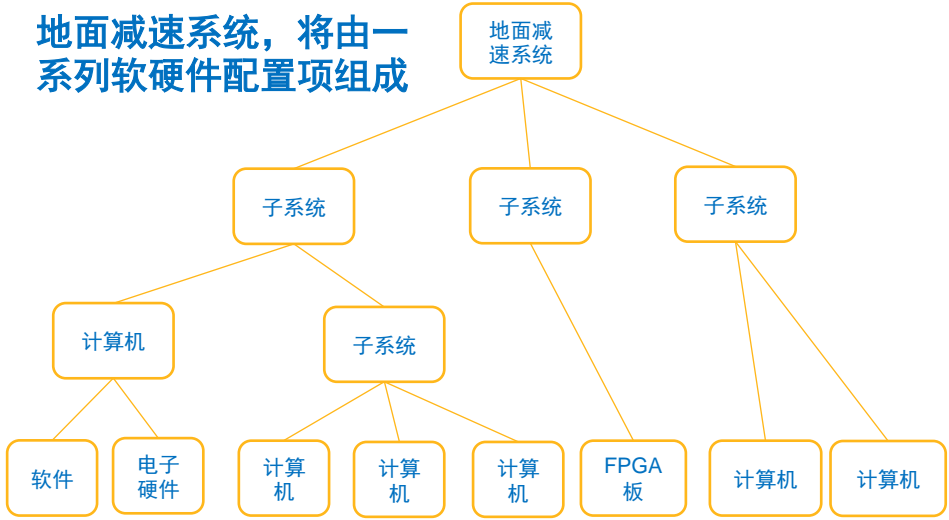
安全生命周期 — 初步飞机/系统安全评估

Preliminary Aircraft/System safety assessment

开发系统的
体系结构

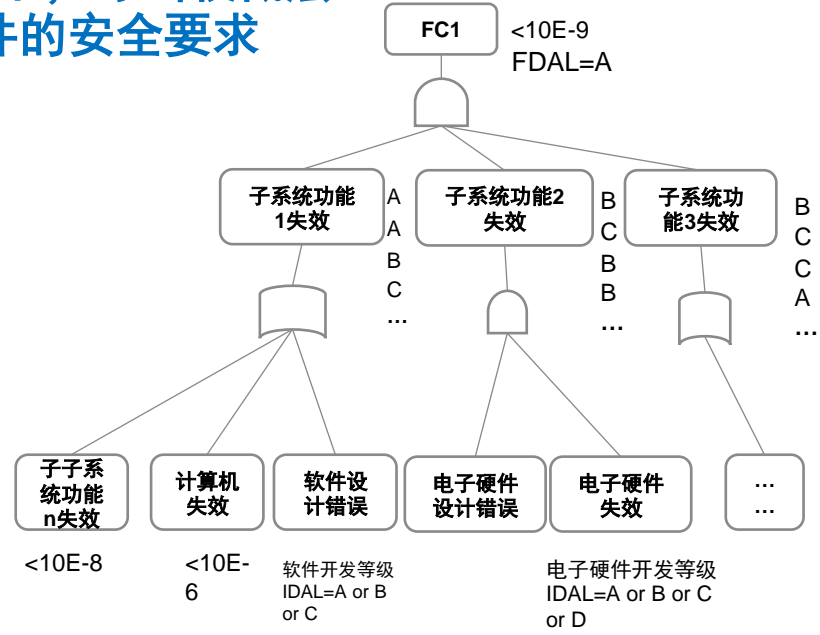
定义“地面减速”系统

地面减速系统，将由一系列软硬件配置项组成

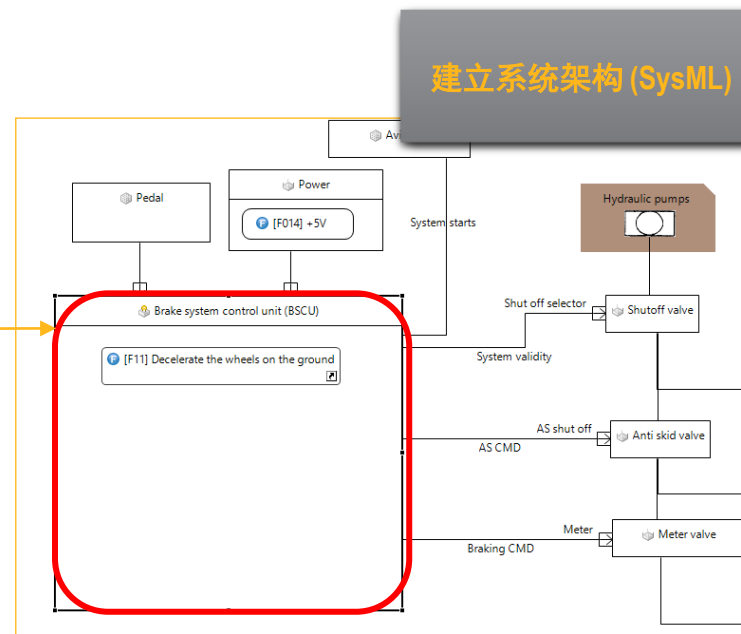
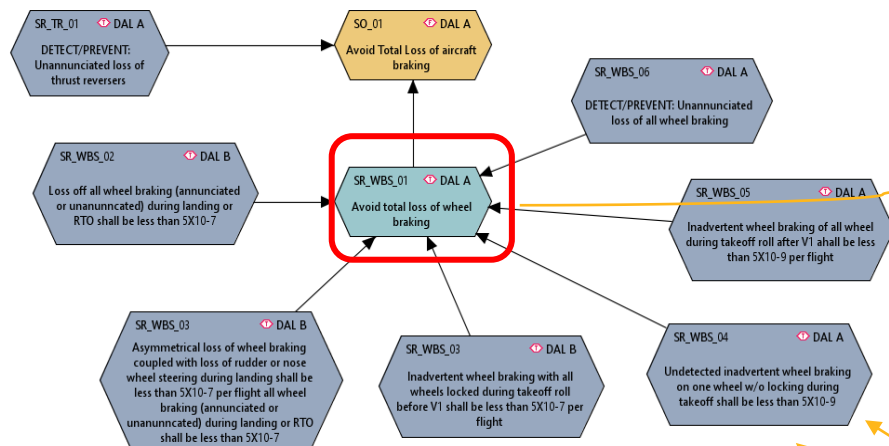


PSSA (FTA)

自上而下，导出较低层组件的安全要求



medini 用于PSSA

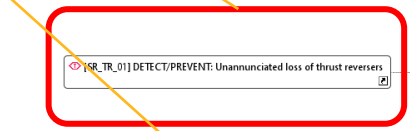


Safety Requirements Editor

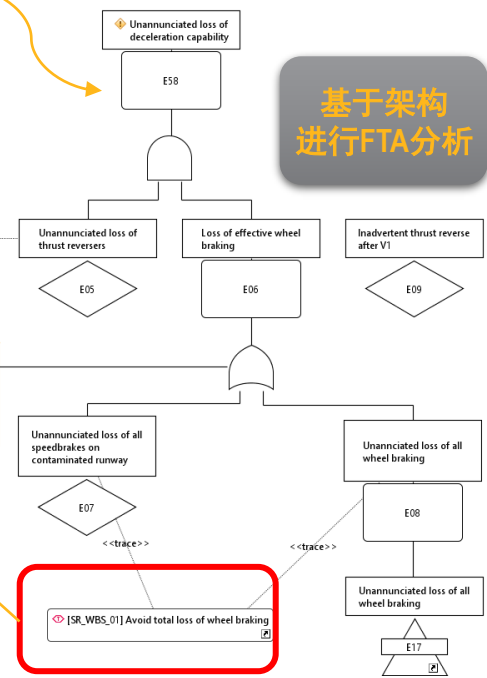
type filter text

N°	ID	Name	Kind	DAL	Status	All
1	SO_01	Avoid Total Loss of aircraft braking	FUNCTIONAL	A	PROPOSED	[F3] Provide control on ground (FDAL A) [F7] Decelerate 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] Decelerate 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] Decelerate aircraft on the ground (FDAL A)
4	SR_WBS_02	Loss off all wheel braking (annunciated or unannunciated) 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] Decelerate 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)

多种视图管理安全需求



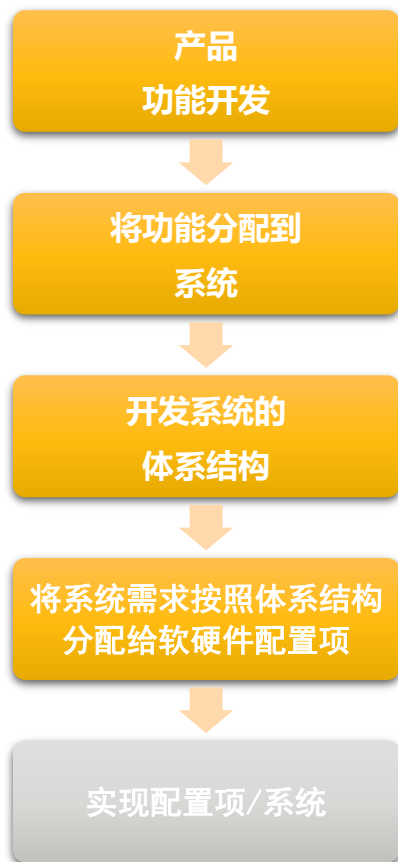
The requirements of 5E-7 per flight for "Unannunciated loss of all speed brakes on contaminated runway" and for "Unannunciated loss of all wheel brakes" result from the classification of these failure conditions as Hazardous (this classification is equivalent to 1E-7 per flight hour). These classifications are based on knowledge and experience with these system failures conditions. These requirements result in a requirement probability of 1E-6 per flight (i.e., 2x5E-7 per flight hr.) at the next higher level of "Unannunciated loss of effective wheel braking".



