Performing Safety Analyses in Capella with ATICA

Our Experience

Capella Webinar

by

Samuel García Lorente
Senior Safety Engineer
Anzen Engineering
samuelgarcia@anzenengineering.com

Fernando Macías
Senior Software Engineer
Anzen Engineering
fernandomacias@anzenengineering.com

Daniel Villafañe
Digital Engineering Lead
Anzen Engineering
danielvilla@anzenengineering.com

25th September 2025

About Anzen

ANZEN
ANZEN Engineering
5th Anniversary
European Space Astronomy Centre (ESAC)
Villafranca del Castillo, Madrid
esa

- Madrid, Spain (Headquarters – Europe)
- Lucerne, Switzerland
- Washington D.C., USA (fully incorporated U.S. company)

System Safety & Reliability

- Typical services include:
  - Reliability Prediction Reports
  - Failure Modes and Effects Analysis
  - System Safety Assessments

Model-Based Systems Engineering

- A team working on Digital Engineering projects
- Our work consists of:
  - Support to ATICA users
  - Software development
  - Consultancy
  - Participation in R&D projects

Integrated Logistics Support (ILS)

Hardware & Software Assurance

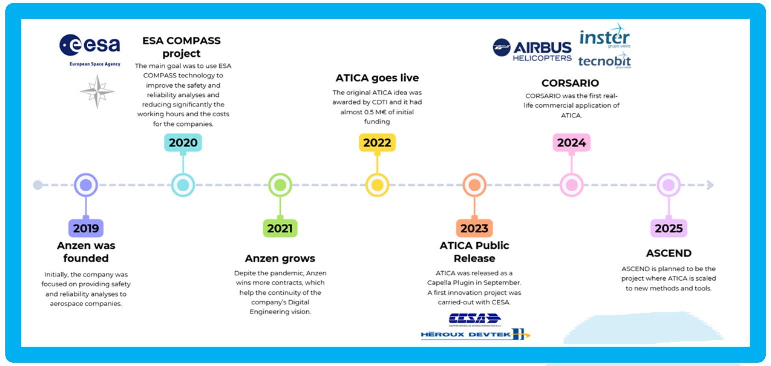
UAS Certification

Cybersecurity

Outcomes of this webinar

- Show advantages of an MBSE approach.
- Share our experience in developing ATICA, a Capella-based solution.
- Showcase ATICA capabilities.
- Offer Anzen’s expertise to companies with the same challenges.

Atica4Capella



ESA COMPASS project
The main goal was to use ESA COMPASS technology to improve the safety and reliability analyses and reducing significantly the working hours and the costs for the companies.

ATICA goes live
The original ATICA idea was awarded by CDTI and it had almost 0.5 M€ of initial funding

CORSARIO
CORSARIO was the first real-life commercial application of ATICA.

2019 — Anzen was founded
Initially, the company was focused on providing safety and reliability analyses to aerospace companies.

2020 — ESA COMPASS project

2021 — Anzen grows
Depite the pandemic, Anzen wins more contracts, which help the continuity of the company's Digital Engineering vision.

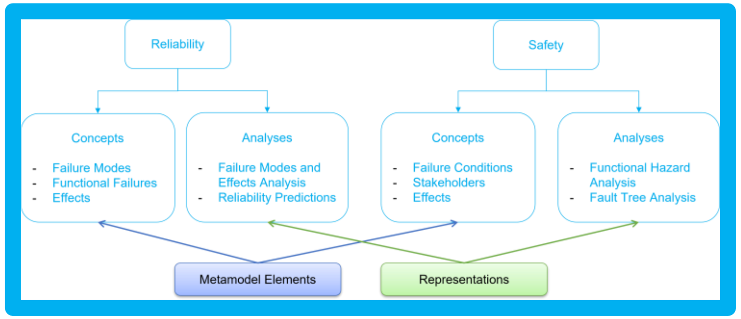
2022 — ATICA goes live

2023 — ATICA Public Release
ATICA was released as a Capella Plugin in September. A first innovation project was carried-out with CESA.

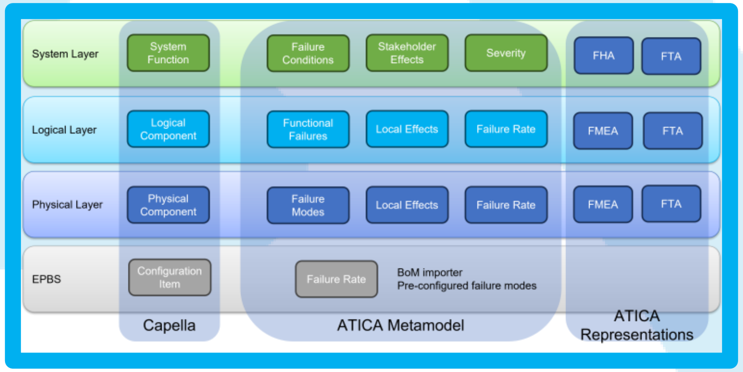
2024 — CORSARIO

2025 — ASCEND
ASCEND is planned to be the project where ATICA is scaled to new methods and tools.

When?



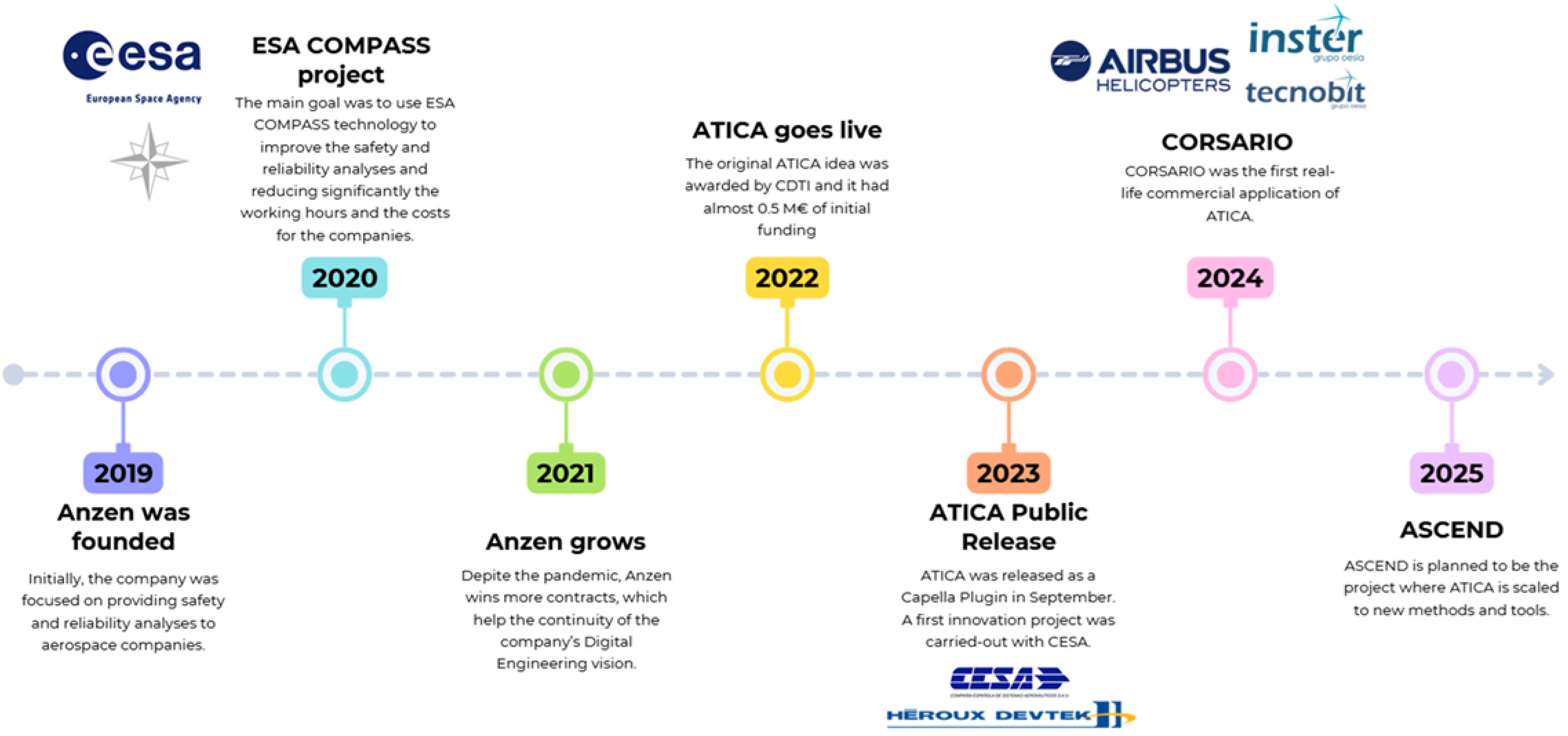
Why?



	Capella	ATICA Metamodel			ATICA Representations	
System Layer	System Function	Failure Conditions	Stakeholder Effects	Severity	FHA	FTA
Logical Layer	Logical Component	Functional Failures	Local Effects	Failure Rate	FMEA	FTA
Physical Layer	Physical Component	Failure Modes	Local Effects	Failure Rate	FMEA	FTA
EPBS	Configuration Item	Failure Rate	BoM importer Pre-configured failure modes			

How?

Atica4Capella –When?



2019

Anzen was founded

Initially, the company was focused on providing safety and reliability analyses to aerospace companies.

2020

ESA COMPASS project

The main goal was to use ESA COMPASS technology to improve the safety and reliability analyses and reducing significantly the working hours and the costs for the companies.

2021

Anzen grows

Depite the pandemic, Anzen wins more contracts, which help the continuity of the company's Digital Engineering vision.

2022

ATICA goes live

The original ATICA idea was awarded by CDTI and it had almost 0.5 M€ of initial funding

2023

ATICA Public Release

ATICA was released as a Capella Plugin in September. A first innovation project was carried-out with CESA.

2024

CORSARIO

CORSARIO was the first real-life commercial application of ATICA.

2025

ASCEND

ASCEND is planned to be the project where ATICA is scaled to new methods and tools.

