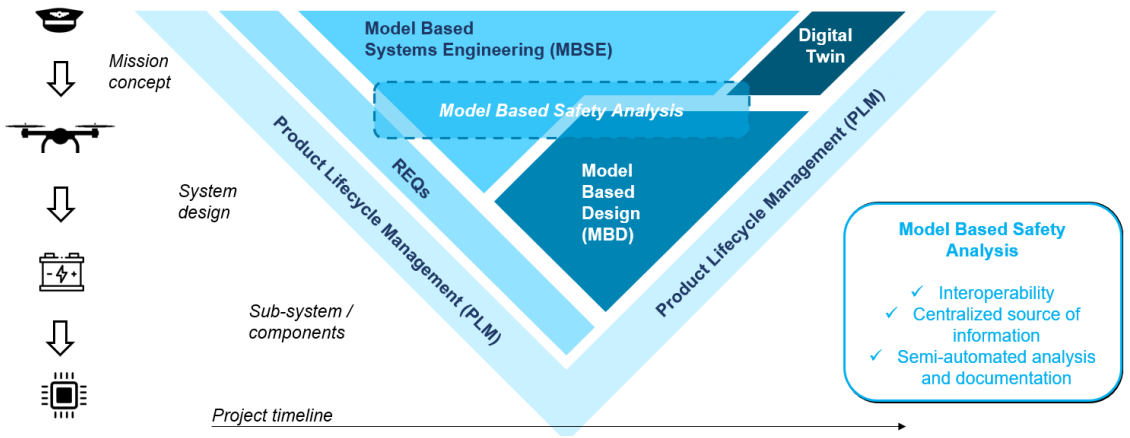
Model-driven design and development of an electromechanical actuation system

Outline

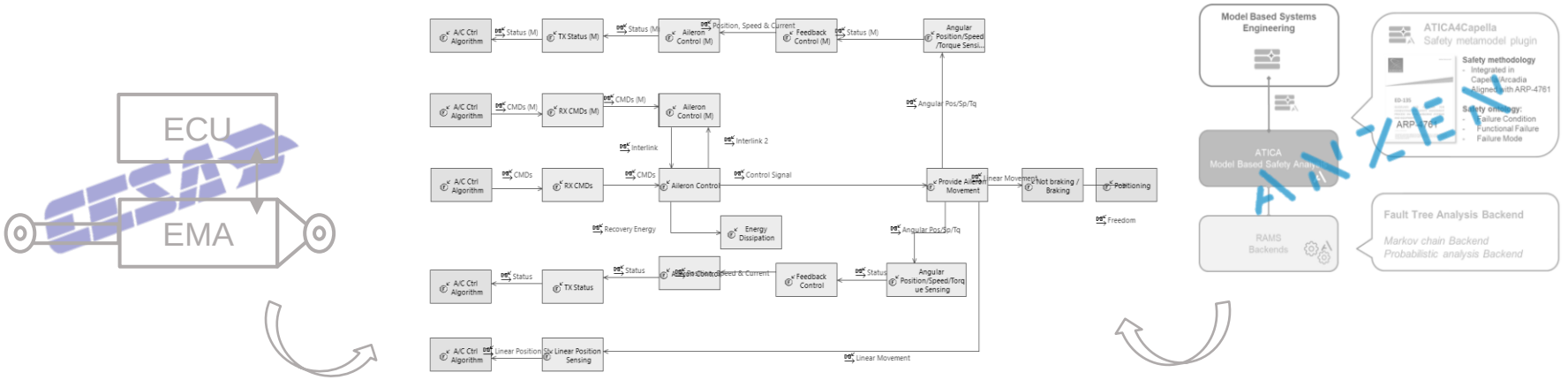
- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



Project Scope

- Model Based System Engineering (MBSE) applied to an Electromechanical actuation system
  - Evaluate the advantages of Model Based Safety Analysis (MBSA) offered by ATICA

- Collaboration between CESA and ANZEN:
  - CESA: Proposes system case study. Provides requirements and architecture. Builds the model.
  - ANZEN: Collaborates on CESA model creation. Provides MBSA tool.



Héroux-Devtek at a glance

≈ 70 Aerospace Platforms	
18 Commercial	18 Military cargo
6 Business Jet	12 Fighter Jet
7 Civil Helicopter	6 Military Helicopter
Apollo lunar module	≈ 300 Satellites

AEROSPACE COMPANY

WORLD'S 3RD LARGEST

LANDING GEAR MANUFACTURER

HÉROUX-DEVTEK SPAIN - CESA

310
EMPLOYEES

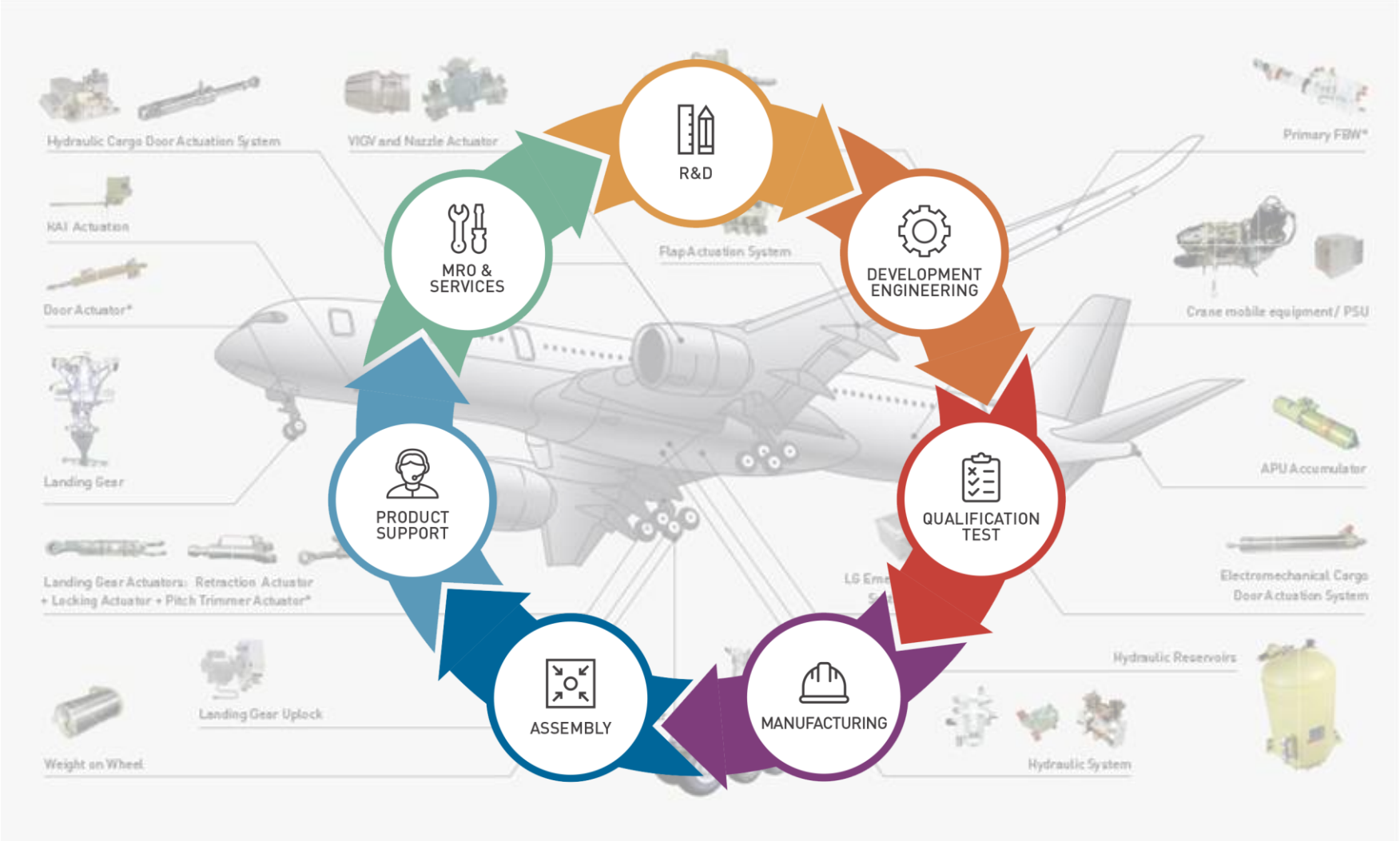
38.500
MANUFACTURING SQM
(MADRID & SEVILLE)

CUSTOMERS IN
ALL COUNTRIES

Hydraulic systems
EM Actuation System
Landing Gear Systems
Electronics

15% R&D of SALES
ANNUAL INVESTMENT

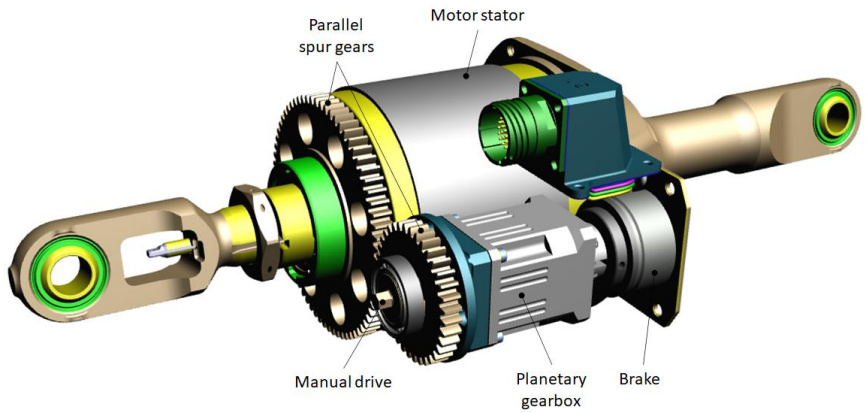
CESA S.A.U


R&D
DEVELOPMENT ENGINEERING
QUALIFICATION TEST
MANUFACTURING
ASSEMBLY
PRODUCT SUPPORT
MRO & SERVICES
Hydraulic Cargo Door Actuation System
VIGV and Nozzle Actuator
KAI Actuation
Door Actuator*
Landing Gear
Landing Gear Actuators: Retraction Actuator + Locking Actuator + Pitch Trimmer Actuator*
Landing Gear Uplock
Weight on Wheel
Flap Actuation System
Primary FBW*
Crane mobile equipment / PSU
APU Accumulator
Electromechanical Cargo Door Actuation System
Hydraulic Reservoirs
Hydraulic System