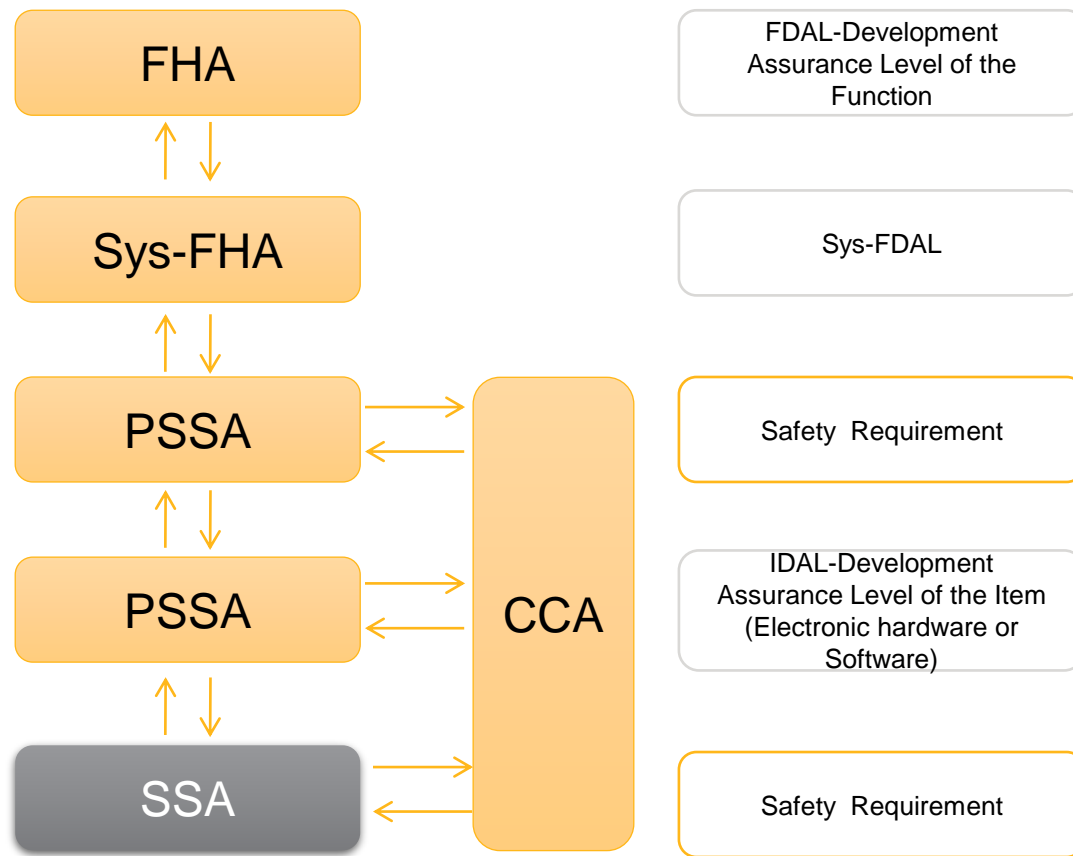
安全生命周期 — 系统安全评估

System Safety Assessment

ARP 4754A的开发过程



ARP 4761的安全性评估过程



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。
- SSA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

验证系统级FHA中确立的设计需求被满足

认可所确定的飞机级影响分类是正确的

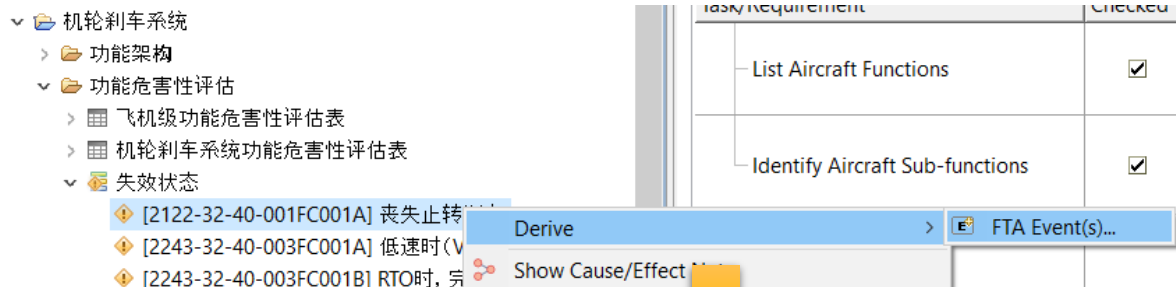
验证由飞机设计要求和目标派生的安全性需求被满足

验证在CCA过程中确认的设计需求被满足

系统级SSA和飞机级FHA的连接：对每个SSA进行评审

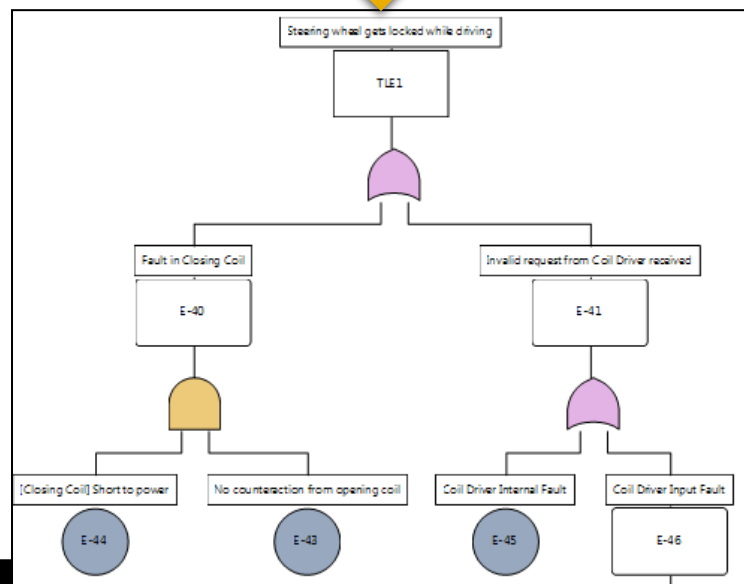
medini 用于SSA - FTA

■ 定性故障树分析 (Qualitative FTA)



自动计算最小割集,
识别单点故障、多点故障

基于失效状态/功能失效/
失效模式自动生成FTA事件



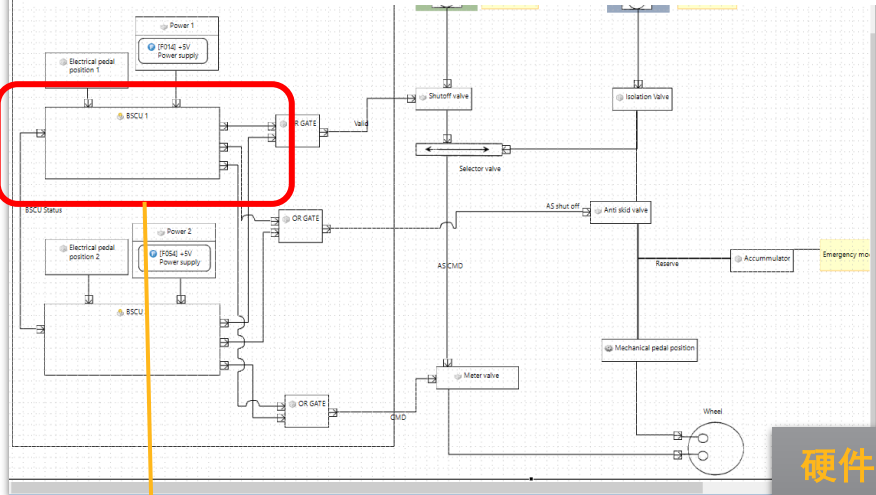
Minimal Cut Sets The analysis model needs to b

