Practice in COMAC to Conduct MBSA in Avionics System Based on Capella

COMAC
&
PGM

目录

1 Introduction

2 Background

3 COMSPEC

4 Summary

5 Demo

Introduction

1.1 Profile of SADRI (Shanghai Aircraft Design and Research Institute)

COMAC functions as the main vehicle in implementing large passenger aircraft programs in China.

About SADRI Design and Research Center of COMAC

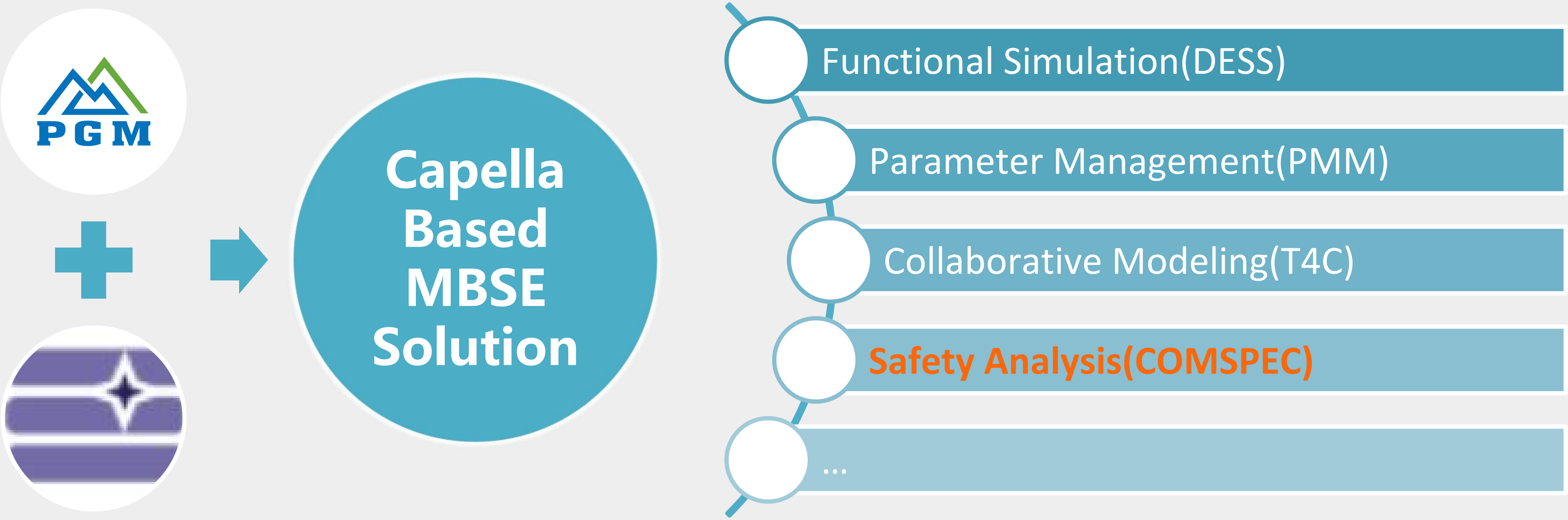
Responsibility Engineering design tasks and technical grasp of civil aircraft projects in China

Engaged Research, Manufacture and Flight Tests of civil aircraft and related products

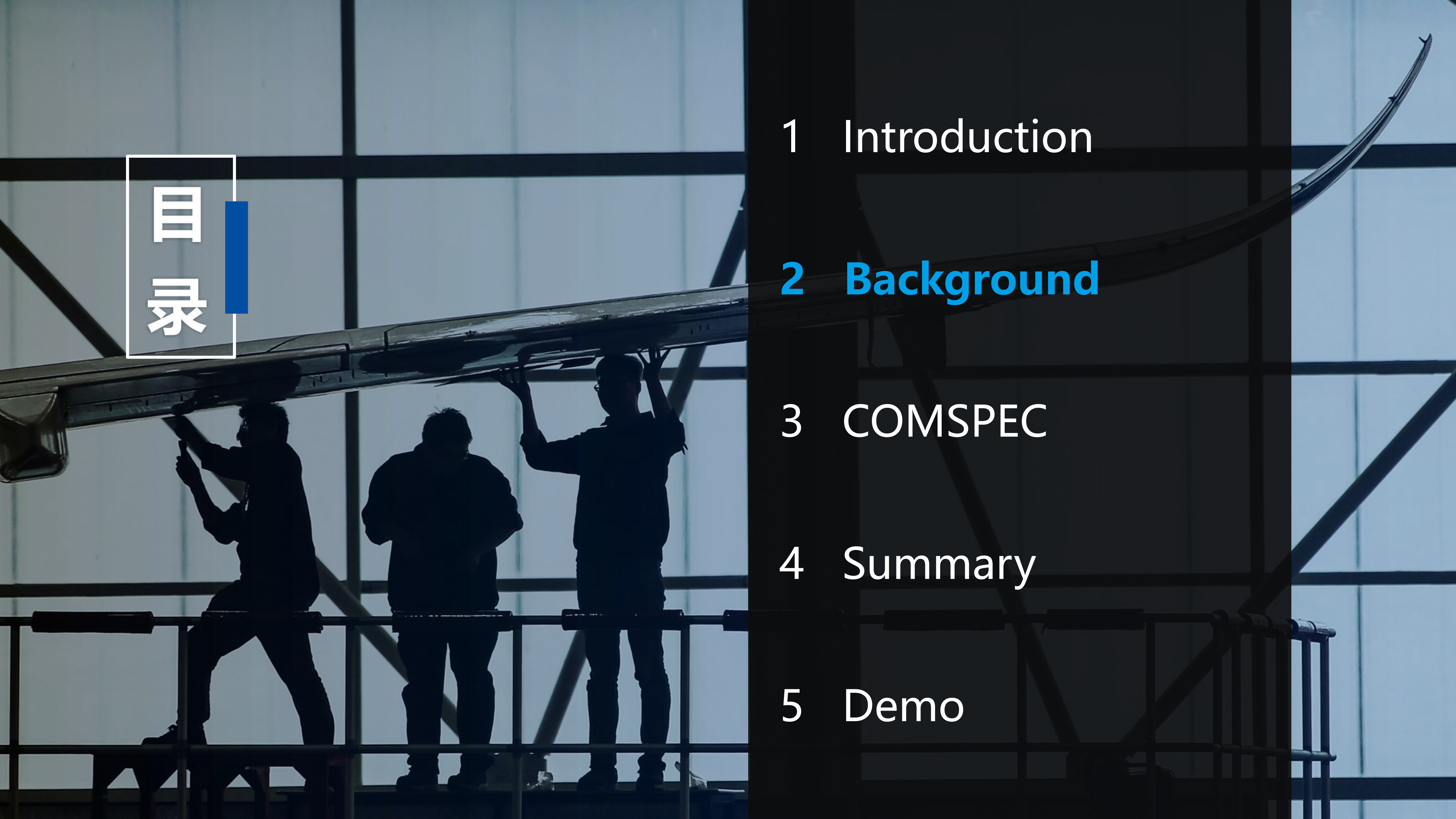
Introduction

1.2 Profile of PGM

- **PGM** (Shanghai PGM Technology Co., Ltd.) is short for **Pu Gou Moutain**.
- A Leading provider of **MBSE solutions and consulting** services in China.
- Many happy customers.
  - Aeronautics, Astronautics, Nuclear power and Automobile domain
- Many **addons for Capella**.



PGM
Capella Based MBSE Solution
Functional Simulation(DESS)
Parameter Management(PMM)
Collaborative Modeling(T4C)
Safety Analysis(COMSPEC)
...



目录

1 Introduction

2 Background

3 COMSPEC

4 Summary

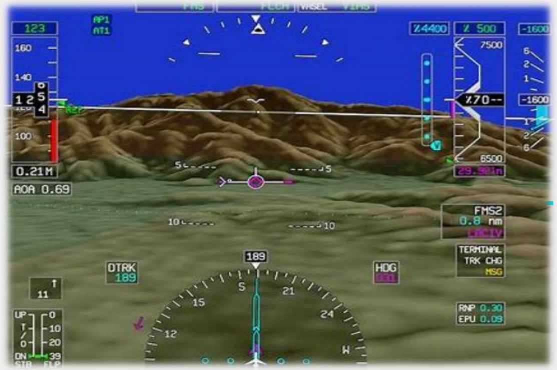
5 Demo

Background

2.1 Introduction of Avionics system

Display & Alarm

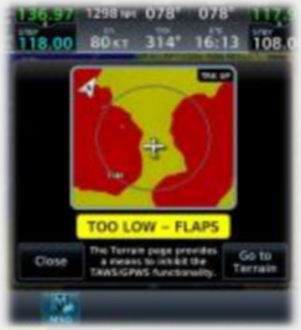
Navigation



FMS

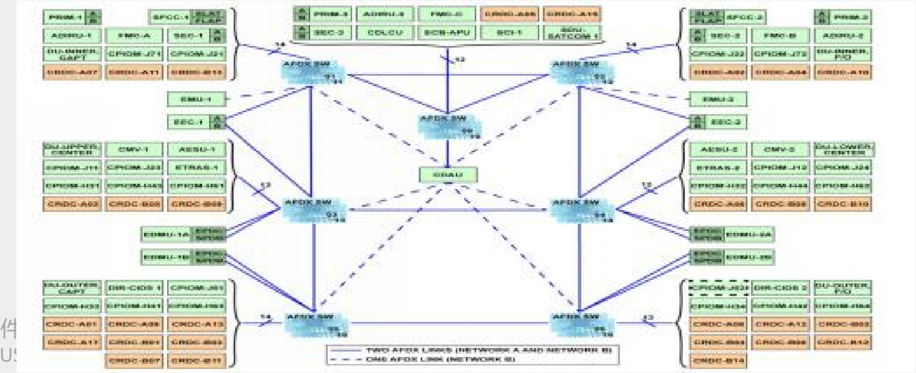
OMS

ISS



The Terrain page provides a means to inhibit the TAWS/GPWS functionality.

ACPS



Background

2.2 Avionics Safety Analysis Background

Abbreviation
FT: Fault Tree
CCA: Common Cause Analysis
MCS: Minimum Cut Set

Safety Analysis is Isolated from System Architecture

- Fault tree hierarchy depends on personal experience.
- Difficult to verify safety requirements of system architecture

Lack of Standardization in fault tree naming

- There are different naming rules for aircraft public resources.
- It is difficult to carry CCA of public resources;

FT cannot be created Automatically

- Fault tree is done manually,
- Relay on personal experience, subjective.
- Laborious and error-prone.

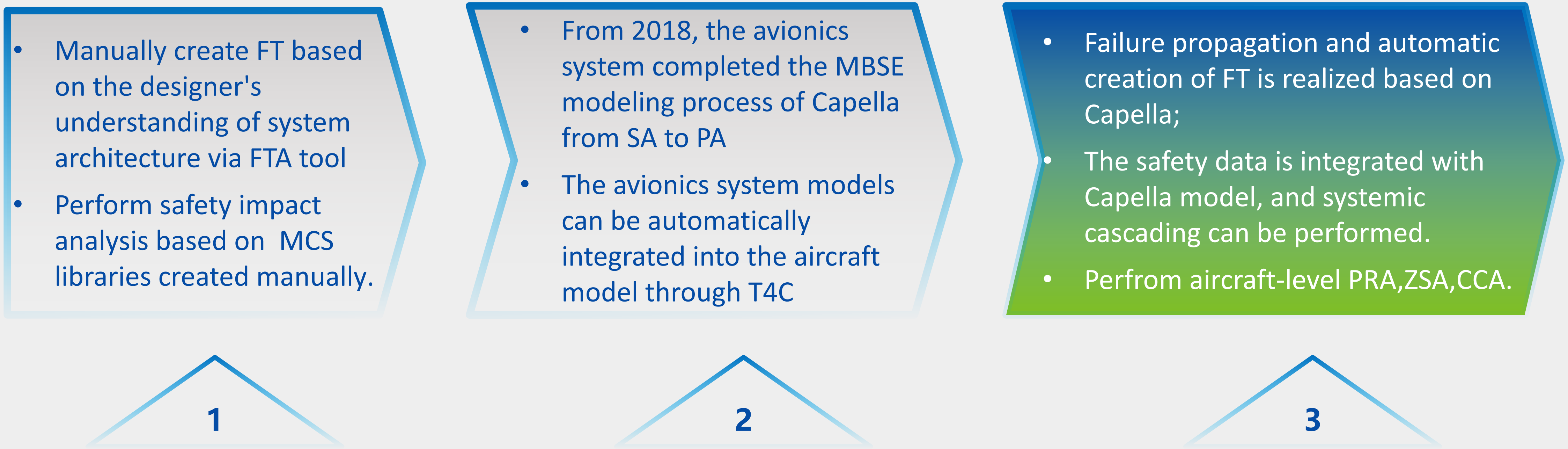
Safety impact analysis cannot be automated

- Manually create database for safety analysis based on MCSs
- Fault tree can‘t be integrated automatically, and systemic cascading impact analysis is time-consuming

Background

2.3 Practice of MBSA in SADRI(COMAC)

Abbreviation
FTA: Fault Tree Analysis
ZSA: Zonal Safety Analysis
PRA: Particular Risk Analysis



1

- Manually create FT based on the designer's understanding of system architecture via FTA tool
- Perform safety impact analysis based on MCS libraries created manually.

2

- From 2018, the avionics system completed the MBSE modeling process of Capella from SA to PA
- The avionics system models can be automatically integrated into the aircraft model through T4C

3

- Failure propagation and automatic creation of FT is realized based on Capella;
- The safety data is integrated with Capella model, and systemic cascading can be performed.
- Perfrom aircraft-level PRA,ZSA,CCA.