FOOTPRINT

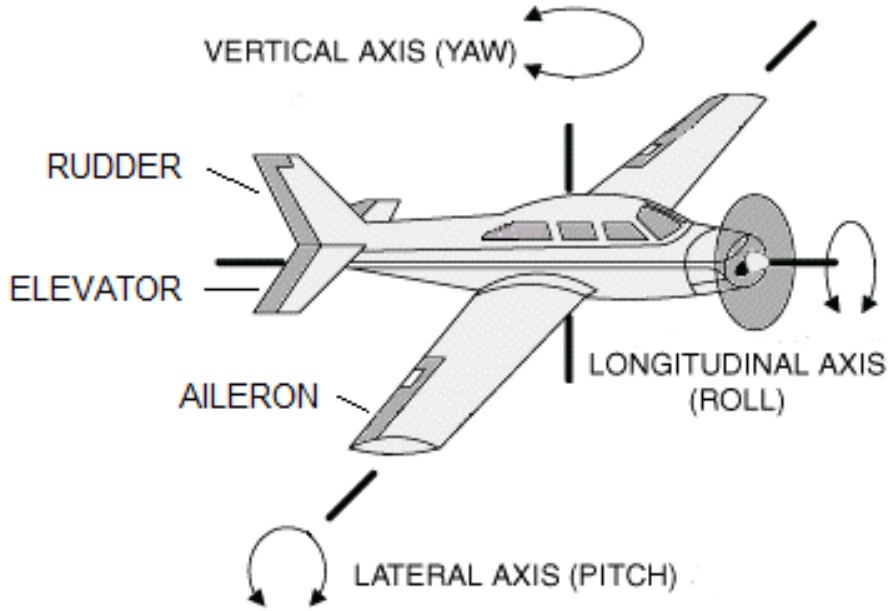
Outline

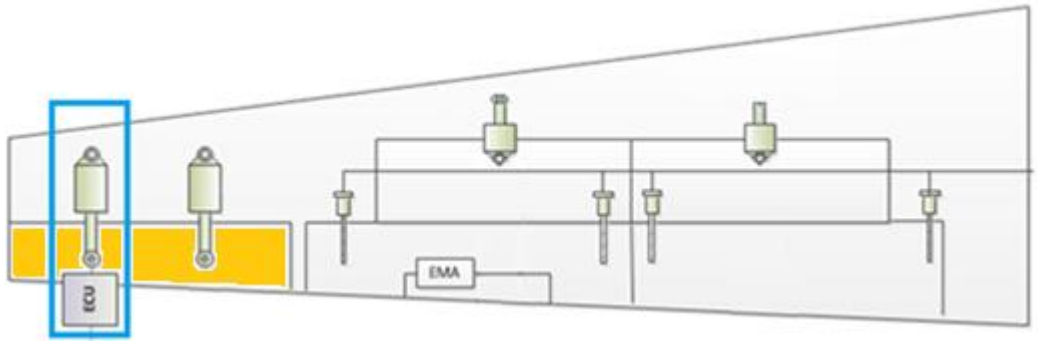
- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



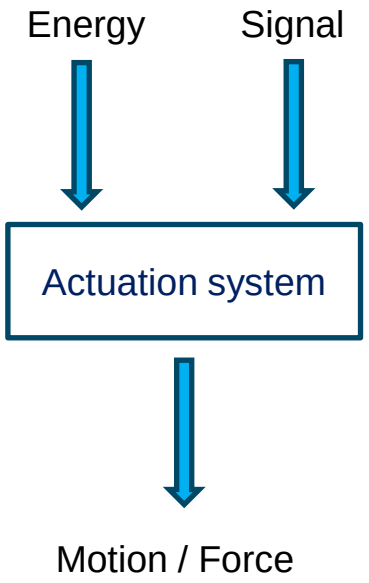
Electromechanical actuation system

- Primary flight control actuation system for a Turboprop Regional Aircraft
  - Linear electromechanical actuation for aileron Surface
  - Two actuation systems per Surface
  - The actuation system is based on an **Electromechanical Actuator** (EMA) and an **Electronic Control Unit** (ECU)
  - Two working modes:
    - Active: Responsible for aileron movement
    - Backdrive: No control over the aileron movement

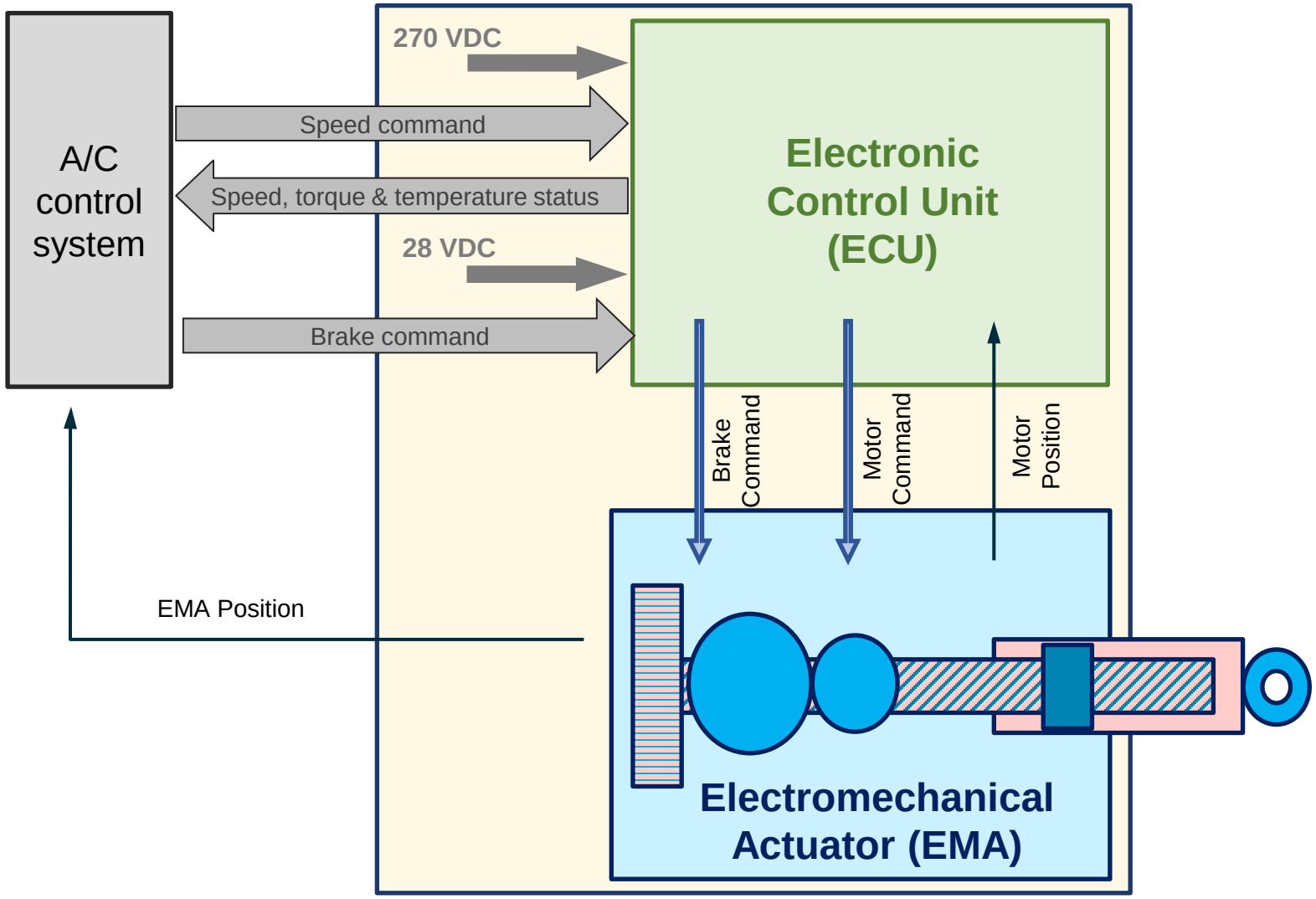




Electromechanical actuation system



Converts electric energy into linear mechanical force

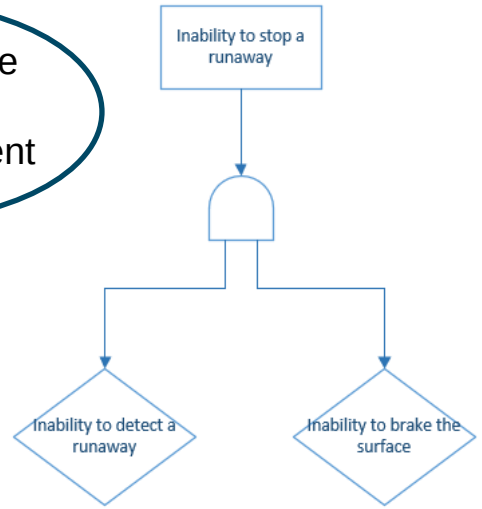


Electromechanical actuation system

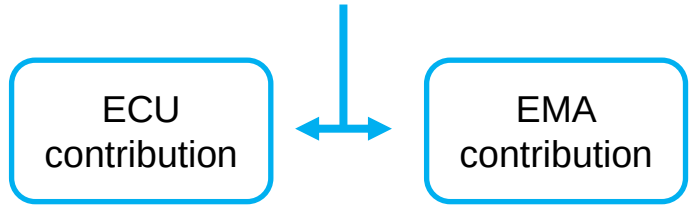
- System Safety Aspects
  - SAE-ARP4761 within the SAE-ARP4754A framework
  - Development Assurance Level A – most stringent

Catastrophic event	Hazardous event
Inability to stop a runaway	Runaway

No single failure shall lead to a catastrophic event



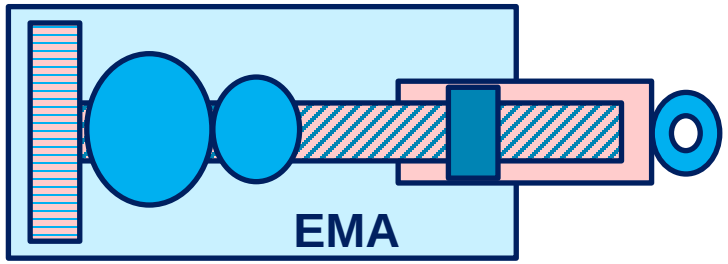
System Safety Requirements	
Failure to detect or correct runaway	1E-06/FH
Loss of control	1E-06/FH
Jamming	1E-08/FH
Runaway	1E-08/FH
Fail to brake the Surface	1E-06/FH

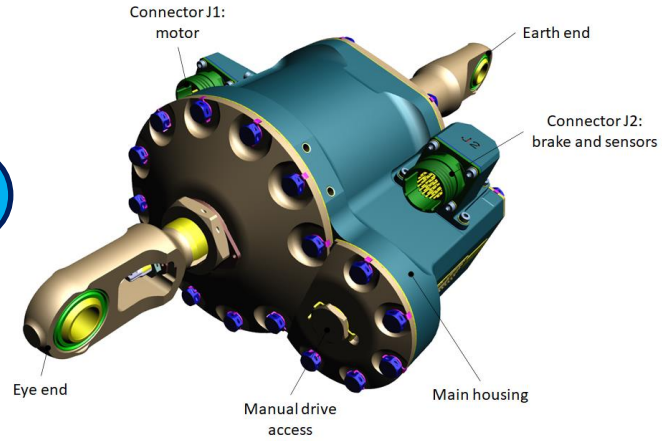


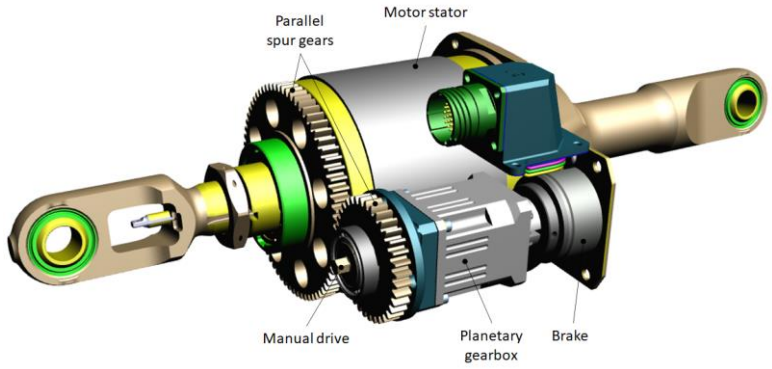
Electromechanical actuation system

- Electromechanical Actuator (EMA) – Main characteristics

	AILERON EMA
Architecture	Linear Direct Drive
Motor	PMSM
Power Supply	270 VDC (28 VDC for brake)
Stroke	± 31.4 mm
Rated Speed	65 mm/s @ 13.1 kN (ret.) 65 mm/s @ 5 kN (ext.)
Maximum Operational Load	27.5 kN
Power Consumption	2 kW
Includes	Normally closed brake Dual LVDT Dual resolver for rotor position feedback PT100 for motor temperature monitoring