type filter text

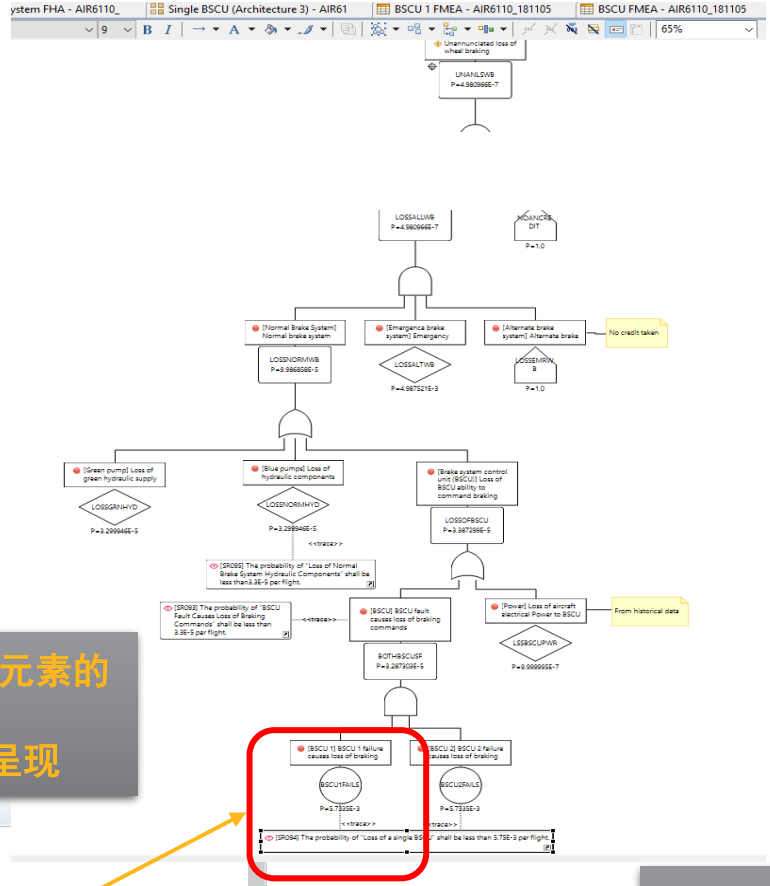
#	Events of Cut Set
1	E-45
2	E-43, E-44
3	E-53, E-58
4	E-54, E-58
5	E-55, E-58
6	E-56, E-58
7	E-57, E-58

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

Properties BSCU 1

Base Failure Rate: 0.000115 FIT Transient Rate: 0.0 FIT Failure Rate of nested elements: 0.0 FIT

Safety

Failures Failure Modes:

Mode	Type	Distribution (in %)	Fra
BSCU 1 failure causes loss of braking commands	PERMANENT	100.0	0.00

机轮刹车系统功能危害性评估表 安全性需求 - 机轮刹车系统 丧失止转刹车 - 机轮刹车系统 BSCU - S18

Minimal Cut Sets The analysis model needs to be saved before additional properties can be edited

Evaluated event [AFHA3.2.3.TLA] Unable to decel within available runway with crew aware, landing

Unavailability	4.91827E-8	Unreliability (Vesely)	4.918218E-8	Unreliability (Murchland)	4.918218E-8	Mission time T	100	h	Average flight time	5	h
PFD	1.746602E-8	Avg. per FH (Vesely)	4.918218E-10	Avg. per FH (Murchland)	4.918218E-10	CFI average	4.918218E-10				

type filter text

#	IDs of Events	Events of Cut Set	Q(T)	w(T)	Importance
1	PRS.MF	[PRS.MF] FF5.3 Uncommanded engine high thrust resulting in high speed overrun	6.0E-9	6.0E-11	0.121994110548609779

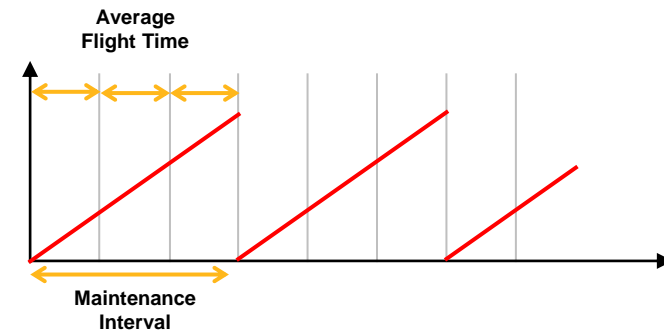
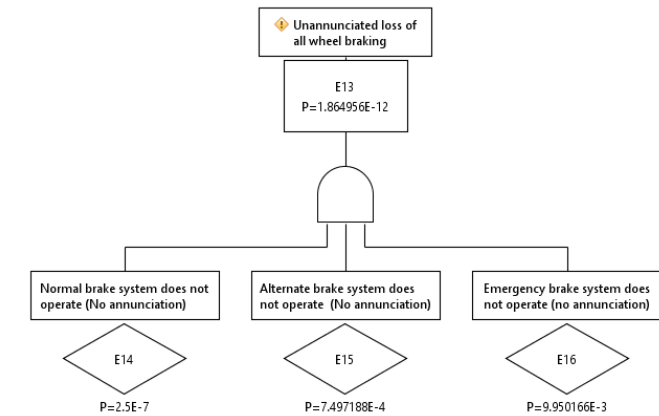
FTA – 考虑飞行阶段

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”

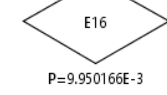
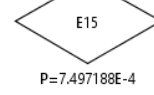
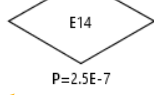
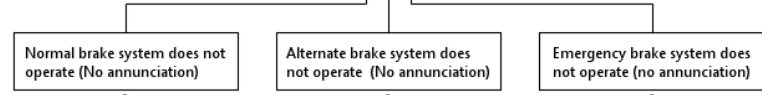
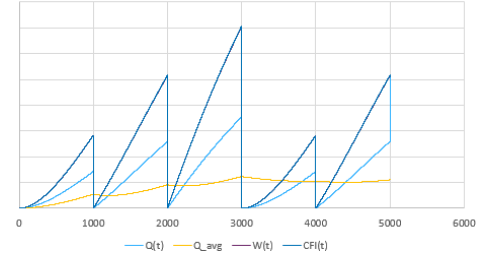
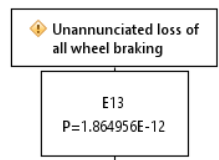


例子: Risk Times

PSSA Wheel brake System FTA (first try) - ATA-32-40-00_Demo

Mission Time (h): 100000 Average Flight Time (h): 2.5

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

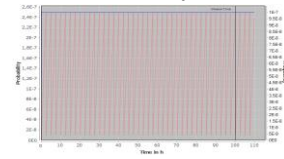


Inspected before every flight

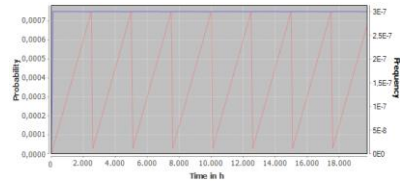
Inspection after every 300 h

No maintenance/inspection interval

Risk Time: 2.5 h
(Maximum Probability of Failure)