Background

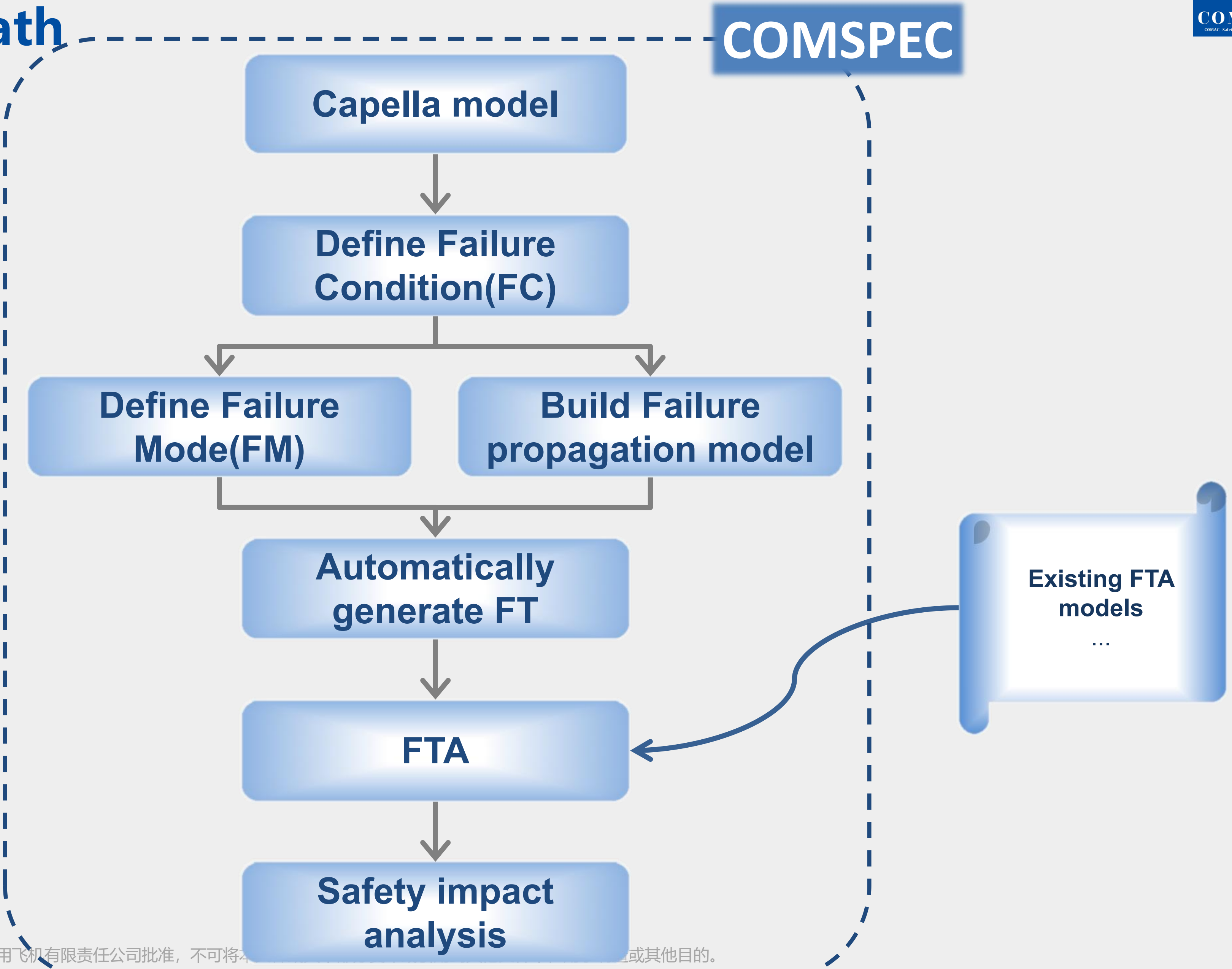
2.4 Our Technical Path

Safety Analysis is Isolated from System Architecture

Lack of standardization in fault tree naming

FT cannot be created Automatically

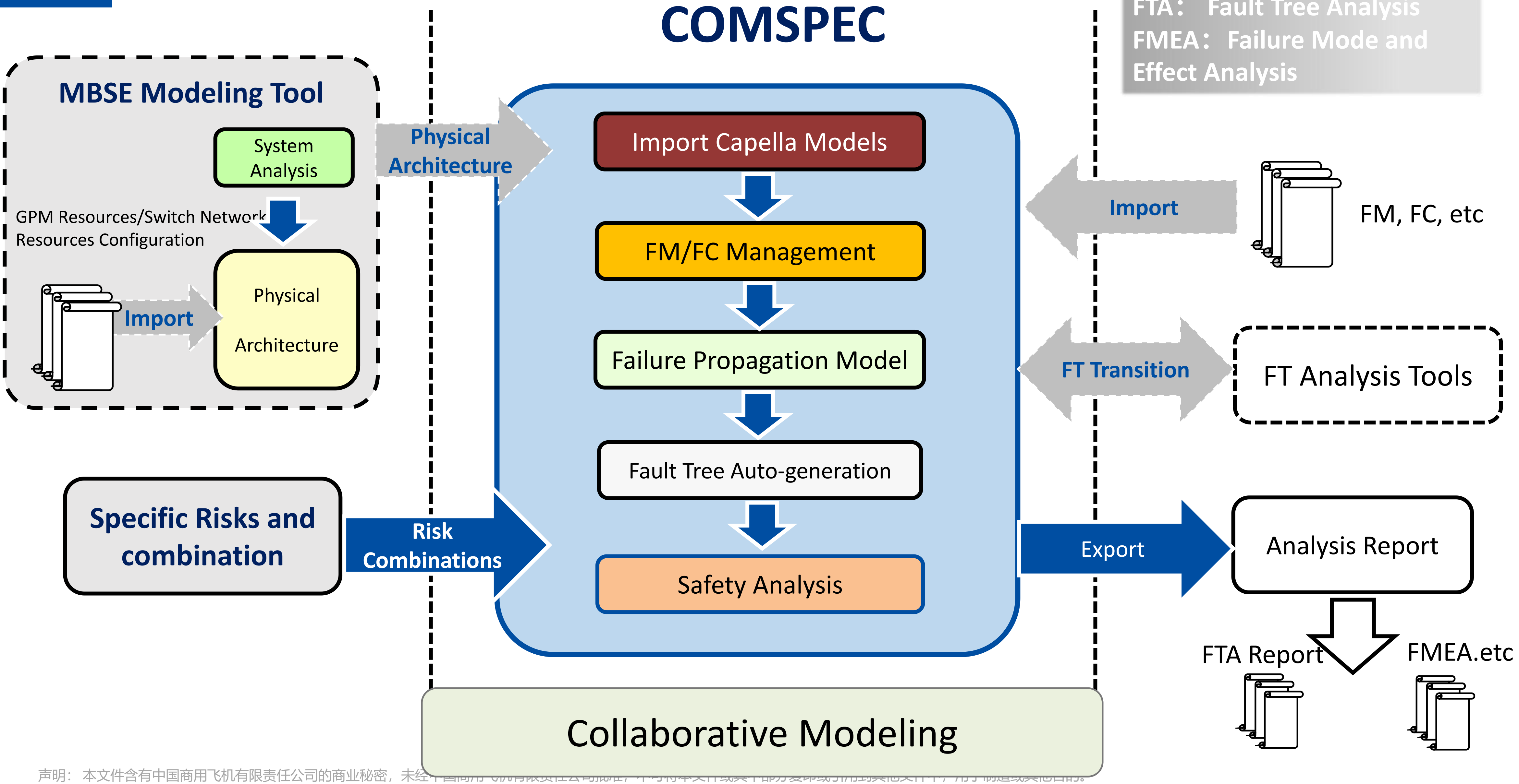
Safety impact analysis cannot be automated



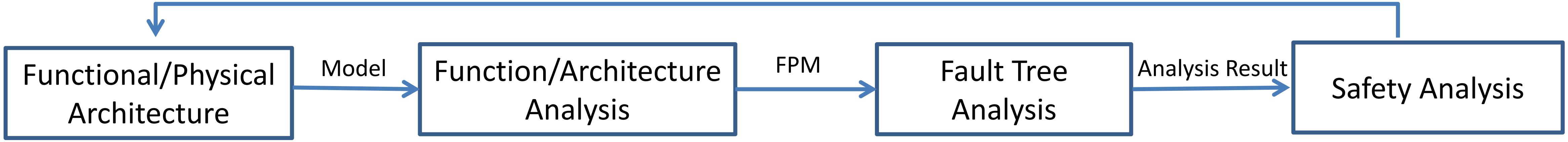
Introduction of the Avionics System Safety Analysis Platform

3.1 Overview

FM : Failure Modes
FC： Failure Conditions
FT： Fault Tree
FTA： Fault Tree Analysis
FMEA： Failure Mode and Effect Analysis



3.2 MBSA analysis process based on MBSE modeling



Functional/Physical Architecture

Model

Function/Architecture Analysis

FPM

Fault Tree Analysis

Analysis Result

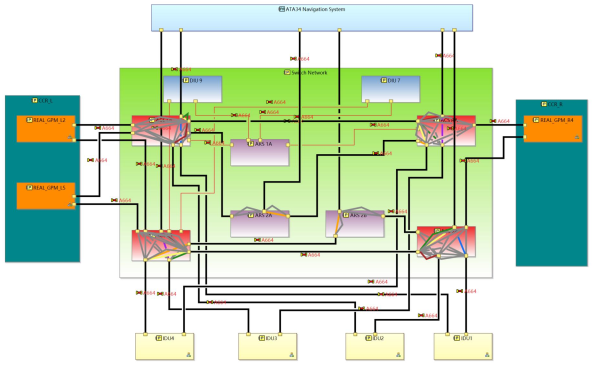
Safety Analysis

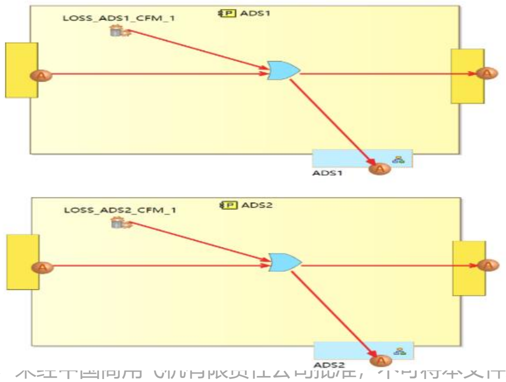
- Model the functional architecture of each system hierarchically;
- Model functions and interfaces redundancies;
- Model the actual physical architecture.

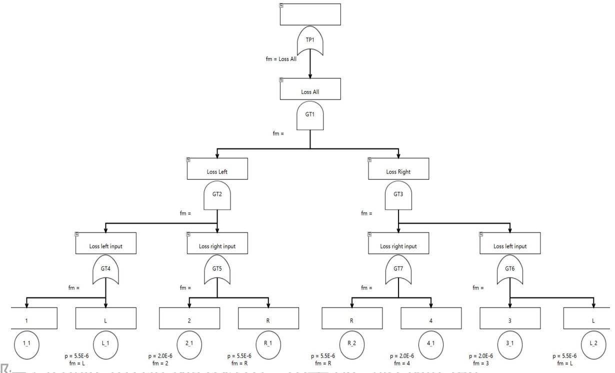
- Define both internal Failure Modes(FM) and interface Failure Modes;
- Define propagation links and logical relationships of each Failure Mode;
- Define Failure Conditions (FC) and allocate FMs to FCs.

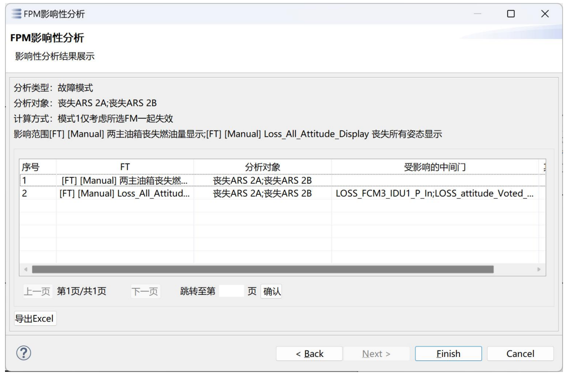
- Auto-generate Fault Tree based on Failure Propagation Models (FPM)
- Qualitative and quantitative analysis of Fault Trees;
- Auto-generate the Safety analysis database of the whole aircraft.

- Automate single point failure, combined failure, common cause, and cascade analysis
- Use analysis results to identify the physical architecture and safety requirements.









FPM影响性分析

影响性分析结果展示

分析类型：故障模式

分析对象：丧失ARS 2A;丧失ARS 2B

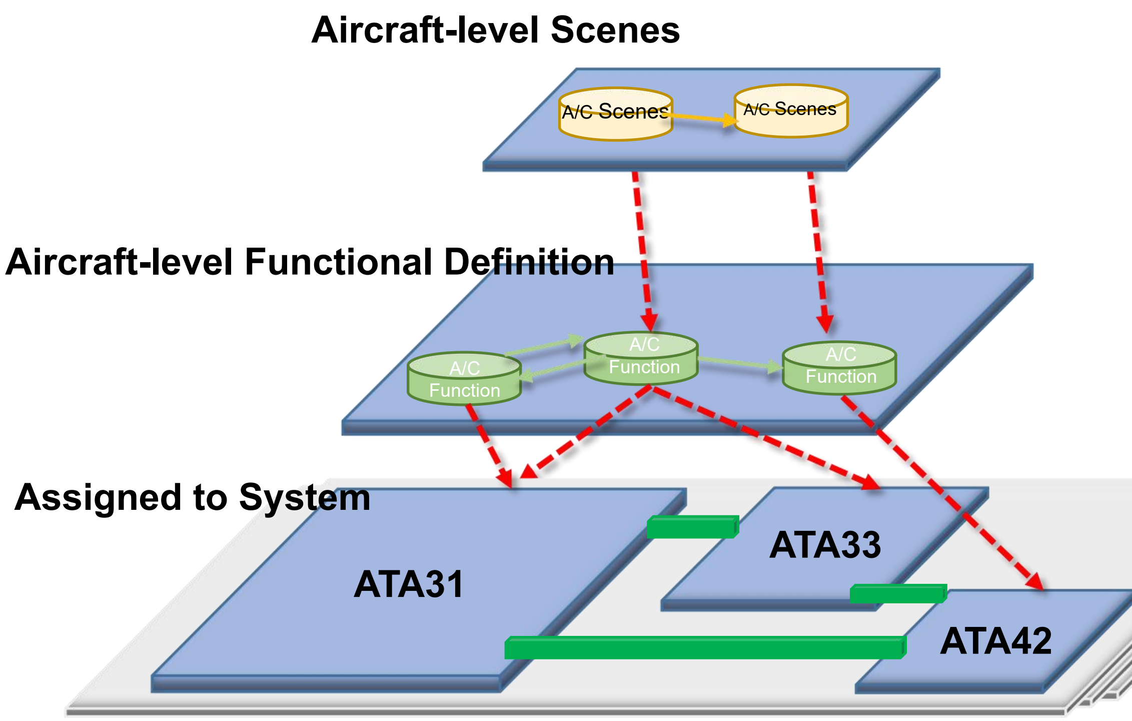
计算方式：模式1仅考虑所选FM一起失效

影响范围[FT] [Manual] 两主油箱丧失燃油量显示;[FT] [Manual] Loss_All_Attitude_Display 丧失所有姿态显示

序号	FT	分析对象	受影响的中间门
1	[FT] [Manual] 两主油箱丧失燃...	丧失ARS 2A;丧失ARS 2B	
2	[FT] [Manual] Loss_All_Attitud...	丧失ARS 2A;丧失ARS 2B	LOSS_FCM3_IDU1_P_In;LOSS_attitude_Voted_...