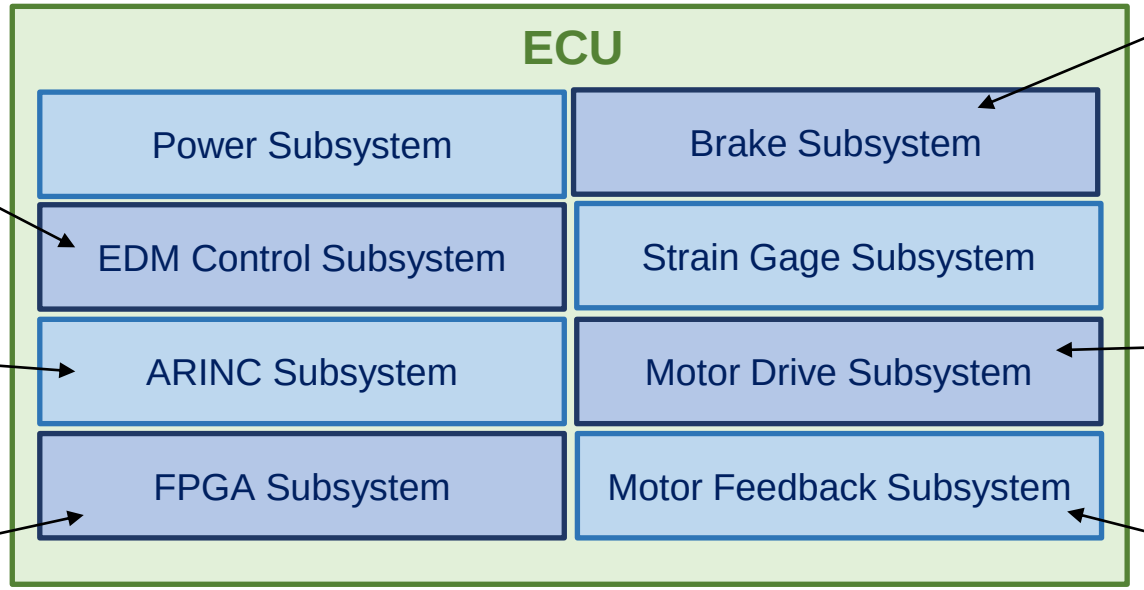


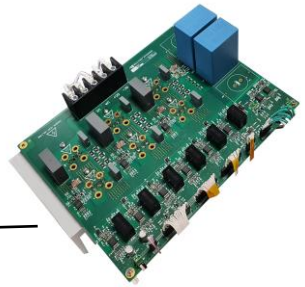




Electromechanical actuation system

- Electronic Control Unit (ECU) – Main characteristics
  - CONTROL / MONITOR architecture

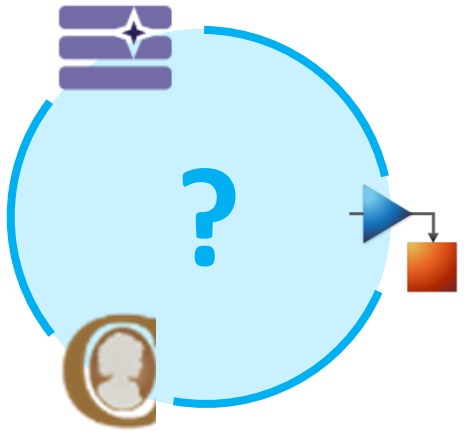




- Position loop closed by the A/C control system
- Brake command is managed by the A/C control system

Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



ANZEN worldwide

Specialization

- ✓ Complex electronics
- ✓ Safety Critical Systems
- ✓ Autonomous & software defined systems

Digitalization of systems engineering

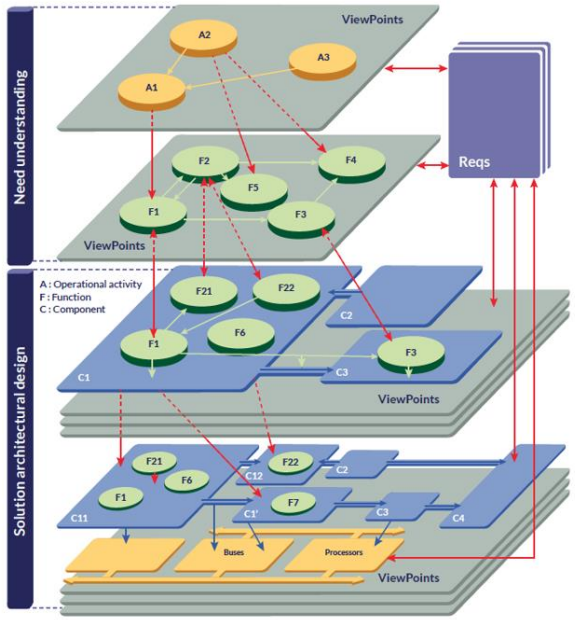
- ✓ Development and extension of model-based software tools for digitalization of the system & safety engineering process

System, safety and reliability experts

- ✓ Highly experienced system-safety & reliability engineers
- ✓ Specialization in complying with the highest quality standards for safety/availability critical missions

MBSE tools trade-off

Architectures and requirements outline

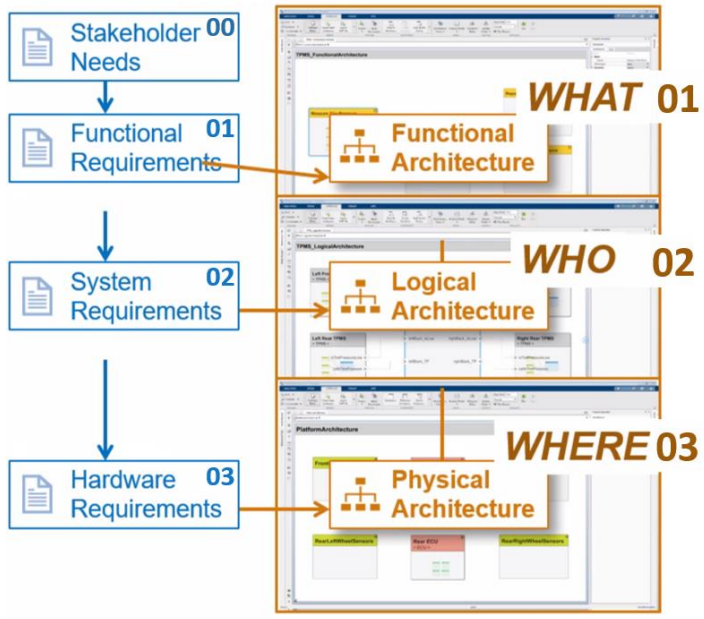


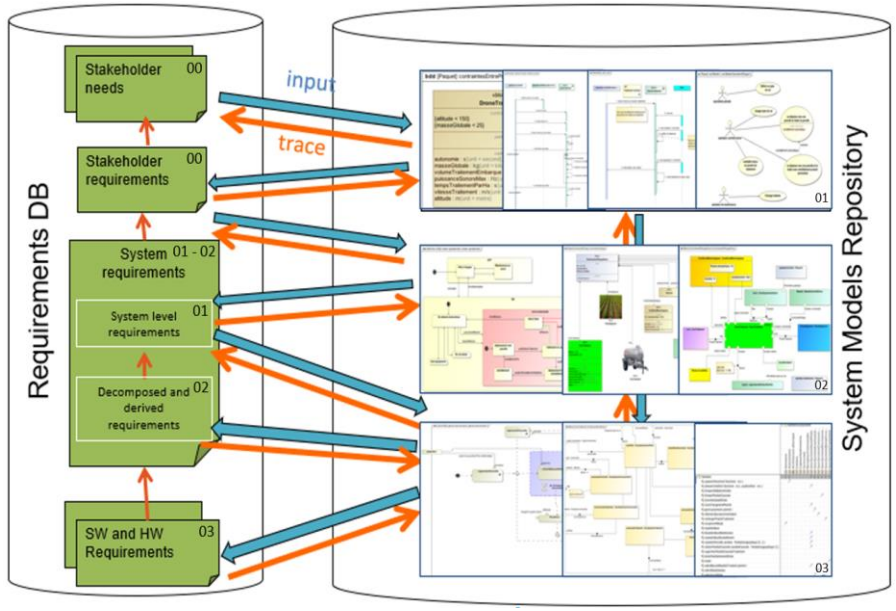
Operational Analysis 00
What the users of the system need to accomplish

Functional & Non Functional Need 01
What the system has to accomplish for the users

Logical Architecture 02
How the system will work to fulfill expectations

Physical Architecture 03
How the system will be developed and built





Capella (Arcadia method)

System Composer (Matlab)

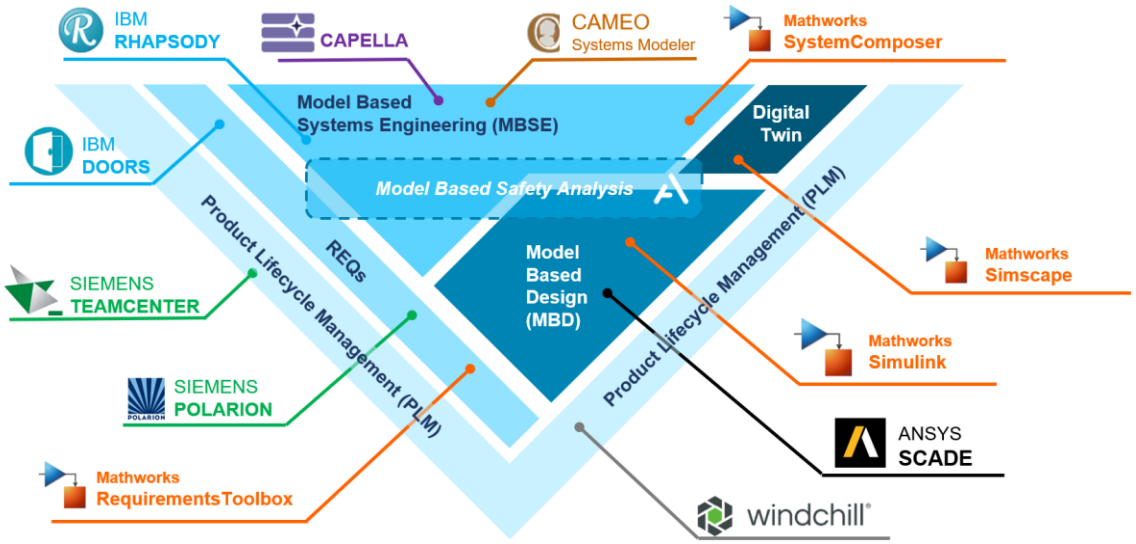
Cameo System Modeler (SysML)