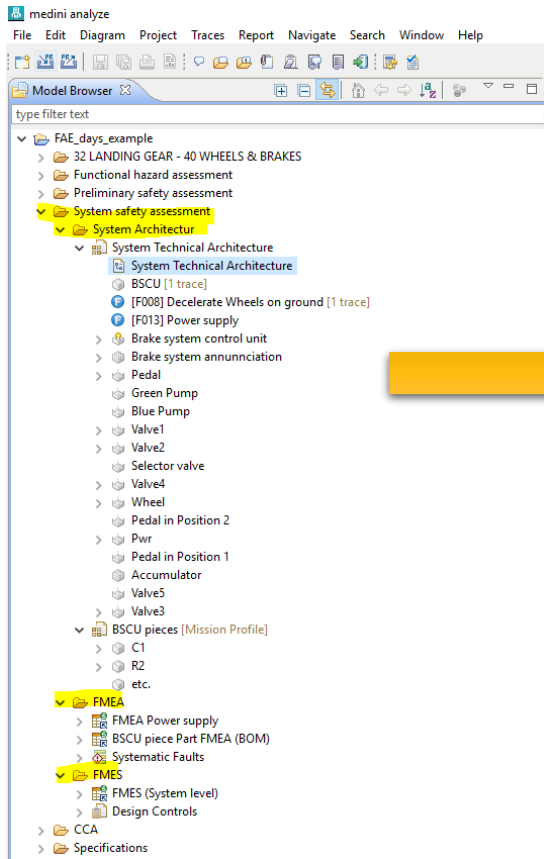


Maximum Risk at 300h

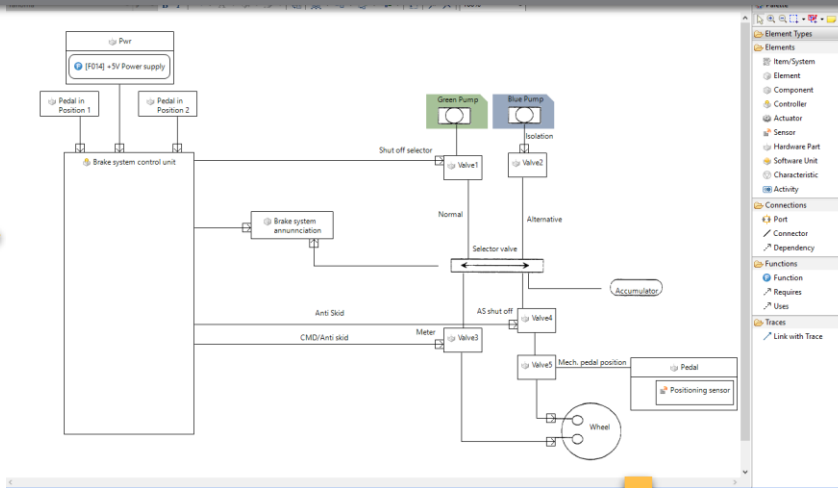


Risk increases over aircraft lifetime
(maximum at 100 000h)

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

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。

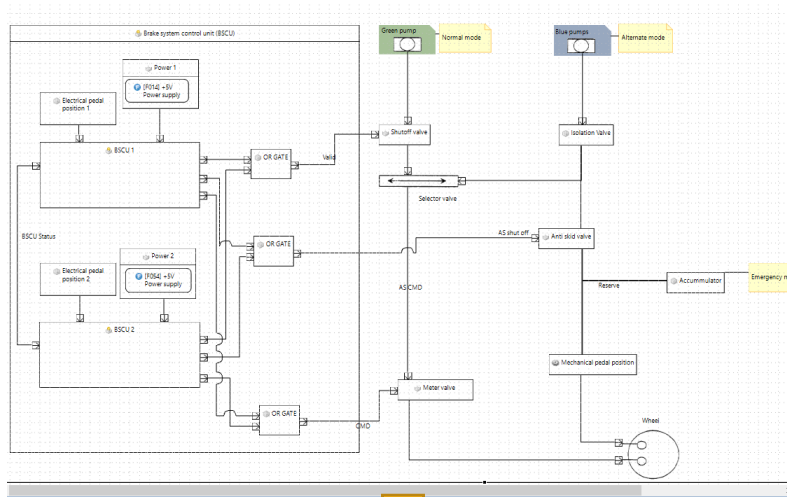
System FMEA Worksheet

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	Red	Green	Green
		[[F-004] Evaluate Vehicle state] [[MF-033] NO Vehicle State Information	[HZ 1] Steering blocked	8	9	S	[[PUMT1] TR8 : ● [TRANSISTOR] Open	3	2	54	Red	Green	Green
		[[F-005] Derive Command] [[MF-037] NO Command issued		9	9	S	[[PUMT1] TR7 : ● [TRANSISTOR] Short	3	2	54	Red	Green	Green
		[[F-006] Supervise Execution] [[MF-044] NO Lock State Information	[MF-027] NO Driver Information	0	0	S	[[PUMT1] TR7 : ● [TRANSISTOR] Open	0				Yellow	

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

Design Controls

- [D1] signal to crew alerting system
- [D2] Indication on system display "loss of normal braking"
- [P1] Waterproof compartment
- [P2] Create an alternate braking system
- [P3] Monitor status of normal braking system
- [P4] Create an emergency braking system

- 直接用于FMEA分析

BSCU 1	BSCU 1 failure causes loss of braking commands	[AFHA_H1.1] Unannounced loss of deceleration capability	[E] [BSCU1FAILS] [BSCU 1] BSCU 1 failure causes loss of braking commands	[Brake system control unit (BSCU)] BSCU fault causes loss of braking commands	10	[[F014] +5V Power supply] [MF010] +5V out of spec.			
					10	[[F014] +5V Power supply] [MF012] +5V open			
				S	0	[[F014] +5V Power supply] [MF059] Short to ground or other voltage	<div style="border: 2px solid red; border-radius: 15px; padding: 5px;"> <ul style="list-style-type: none"> [P1] Waterproof compartment [P2] Create an alternate braking system [P4] Create an emergency braking system [P3] Monitor status of normal braking system </div>	<ul style="list-style-type: none"> [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）

FMECA - FMECA

Cover Sheet

Design: System Design

Kind: System
 Subsystem
 Component
 Function
 Process

Analysis Depth: unlimited Restrict analysis to that level

Presets: [VDA](#) [AIAG](#) [SAE J1739](#) [MIL-STD-1629A](#)

Hide ports
 Hide action columns
 Hide measure group information

Criticality Assessment:
 Risk Priority Numbers (RPN)
 Failure and Component Criticality (FMECA)

Operating Time (h): 500

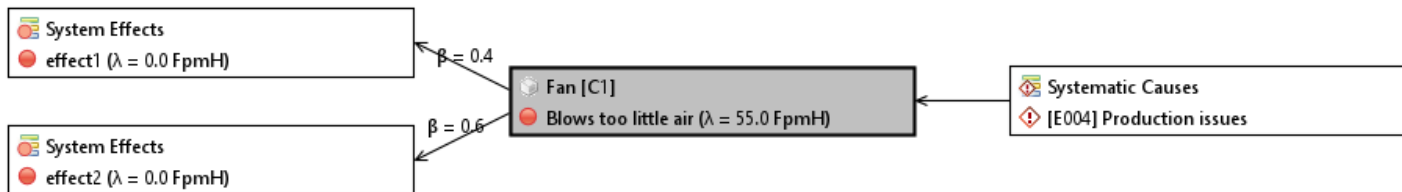
Mission profiles:

- [IEC/SN] Engine Compartment

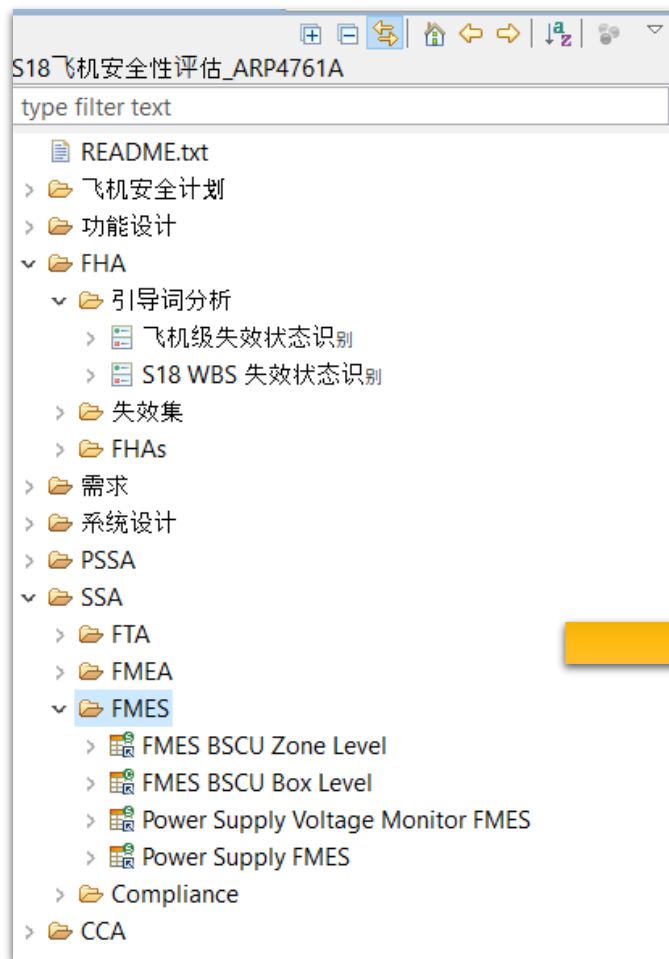
System FMEA Worksheet

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	
				C_10: 16500.0	Blows too much air	5.0	5.0	[System Effects] effect2	0.6	16500	10			
					Blows no air	40.0	40.0							
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