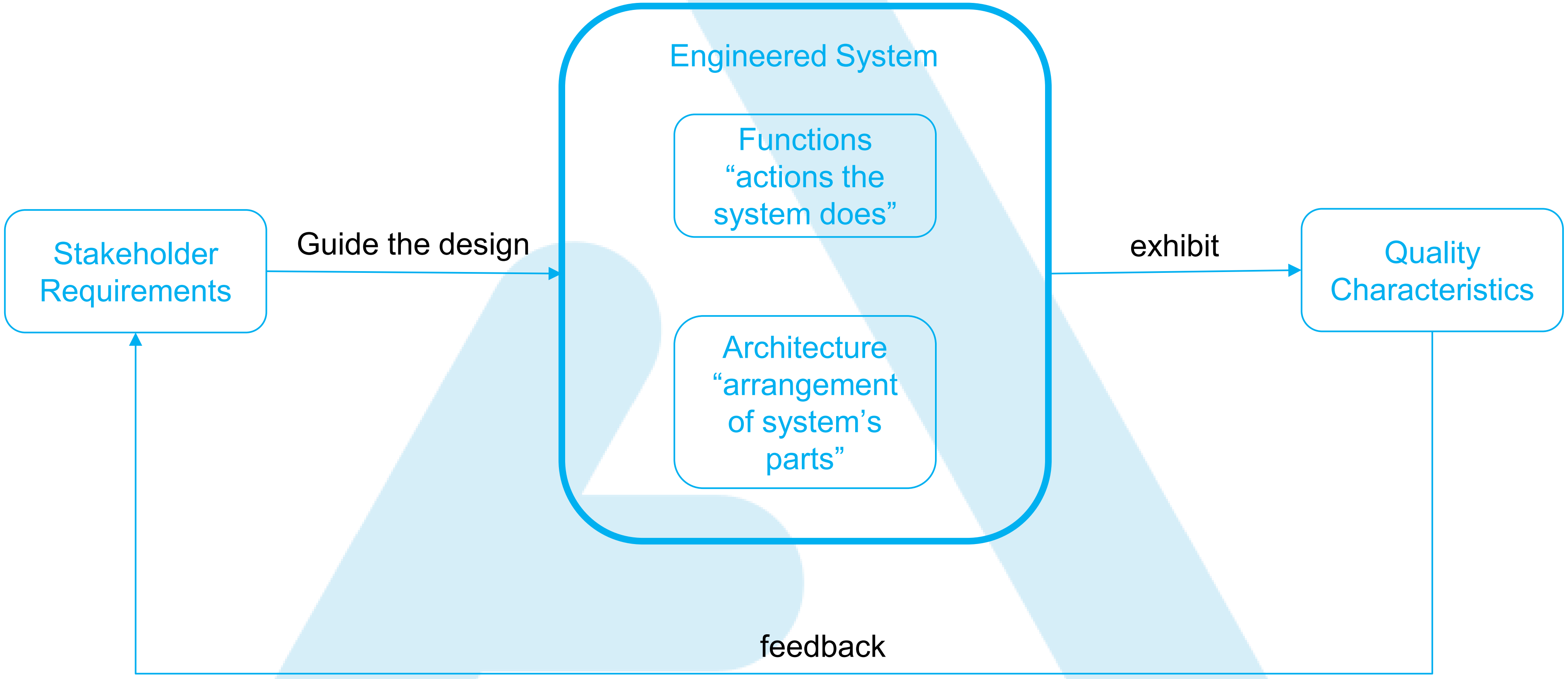
Atica4Capella – Why?

- ATICA made our life easier

- The Process of Safety and Reliability in ATICA

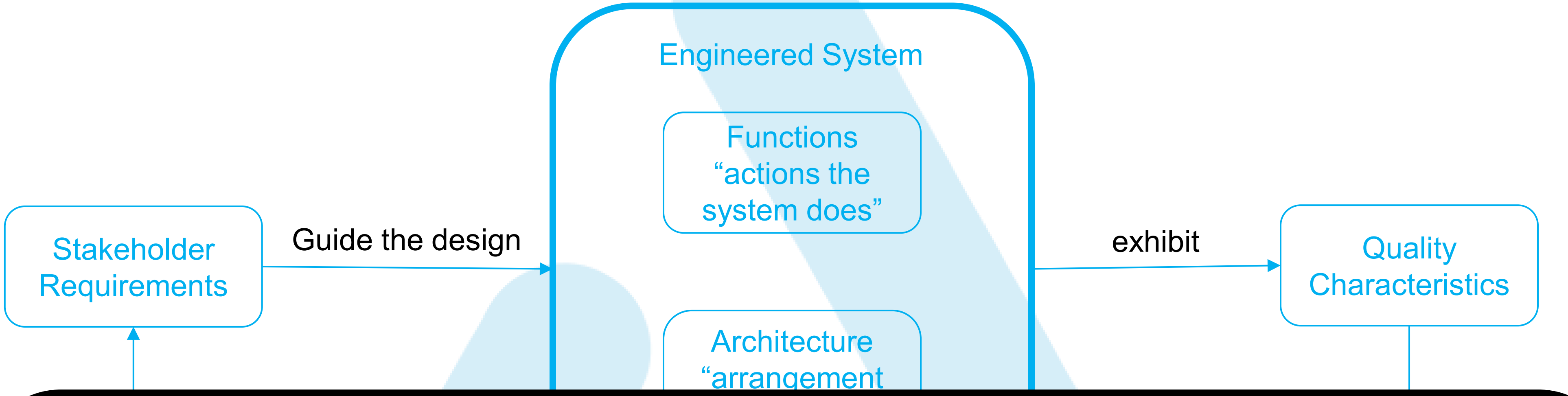
- The Standards used

ATICA made our life easier



The good part: Quality Characteristics can be analysed <u>before</u> the system is built

ATICA made our life easier



1. Use the same source of truth as the Systems Engineering team.
2. Impact design by creating requirements directly in the project database.
3. Anticipate safety risks from the very beginning and SAVE time and money.

ilt

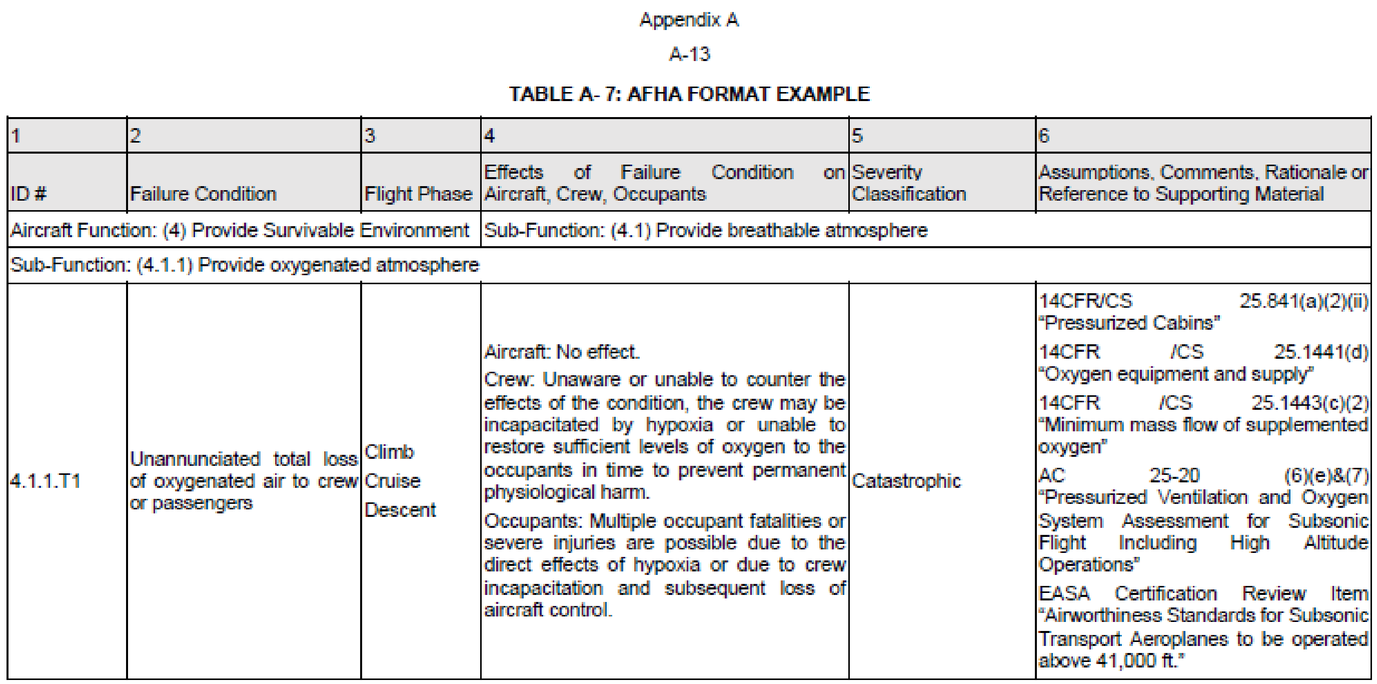
The Standards

ED-135

GUIDELINES FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRCRAFT, SYSTEMS, AND EQUIPMENT

© EUROCAE

- **ED-135 Appendices A & B “Failure Hazard Analysis”**
- **ED-135 Appendix J “Failure Modes and Effects Analysis”**
- **ED-135 Appendix G “Fault Tree Analysis”**