MBSE tools trade-off

	Capella	System Composer	Cameo System Modeler
Architectures: Operational, System, Logical, Physical	Yes	Yes, with custom extension	Yes, with custom extension
Sequence diagrams	Yes	Yes	Yes
Mode / States diagrams	Yes	Yes, with State Flow	Yes
Requirement Management	Yes, with Requirements Viewpoint	Yes, with Requirements Toolbox	Yes, with Requirements Plugin
Functional Chains	Yes	No	Yes
Simulation	No	Yes, with Simulink	Yes, with Simulink
Safety model	Yes, with ATICA4Capella	Yes, with custom extension	Yes, with custom extension
Collaborative Work	Yes, with Team for Capella	No	Yes, with Cameo Collaborator
Open-Source Customization	Yes	No	No
Licenses	Free	Commercial	Commercial

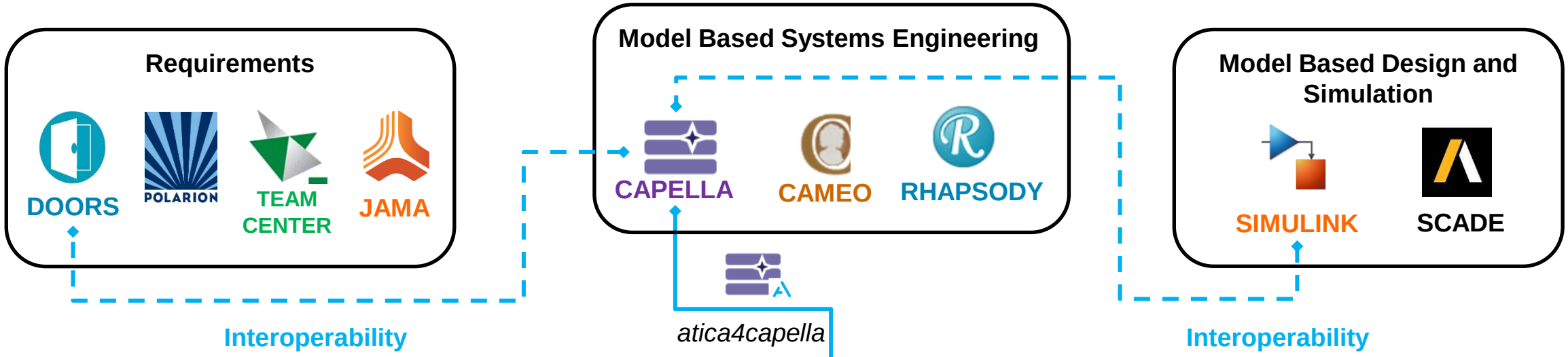
Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps

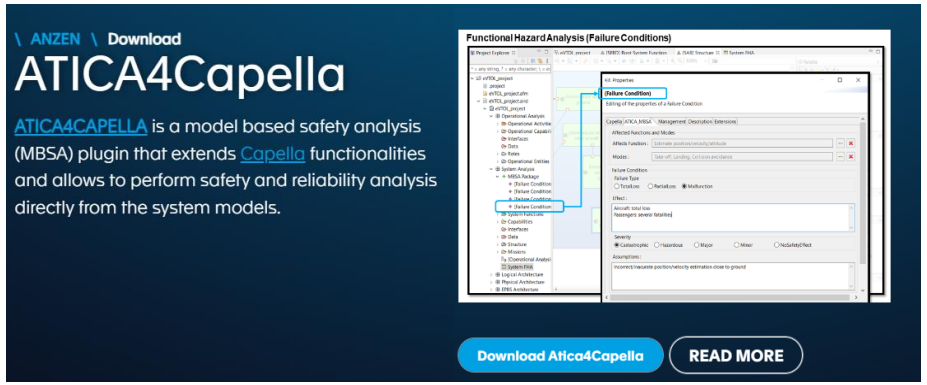


Digital engineering framework

ATICA
Digital engineering for complex systems



anzenengineering.com/atica4capella-download/



ATICA MBSA

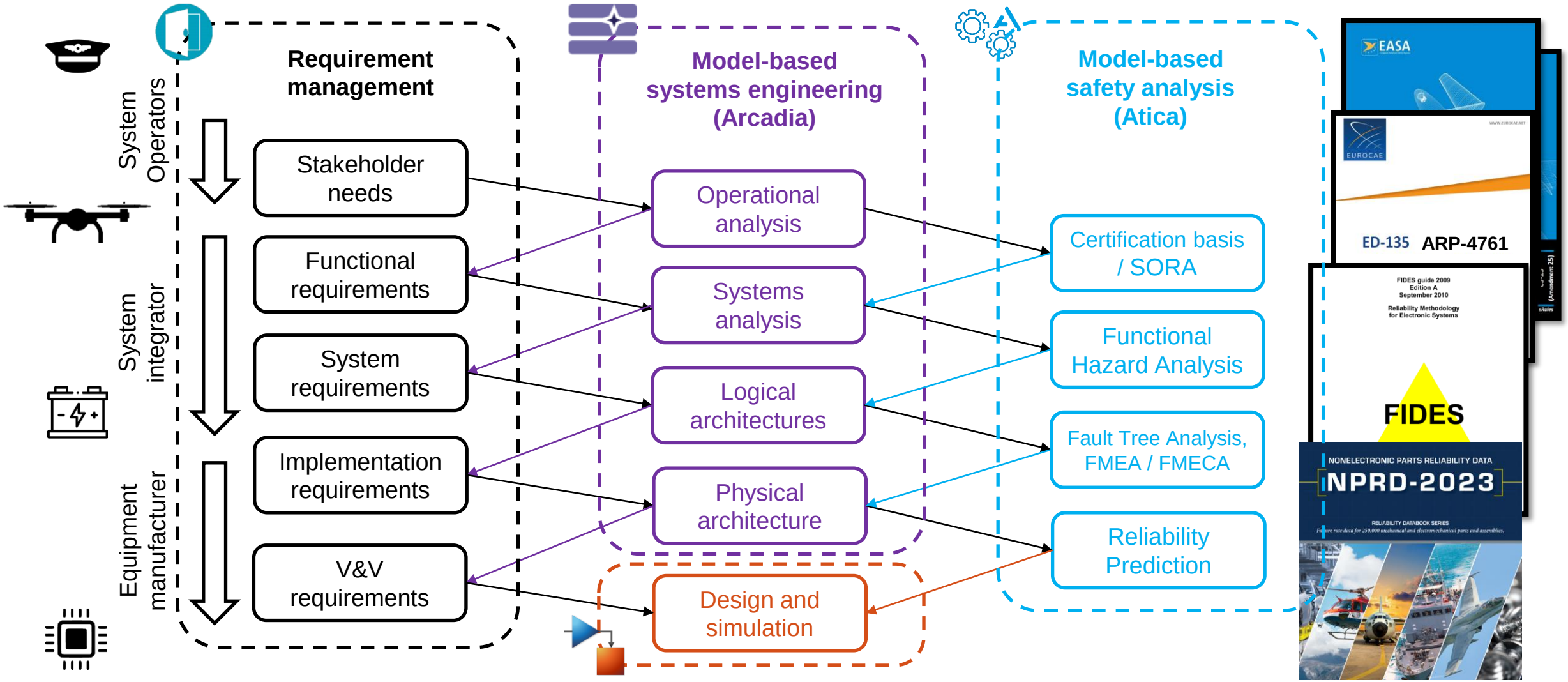
Safety & Reliability Analysis Backends

mbse-capella.org/webinars.html

Digital engineering framework

For systems engineering

ATICA
Digital engineering for complex systems



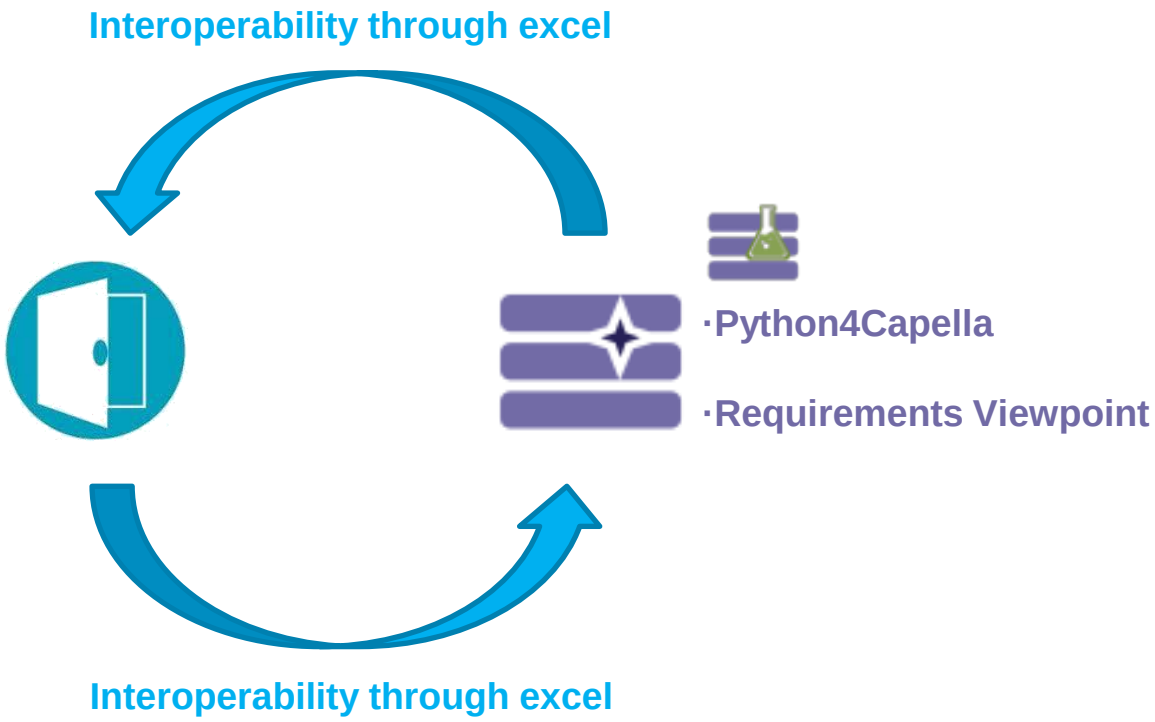
Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps

Interoperability

Requirements Management

with IBM DOORS



Purposes:

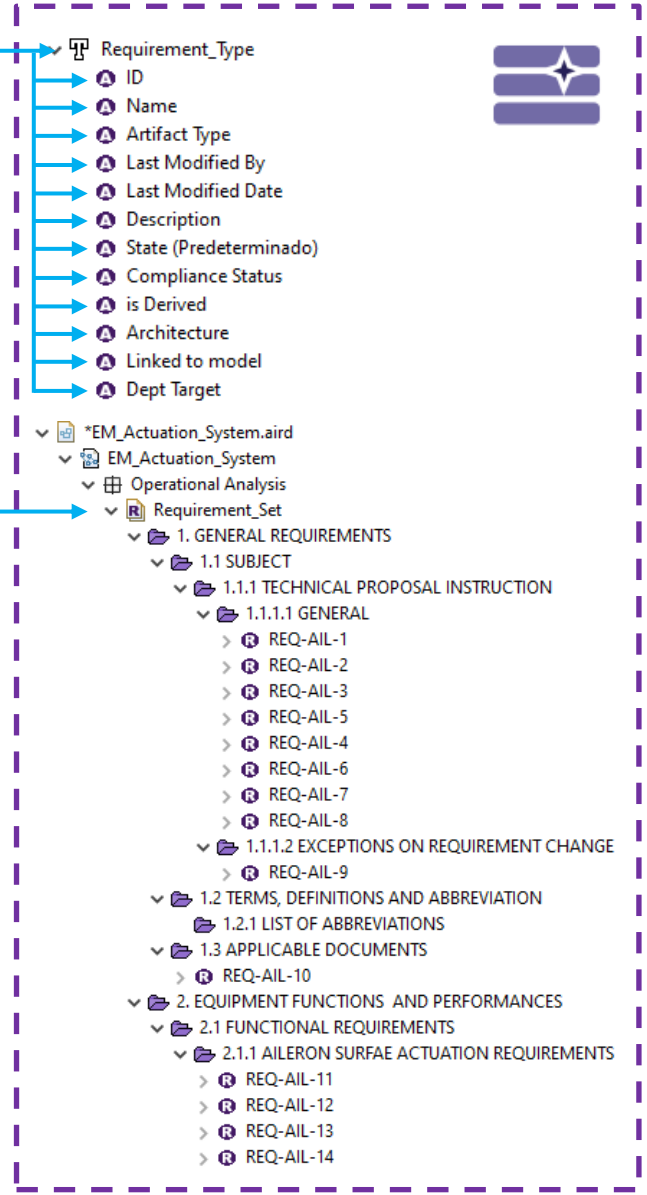
- Bidirectional interoperability between DOORS and Capella
- Requirements Management in Capella with Requirements Viewpoint
- Import / export test case working with Python4Capella
- Future replacement of Python4Capella by a GUI to import / export requirements inside the ATICA4Capella viewpoint

Requirements Management

with IBM DOORS

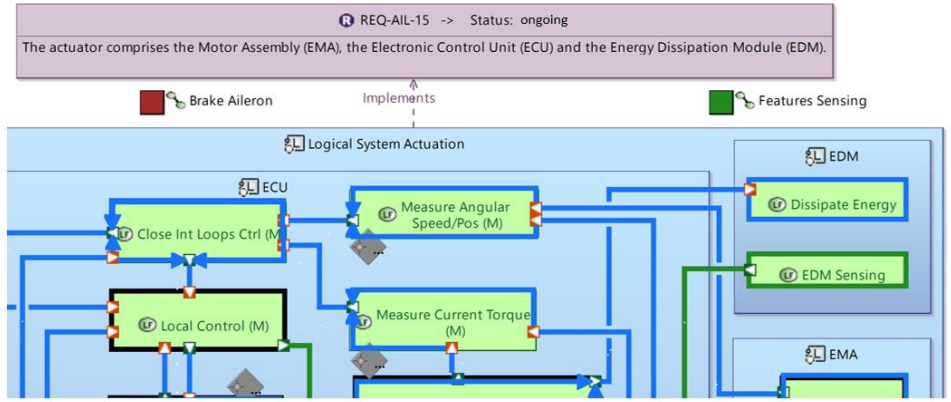
ID	Name	Artifact Type	Modified By	Modified On	State (...	Compliance Status	is Derived	Architecture	Linked to model	Dept Target
22656	1.	Header	Luis Cardenas	23 oct. 2023 14:39:29				System		
22657	1.1	Header	Luis Cardenas	23 oct. 2023 14:39:29				System		
22658	REQ-AIL-1	Requirement	Luis Cardenas	25 oct. 2023 16:49:40	Nuevo	Understood	False	System	No	RMTS
22659	REQ-AIL-2	Requirement	Luis Cardenas	25 oct. 2023 16:49:03	Nuevo	Compliance	False	System	No	RMTS
22660	REQ-AIL-3	Requirement	Luis Cardenas	25 oct. 2023 16:49:06	Nuevo	Compliance	False	System	No	RMTS
22661	REQ-AIL-4	Requirement	Luis Cardenas	25 oct. 2023 16:49:30	Nuevo	Compliance	False	System	No	RMTS
22662	1.1.1	Header	Luis Cardenas	23 oct. 2023 14:39:29				System		
22663	1.1.1.1	Header	Luis Cardenas	23 oct. 2023 14:39:29				System		
22664	REQ-AIL-5	Requirement	Luis Cardenas	25 oct. 2023 16:49:55	Nuevo	Compliance	False	System	No	RMTS
22665	REQ-AIL-6	Requirement	Luis Cardenas	25 oct. 2023 16:50:14	Nuevo	Compliance	False	System	No	RMTS
22666	REQ-AIL-7	Requirement	Luis Cardenas	23 oct. 2023 14:39:29	Nuevo	Understood	False	System	No	RMTS

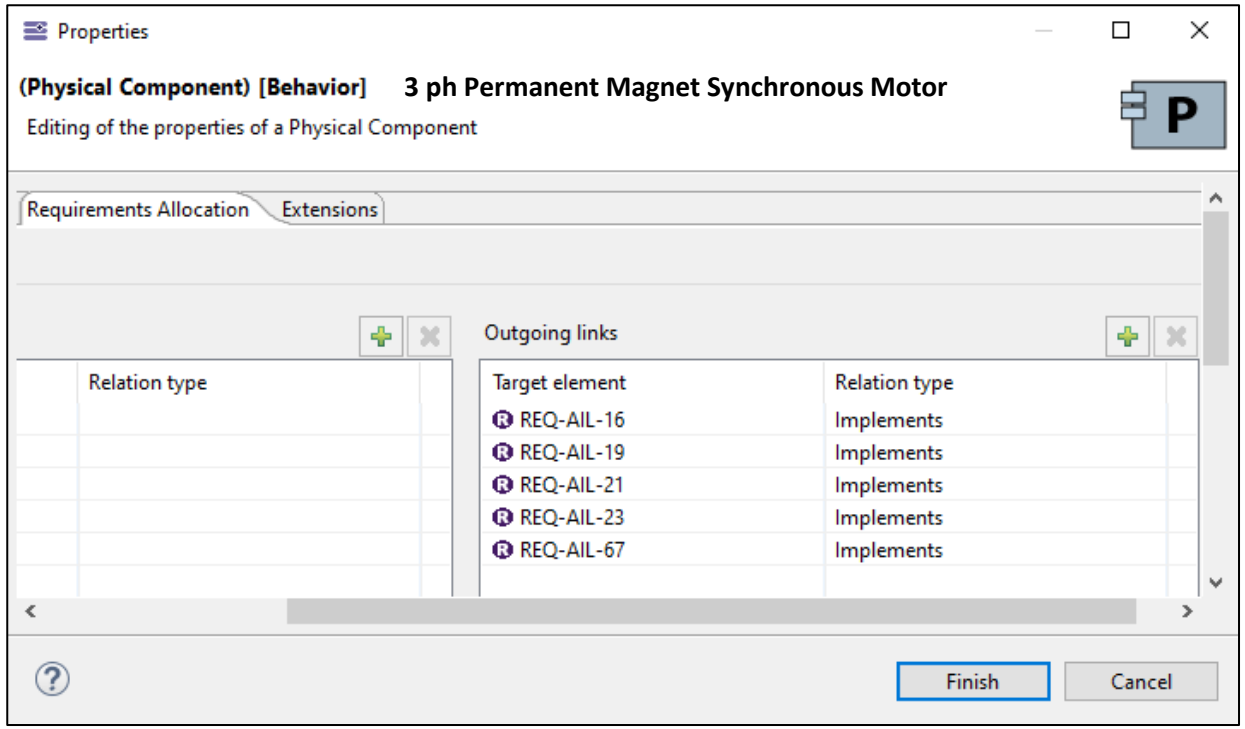
Showing 25 of 97 Artifacts



Requirements Management

with IBM DOORS





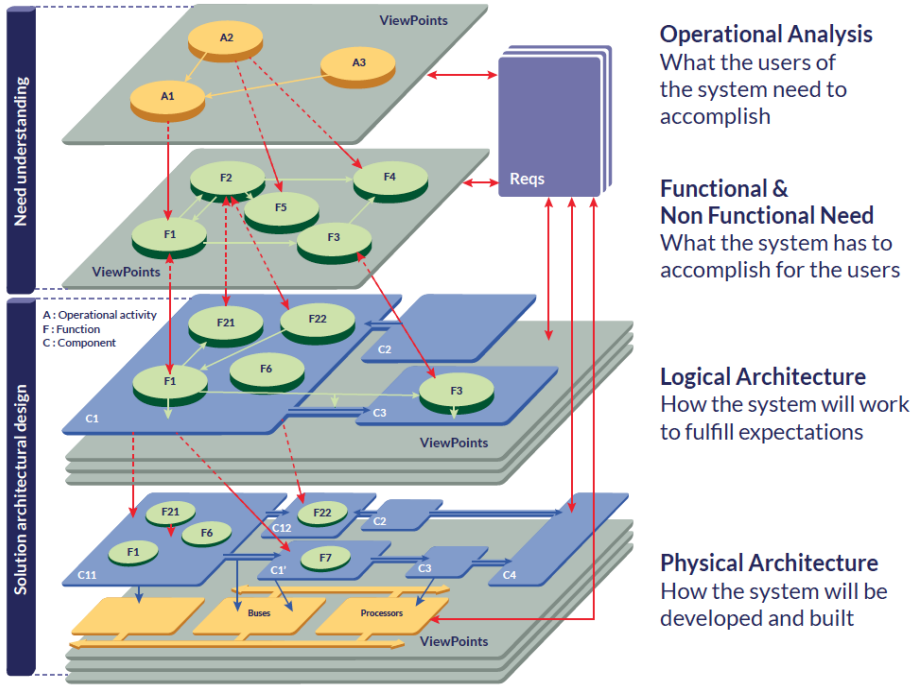
Properties | Console | Mass Visualization