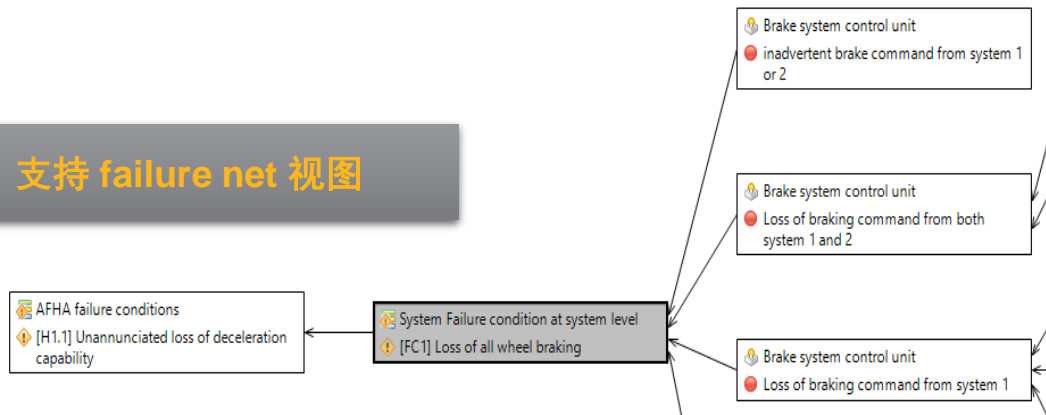


来自FMEA的相同失效影响在FMES中被归类为一种模式；
FMES总结了所有与FMEA具有相同效果的较低级失效模式。

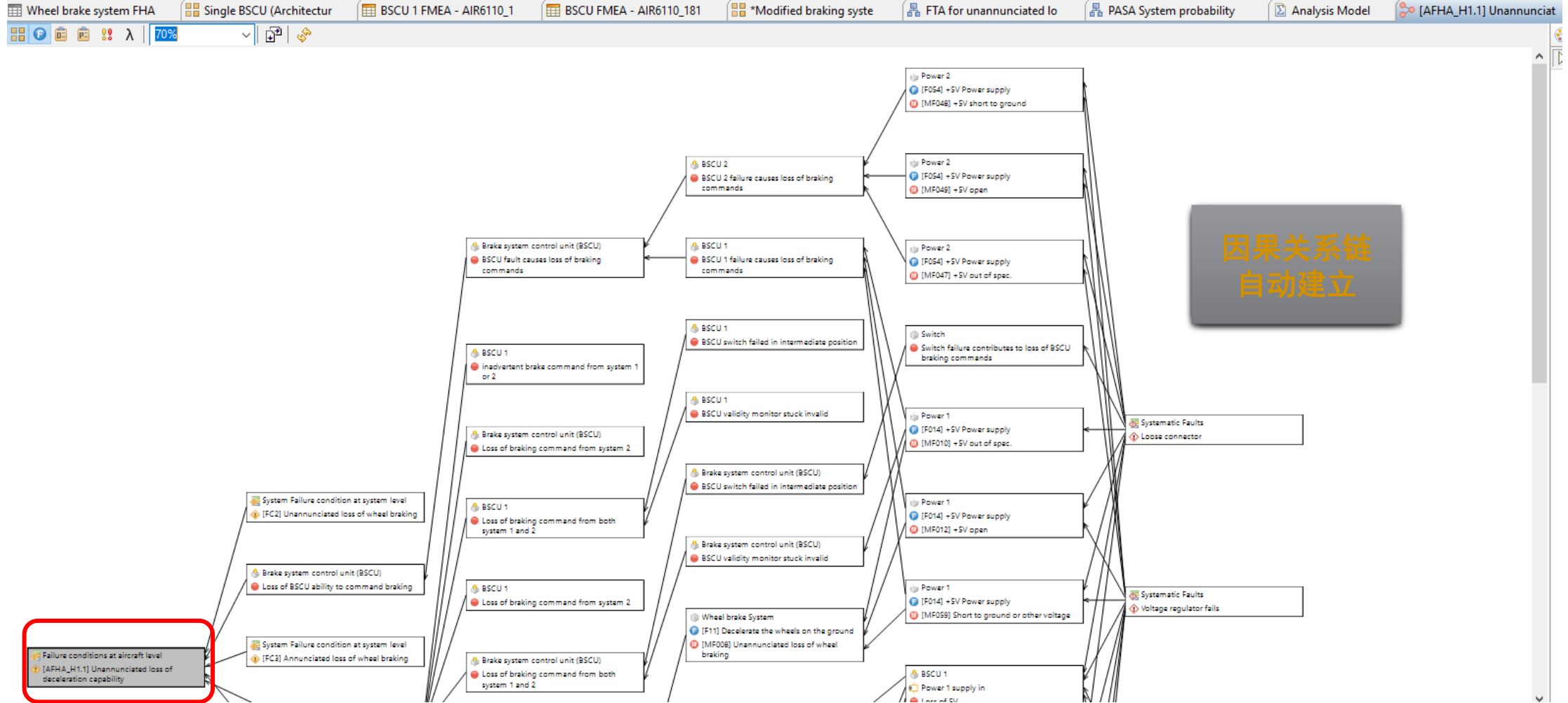
FMES和FMEA表格视图可完全自定义、支持从第三方导入。

Component/Function	Potential Failures	Failure Rate Distribution (in %)	Failure Rate Fraction (in EPH)	Potential Failure Causes	Detectability	Comments	Unmitigated Failure Effect	relatedFTAevent
Zone C	BSCU validity ● monitor stuck invalid	0.0	0.0					
	BSCU incorrectly reports a ● failure causing switch to Alternate	9.46745562	1.6E-7					
Zone A (Channel 1)	BSCU System ● 1 Electronics Failure	95.1520053	0.00003	[PWR] ● Channel 1 command failed				
	BSCU System ● 1 Power Supply Failure	4.84799467	0.000001528	[PWR]: ● Power P/S sh				
	● Unknown	0.0	0.0	[PWR]: ● Power Increa: ICMD				
Zone B (Channel 2)	BSCU System ● 2 Electronics Failure	95.1520053	0.00003					

支持 failure net 视图



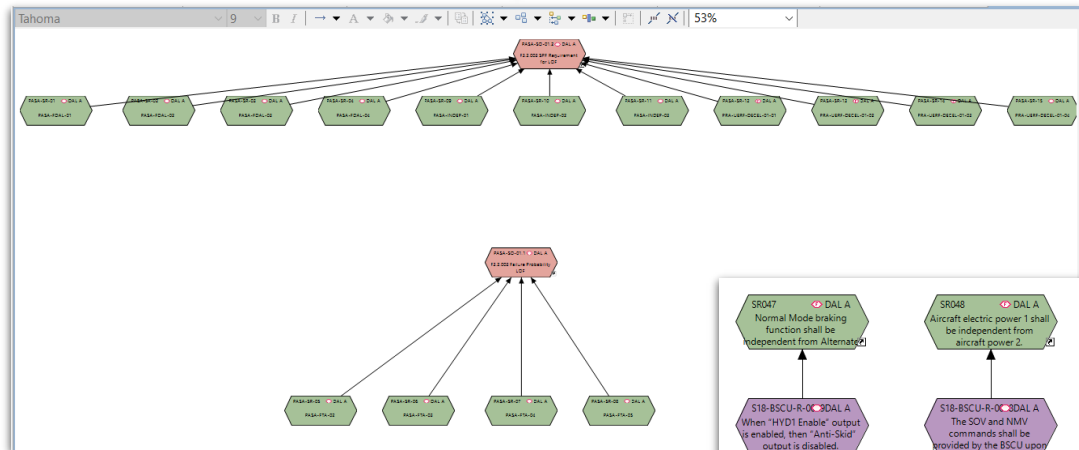
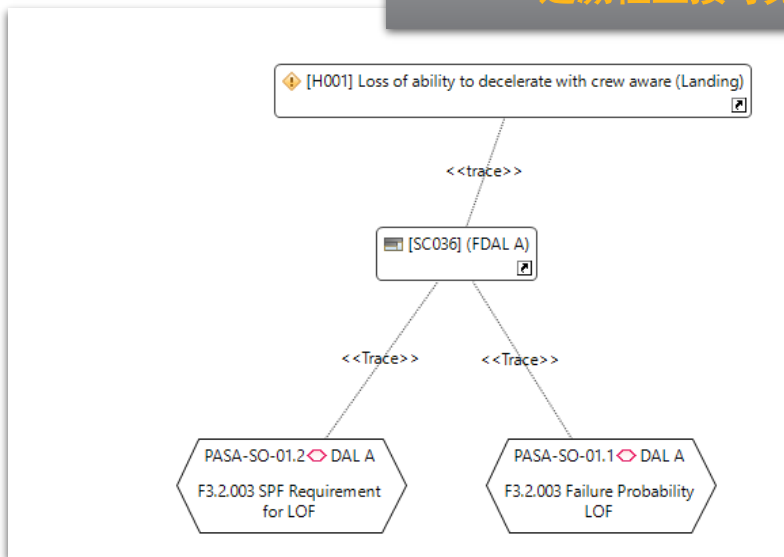
medini 用于SSA – FMES/Cause-effect net