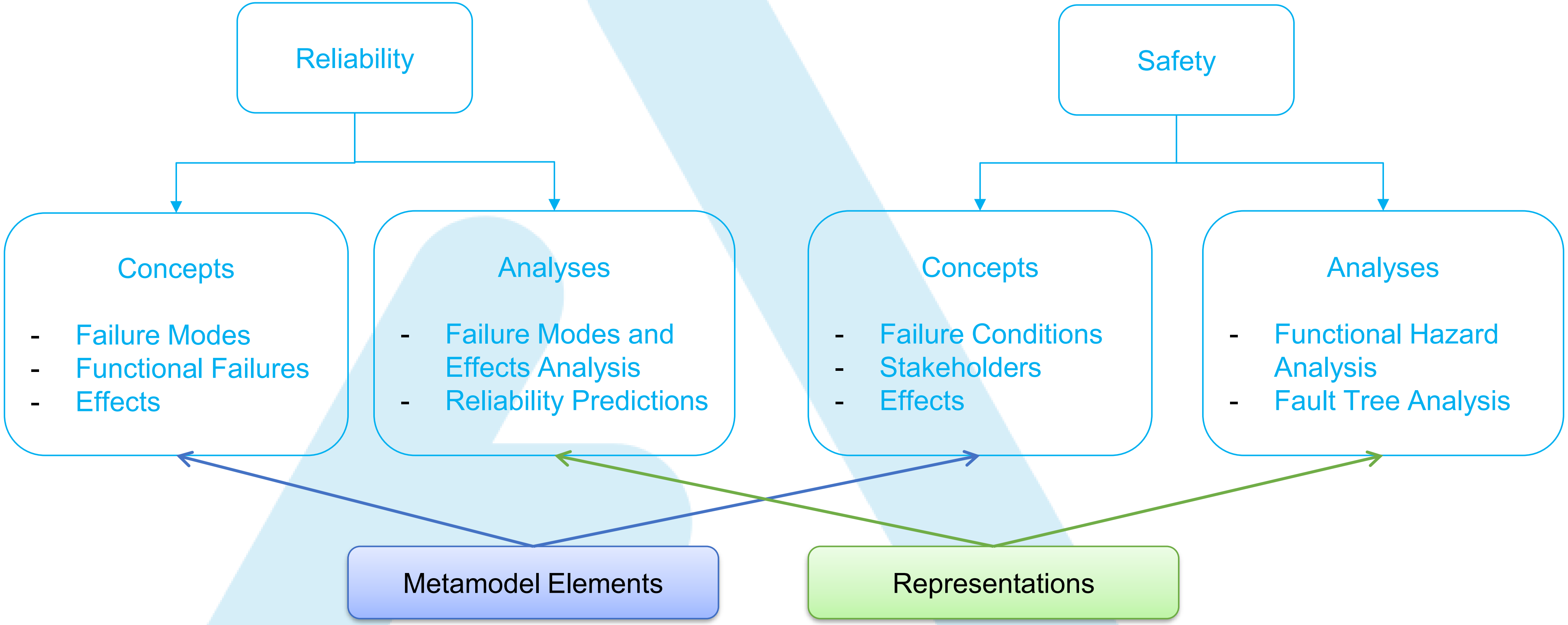
Appendix A

A-13

TABLE A- 7: AFHA FORMAT EXAMPLE

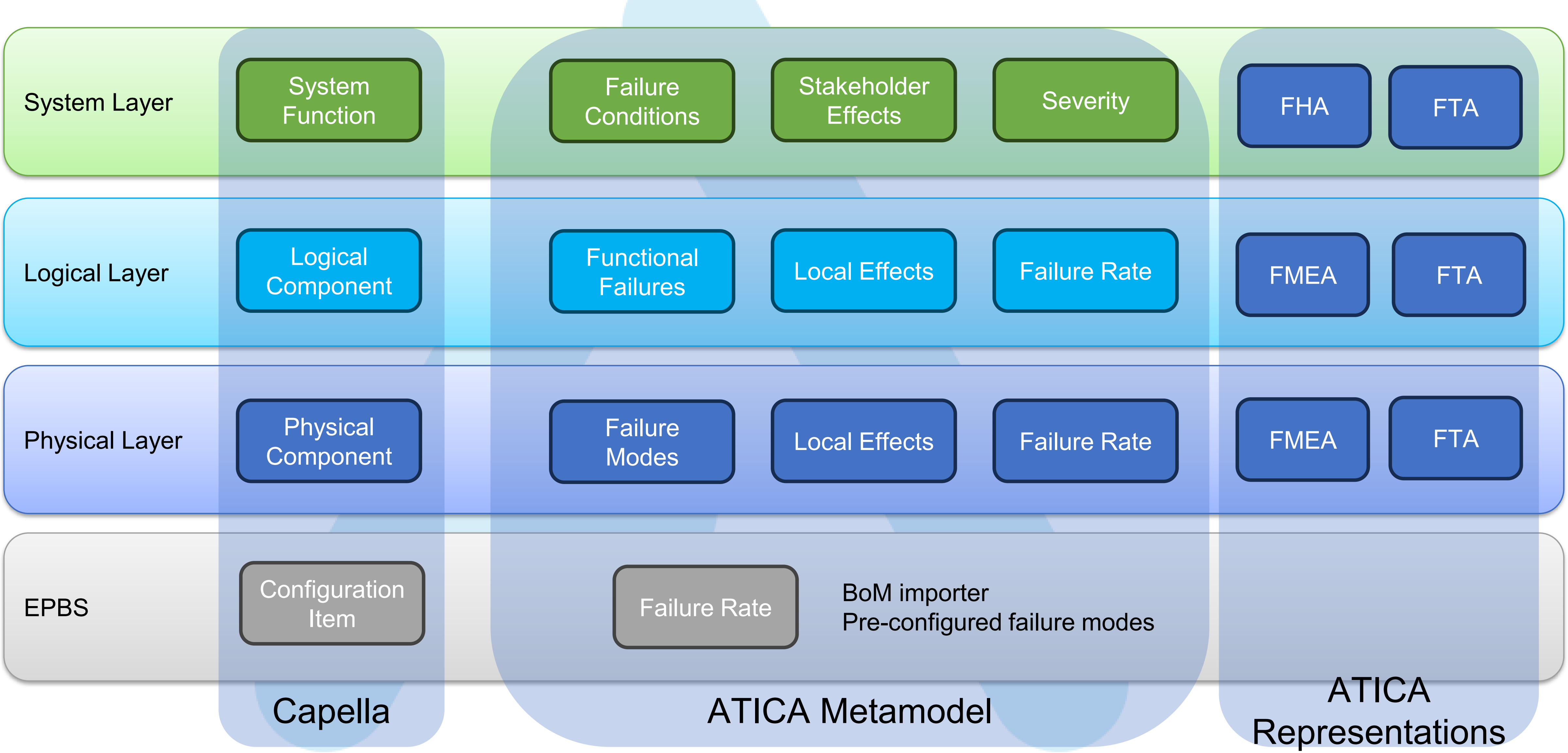
1	2	3	4	5	6
ID #	Failure Condition	Flight Phase	Effects of Failure Condition on Aircraft, Crew, Occupants	Severity Classification	Assumptions, Comments, Rationale or Reference to Supporting Material
Aircraft Function: (4) Provide Survivable Environment			Sub-Function: (4.1) Provide breathable atmosphere		
Sub-Function: (4.1.1) Provide oxygenated atmosphere					
4.1.1.T1	Unannunciated total loss of oxygenated air to crew or passengers	Climb Cruise Descent	Aircraft: No effect. Crew: Unaware or unable to counter the effects of the condition, the crew may be incapacitated by hypoxia or unable to restore sufficient levels of oxygen to the occupants in time to prevent permanent physiological harm. Occupants: Multiple occupant fatalities or severe injuries are possible due to the direct effects of hypoxia or due to crew incapacitation and subsequent loss of aircraft control.	Catastrophic	14CFR/CS 25.841(a)(2)(ii) “Pressurized Cabins” 14CFR /CS 25.1441(d) “Oxygen equipment and supply” 14CFR /CS 25.1443(c)(2) “Minimum mass flow of supplemented oxygen” AC 25-20 (6)(e)&(7) “Pressurized Ventilation and Oxygen System Assessment for Subsonic Flight Including High Altitude Operations” EASA Certification Review Item “Airworthiness Standards for Subsonic Transport Aeroplanes to be operated above 41,000 ft.”

Atica4Capella – How?



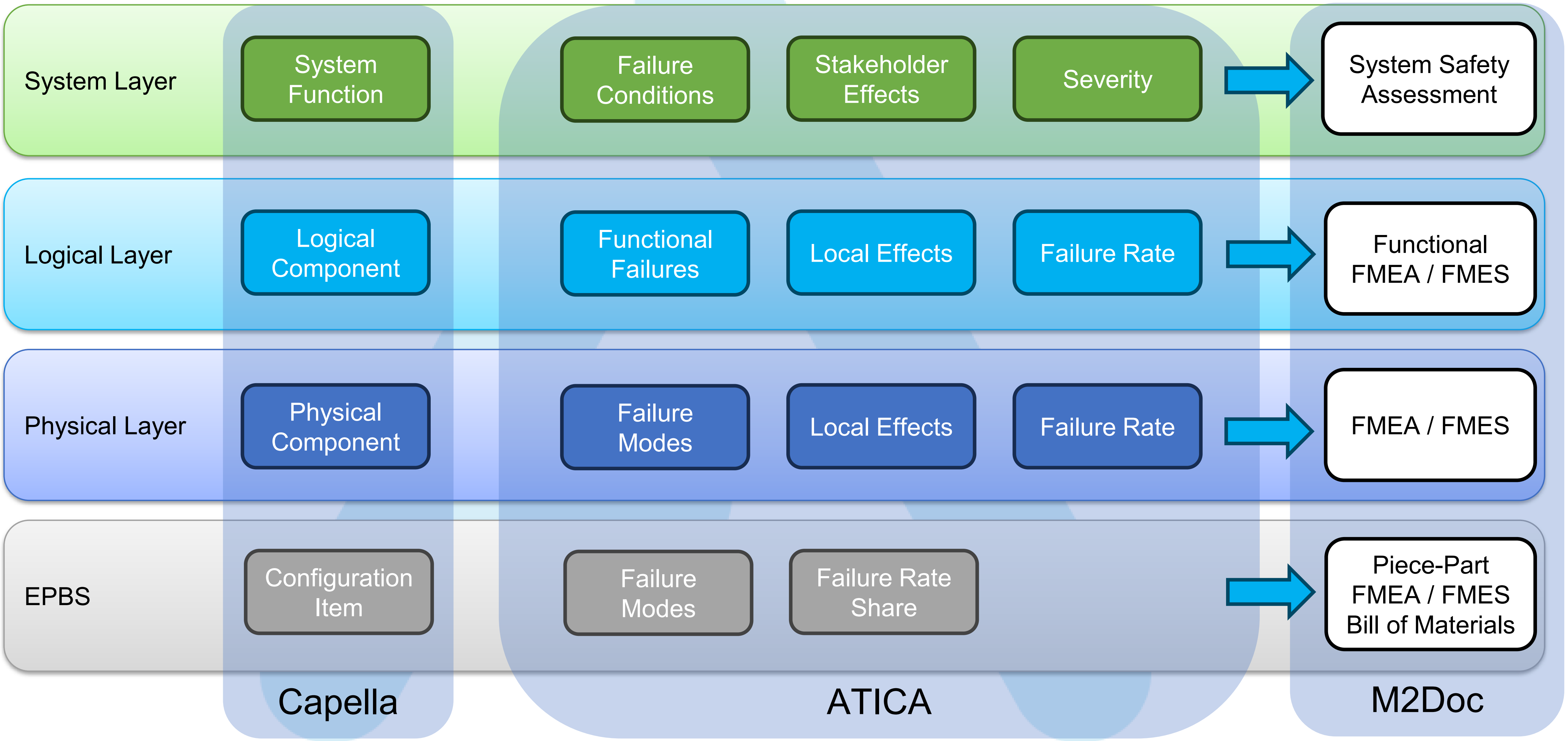
The challenge is to move all these concepts and analyses into Capella