Drag columns here to group by column values

	ReqIFName	ReqIFChapterName	ReqIFText	State (Pred...	Compliance Status	is Derived	Last Modified By	ID	Dept Target
R	REQ-AIL-67	2.1.3 | Actuator Design and C...	The motor assembly shall include the following major items at least:	Nuevo	Understood	false	Luis Cardenas	22751	RMTS
R	REQ-AIL-23	2. | EQUIPMENT FUNCTIONS ...	The actuator is responsible for the implementation of the movement command...	Nuevo	Understood	false	Luis Cardenas	22690	RMTS
R	REQ-AIL-21	2. | EQUIPMENT FUNCTIONS ...	The actuator will work in the following modes:	Nuevo	Understood	false	Luis Cardenas	22688	RMTS
R	REQ-AIL-19	2. | EQUIPMENT FUNCTIONS ...	Two dedicated EMA position sensors shall provide to ACE with the position of t...	Nuevo	Understood	false	Luis Cardenas	22686	RMTS
R	REQ-AIL-16	2. | EQUIPMENT FUNCTIONS ...	The magnet brushless motor shall provide rotary motion that should be convert...	Nuevo	Understood	false	Luis Cardenas	22683	RMTS

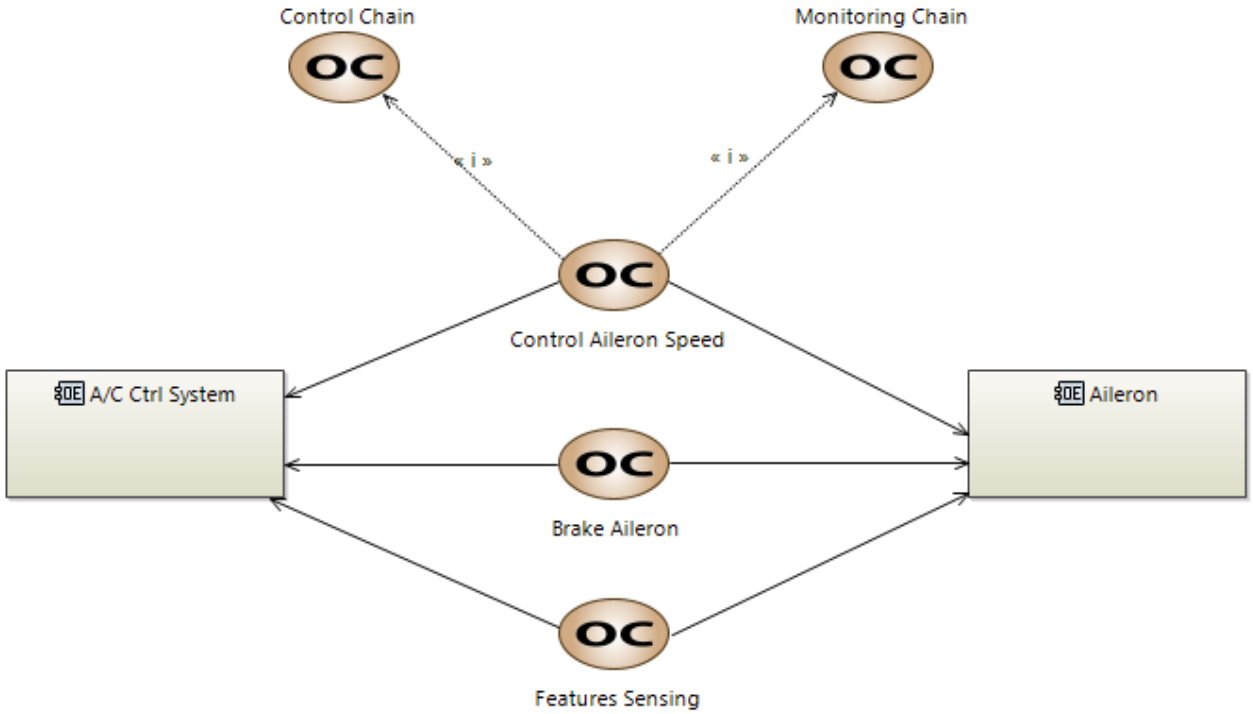
Outline

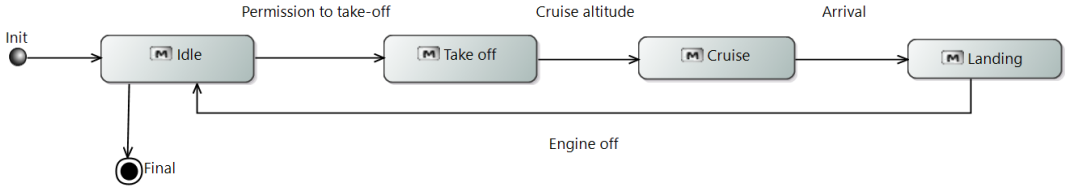
- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



System model

- Operational analysis
  - What the Customer expects

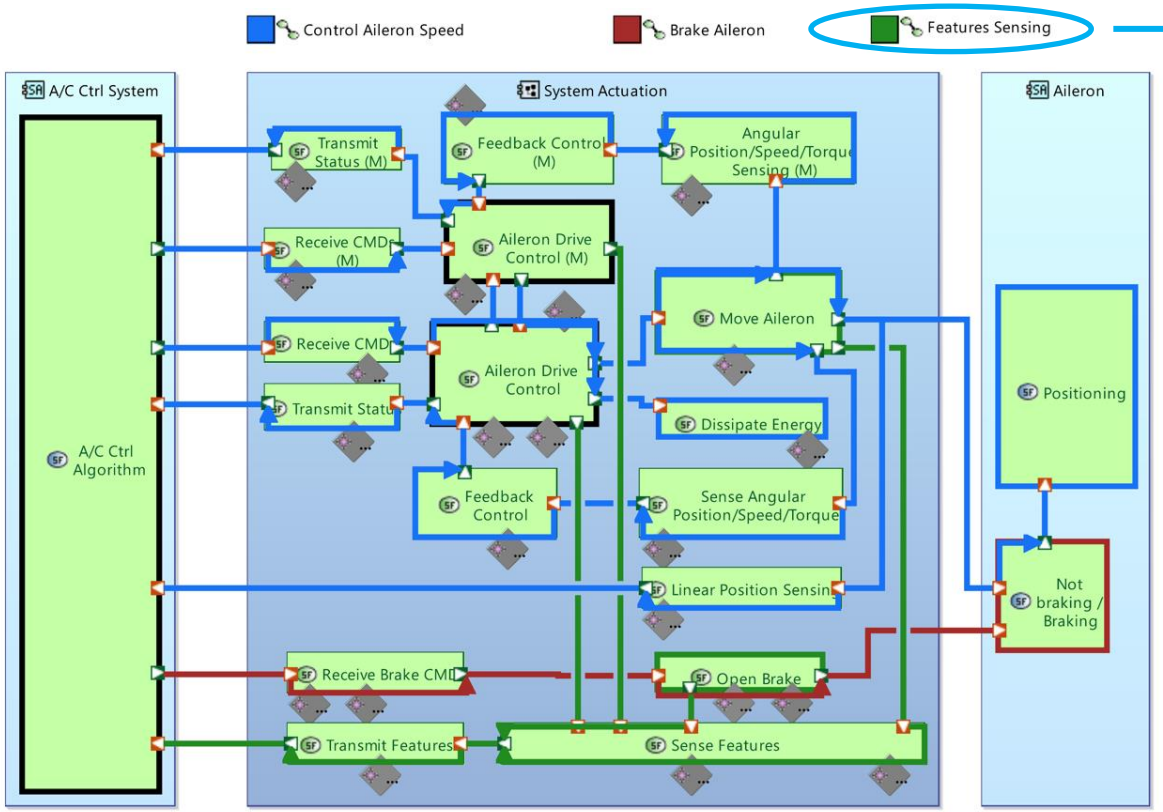


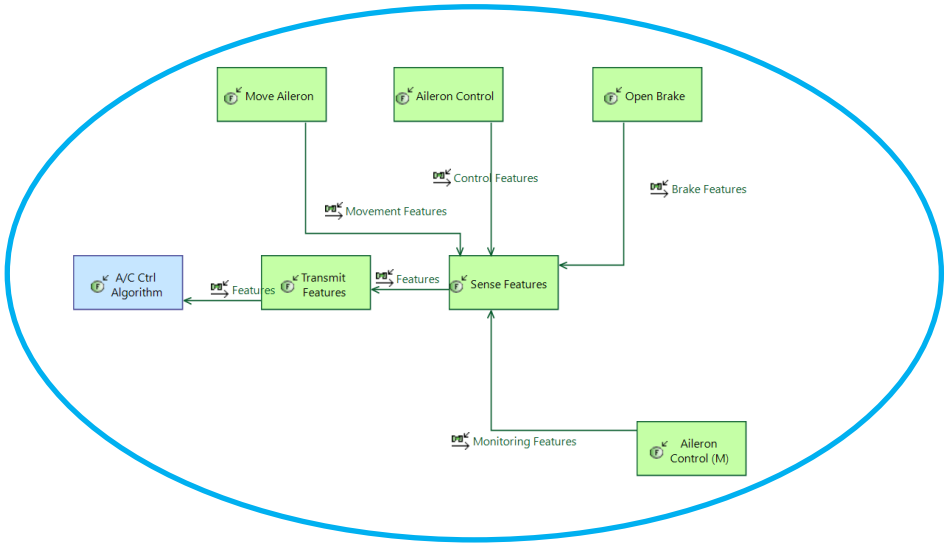


- Provide controlled linear movement compatible with DAL A → Control / Monitor architecture
- Enable to stop the movement and maintain position
- Provide status of parameters
- Definition of modes and states