3.3 Functional and Physical Architecture

System Engineering Process	
Need	Aircraft-level Design
Function	
Requirement	
Product	

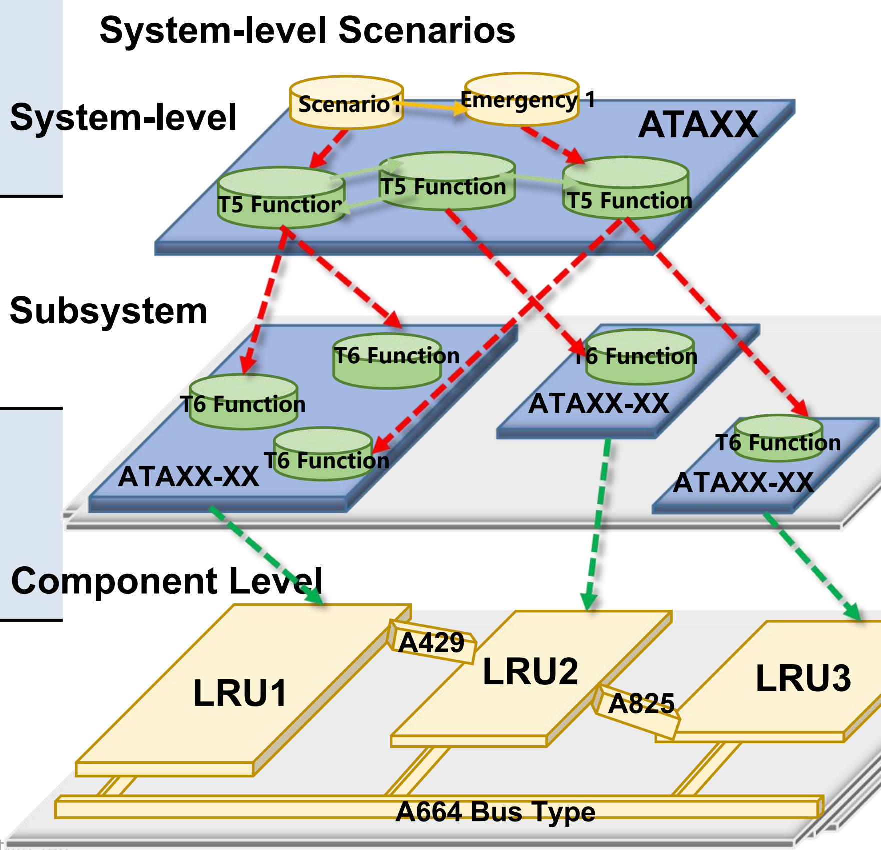


3.3 Functional and Physical Architecture

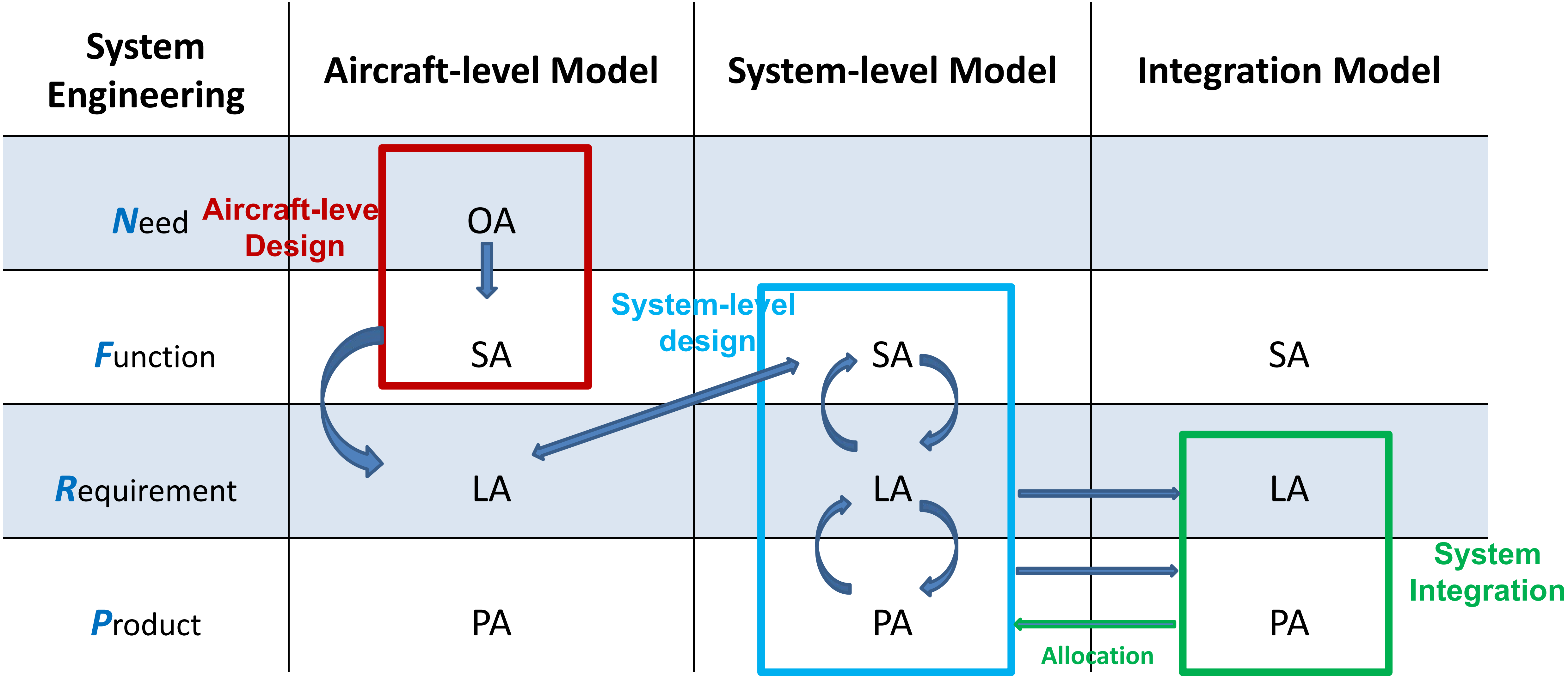
System Engineering Process	Aircraft Model	System-level Model
Need	OA	
Function	SA	SA
Requirement	LA	LA
Product	PA	PA

Aircraft-leve Design

System-level design



3.3 Functional and Physical Architecture



System Engineering	Aircraft-level Model	System-level Model	Integration Model
*N*eed	OA		
*F*unction	SA	SA	SA
*R*equirement	LA	LA	LA
*P*roduct	PA	PA	PA

Aircraft-level Design

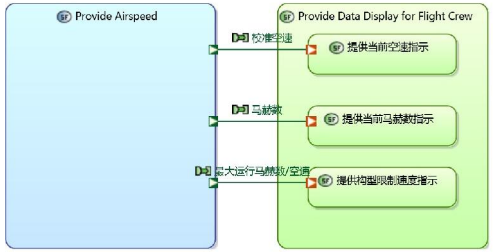
System-level design

System Integration

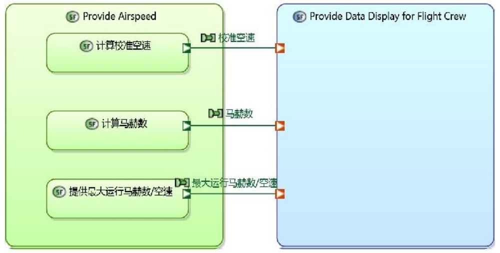
Allocation

3.3 Functional and Physical Architecture

System Analysis：
Cross-model, Real-Time collaborative modeling

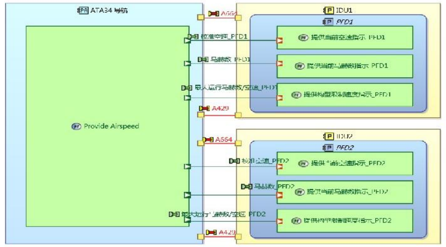


Project 1:Indication and Recording System

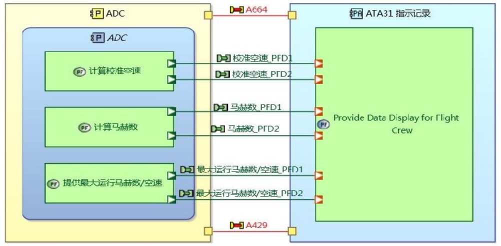


Project 2:Navigation System

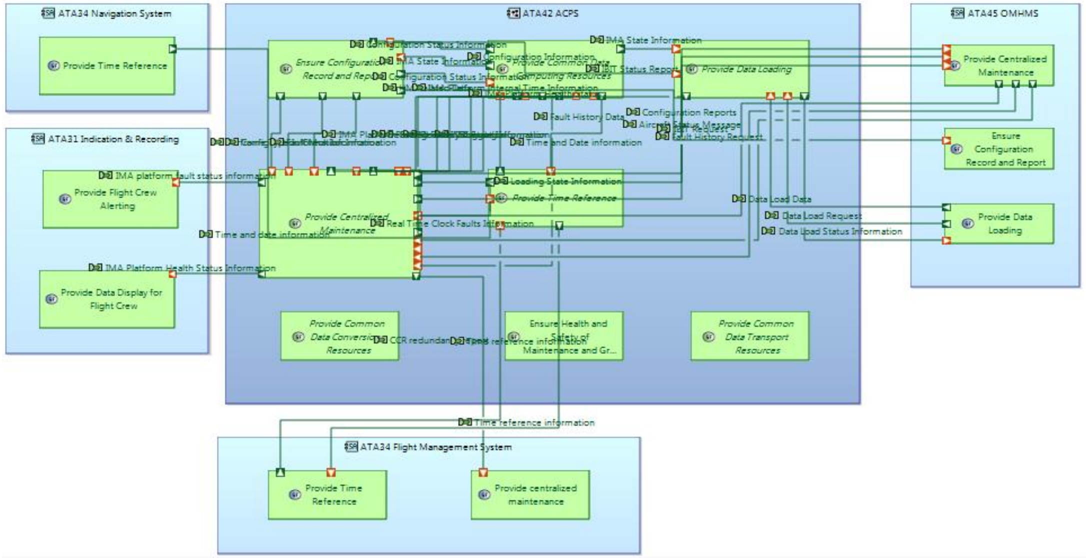
Physical Architecture Modeling:
Cross-model, Real-Time Collaboration modeling

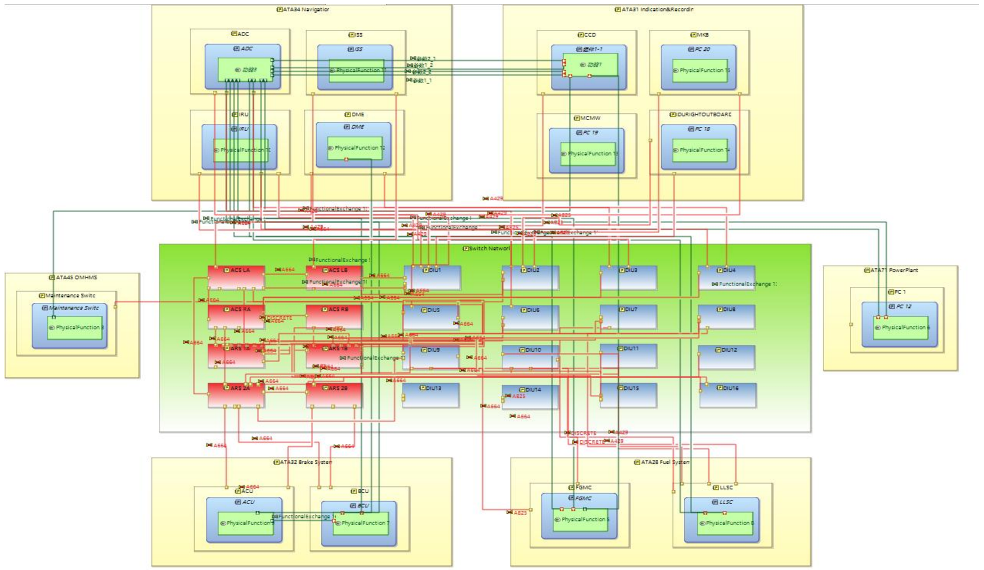


Project 1:Indication and Recording System



Project 2: Navigation System

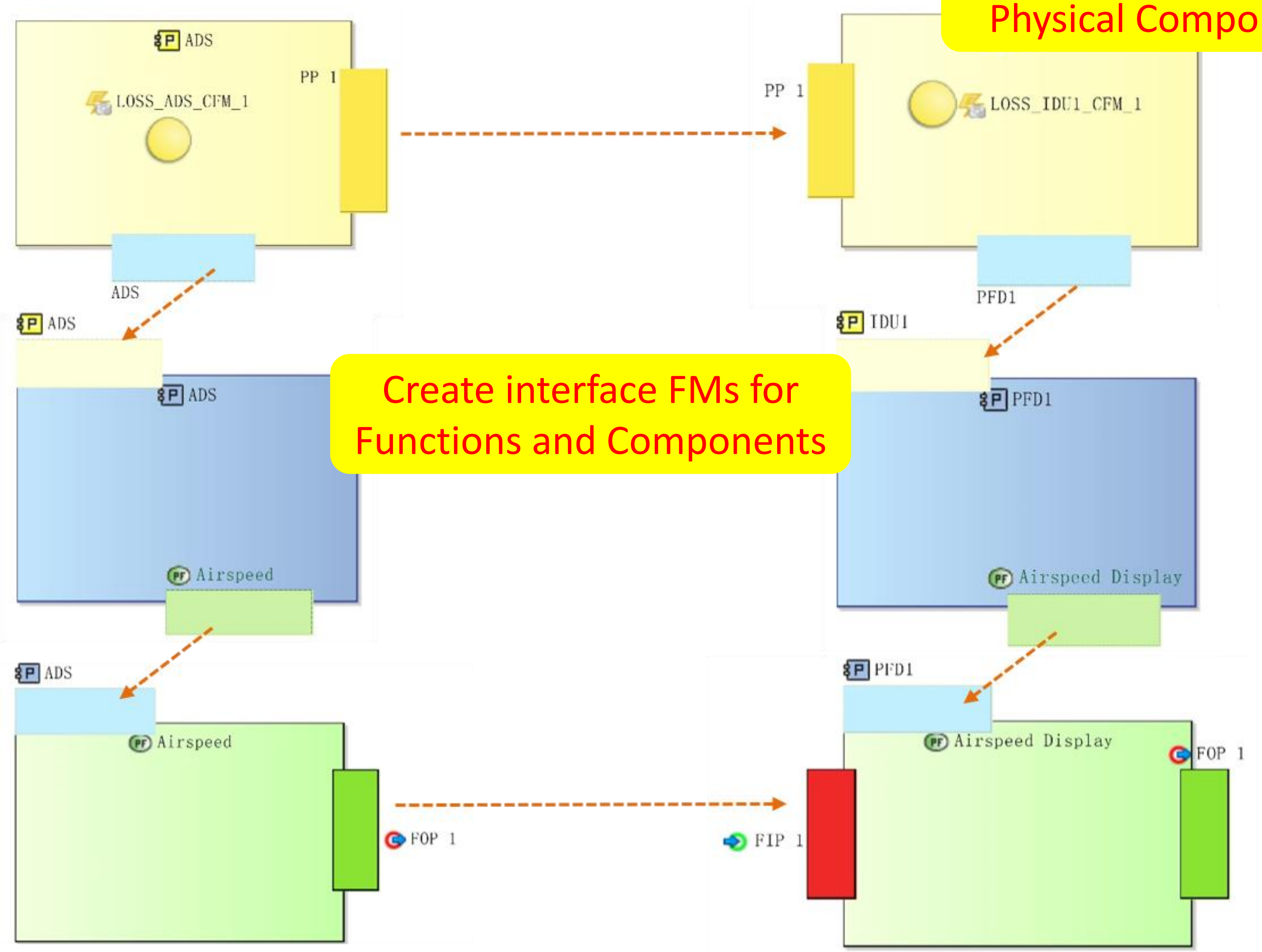

ATA34 Navigation System
Provide Time Reference
ATA31 Indication & Recording
Provide Flight Crew Alerting
Provide Data Display for Flight Crew
IMA platform fault status information
IMA Platform Health Status Information
Time and date information
ATA42 ACPS
Ensure Configuration Record and Report
Provide Common Computing Resources
Provide Data Loading
Provide Centralized Maintenance
Provide Time Reference
Provide Common Data Conversion Resources
Ensure Health and Safety of Maintenance and Gr...
Provide Common Data Transport Resources
Configuration Status Information
IMA State Information
Configuration Information
IBIT Status Report
Internal Time Information
Fault History Data
Configuration Reports
Aircraft Status Message
IBIT Request
Fault History Request
Time and Date information
Loading State Information
Real Time Clock Faults Information
Data Load Data
Data Load Request
Data Load Status Information
CCR redundancy
Time reference information
ATA45 OMHMS
Provide Centralized Maintenance
Ensure Configuration Record and Report
Provide Data Loading
ATA34 Flight Management System
Provide Time Reference
Provide centralized maintenance



FM : Failure Modes
FPM: Failure Propagation Model

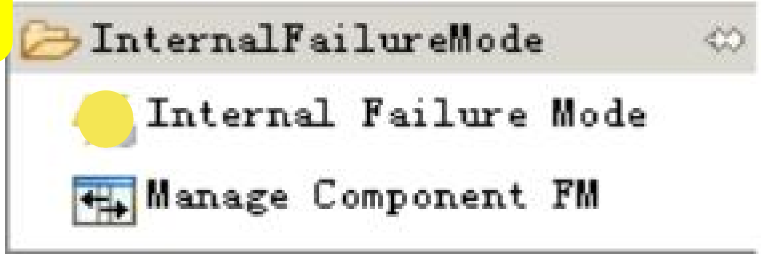
3.4 Functional/Physical Architecture Analysis—FM Management