The Process: Full Picture



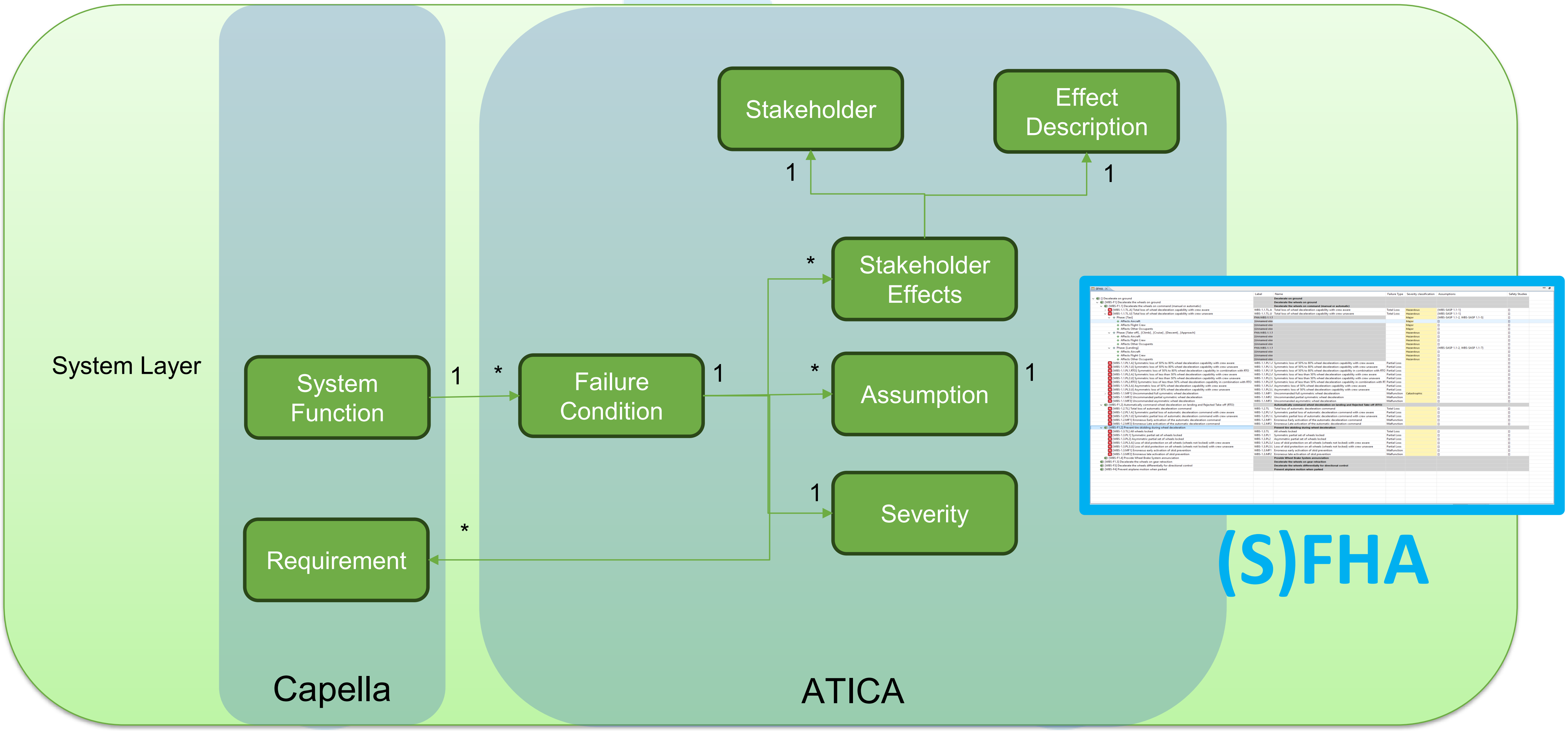
	Capella	ATICA Metamodel			ATICA Representations	
System Layer	System Function	Failure Conditions	Stakeholder Effects	Severity	FHA	FTA
Logical Layer	Logical Component	Functional Failures	Local Effects	Failure Rate	FMEA	FTA
Physical Layer	Physical Component	Failure Modes	Local Effects	Failure Rate	FMEA	FTA
EPBS	Configuration Item	Failure Rate	BoM importer Pre-configured failure modes			

The Process: Reporting



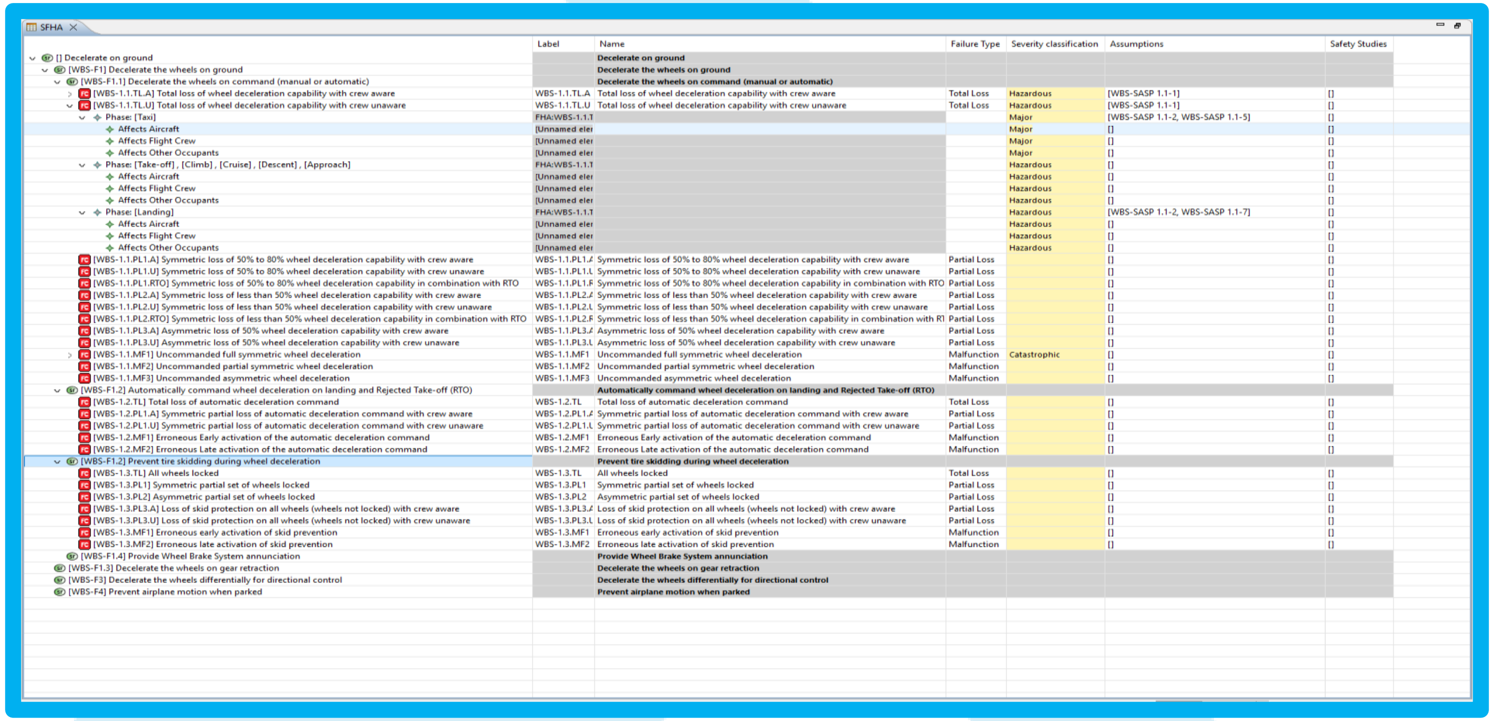
System Layer	System Function	Failure Conditions	Stakeholder Effects	Severity	System Safety Assessment
Logical Layer	Logical Component	Functional Failures	Local Effects	Failure Rate	Functional FMEA / FMES
Physical Layer	Physical Component	Failure Modes	Local Effects	Failure Rate	FMEA / FMES
EPBS	Configuration Item	Failure Modes	Failure Rate Share		Piece-Part FMEA / FMES Bill of Materials
	Capella		ATICA		M2Doc