System model

- System analysis
  - What the system has to accomplish

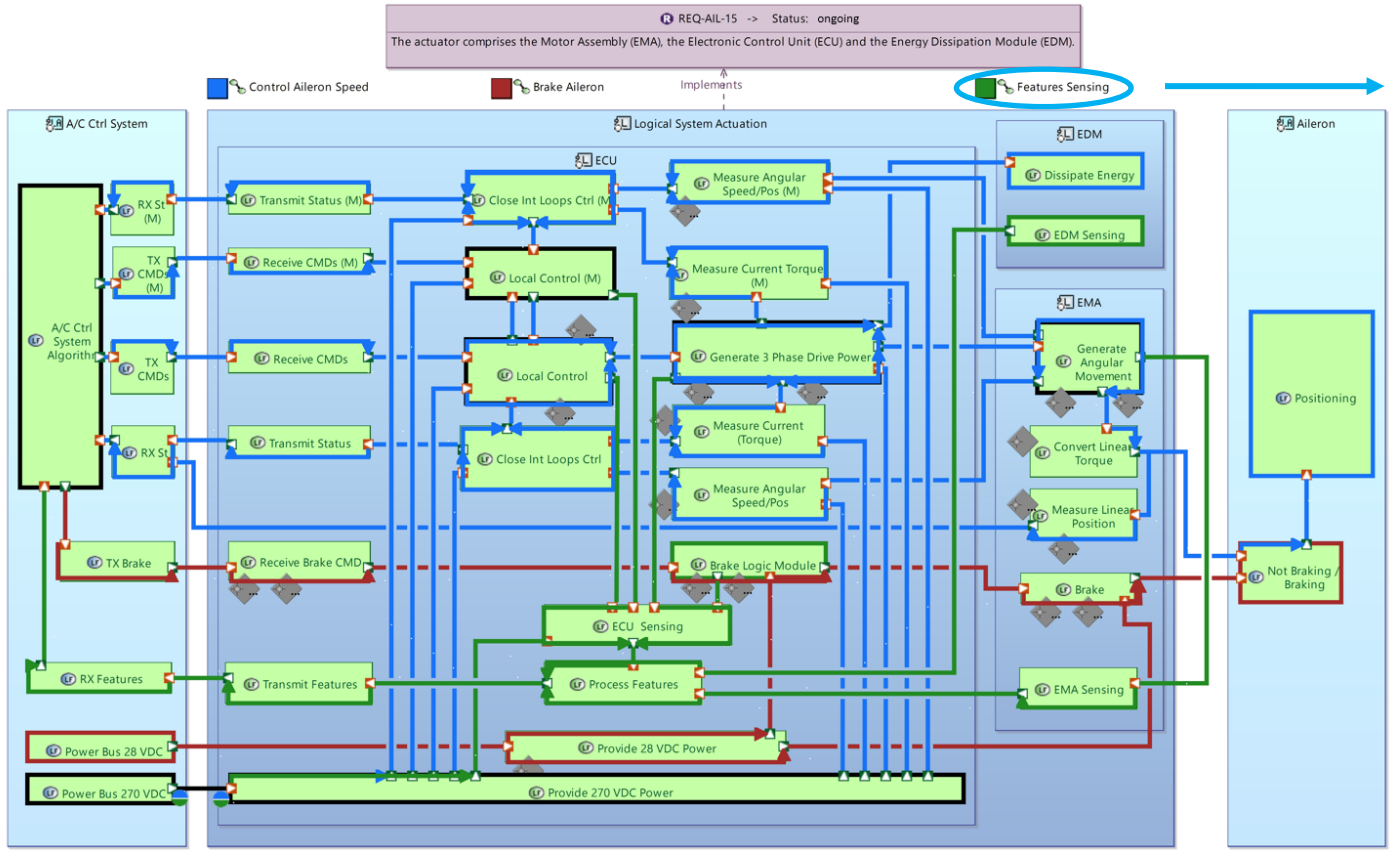


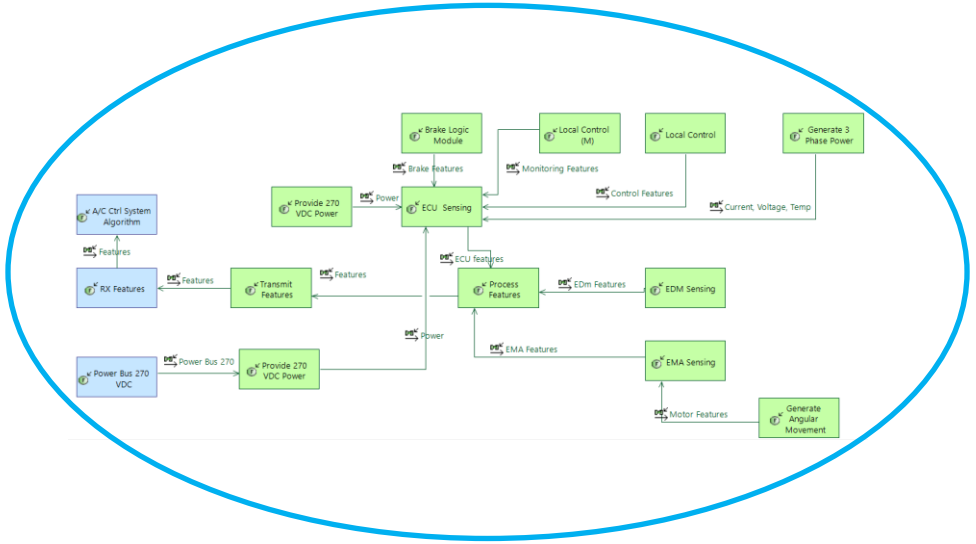


- Functions within the system to carry out the operational capabilities defined at Operational level
- Functional chains created for each operational capability
- System failure conditions
- Linked with requirements

System model

- Logical architecture
  - How the system is going to accomplish it

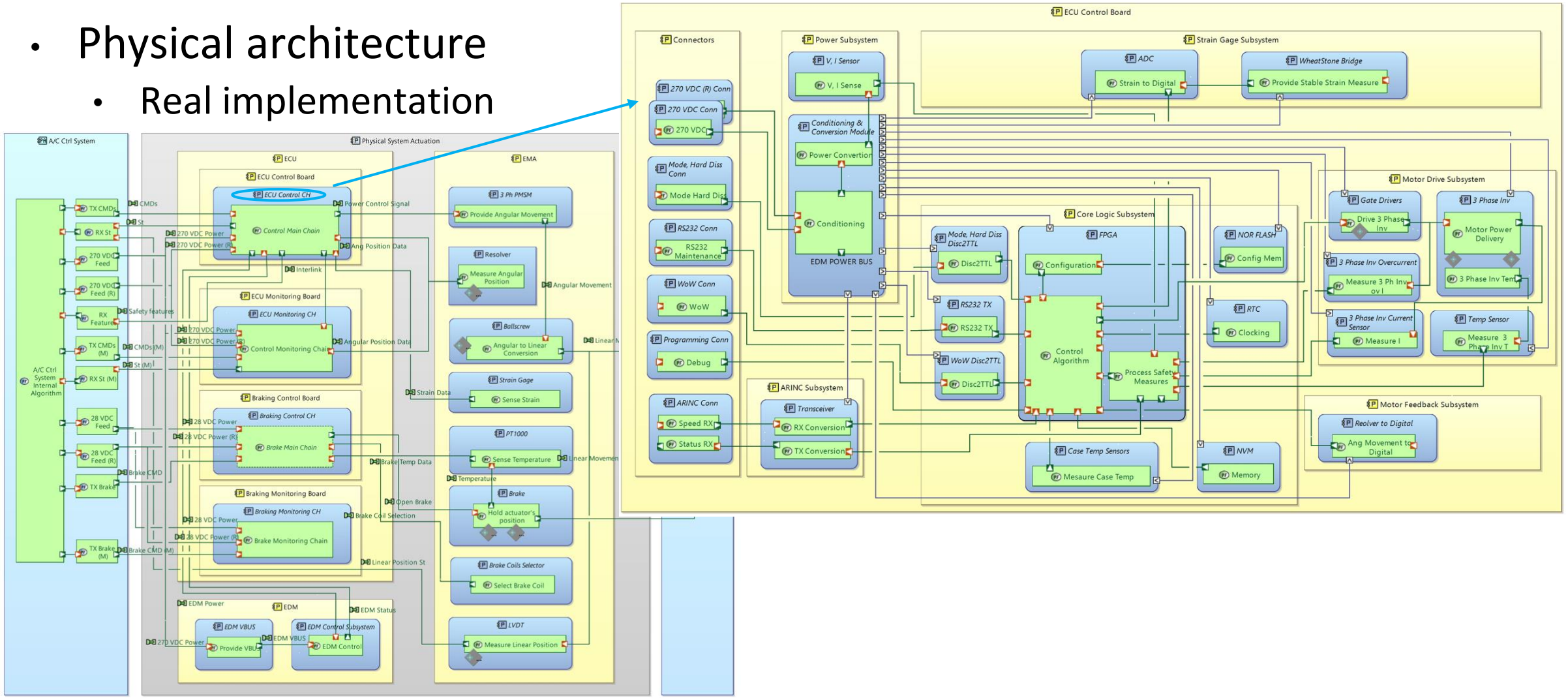




- Main components of the system
- Increased decomposition of the functional chains defined
- Main components failure modes
- Linked with requirements