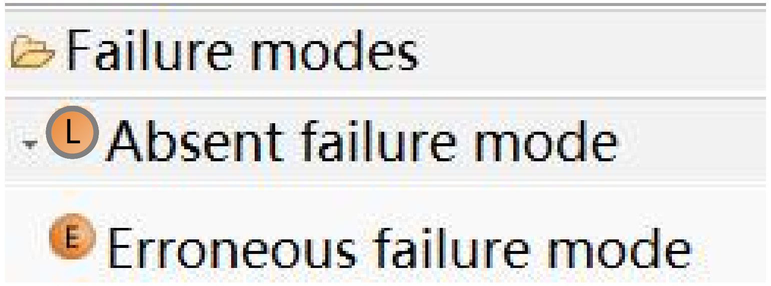
- Create functional/component FM via FPM diagram



Create Internal FMs for Physical Components

Create interface FMs for Functions and Components

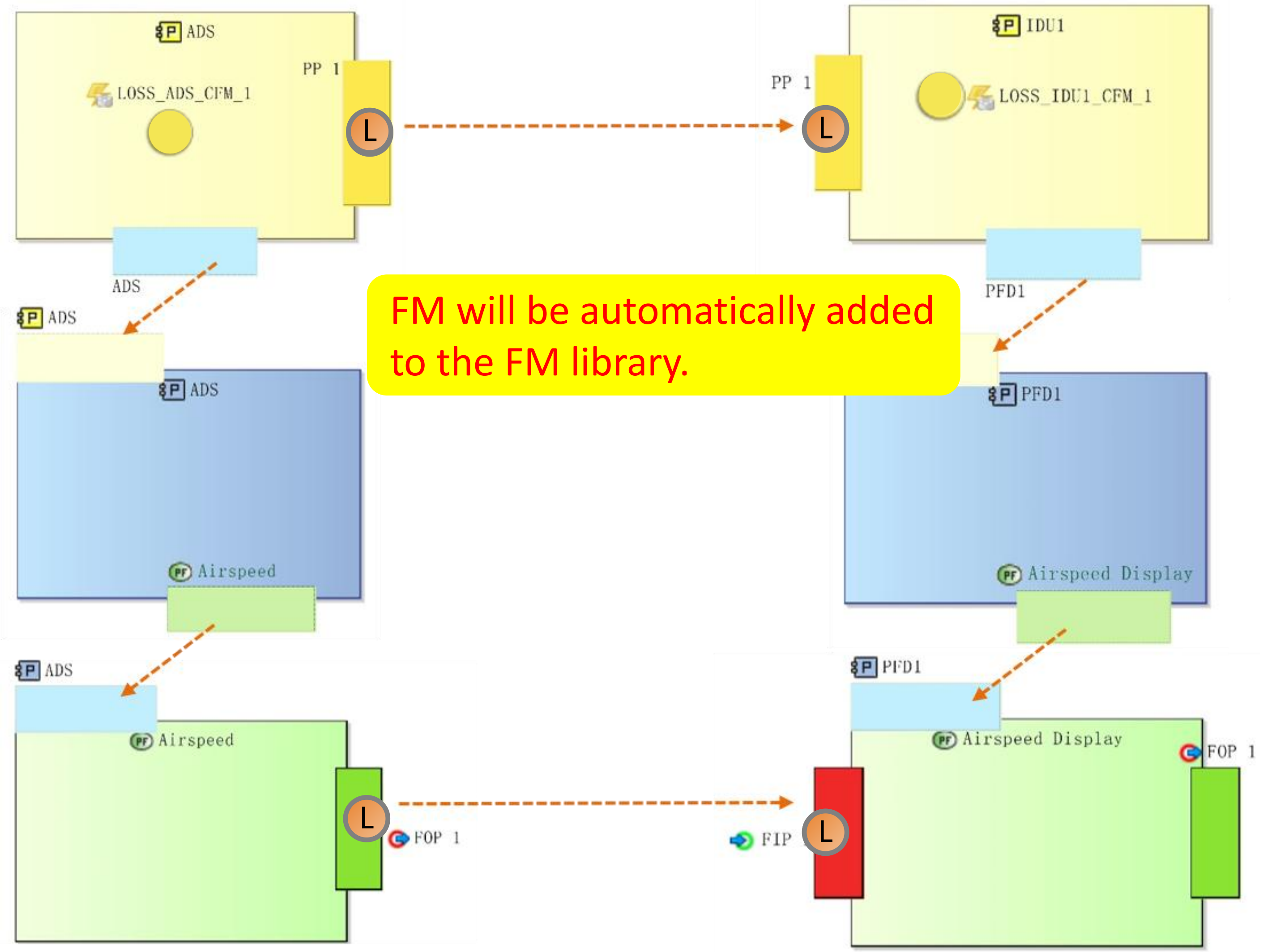




FM : Failure Modes

3.4 Functional/Physical Architecture Analysis—FM Management

- Failure modes are automatically added to the FM library.



FM will be automatically added to the FM library.