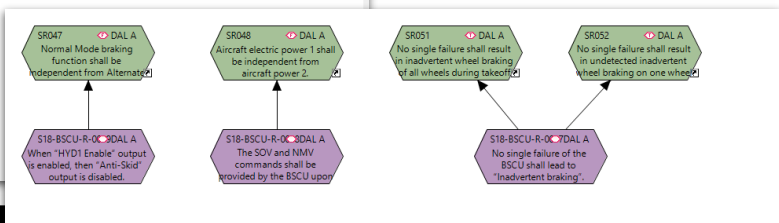
medini 用于SSA – 安全需求管理

追溯性直接可见，例如 追溯至失效状态

- 需求
 - Aircraft Description
 - S18 Safety Objectives
 - S18 Assumptions
 - S18 PASA Requirements
 - S18 WBS PSSA Requirements
 - S18 BSCU Independence Requirements derived from BSCU PSSA
 - S18 BSCU PSSA safety requirements
 - S18 WBS Interface Requirements
 - S18 WBS Interface Requirements



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。

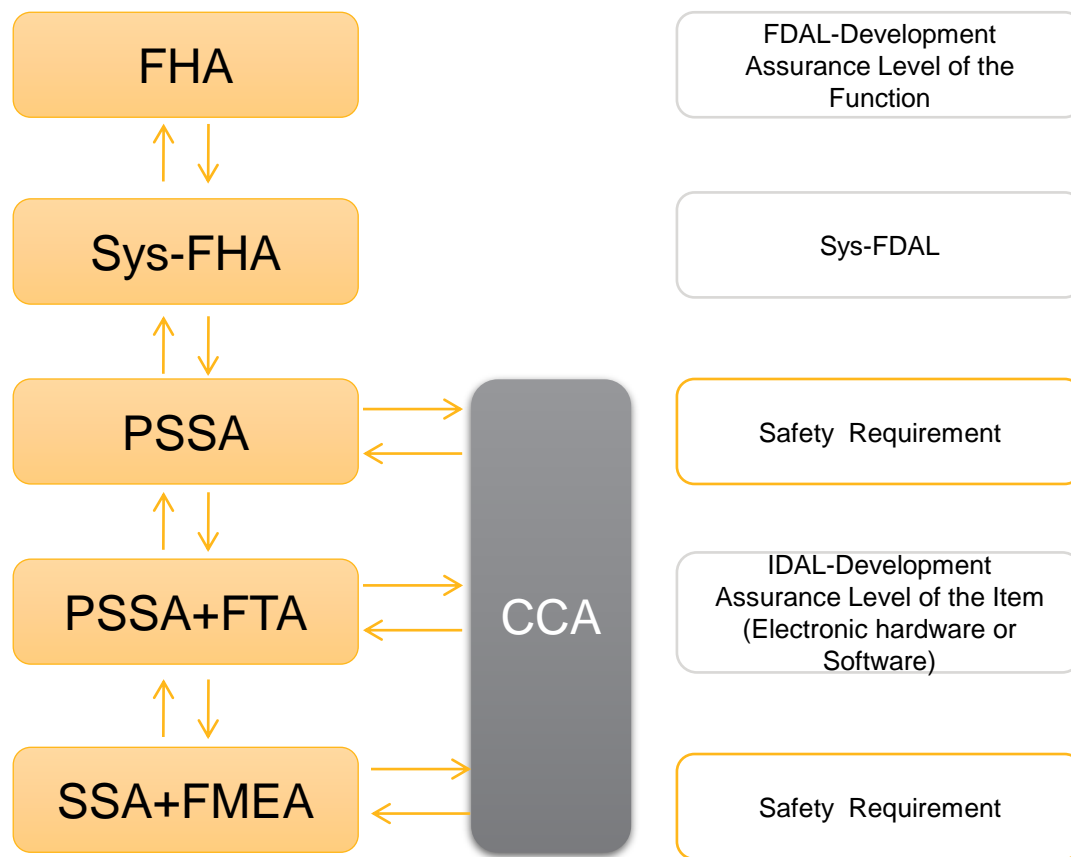


安全生命周期 — 共因分析 Common Cause Analysis

ARP 4754A的开发过程

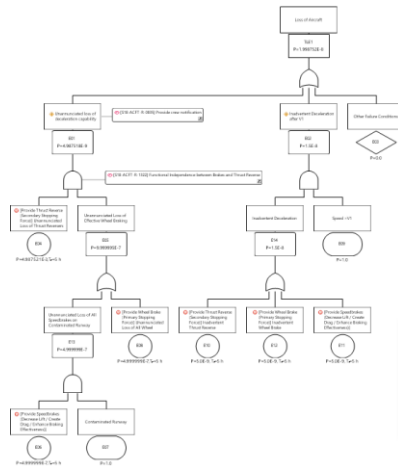
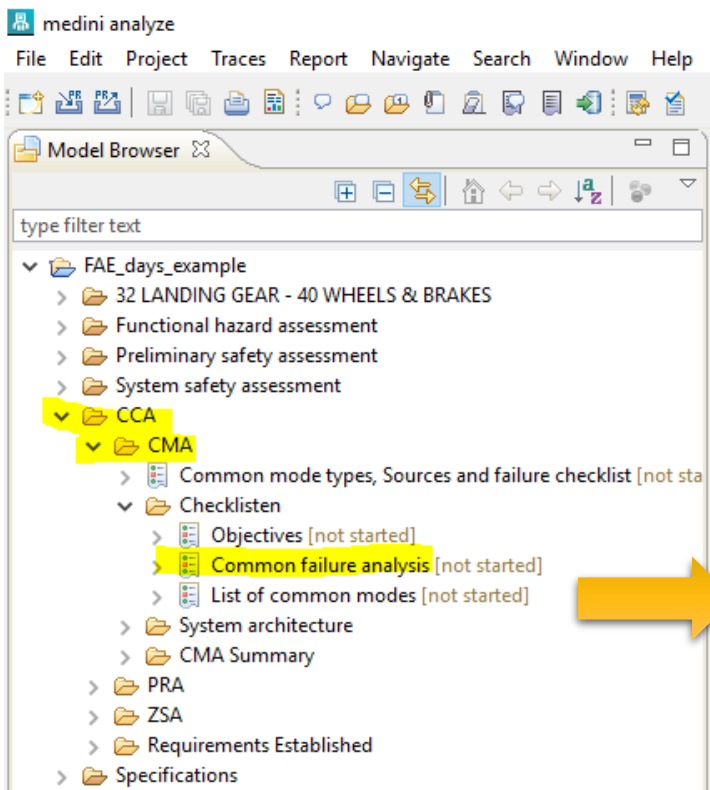