The Process: Functional Hazard Analysis



	Label	Name	Failure Type	Severity classification	Assumptions	Safety Studies
[] Decelerate on ground		**Decelerate on ground**				
[WBS-F1] Decelerate the wheels on ground		**Decelerate the wheels on ground**				
[WBS-F1.1] Decelerate the wheels on command (manual or automatic)		**Decelerate the wheels on command (manual or automatic)**				
[WBS-1.1.TL.A] Total loss of wheel deceleration capability with crew aware	WBS-1.1.TL.A	Total loss of wheel deceleration capability with crew aware	Total Loss	Hazardous	[WBS-SASP 1.1-1]	[]
[WBS-1.1.TL.U] Total loss of wheel deceleration capability with crew unaware	WBS-1.1.TL.U	Total loss of wheel deceleration capability with crew unaware	Total Loss	Hazardous	[WBS-SASP 1.1-1]	[]
Phase: [Taxi]	FHA:WBS-1.1.T			Major	[WBS-SASP 1.1-2, WBS-SASP 1.1-5]	[]
Affects Aircraft	[Unnamed eler			Major	[]	[]
Affects Flight Crew	[Unnamed eler			Major	[]	[]
Affects Other Occupants	[Unnamed eler			Major	[]	[]
Phase: [Take-off] , [Climb] , [Cruise] , [Descent] , [Approach]	FHA:WBS-1.1.T			Hazardous	[]	[]
Affects Aircraft	[Unnamed eler			Hazardous	[]	[]
Affects Flight Crew	[Unnamed eler			Hazardous	[]	[]
Affects Other Occupants	[Unnamed eler			Hazardous	[]	[]
Phase: [Landing]	FHA:WBS-1.1.T			Hazardous	[WBS-SASP 1.1-2, WBS-SASP 1.1-7]	[]
Affects Aircraft	[Unnamed eler			Hazardous	[]	[]
Affects Flight Crew	[Unnamed eler			Hazardous	[]	[]
Affects Other Occupants	[Unnamed eler			Hazardous	[]	[]
[WBS-1.1.PL1.A] Symmetric loss of 50% to 80% wheel deceleration capability with crew aware	WBS-1.1.PL1.A	Symmetric loss of 50% to 80% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL1.U] Symmetric loss of 50% to 80% wheel deceleration capability with crew unaware	WBS-1.1.PL1.U	Symmetric loss of 50% to 80% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.PL1.RTO] Symmetric loss of 50% to 80% wheel deceleration capability in combination with RTO	WBS-1.1.PL1.R	Symmetric loss of 50% to 80% wheel deceleration capability in combination with RTO	Partial Loss		[]	[]
[WBS-1.1.PL2.A] Symmetric loss of less than 50% wheel deceleration capability with crew aware	WBS-1.1.PL2.A	Symmetric loss of less than 50% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL2.U] Symmetric loss of less than 50% wheel deceleration capability with crew unaware	WBS-1.1.PL2.U	Symmetric loss of less than 50% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.PL2.RTO] Symmetric loss of less than 50% wheel deceleration capability in combination with RTO	WBS-1.1.PL2.R	Symmetric loss of less than 50% wheel deceleration capability in combination with RT	Partial Loss		[]	[]
[WBS-1.1.PL3.A] Asymmetric loss of 50% wheel deceleration capability with crew aware	WBS-1.1.PL3.A	Asymmetric loss of 50% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL3.U] Asymmetric loss of 50% wheel deceleration capability with crew unaware	WBS-1.1.PL3.U	Asymmetric loss of 50% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.MF1] Uncommanded full symmetric wheel deceleration	WBS-1.1.MF1	Uncommanded full symmetric wheel deceleration	Malfunction	Catastrophic	[]	[]
[WBS-1.1.MF2] Uncommanded partial symmetric wheel deceleration	WBS-1.1.MF2	Uncommanded partial symmetric wheel deceleration	Malfunction		[]	[]
[WBS-1.1.MF3] Uncommanded asymmetric wheel deceleration	WBS-1.1.MF3	Uncommanded asymmetric wheel deceleration	Malfunction		[]	[]
[WBS-F1.2] Automatically command wheel deceleration on landing and Rejected Take-off (RTO)		**Automatically command wheel deceleration on landing and Rejected Take-off (RTO)**				
[WBS-1.2.TL] Total loss of automatic deceleration command	WBS-1.2.TL	Total loss of automatic deceleration command	Total Loss		[]	[]
[WBS-1.2.PL1.A] Symmetric partial loss of automatic deceleration command with crew aware	WBS-1.2.PL1.A	Symmetric partial loss of automatic deceleration command with crew aware	Partial Loss		[]	[]
[WBS-1.2.PL1.U] Symmetric partial loss of automatic deceleration command with crew unaware	WBS-1.2.PL1.U	Symmetric partial loss of automatic deceleration command with crew unaware	Partial Loss		[]	[]
[WBS-1.2.MF1] Erroneous Early activation of the automatic deceleration command	WBS-1.2.MF1	Erroneous Early activation of the automatic deceleration command	Malfunction		[]	[]
[WBS-1.2.MF2] Erroneous Late activation of the automatic deceleration command	WBS-1.2.MF2	Erroneous Late activation of the automatic deceleration command	Malfunction		[]	[]
[WBS-F1.2] Prevent tire skidding during wheel deceleration		**Prevent tire skidding during wheel deceleration**				
[WBS-1.3.TL] All wheels locked	WBS-1.3.TL	All wheels locked	Total Loss		[]	[]
[WBS-1.3.PL1] Symmetric partial set of wheels locked	WBS-1.3.PL1	Symmetric partial set of wheels locked	Partial Loss		[]	[]
[WBS-1.3.PL2] Asymmetric partial set of wheels locked	WBS-1.3.PL2	Asymmetric partial set of wheels locked	Partial Loss		[]	[]
[WBS-1.3.PL3.A] Loss of skid protection on all wheels (wheels not locked) with crew aware	WBS-1.3.PL3.A	Loss of skid protection on all wheels (wheels not locked) with crew aware	Partial Loss		[]	[]
[WBS-1.3.PL3.U] Loss of skid protection on all wheels (wheels not locked) with crew unaware	WBS-1.3.PL3.U	Loss of skid protection on all wheels (wheels not locked) with crew unaware	Partial Loss		[]	[]
[WBS-1.3.MF1] Erroneous early activation of skid prevention	WBS-1.3.MF1	Erroneous early activation of skid prevention	Malfunction		[]	[]
[WBS-1.3.MF2] Erroneous late activation of skid prevention	WBS-1.3.MF2	Erroneous late activation of skid prevention	Malfunction		[]	[]
[WBS-F1.4] Provide Wheel Brake System annunciation		**Provide Wheel Brake System annunciation**				
[WBS-F1.3] Decelerate the wheels on gear retraction		**Decelerate the wheels on gear retraction**				
[WBS-F3] Decelerate the wheels differentially for directional control		**Decelerate the wheels differentially for directional control**				
[WBS-F4] Prevent airplane motion when parked		**Prevent airplane motion when parked**				