Failure Mode Lib

LOSS Component Interface 1

LOSS Component Interface 2

LOSS Function 4

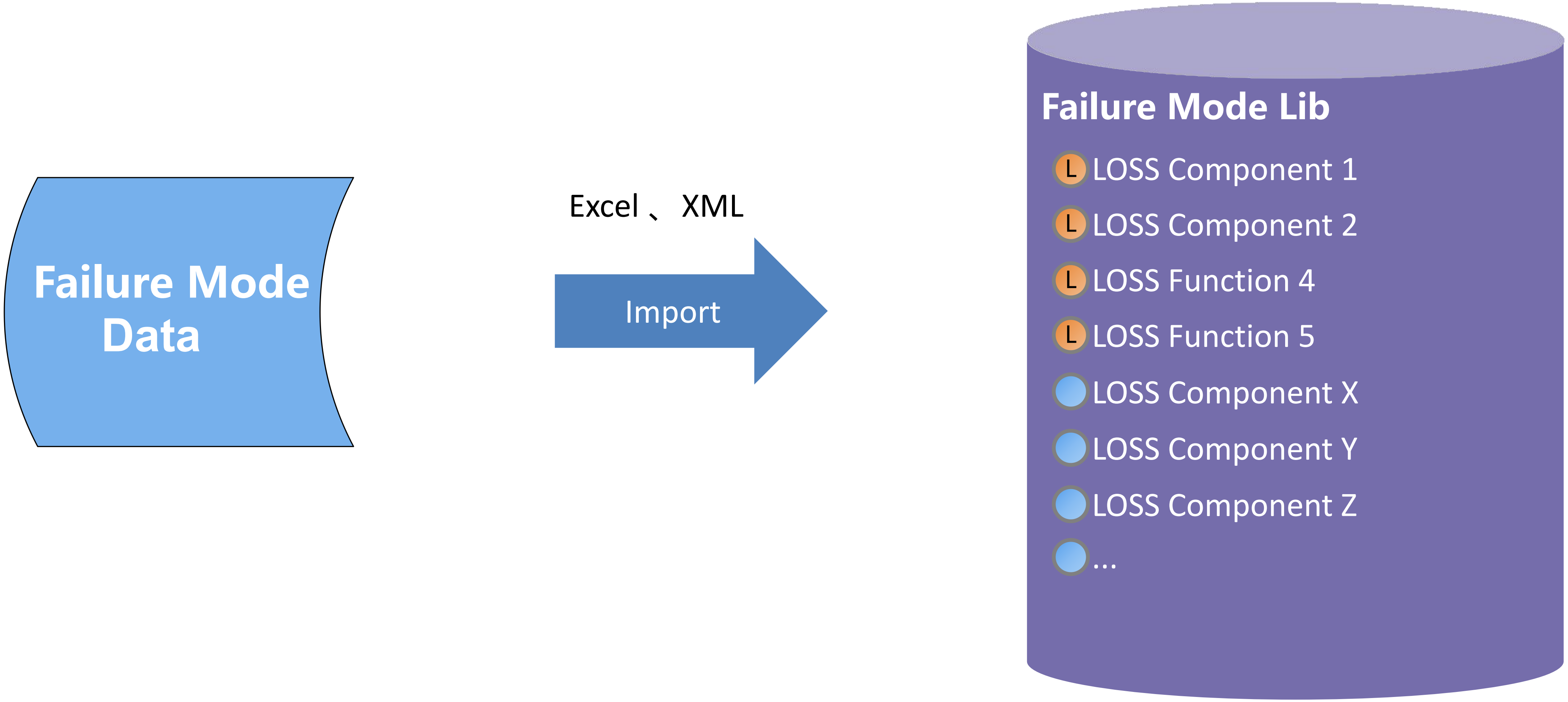
LOSS Function 5

LOSS Component 1

LOSS Component 2

3.4 Functional/Physical Architecture Analysis—FM Management

- Import Component FM to the MBSA tool

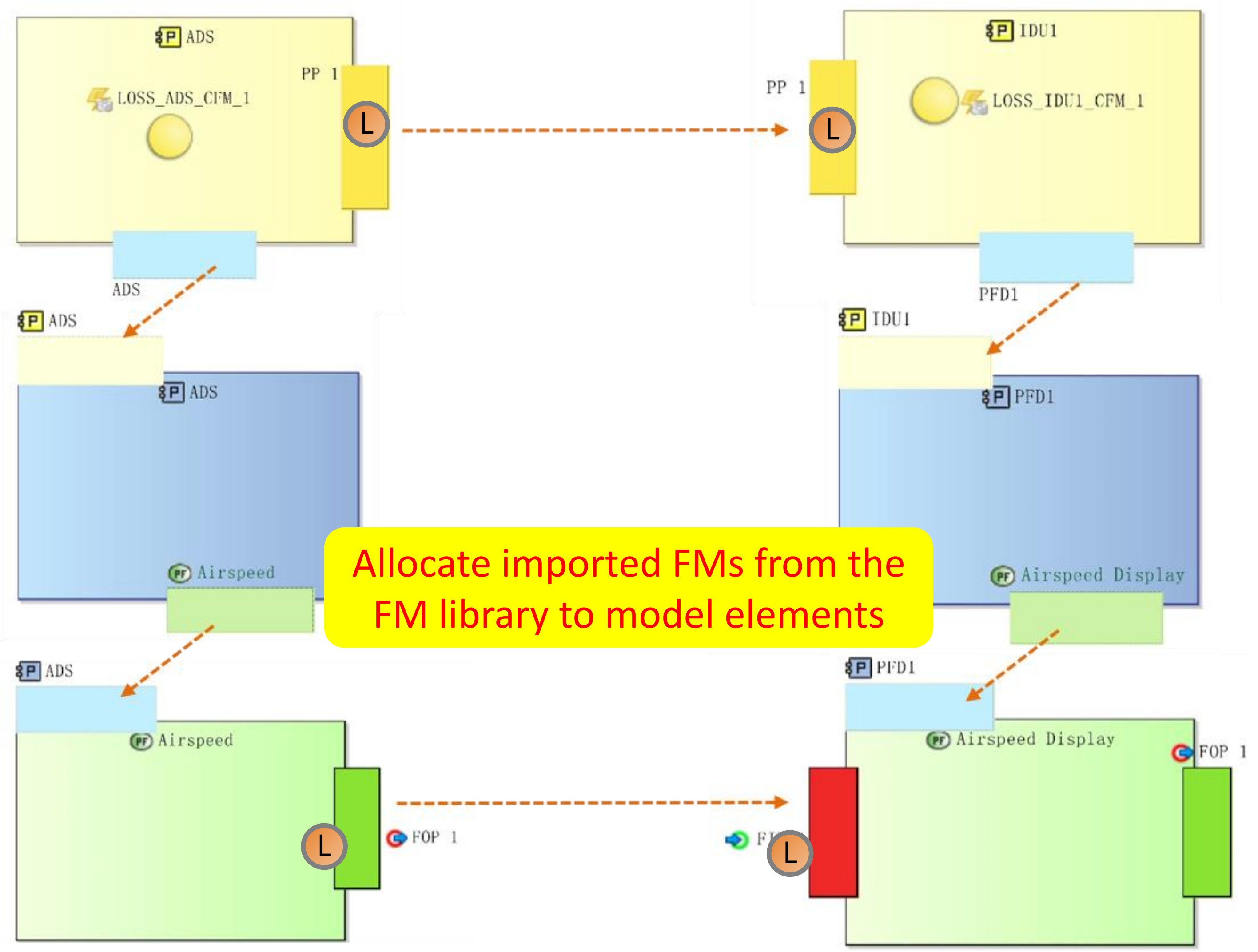


MBSA Modeling Process

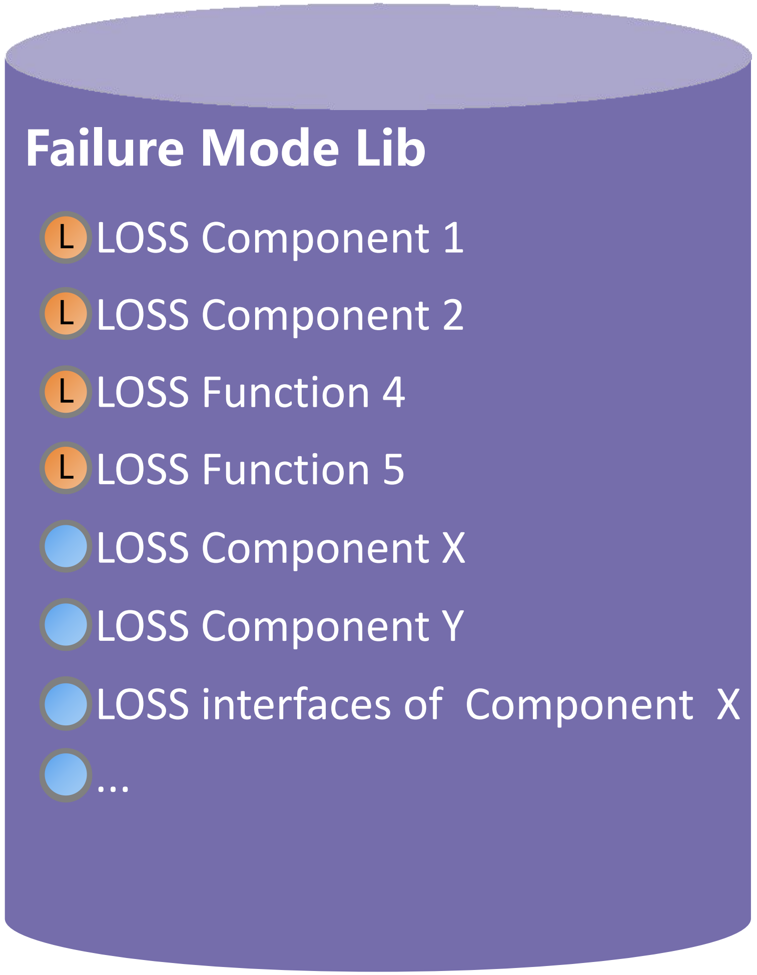
FM : Failure Modes

3.4 Functional/Physical Architecture Analysis—FM Management

- Allocate the imported FM to the physical components



Allocate imported FMs from the FM library to model elements



Failure Mode Lib

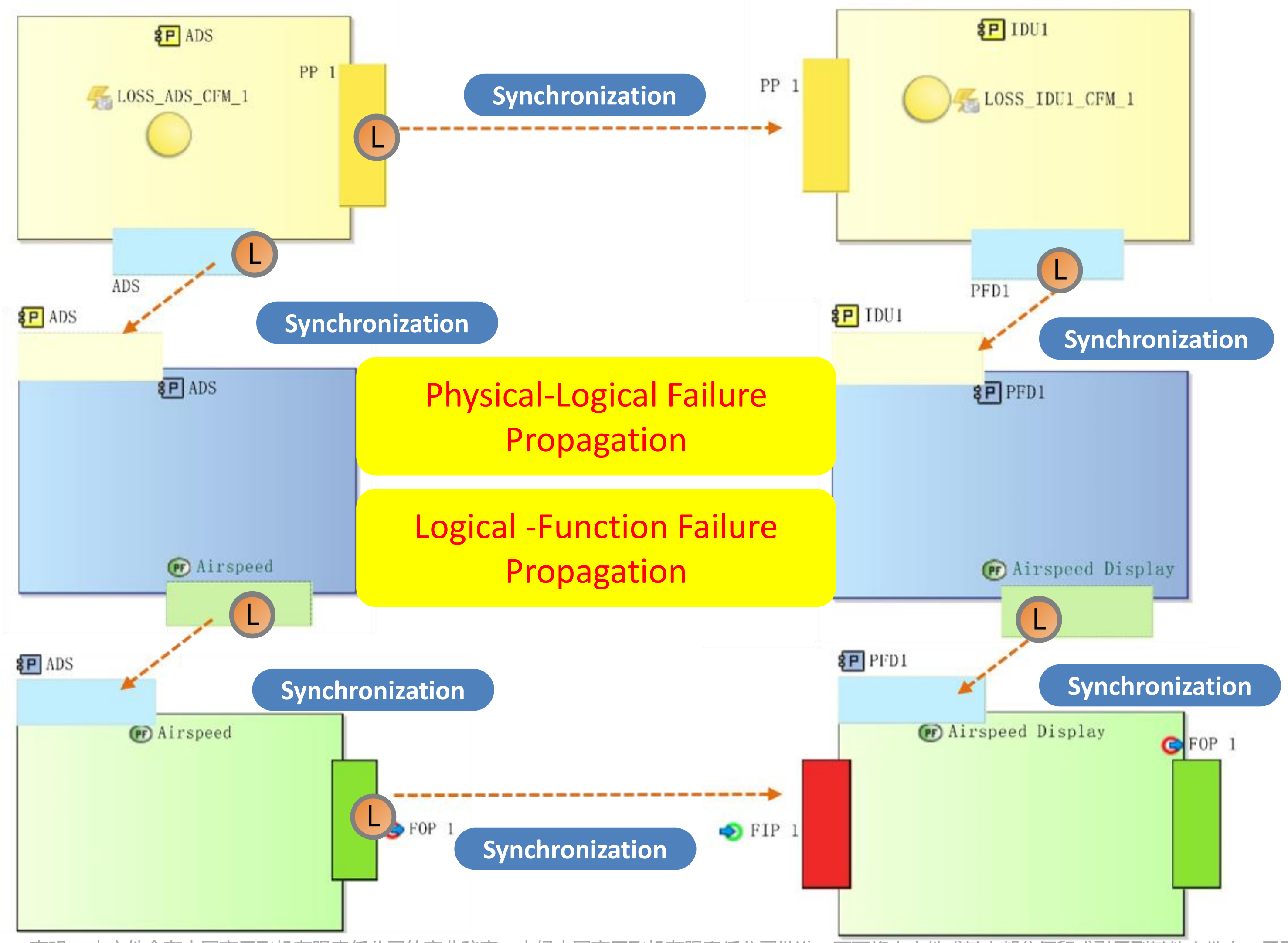
- L LOSS Component 1
- L LOSS Component 2
- L LOSS Function 4
- L LOSS Function 5
- ● LOSS Component X
- ● LOSS Component Y
- ● LOSS interfaces of Component X
- ● ...

MBSA Modeling Process

FPM: Failure Propagation Model

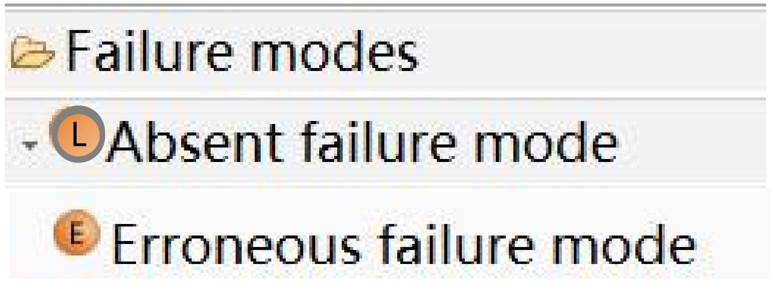
3.5 Functional/Physical Architecture Analysis——FPM