ARP 4761的安全性评估过程



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。



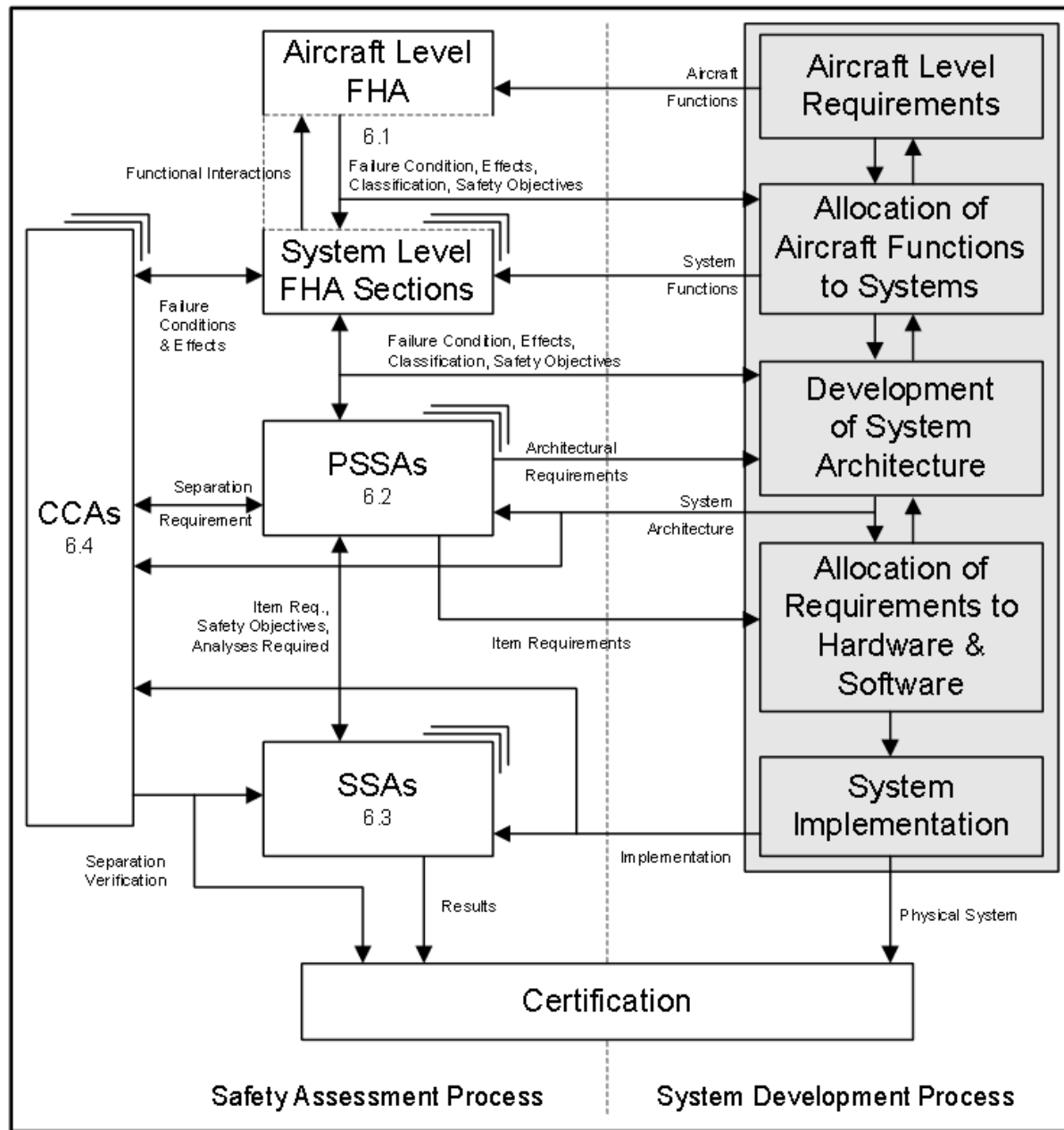
#	Events of Cut Set
1	E-45
2	E-43, E-44
3	E-53, E-58
4	E-54, E-58
5	E-55, E-58
6	E-56, E-58
7	E-57, E-58

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	[E] [E13] Unannounced 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 appropriately 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 inappropriate power supply monitor independence in the presence of anomalous system power supply outputs		Violation of power supply and monitor segregation zones or inappropriate 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

The screenshot displays the S18 AFHA software interface. On the left, a tree view shows the project structure under '飞机安全计划' (Aircraft Safety Plan), including various checklists like 'S18 AFHA [completed]', 'S18 PASA [completed]', and 'S18 WBS SFHA Checklist [completed]'. The main window shows a table with columns: Task/Requirement, Checked, Related Artifacts, Checked By, Date of Check, Note, and Comment. The table lists tasks such as 'Gather AFHA Inputs', 'Review and Confirm Aircraft Level Functions are Complete', 'List Aircraft Functions', 'Identify Aircraft Sub-functions', and 'Identify Aircraft Failure Conditions'. A yellow callout box highlights the 'Identify Aircraft Failure Conditions' row, which is linked to the artifact '飞机级失效状态识别...'. An orange callout box at the top right says '支持模板定制、支持中文' (Supports template customization, supports Chinese). A 'Select Artifacts' dialog box is open in the foreground, showing a tree view of the project structure with '飞机级失效状态识别' selected under the 'FHA' folder. An orange arrow points from the text '直接链接到工作产物' (Directly link to work products) to the dialog box.

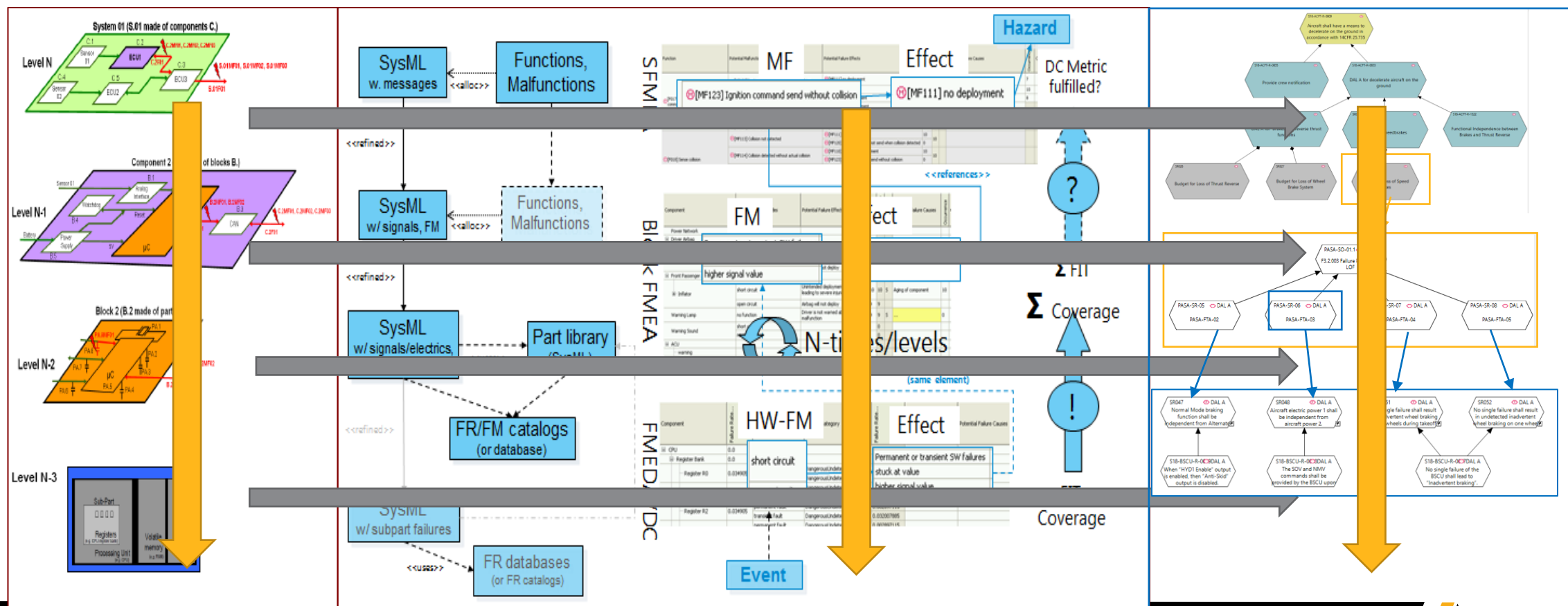
Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note	Comment
Gather AFHA Inputs	<input checked="" type="checkbox"/>	Table A2.docx	jyang	4/29/20 4:23 PM	The inputs to the AFHA are the aircraft level functions, derived from the aircraft design objectives and the fundamental necessities of flight due to the laws of physics, and the operational and environmental conditions the aircraft is designed to encounter.	
Review and Confirm Aircraft Level Functions are Complete	<input checked="" type="checkbox"/>		jyang	4/29/20 4:23 PM	The AFHA does not define aircraft functions; however, it requires a clear, explicit and complete list of aircraft functions as an input.	
List Aircraft Functions	<input checked="" type="checkbox"/>	飞机级功能层次设计	jyang	4/29/20 4:23 PM	Aircraft functions are broadly stated and intended to be inclusive of all possible implementations, as no functional decomposition or design decisions have	
Identify Aircraft Sub-functions	<input checked="" type="checkbox"/>	飞机级功能层次设计	jyang	4/29/20 4:23 PM	The aircraft functions may contain a breakdown into sub-functions, resulting in a hierarchical structure with two or more levels. Failure conditions are	
Identify Aircraft Failure Conditions	<input checked="" type="checkbox"/>	飞机级失效状态识别...	jyang	4/29/20 4:23 PM	A failure condition is described by a statement that characterizes an abnormal state of a function. Failure conditions describe a failed state of the aircraft function including the amount and type of	