Atica4Capella – Live demo

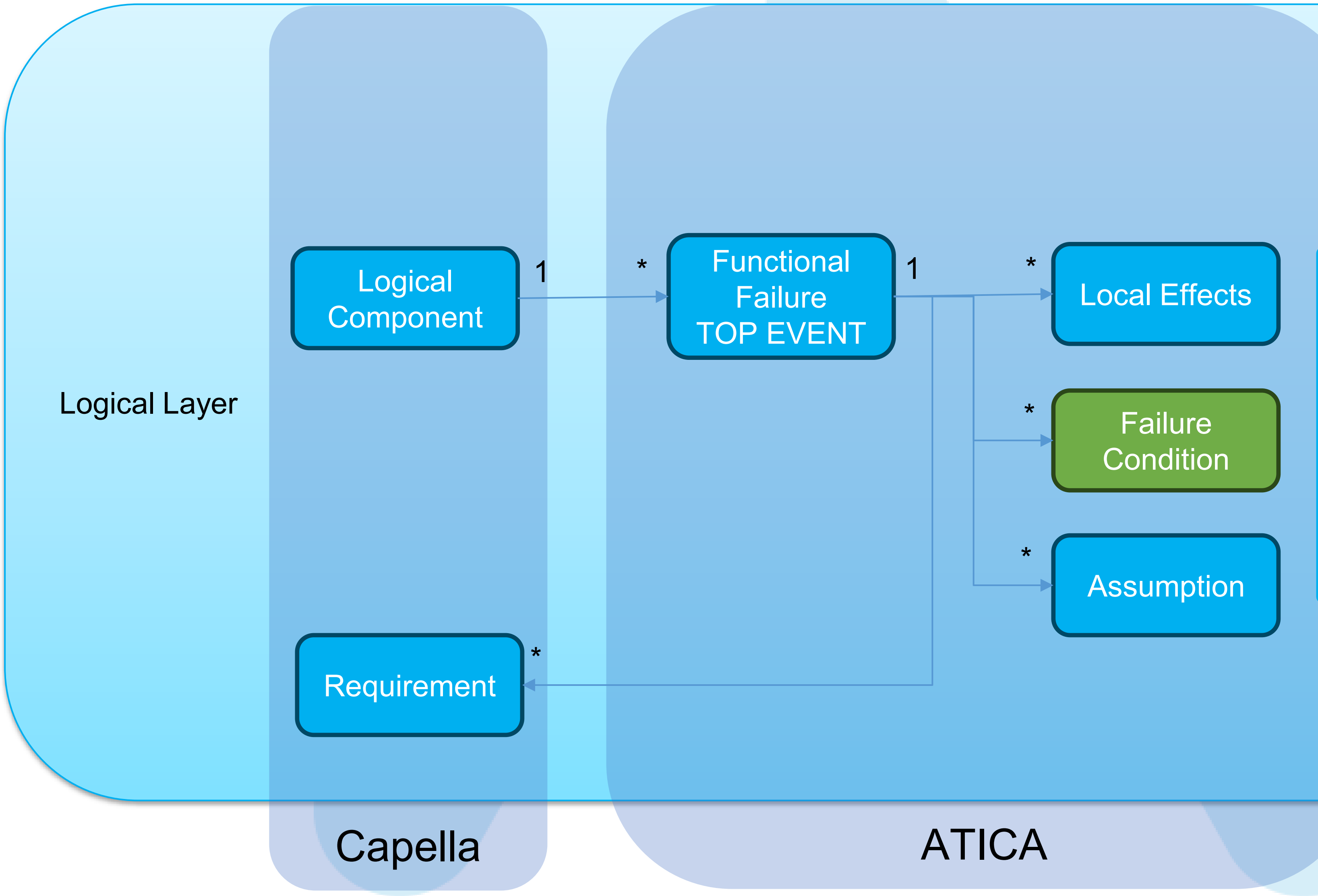


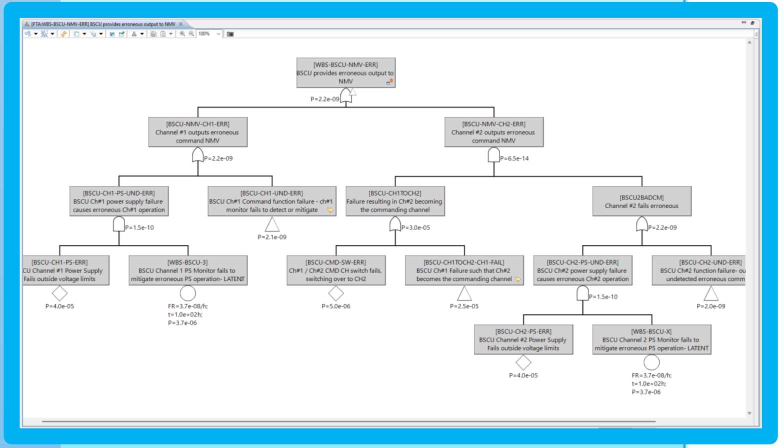
SFHA

	Label	Name	Failure Type	Severity classification	Assumptions	Safety Studies
[] Decelerate on ground		**Decelerate on ground**				
[WBS-F1] Decelerate the wheels on ground		**Decelerate the wheels on ground**				
[WBS-F1.1] Decelerate the wheels on command (manual or automatic)		**Decelerate the wheels on command (manual or automatic)**				
[WBS-1.1.TL.A] Total loss of wheel deceleration capability with crew aware	WBS-1.1.TL.A	Total loss of wheel deceleration capability with crew aware	Total Loss	Hazardous	[WBS-SASP 1.1-1]	[]
[WBS-1.1.TL.U] Total loss of wheel deceleration capability with crew unaware	WBS-1.1.TL.U	Total loss of wheel deceleration capability with crew unaware	Total Loss	Hazardous	[WBS-SASP 1.1-1]	[]
Phase: [Taxi]	FHA:WBS-1.1.T			Major	[WBS-SASP 1.1-2, WBS-SASP 1.1-5]	[]
Affects Aircraft	[Unnamed ele			Major	[]	[]
Affects Flight Crew	[Unnamed ele			Major	[]	[]
Affects Other Occupants	[Unnamed ele			Major	[]	[]
Phase: [Take-off] , [Climb] , [Cruise] , [Descent] , [Approach]	FHA:WBS-1.1.T			Hazardous	[]	[]
Affects Aircraft	[Unnamed ele			Hazardous	[]	[]
Affects Flight Crew	[Unnamed ele			Hazardous	[]	[]
Affects Other Occupants	[Unnamed ele			Hazardous	[]	[]
Phase: [Landing]	FHA:WBS-1.1.T			Hazardous	[WBS-SASP 1.1-2, WBS-SASP 1.1-7]	[]
Affects Aircraft	[Unnamed ele			Hazardous	[]	[]
Affects Flight Crew	[Unnamed ele			Hazardous	[]	[]
Affects Other Occupants	[Unnamed ele			Hazardous	[]	[]
[WBS-1.1.PL1.A] Symmetric loss of 50% to 80% wheel deceleration capability with crew aware	WBS-1.1.PL1.A	Symmetric loss of 50% to 80% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL1.U] Symmetric loss of 50% to 80% wheel deceleration capability with crew unaware	WBS-1.1.PL1.U	Symmetric loss of 50% to 80% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.PL1.RTO] Symmetric loss of 50% to 80% wheel deceleration capability in combination with RTO	WBS-1.1.PL1.R	Symmetric loss of 50% to 80% wheel deceleration capability in combination with RTO	Partial Loss		[]	[]
[WBS-1.1.PL2.A] Symmetric loss of less than 50% wheel deceleration capability with crew aware	WBS-1.1.PL2.A	Symmetric loss of less than 50% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL2.U] Symmetric loss of less than 50% wheel deceleration capability with crew unaware	WBS-1.1.PL2.U	Symmetric loss of less than 50% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.PL2.RTO] Symmetric loss of less than 50% wheel deceleration capability in combination with RTO	WBS-1.1.PL2.R	Symmetric loss of less than 50% wheel deceleration capability in combination with RT	Partial Loss		[]	[]
[WBS-1.1.PL3.A] Asymmetric loss of 50% wheel deceleration capability with crew aware	WBS-1.1.PL3.A	Asymmetric loss of 50% wheel deceleration capability with crew aware	Partial Loss		[]	[]
[WBS-1.1.PL3.U] Asymmetric loss of 50% wheel deceleration capability with crew unaware	WBS-1.1.PL3.U	Asymmetric loss of 50% wheel deceleration capability with crew unaware	Partial Loss		[]	[]
[WBS-1.1.MF1] Uncommanded full symmetric wheel deceleration	WBS-1.1.MF1	Uncommanded full symmetric wheel deceleration	Malfunction	Catastrophic	[]	[]
[WBS-1.1.MF2] Uncommanded partial symmetric wheel deceleration	WBS-1.1.MF2	Uncommanded partial symmetric wheel deceleration	Malfunction		[]	[]
[WBS-1.1.MF3] Uncommanded asymmetric wheel deceleration	WBS-1.1.MF3	Uncommanded asymmetric wheel deceleration	Malfunction		[]	[]
[WBS-F1.2] Automatically command wheel deceleration on landing and Rejected Take-off (RTO)		**Automatically command wheel deceleration on landing and Rejected Take-off (RTO)**				
[WBS-1.2.TL] Total loss of automatic deceleration command	WBS-1.2.TL	Total loss of automatic deceleration command	Total Loss		[]	[]
[WBS-1.2.PL1.A] Symmetric partial loss of automatic deceleration command with crew aware	WBS-1.2.PL1.A	Symmetric partial loss of automatic deceleration command with crew aware	Partial Loss		[]	[]
[WBS-1.2.PL1.U] Symmetric partial loss of automatic deceleration command with crew unaware	WBS-1.2.PL1.U	Symmetric partial loss of automatic deceleration command with crew unaware	Partial Loss		[]	[]
[WBS-1.2.MF1] Erroneous Early activation of the automatic deceleration command	WBS-1.2.MF1	Erroneous Early activation of the automatic deceleration command	Malfunction		[]	[]
[WBS-1.2.MF2] Erroneous Late activation of the automatic deceleration command	WBS-1.2.MF2	Erroneous Late activation of the automatic deceleration command	Malfunction		[]	[]
[WBS-F1.2] Prevent tire skidding during wheel deceleration		**Prevent tire skidding during wheel deceleration**				
[WBS-1.3.TL] All wheels locked	WBS-1.3.TL	All wheels locked	Total Loss		[]	[]
[WBS-1.3.PL1] Symmetric partial set of wheels locked	WBS-1.3.PL1	Symmetric partial set of wheels locked	Partial Loss		[]	[]
[WBS-1.3.PL2] Asymmetric partial set of wheels locked	WBS-1.3.PL2	Asymmetric partial set of wheels locked	Partial Loss		[]	[]
[WBS-1.3.PL3.A] Loss of skid protection on all wheels (wheels not locked) with crew aware	WBS-1.3.PL3.A	Loss of skid protection on all wheels (wheels not locked) with crew aware	Partial Loss		[]	[]
[WBS-1.3.PL3.U] Loss of skid protection on all wheels (wheels not locked) with crew unaware	WBS-1.3.PL3.U	Loss of skid protection on all wheels (wheels not locked) with crew unaware	Partial Loss		[]	[]
[WBS-1.3.MF1] Erroneous early activation of skid prevention	WBS-1.3.MF1	Erroneous early activation of skid prevention	Malfunction		[]	[]
[WBS-1.3.MF2] Erroneous late activation of skid prevention	WBS-1.3.MF2	Erroneous late activation of skid prevention	Malfunction		[]	[]
[WBS-F1.4] Provide Wheel Brake System annunciation		**Provide Wheel Brake System annunciation**				
[WBS-F1.3] Decelerate the wheels on gear retraction		**Decelerate the wheels on gear retraction**				
[WBS-F3] Decelerate the wheels differentially for directional control		**Decelerate the wheels differentially for directional control**				
[WBS-F4] Prevent airplane motion when parked		**Prevent airplane motion when parked**				

(S)FHA

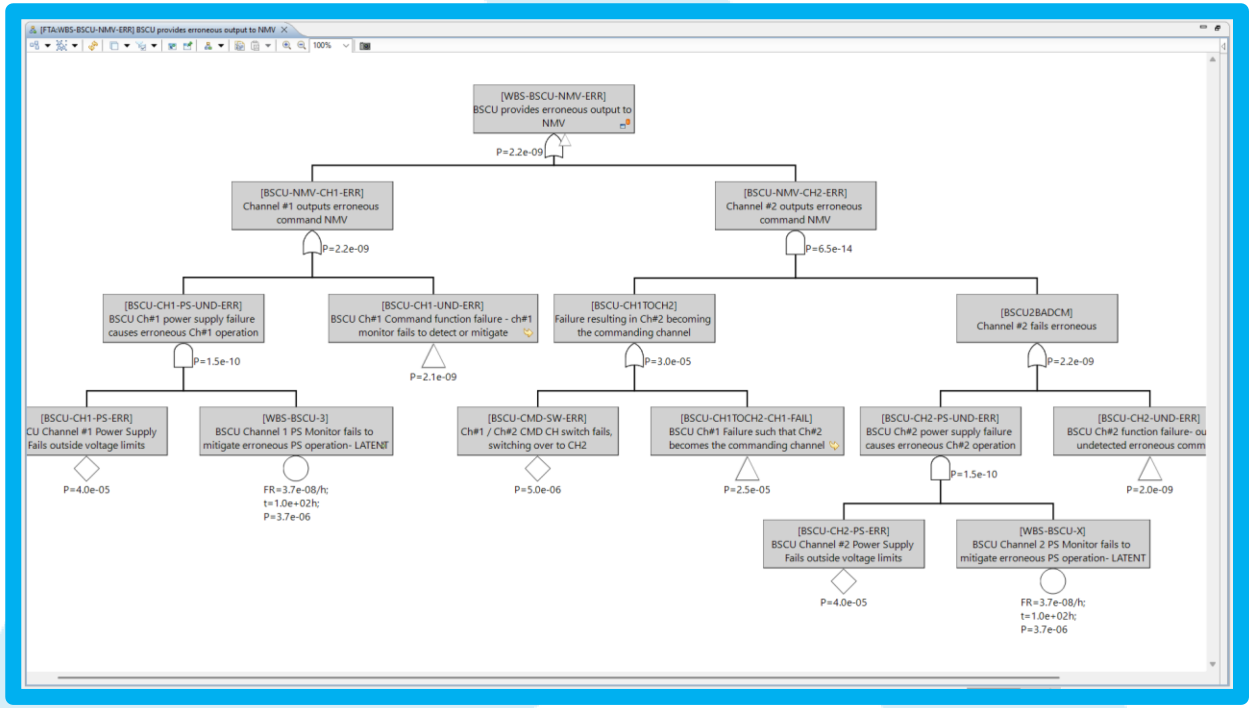
The Process: Fault Tree Analysis




[FTA:WBS-BSCU-NMV-ERR] BSCU provides erroneous output to NMV
100%
[WBS-BSCU-NMV-ERR]
BSCU provides erroneous output to NMV
P=2.2e-09
[BSCU-NMV-CH1-ERR]
Channel #1 outputs erroneous command NMV
P=2.2e-09
[BSCU-NMV-CH2-ERR]
Channel #2 outputs erroneous command NMV
P=6.5e-14
[BSCU-CH1-PS-UND-ERR]
BSCU Ch#1 power supply failure causes erroneous Ch#1 operation
P=1.5e-10
[BSCU-CH1-UND-ERR]
BSCU Ch#1 Command function failure - ch#1 monitor fails to detect or mitigate
P=2.1e-09
[BSCU-CH1TOCH2]
Failure resulting in Ch#2 becoming the commanding channel
P=3.0e-05
[BSCU2BADCM]
Channel #2 fails erroneous
P=2.2e-09
[BSCU-CH1-PS-ERR]
CU Channel #1 Power Supply Fails outside voltage limits
P=4.0e-05
[WBS-BSCU-3]
BSCU Channel 1 PS Monitor fails to mitigate erroneous PS operation- LATENT
FR=3.7e-08/h;
t=1.0e+02h;
P=3.7e-06
[BSCU-CMD-SW-ERR]
Ch#1 / Ch#2 CMD CH switch fails, switching over to CH2
P=5.0e-06
[BSCU-CH1TOCH2-CH1-FAIL]
BSCU Ch#1 Failure such that Ch#2 becomes the commanding channel
P=2.5e-05
[BSCU-CH2-PS-UND-ERR]
BSCU Ch#2 power supply failure causes erroneous Ch#2 operation
P=1.5e-10
[BSCU-CH2-UND-ERR]
BSCU Ch#2 function failure- ou undetected erroneous comm
P=2.0e-09
[BSCU-CH2-PS-ERR]
BSCU Channel #2 Power Supply Fails outside voltage limits
P=4.0e-05
[WBS-BSCU-X]
BSCU Channel 2 PS Monitor fails to mitigate erroneous PS operation- LATENT
FR=3.7e-08/h;
t=1.0e+02h;
P=3.7e-06