- Physical-Logical-Functional Failure Propagation



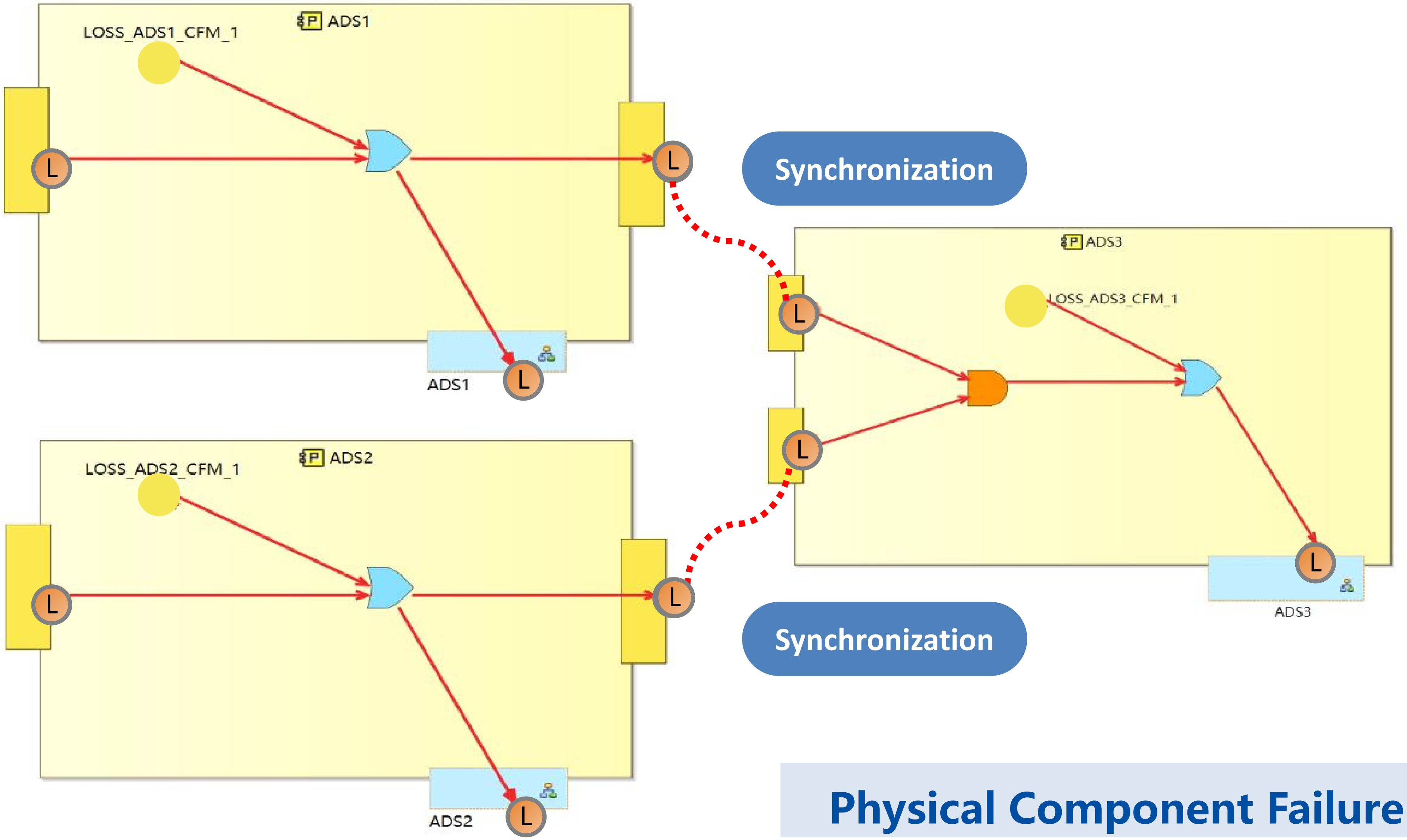
Physical-Logical Failure Propagation

Logical -Function Failure Propagation



Failure modes
- L Absent failure mode
- E Erroneous failure mode

3.5 Functional/Physical Architecture Analysis——FPM



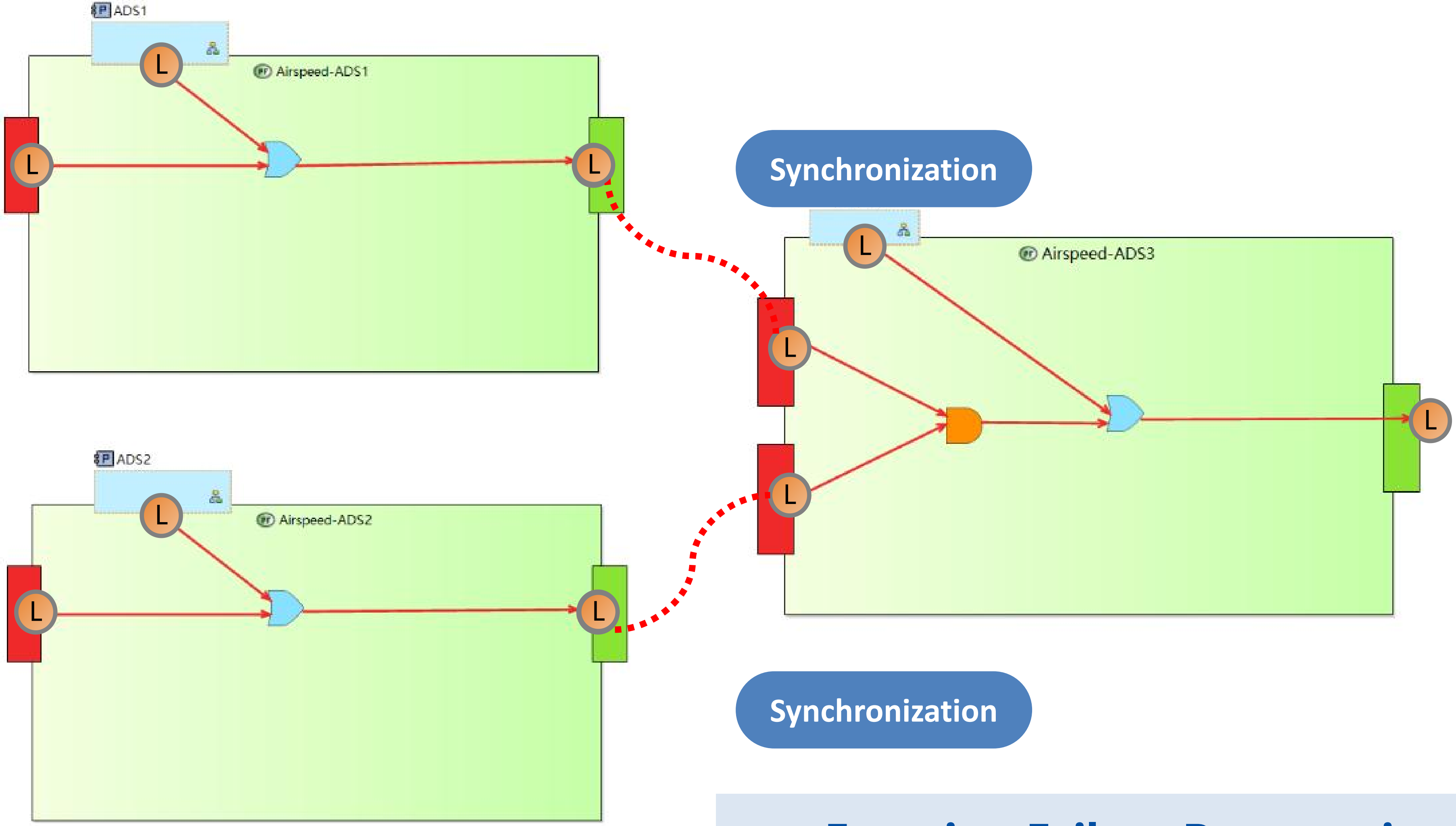
Synchronization

Synchronization

Physical Component Failure Propagation

FPM: Failure Propagation Model

3.5 Functional/Physical Architecture Analysis——FPM



Synchronization

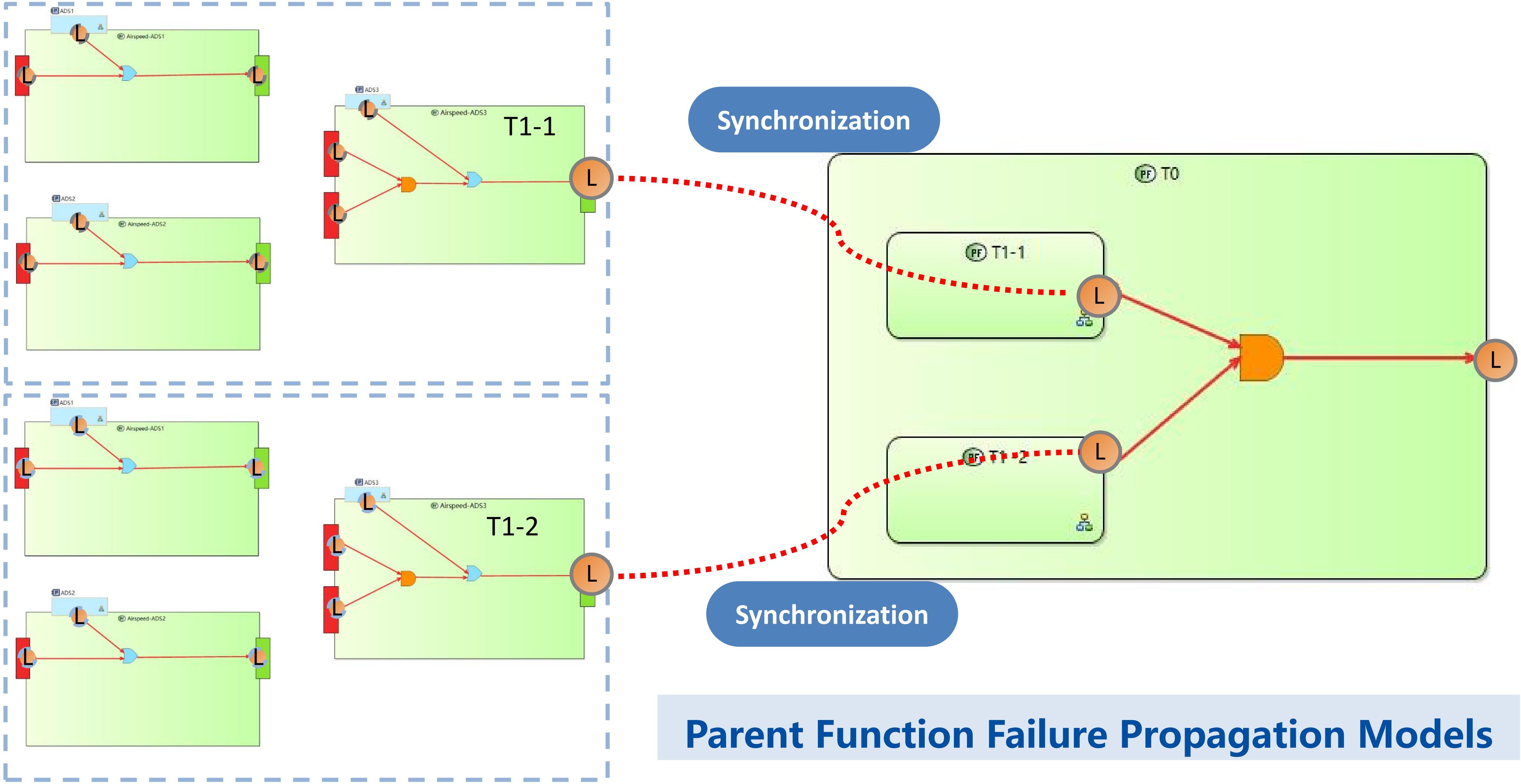
Synchronization

Function Failure Propagation Models

FPM: Failure Propagation Model

COMSPEC

3.5 Functional/Physical Architecture Analysis——FPM

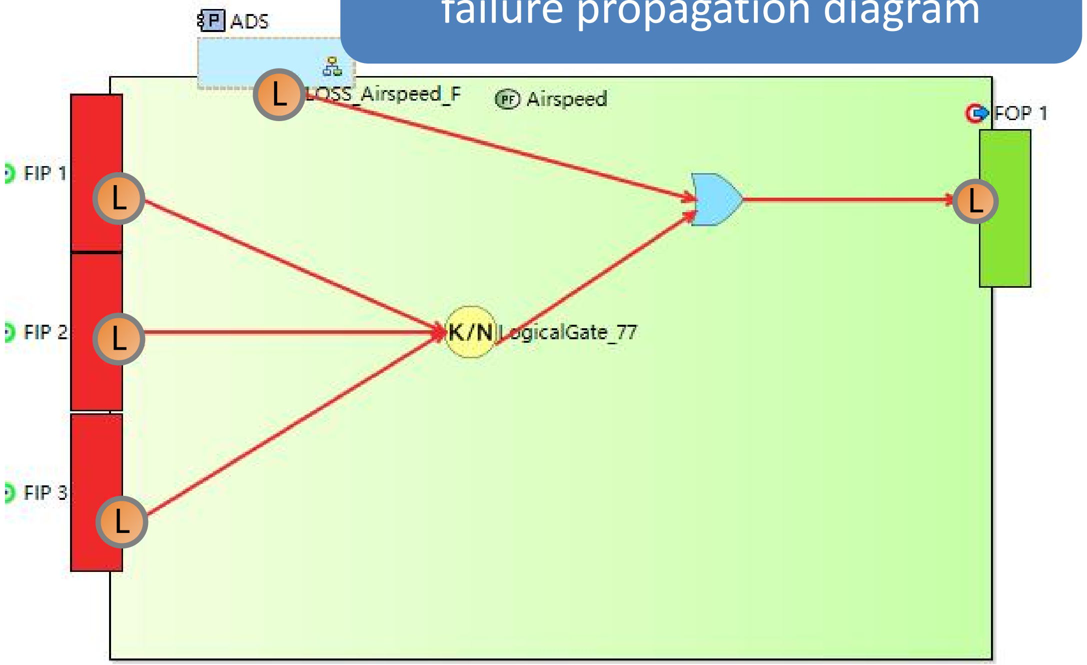


Parent Function Failure Propagation Models

3.5 Functional/Physical Architecture Analysis——FC Management

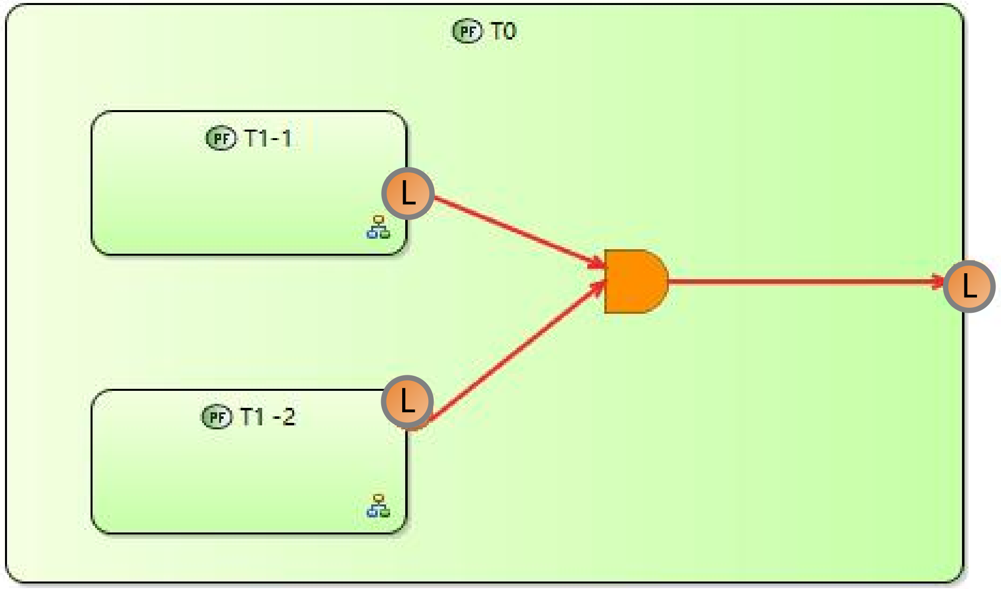
- Define the occurrence conditions of the FC

Allocate FC to FMs in the function failure propagation diagram



🟠 [FC]LOSS the Left Redundancy

Allocate FC to FMs in the parent function failure propagation diagram

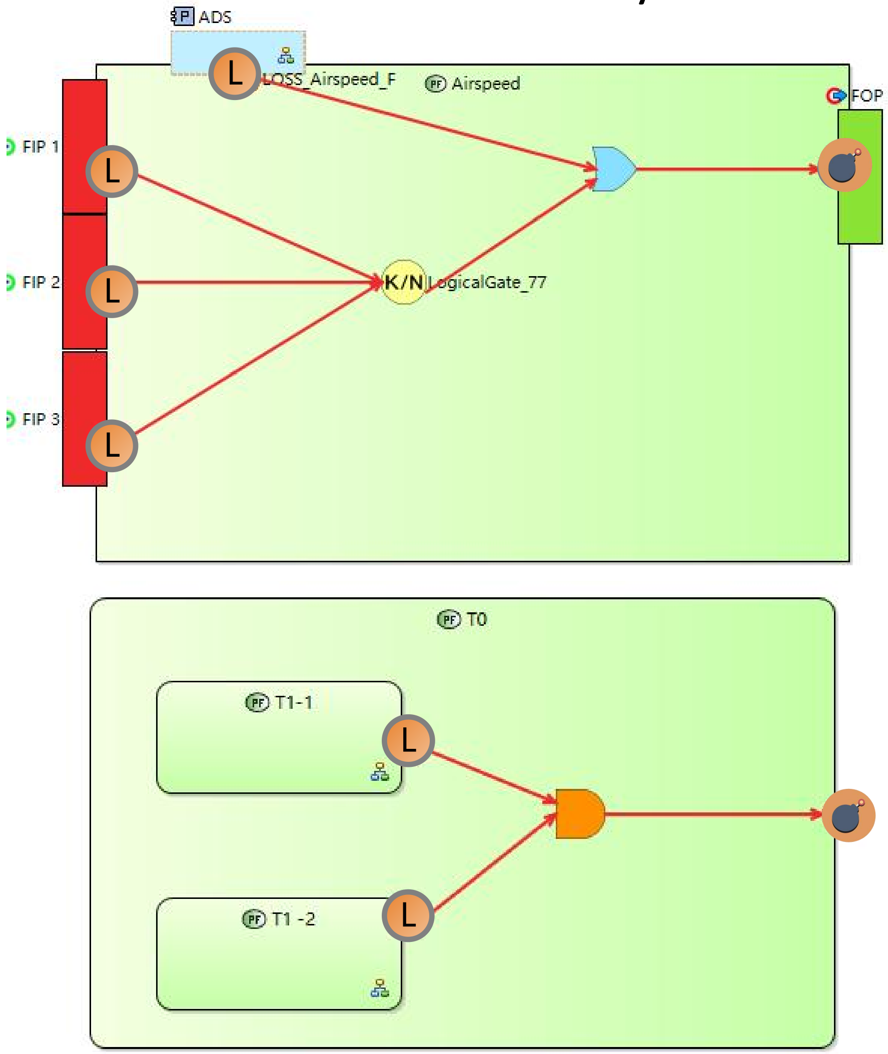


🟠 [FC]LOSS All Redundancies

FC: Failure Conditions

3.5 Functional/Physical Architecture Analysis——FC Management

- All FCs will be stored in the FC library.



Failure Condition Lib

[FC]Loss of the left redundancy

[FC] Loss all redundancies

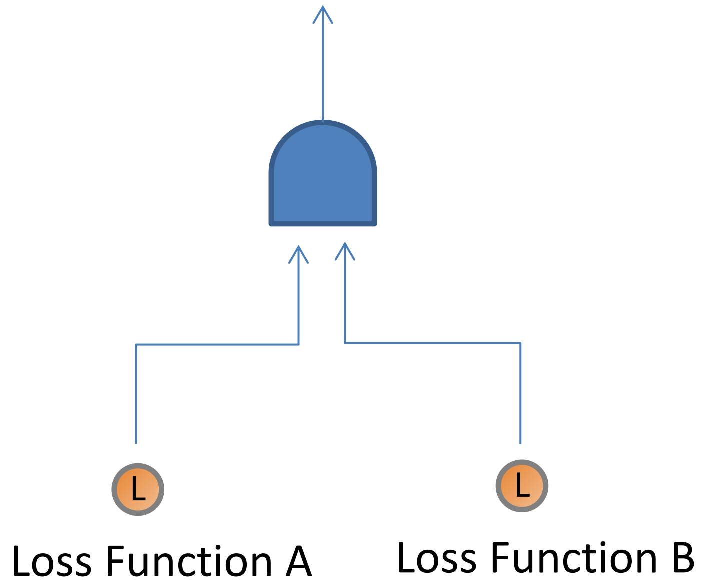
MBSA Modeling Process

3.5 FT Analysis

FM : Failure Modes
FC： Failure Conditions
FT： Fault Tree
FPM: Failure Propagation Model

COMSPEC

- The FC establishes failure logical propagation relationships with multiple functional FMs.
  - The MBSA tool will create a complete FT based on FPM



Failure Condition Lib

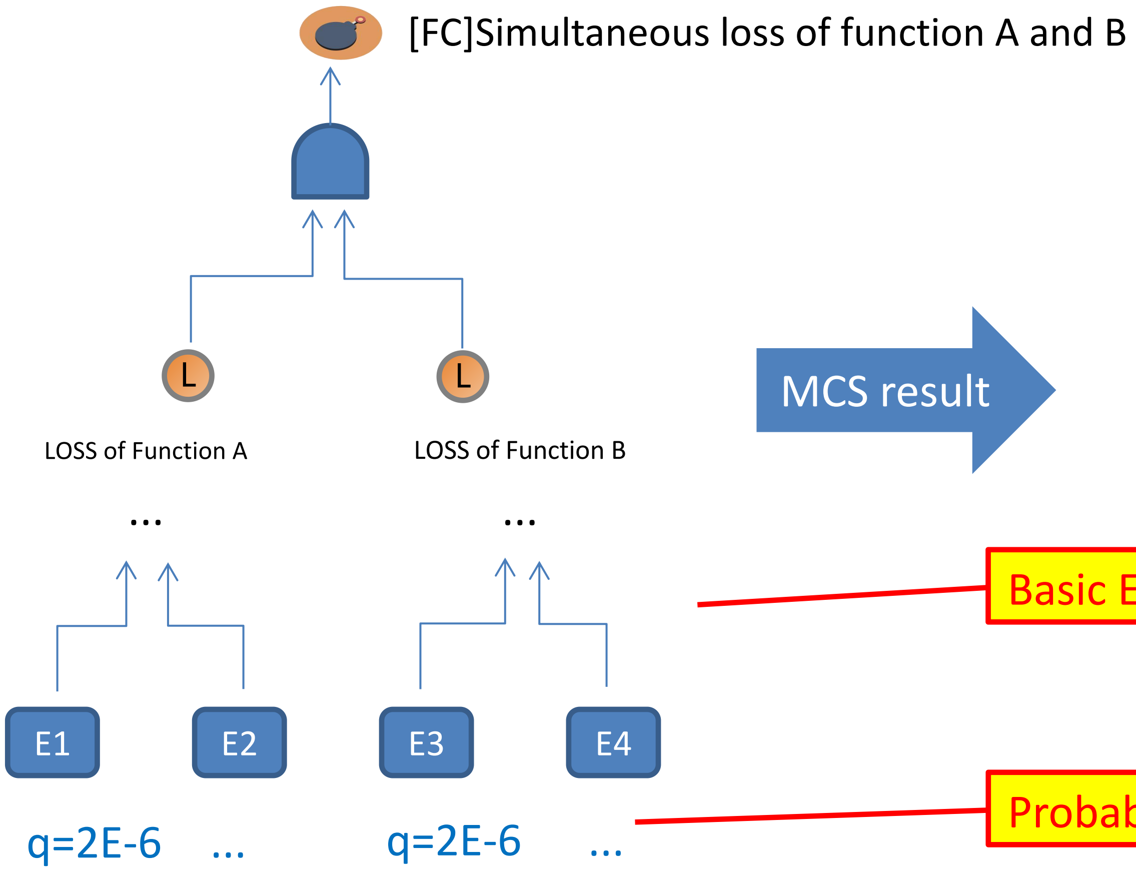
- [FC]Loss of the left redundancy
- [FC]Loss all redundancies
- [FC]Simultaneous loss of function A and B

MBSA Modeling Process

3.5 FT Analysis

FC： Failure Conditions
FT： Fault Tree
MCS: Minimum Cut Set

- Generate a fault tree from the selected FC
- Calculate the minimum cut sets of the FC



MCS result

Failure Condition Lib

No.	MCS	Q
1	E1， E3	2E-6
2	E1， E4	2.1E-7
3	E2， E4	3E-8
...	...	...

Basic Ev

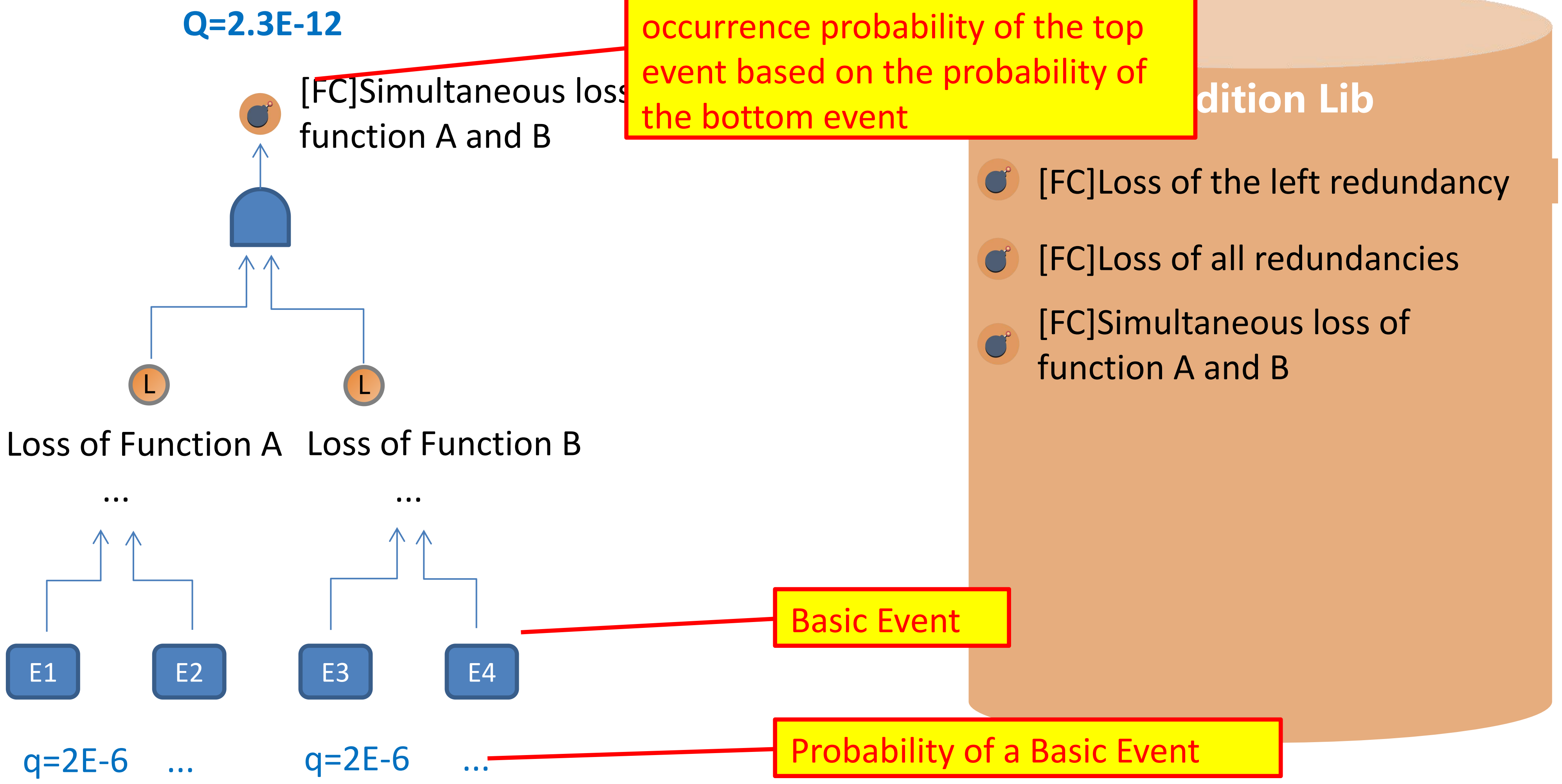
Probability of a basic event

MBSA Modeling Process

3.5 FT Analysis

FC： Failure Conditions
FT： Fault Tree
MCS: Minimum Cut Set

- Calculate the occurrence probability of the top event, and verify whether the occurrence probability is consistent with the safety impact