直接链接到工作产物

安全项目管理：成熟的跟踪功能，保证全流程的一致性

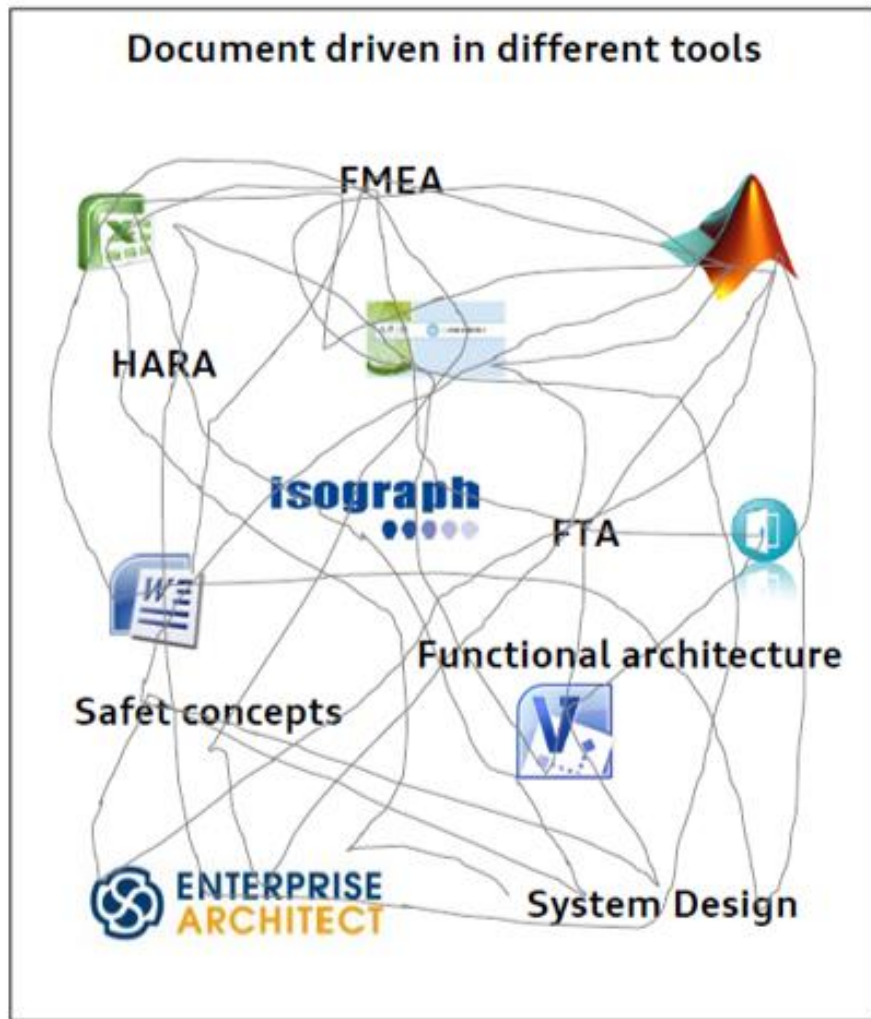
任何信息元素之间可以定义追踪关系

- ✓ 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)

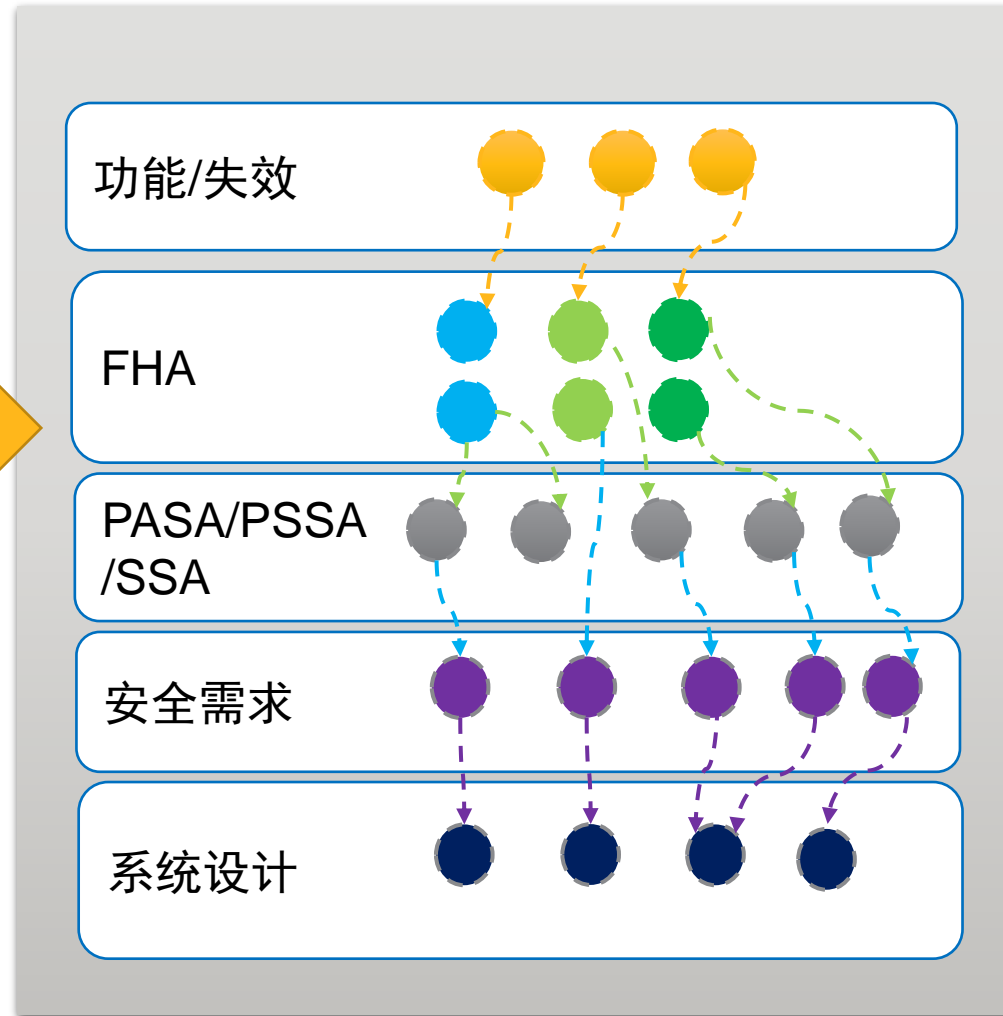


小结

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



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

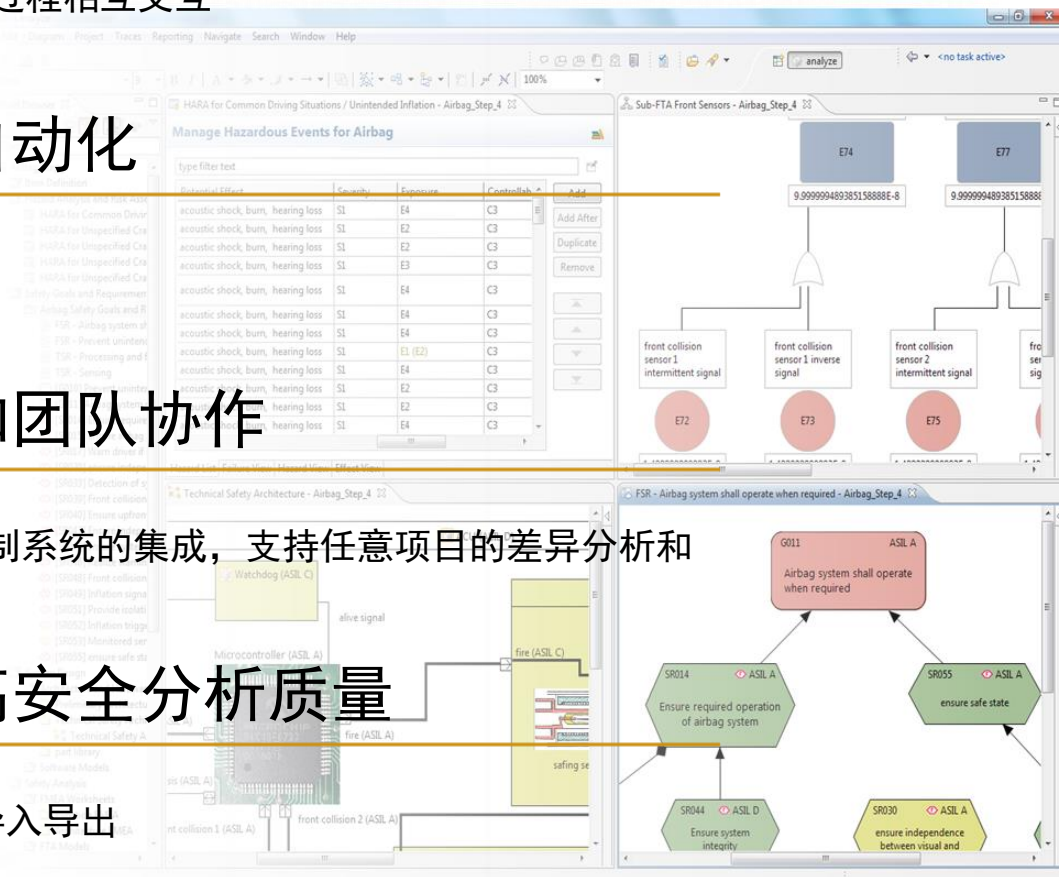
支持项目管理、安全计划和团队协作

- 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