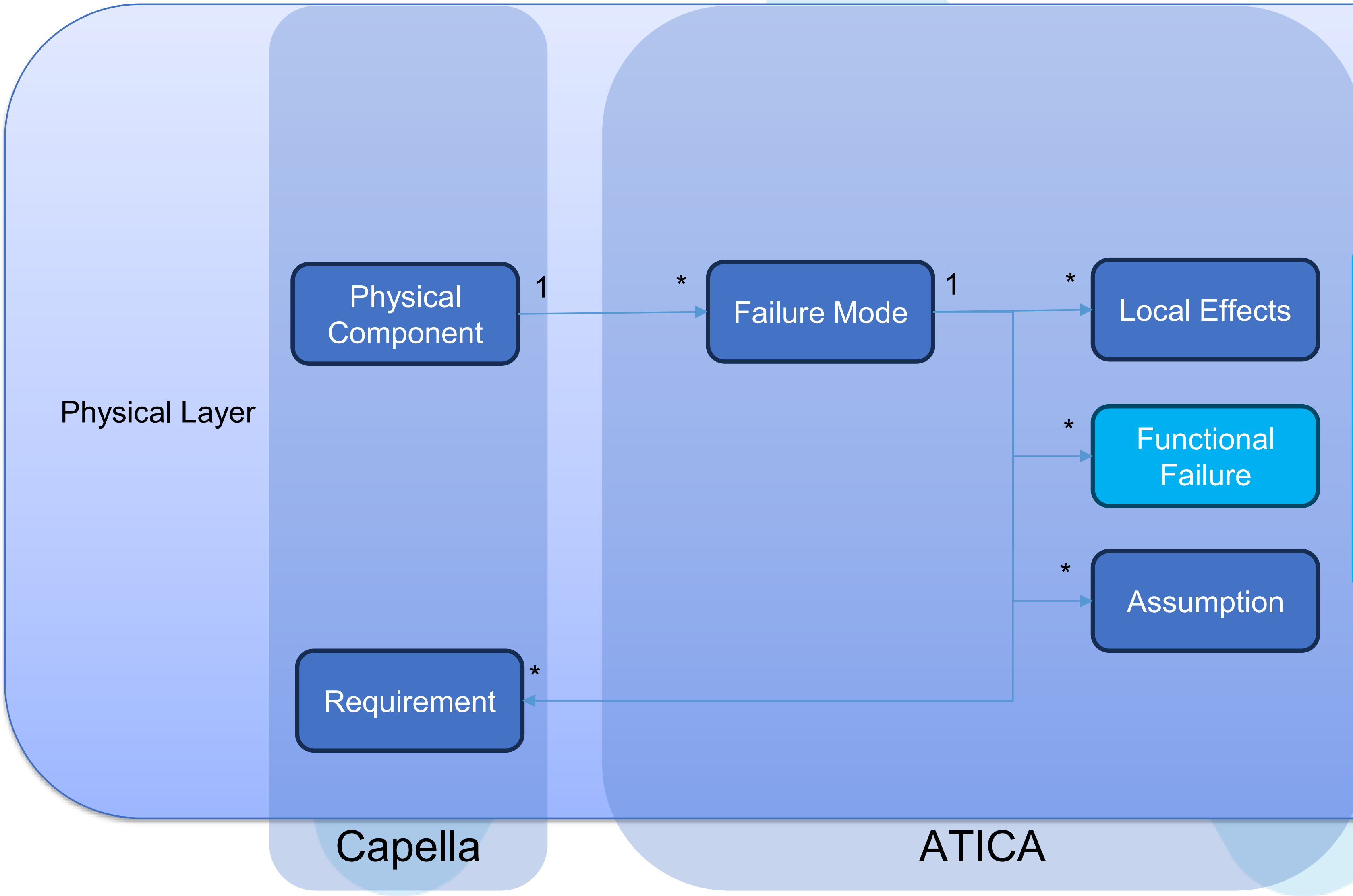
FTA

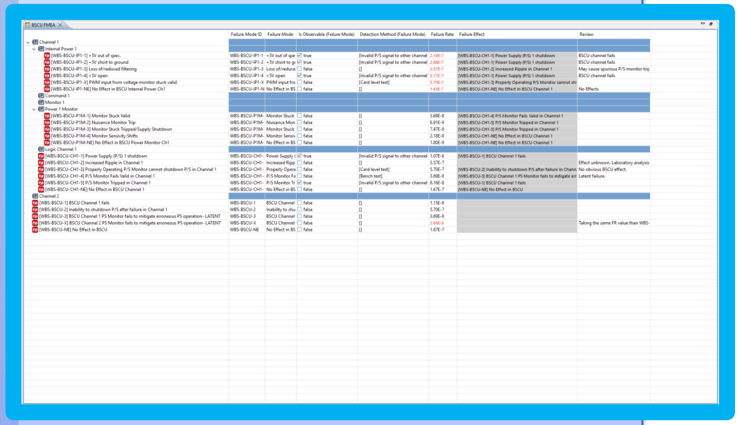
Atica4Capella – Live demo


[FTA:WBS-BSCU-NMV-ERR] BSCU provides erroneous output to NMV
100%
[WBS-BSCU-NMV-ERR] BSCU provides erroneous output to NMV
P=2.2e-09
[BSCU-NMV-CH1-ERR] Channel #1 outputs erroneous command NMV
P=2.2e-09
[BSCU-NMV-CH2-ERR] Channel #2 outputs erroneous command NMV
P=6.5e-14
[BSCU-CH1-PS-UND-ERR] BSCU Ch#1 power supply failure causes erroneous Ch#1 operation
P=1.5e-10
[BSCU-CH1-UND-ERR] BSCU Ch#1 Command function failure - ch#1 monitor fails to detect or mitigate
P=2.1e-09
[BSCU-CH1TOCH2] Failure resulting in Ch#2 becoming the commanding channel
P=3.0e-05
[BSCU2BADCM] Channel #2 fails erroneous
P=2.2e-09
[BSCU-CH1-PS-ERR] CU Channel #1 Power Supply Fails outside voltage limits
P=4.0e-05
[WBS-BSCU-3] BSCU Channel 1 PS Monitor fails to mitigate erroneous PS operation- LATENT
FR=3.7e-08/h;
t=1.0e+02h;
P=3.7e-06
[BSCU-CMD-SW-ERR] Ch#1 / Ch#2 CMD CH switch fails, switching over to CH2
P=5.0e-06
[BSCU-CH1TOCH2-CH1-FAIL] BSCU Ch#1 Failure such that Ch#2 becomes the commanding channel
P=2.5e-05
[BSCU-CH2-PS-UND-ERR] BSCU Ch#2 power supply failure causes erroneous Ch#2 operation
P=1.5e-10
[BSCU-CH2-UND-ERR] BSCU Ch#2 function failure- ou undetected erroneous comm
P=2.0e-09
[BSCU-CH2-PS-ERR] BSCU Channel #2 Power Supply Fails outside voltage limits
P=4.0e-05
[WBS-BSCU-X] BSCU Channel 2 PS Monitor fails to mitigate erroneous PS operation- LATENT
FR=3.7e-08/h;
t=1.0e+02h;
P=3.7e-06