MBSA automatically calculates the occurrence probability of the top event based on the probability of the bottom event

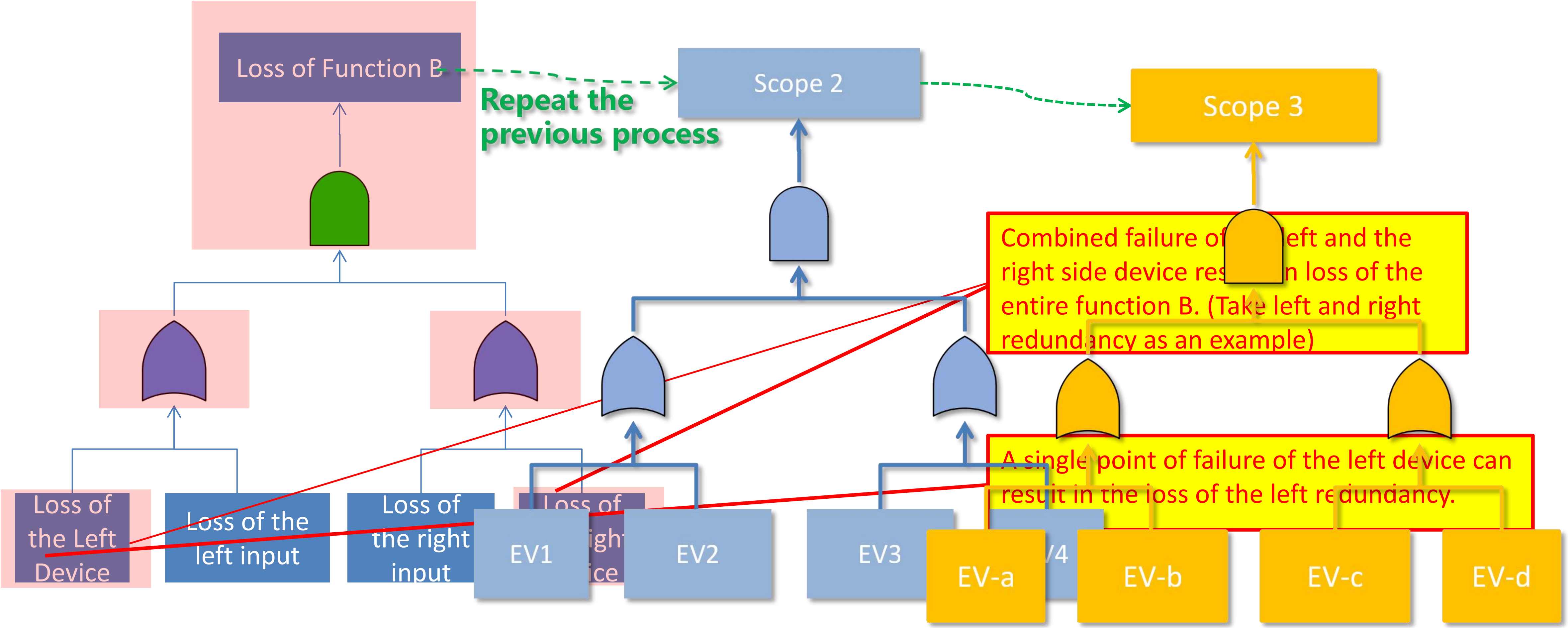
Basic Event

Probability of a Basic Event

MBSA Modeling Process

3.6 Safety Analysis

- Analyze the impact of particular failure sources at a specific scale .



Combined failure of the left and the right side device results in loss of the entire function B. (Take left and right redundancy as an example)

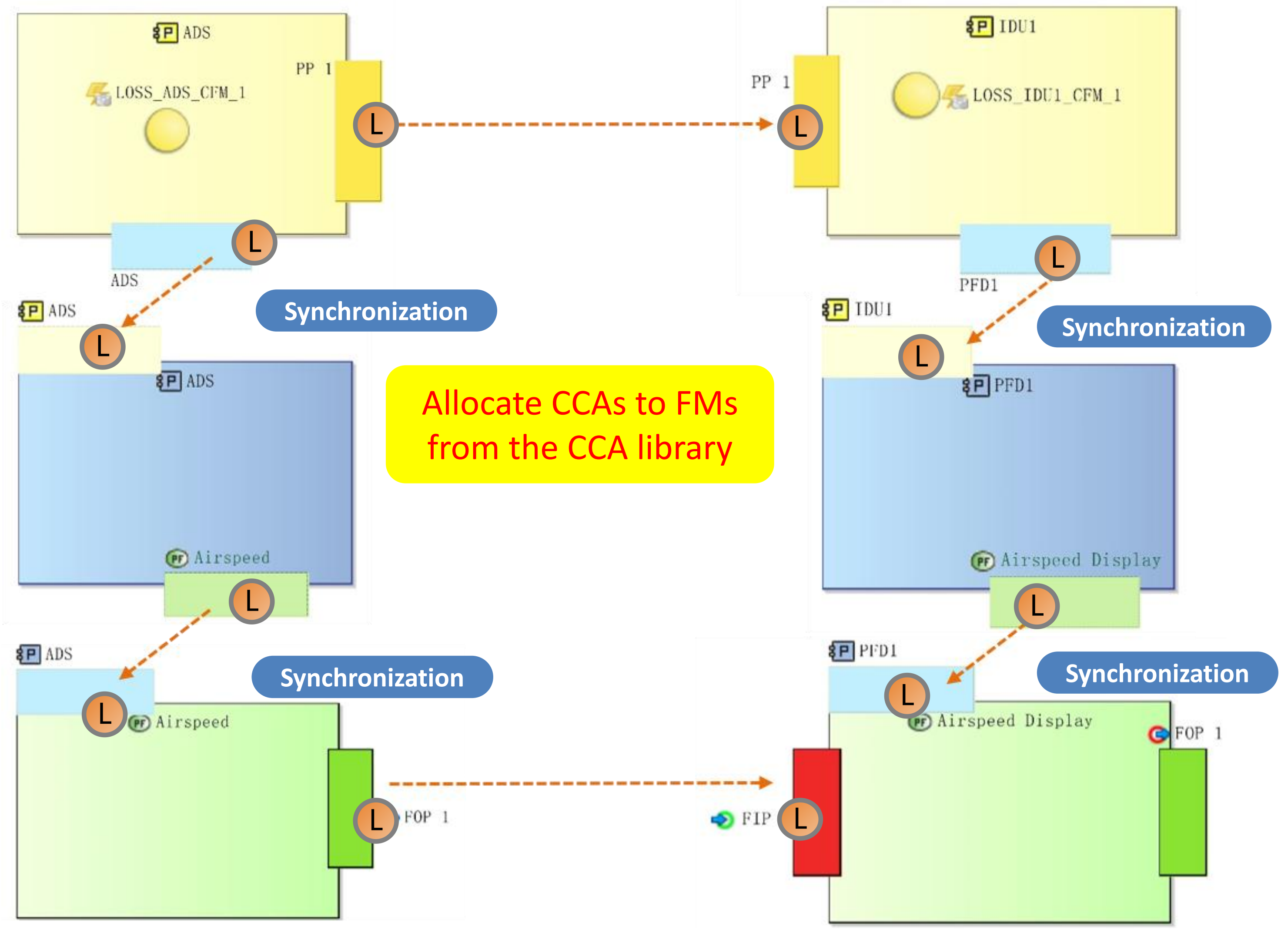
A single point of failure of the left device can result in the loss of the left redundancy.

MBSA Modeling Process

3.6 Safety Analysis

CCA： Common Cause Analysis
FM : Failure Modes

- Allocate Common Cause Sources to Physical Components



Synchronization

Synchronization

Allocate CCAs to FMs from the CCA library

Synchronization

Synchronization

Define CCA

Common Cause Lib

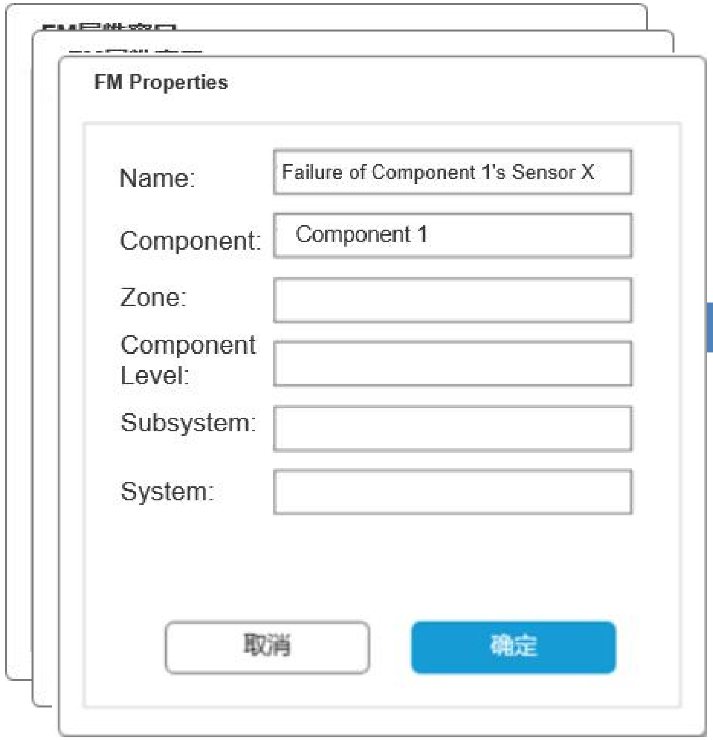
- C Same Supplier
- C Same Manufacturing
- C …
- C …

MBSA Modeling Process

3.6 Safety Analysis

FPM: Failure Propagation Model
FM： Failure Mode

- Fill in Component FM’s properties
- Manage FM based on properties



FM Properties

Name: Failure of Component 1's Sensor X

Component: Component 1

Zone:

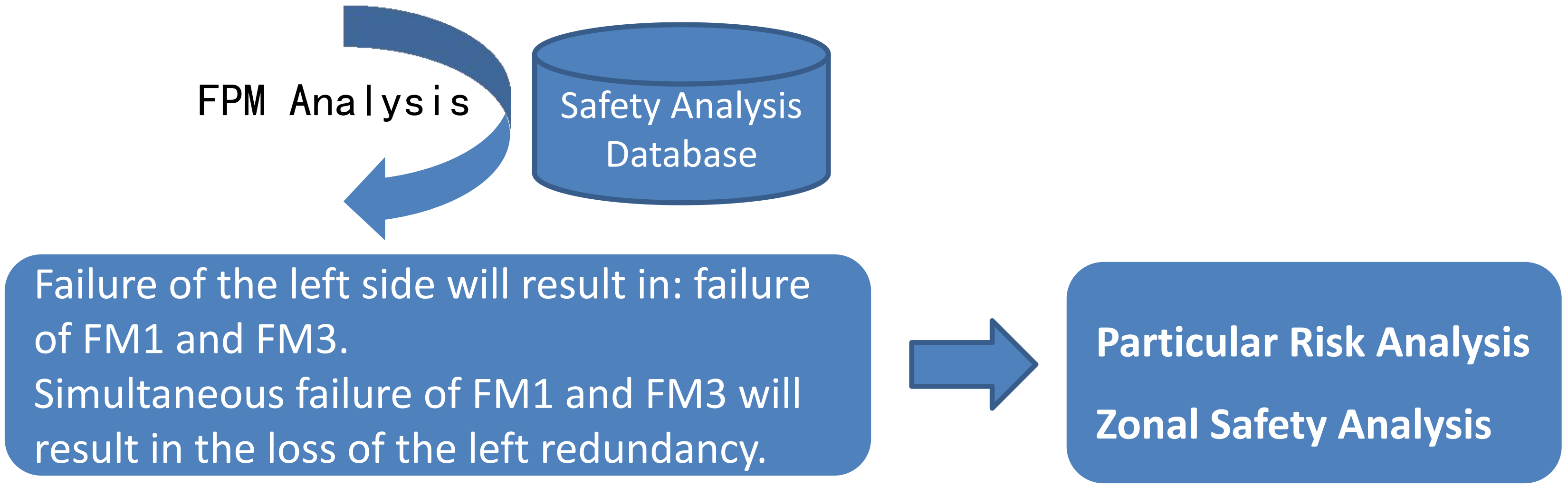
Component Level:

Subsystem:

System:

Filter Failure Zone: Left

FM	Zone	Device	Level	System	Sub-system
FM1	Left	Device 1	2	System A	Display
FM2	Right	Device 2	2	System A	Display
FM3	Left	Device 5	3	System A	Alerting
…	…	…	…	…	…



Failure of the left side will result in: failure of FM1 and FM3.
Simultaneous failure of FM1 and FM3 will result in the loss of the left redundancy.

Particular Risk Analysis

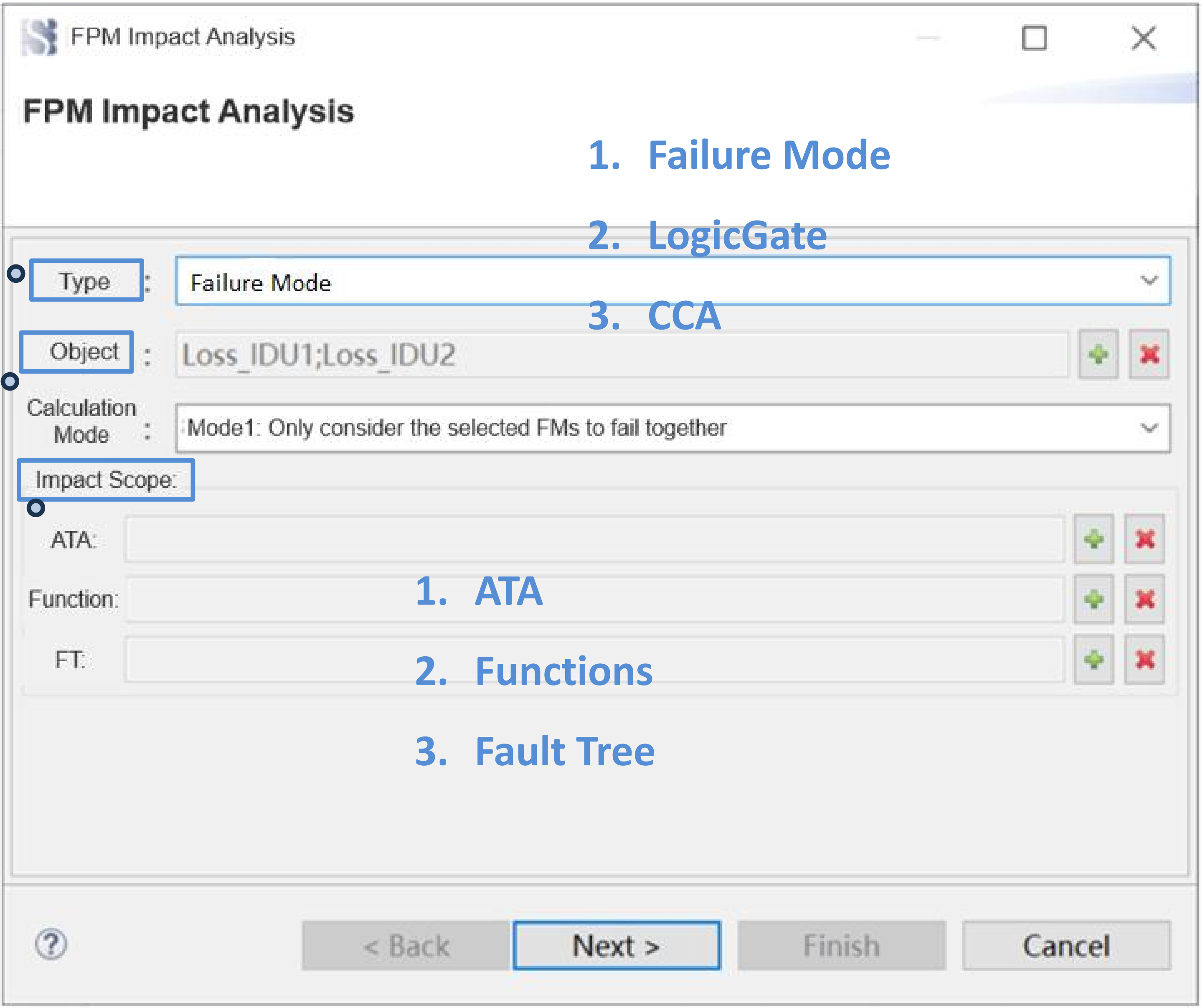
Zonal Safety Analysis

3.6 Safety Analysis

Select the type to be analyzed

Select the object to be analyzed

Select the scope to be analyzed



FPM Impact Analysis

Type : Failure Mode

Object : Loss_IDU1;Loss_IDU2

Calculation Mode : Mode1: Only consider the selected FMs to fail together

Impact Scope:

ATA:

Function:

FT:

1. Failure Mode
2. LogicGate
3. CCA

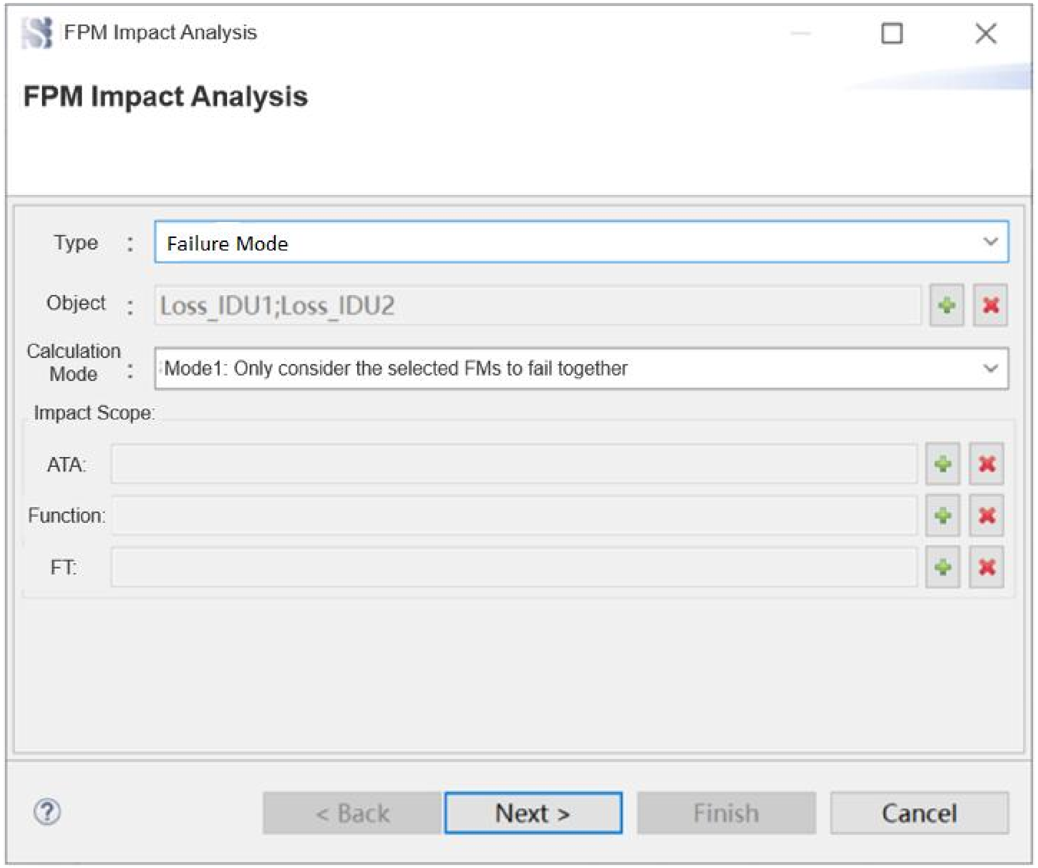
1. ATA
2. Functions
3. Fault Tree

3.6 Safety Analysis

CCA： Common Cause Analysis
FHA： Functional Hazard Assessment
FMEA： Failure Mode and Effect Analysis

COMSPEC

Analyze complex System Architecture based on the Whole Aircraft Safety Database



FPM Impact Analysis

Type : Failure Mode

Object : Loss_IDU1;Loss_IDU2

Calculation Mode : Mode1: Only consider the selected FMs to fail together

Impact Scope:

ATA:

Function:

FT:

Single Point Failure Analysis

The IMA System, power supply system and other public resource systems can perform safety analysis from different functional scopes.

Combination Failure Analysis

Particular risk analysis, zonal safety analysis and CCA can be performed from different functional scope.

Common Cause& Cascade Analysis

Identify the impact of failures at all levels of the architecture, including loss of redundancy and interface failures.

Generate standard reports

Support FHA/FMEA database management that are compliant with 4761A, and the export of FHA/FMEA reports.

3.6 Safety Analysis

Example : Loss of switch A and switch B

Manual analysis results for XX aircraft

manual analysis report conclusions:

Fuel system: Fuel data redundancies for IDUs are reduced;

Display alarm system: Data transmission redundancy to the left IDU is lost, and hasn't affected the function.

Analysis Report of the COMSPEC tool

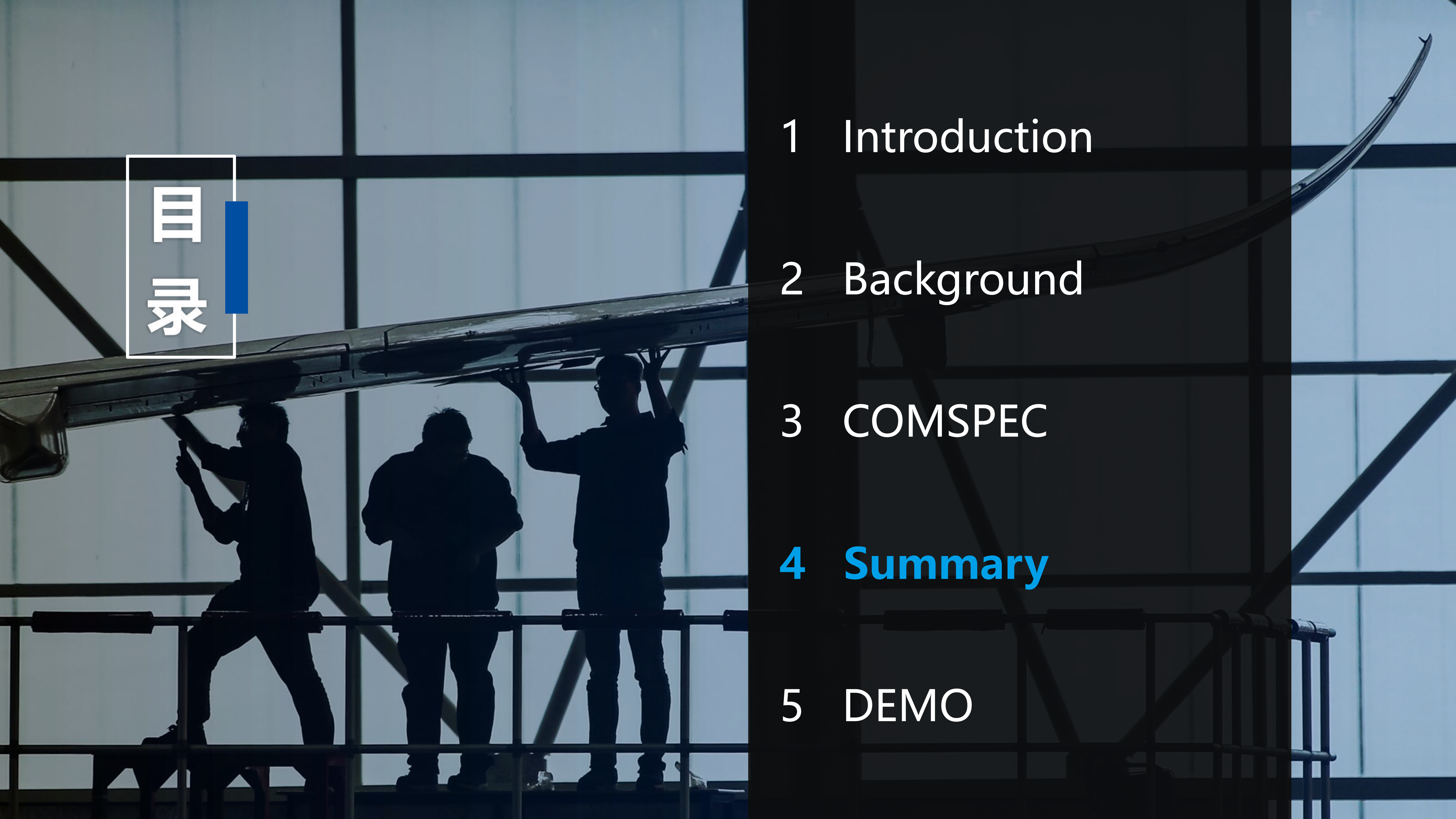
Order	Function	Level	Failure Mode
1	Fuel Display	Functional Level	Loss of IDU2 fuel quantity display function
2			Fuel information input that loses IDU2 fuel quantity display function
3		Interface Level	Loss of IDU2 fuel display information interface input
4	Airspeed Display	Functional Level	Loss of IDU2 calculated airspeed display function
5			Loss of IDU1 calculated airspeed display function
6			Loss of airspeed information input for IDU2 airspeed display function
7			Loss of airspeed information input for IDU1 airspeed display function
8		Interface Level	Loss of IDU2 airspeed display information interface input
[illegible]			Loss of IDU1 airspeed display information interface input

Conclusion

- ✓ Not detailed
- ✓ 30 people are analyzed in each round, working at the same time during the week

≤

- ✓ Accuracy: Consistent with manual analysis result
- ✓ Efficiency: Each analysis takes several seconds/minutes.
- ✓ Convenience: Analysis results are more detailed, objective and standardized.
- ✓ Completeness: The results of the analysis include both functional and physical interface levels



目录

1 Introduction

2 Background

3 COMSPEC

4 Summary

5 DEMO

4.1 Summary

Safety model traceability

- Architecture model and safety model can be traced
- Safety analysis results can confirm and improve the architectural model.

Public device naming consistency

- Modeling and standardization of public equipment failure modes
- Public resources facilitate security impact analysis

Automatically create fault trees

- Function/device define failure propagation logic
- Save time and effort , reduce experience limit

Safety analysis automation

- Automatically form a safety analysis database
- Automatically carry out PRA/ZSA/CCM in ARP4761

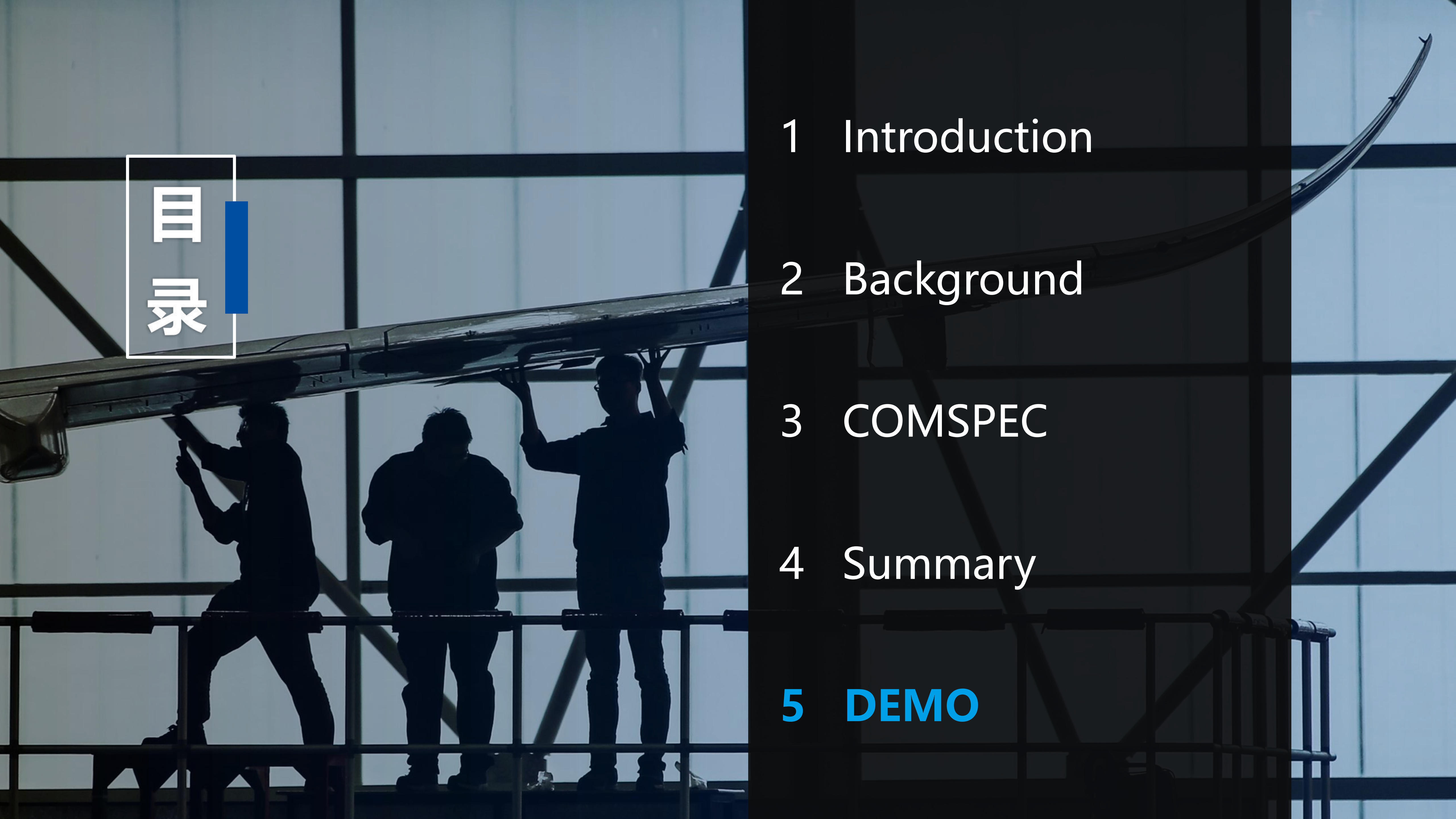
Innovation

- Compatibility
- Intellectual property

4.2 Summary

Wide Application

- Complex system design and verification work
- Highly integrated system
- High requirements for reliability and safety.



目录

1 Introduction

2 Background

3 COMSPEC

4 Summary

5 DEMO

Q&A