FTA

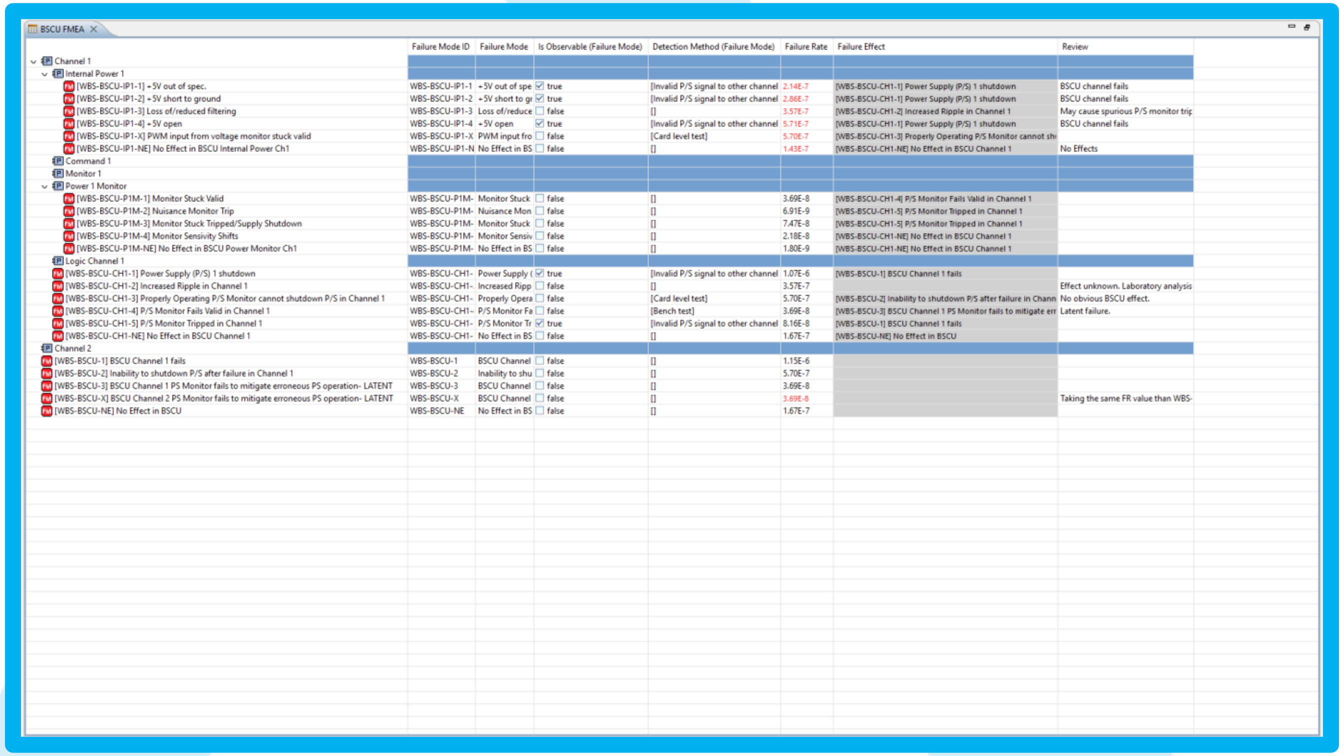
Process: Failure Modes and Effects





	Failure Mode ID	Failure Mode	Is Observable (Failure Mode)	Detection Method (Failure Mode)	Failure Rate	Failure Effect	Review
Channel 1							
Internal Power 1							
[WBS-BSCU-IP1-1] +5V out of spec.	WBS-BSCU-IP1-1	+5V out of spe	☑ true	[Invalid P/S signal to other channel	2.14E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-2] +5V short to ground	WBS-BSCU-IP1-2	+5V short to gr	☑ true	[Invalid P/S signal to other channel	2.86E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-3] Loss of/reduced filtering	WBS-BSCU-IP1-3	Loss of/reduce	☐ false	[]	3.57E-7	[WBS-BSCU-CH1-2] Increased Ripple in Channel 1	May cause spurious P/S monitor trip
[WBS-BSCU-IP1-4] +5V open	WBS-BSCU-IP1-4	+5V open	☑ true	[Invalid P/S signal to other channel	5.71E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-X] PWM input from voltage monitor stuck valid	WBS-BSCU-IP1-X	PWM input fro	☐ false	[Card level test]	5.70E-7	[WBS-BSCU-CH1-3] Properly Operating P/S Monitor cannot sh	
[WBS-BSCU-IP1-NE] No Effect in BSCU Internal Power Ch1	WBS-BSCU-IP1-N	No Effect in BS	☐ false	[]	1.43E-7	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	No Effects
Command 1							
Monitor 1							
Power 1 Monitor							
[WBS-BSCU-P1M-1] Monitor Stuck Valid	WBS-BSCU-P1M-	Monitor Stuck	☐ false	[]	3.69E-8	[WBS-BSCU-CH1-4] P/S Monitor Fails Valid in Channel 1	
[WBS-BSCU-P1M-2] Nuisance Monitor Trip	WBS-BSCU-P1M-	Nuisance Mon	☐ false	[]	6.91E-9	[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	
[WBS-BSCU-P1M-3] Monitor Stuck Tripped/Supply Shutdown	WBS-BSCU-P1M-	Monitor Stuck	☐ false	[]	7.47E-8	[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	
[WBS-BSCU-P1M-4] Monitor Sensivity Shifts	WBS-BSCU-P1M-	Monitor Sensiv	☐ false	[]	2.18E-8	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	
[WBS-BSCU-P1M-NE] No Effect in BSCU Power Monitor Ch1	WBS-BSCU-P1M-	No Effect in BS	☐ false	[]	1.80E-9	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	
Logic Channel 1							
[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	WBS-BSCU-CH1-	Power Supply (	☑ true	[Invalid P/S signal to other channel	1.07E-6	[WBS-BSCU-1] BSCU Channel 1 fails	
[WBS-BSCU-CH1-2] Increased Ripple in Channel 1	WBS-BSCU-CH1-	Increased Ripp	☐ false	[]	3.57E-7		Effect unknown. Laboratory analysis
[WBS-BSCU-CH1-3] Properly Operating P/S Monitor cannot shutdown P/S in Channel 1	WBS-BSCU-CH1-	Properly Opera	☐ false	[Card level test]	5.70E-7	[WBS-BSCU-2] Inability to shutdown P/S after failure in Chann	No obvious BSCU effect.
[WBS-BSCU-CH1-4] P/S Monitor Fails Valid in Channel 1	WBS-BSCU-CH1-	P/S Monitor Fa	☐ false	[Bench test]	3.69E-8	[WBS-BSCU-3] BSCU Channel 1 PS Monitor fails to mitigate err	Latent failure.
[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	WBS-BSCU-CH1-	P/S Monitor Tr	☑ true	[Invalid P/S signal to other channel	8.16E-8	[WBS-BSCU-1] BSCU Channel 1 fails	
[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	WBS-BSCU-CH1-	No Effect in BS	☐ false	[]	1.67E-7	[WBS-BSCU-NE] No Effect in BSCU	
Channel 2							
[WBS-BSCU-1] BSCU Channel 1 fails	WBS-BSCU-1	BSCU Channel	☐ false	[]	1.15E-6		
[WBS-BSCU-2] Inability to shutdown P/S after failure in Channel 1	WBS-BSCU-2	Inability to shu	☐ false	[]	5.70E-7		
[WBS-BSCU-3] BSCU Channel 1 PS Monitor fails to mitigate erroneous PS operation- LATENT	WBS-BSCU-3	BSCU Channel	☐ false	[]	3.69E-8		
[WBS-BSCU-X] BSCU Channel 2 PS Monitor fails to mitigate erroneous PS operation- LATENT	WBS-BSCU-X	BSCU Channel	☐ false	[]	3.69E-8		Taking the same FR value than WBS-
[WBS-BSCU-NE] No Effect in BSCU	WBS-BSCU-NE	No Effect in BS	☐ false	[]	1.67E-7		

Atica4Capella – Live demo



BSCU FMEA

	Failure Mode ID	Failure Mode	Is Observable (Failure Mode)	Detection Method (Failure Mode)	Failure Rate	Failure Effect	Review
Channel 1							
Internal Power 1							
[WBS-BSCU-IP1-1] +5V out of spec.	WBS-BSCU-IP1-1	+5V out of spe	☑ true	[Invalid P/S signal to other channel	2.14E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-2] +5V short to ground	WBS-BSCU-IP1-2	+5V short to gr	☑ true	[Invalid P/S signal to other channel	2.86E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-3] Loss of/reduced filtering	WBS-BSCU-IP1-3	Loss of/reduce	□ false	[]	3.57E-7	[WBS-BSCU-CH1-2] Increased Ripple in Channel 1	May cause spurious P/S monitor trip
[WBS-BSCU-IP1-4] +5V open	WBS-BSCU-IP1-4	+5V open	☑ true	[Invalid P/S signal to other channel	5.71E-7	[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	BSCU channel fails
[WBS-BSCU-IP1-X] PWM input from voltage monitor stuck valid	WBS-BSCU-IP1-X	PWM input fro	□ false	[Card level test]	5.70E-7	[WBS-BSCU-CH1-3] Properly Operating P/S Monitor cannot sh	
[WBS-BSCU-IP1-NE] No Effect in BSCU Internal Power Ch1	WBS-BSCU-IP1-N	No Effect in BS	□ false	[]	1.43E-7	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	No Effects
Command 1							
Monitor 1							
Power 1 Monitor							
[WBS-BSCU-P1M-1] Monitor Stuck Valid	WBS-BSCU-P1M-	Monitor Stuck	□ false	[]	3.69E-8	[WBS-BSCU-CH1-4] P/S Monitor Fails Valid in Channel 1	
[WBS-BSCU-P1M-2] Nuisance Monitor Trip	WBS-BSCU-P1M-	Nuisance Mon	□ false	[]	6.91E-9	[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	
[WBS-BSCU-P1M-3] Monitor Stuck Tripped/Supply Shutdown	WBS-BSCU-P1M-	Monitor Stuck	□ false	[]	7.47E-8	[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	
[WBS-BSCU-P1M-4] Monitor Sensivity Shifts	WBS-BSCU-P1M-	Monitor Sensiv	□ false	[]	2.18E-8	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	
[WBS-BSCU-P1M-NE] No Effect in BSCU Power Monitor Ch1	WBS-BSCU-P1M-	No Effect in BS	□ false	[]	1.80E-9	[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	
Logic Channel 1							
[WBS-BSCU-CH1-1] Power Supply (P/S) 1 shutdown	WBS-BSCU-CH1-	Power Supply (	☑ true	[Invalid P/S signal to other channel	1.07E-6	[WBS-BSCU-1] BSCU Channel 1 fails	
[WBS-BSCU-CH1-2] Increased Ripple in Channel 1	WBS-BSCU-CH1-	Increased Ripp	□ false	[]	3.57E-7		Effect unknown. Laboratory analysis
[WBS-BSCU-CH1-3] Properly Operating P/S Monitor cannot shutdown P/S in Channel 1	WBS-BSCU-CH1-	Properly Opera	□ false	[Card level test]	5.70E-7	[WBS-BSCU-2] Inability to shutdown P/S after failure in Chann	No obvious BSCU effect.
[WBS-BSCU-CH1-4] P/S Monitor Fails Valid in Channel 1	WBS-BSCU-CH1-	P/S Monitor Fa	□ false	[Bench test]	3.69E-8	[WBS-BSCU-3] BSCU Channel 1 PS Monitor fails to mitigate err	Latent failure.
[WBS-BSCU-CH1-5] P/S Monitor Tripped in Channel 1	WBS-BSCU-CH1-	P/S Monitor Tr	☑ true	[Invalid P/S signal to other channel	8.16E-8	[WBS-BSCU-1] BSCU Channel 1 fails	
[WBS-BSCU-CH1-NE] No Effect in BSCU Channel 1	WBS-BSCU-CH1-	No Effect in BS	□ false	[]	1.67E-7	[WBS-BSCU-NE] No Effect in BSCU	
Channel 2							
[WBS-BSCU-1] BSCU Channel 1 fails	WBS-BSCU-1	BSCU Channel	□ false	[]	1.15E-6		
[WBS-BSCU-2] Inability to shutdown P/S after failure in Channel 1	WBS-BSCU-2	Inability to shu	□ false	[]	5.70E-7		
[WBS-BSCU-3] BSCU Channel 1 PS Monitor fails to mitigate erroneous PS operation- LATENT	WBS-BSCU-3	BSCU Channel	□ false	[]	3.69E-8		
[WBS-BSCU-X] BSCU Channel 2 PS Monitor fails to mitigate erroneous PS operation- LATENT	WBS-BSCU-X	BSCU Channel	□ false	[]	3.69E-8		Taking the same FR value than WBS-
[WBS-BSCU-NE] No Effect in BSCU	WBS-BSCU-NE	No Effect in BS	□ false	[]	1.67E-7		

FMEA

Let’s work together!

Anzen Services

Anzen Products

Co-engineering

Gap Analysis

- ✓ Trade-off analysis of digital tools & Engineering frameworks
- ✓ Toolset selection
- ✓ Training

Modeling

- ✓ Support to Model Based Safety Analysis (MBSA)

Tailoring

ATICA adaptations on demand

Distribution

ATICA Distribution under License

Try ATICA from your web browser

https://www.anzenengineering.com/digital-tools/

Thank you very much!

Check out our blog

https://www.anzenengineering.com/anzen-wiki/

ANZEN

SYSTEM SAFETY AND DIGITAL ENGINEERING

Daniel Villafañe
Digital Engineering Lead
Anzen Engineering
danielvilla@anzenengineering.com

Fernando Macías
Senior Software Engineer
Anzen Engineering
fernandomacias@anzenengineering.com

Samuel García Lorente
Senior Safety Engineer
Anzen Engineering
samuelgarcia@anzenengineering.com

Back-up Slides