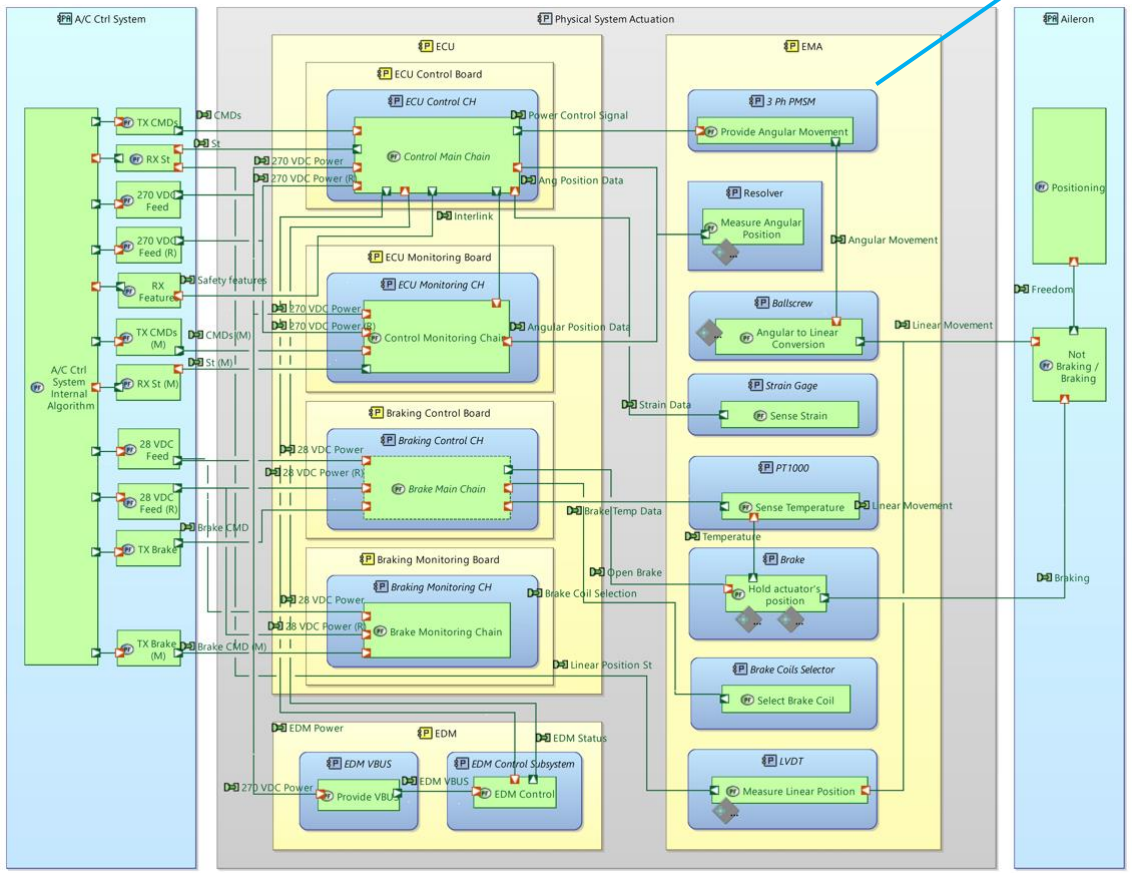
System model

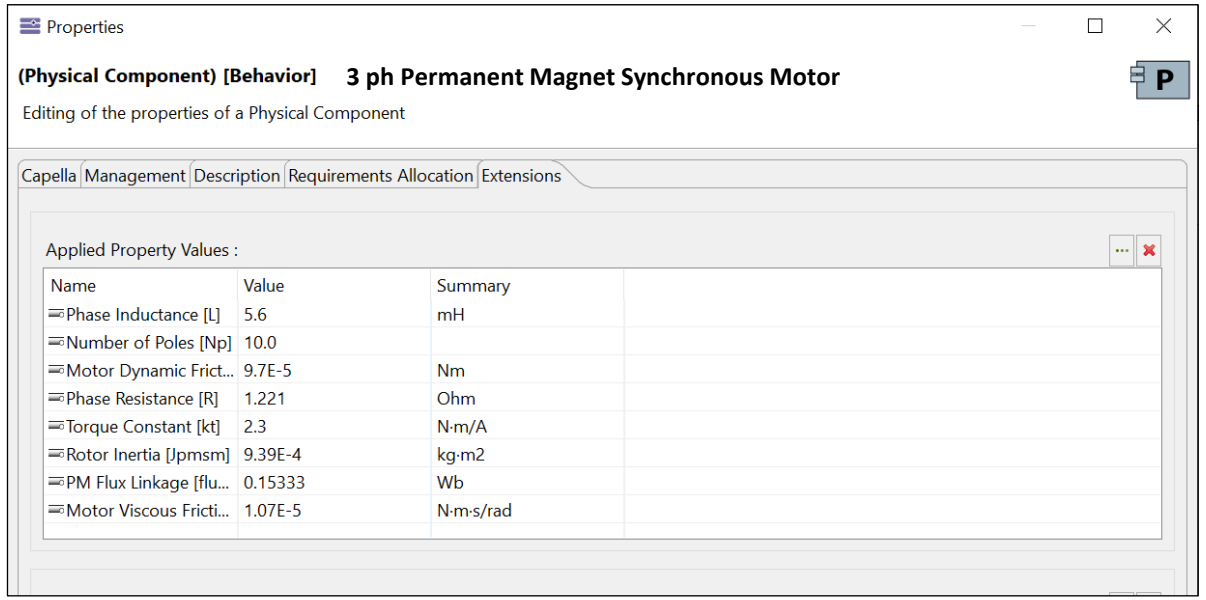
- Physical architecture
  - Real implementation



System model

- Physical architecture
  - Real implementation

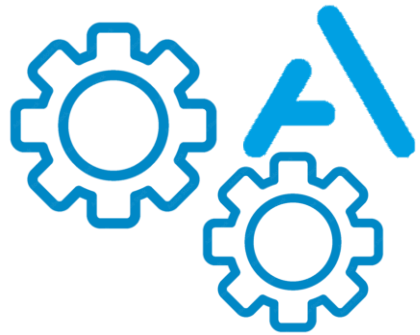




- Breakdown of the system's main components into physical boards and parts
- Component information included
- Lower-level failure modes
- Linked with requirements

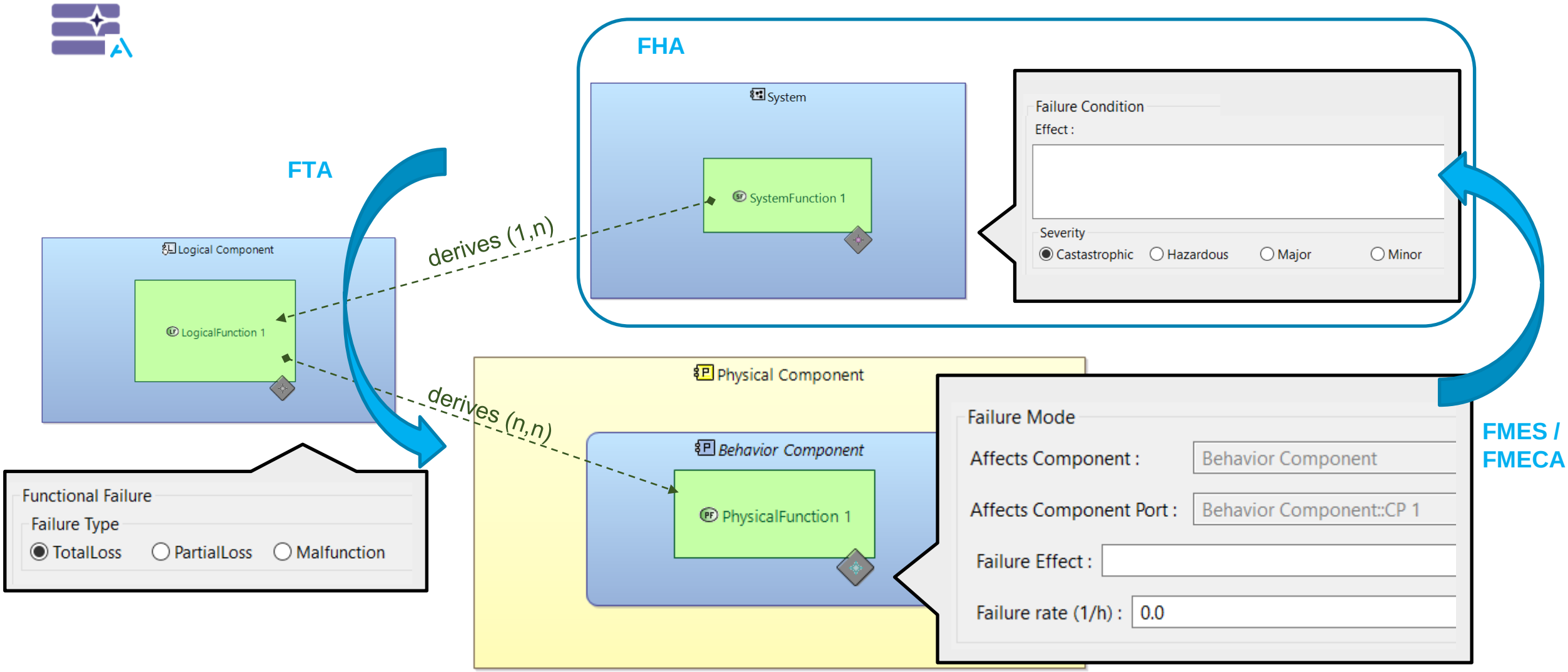
Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



ATICA4Capella | Safety metamodel

ATICA
Digital engineering for complex systems

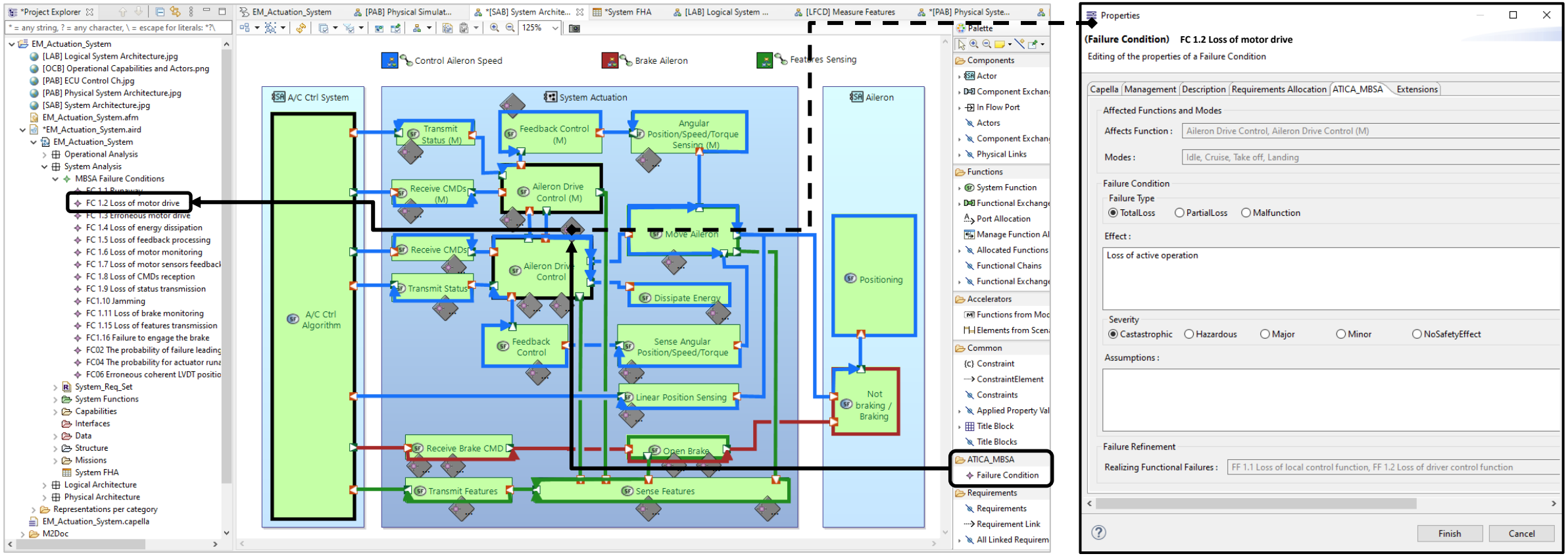


ATICA4Capella

System level

Model Based Safety Analysis
Functional Hazard Analysis (FHA)

ATICA
Digital engineering for complex systems



ATICA4Capella

System level

Model Based Safety Analysis
Functional Hazard Analysis (FHA)

ATICA
Digital engineering for complex systems

	Description	Modes	Failure Type	Effect of failure condition	Severity
Aileron Drive Control		[]			
FC 1.1 Runaway	Erratic and uncontrolled movement of the actuator	[Idle, Cruise, Take off, Landing]	Malfunction	Possible break of the actuator and aileron surfaces	Castastrophic
FC 1.2 Loss of motor drive	Loss of control capabiltiy	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of active operation	Minor
FC 1.3 Erroneous motor drive	Erroneous control capabilty	[Idle, Cruise, Take off, Landing]	Malfunction	Erroneous active operation	Hazardous
Open Brake		[]			
FC1.6 Jamming	Locking of any movable component	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of all operations	Hazardous
FC1.16 Failure to engage the brake	Loss of brakring capability	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of blocking operation	Castastrophic
Receive CMDs		[]			
FC 1.8 Loss of CMDs reception	Loss of CMD from the A/C control	[Idle, Cruise, Take off, Landing]	TotalLoss	Erroneous operation	Hazardous
Move Aileron		[]			
FC1.6 Jamming	Locking of any movable component	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of all operations	Hazardous
Dissipate Energy		[]			
FC 1.4 Loss of energy dissipation	Loss of motor recovery enery dissipation	[Idle, Cruise, Take off, Landing]	TotalLoss	Possible break of the control electronics due to overvoltage	Castastrophic
Receive Brake CMD		[]			
FC1.6 Jamming	Locking of any movable component	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of all operations	Hazardous
FC1.16 Failure to engage the brake	Loss of brakring capability	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of blocking operation	Castastrophic
Sense Angular Position/Speed/Torque		[]			
FC 1.7 Loss of motor sensors feedback adquisition	Loss of control feedback data	[Idle, Cruise, Take off, Landing]	TotalLoss	Loss of active operation	Minor

FHA

Aligned with **ARP4761** prescriptions

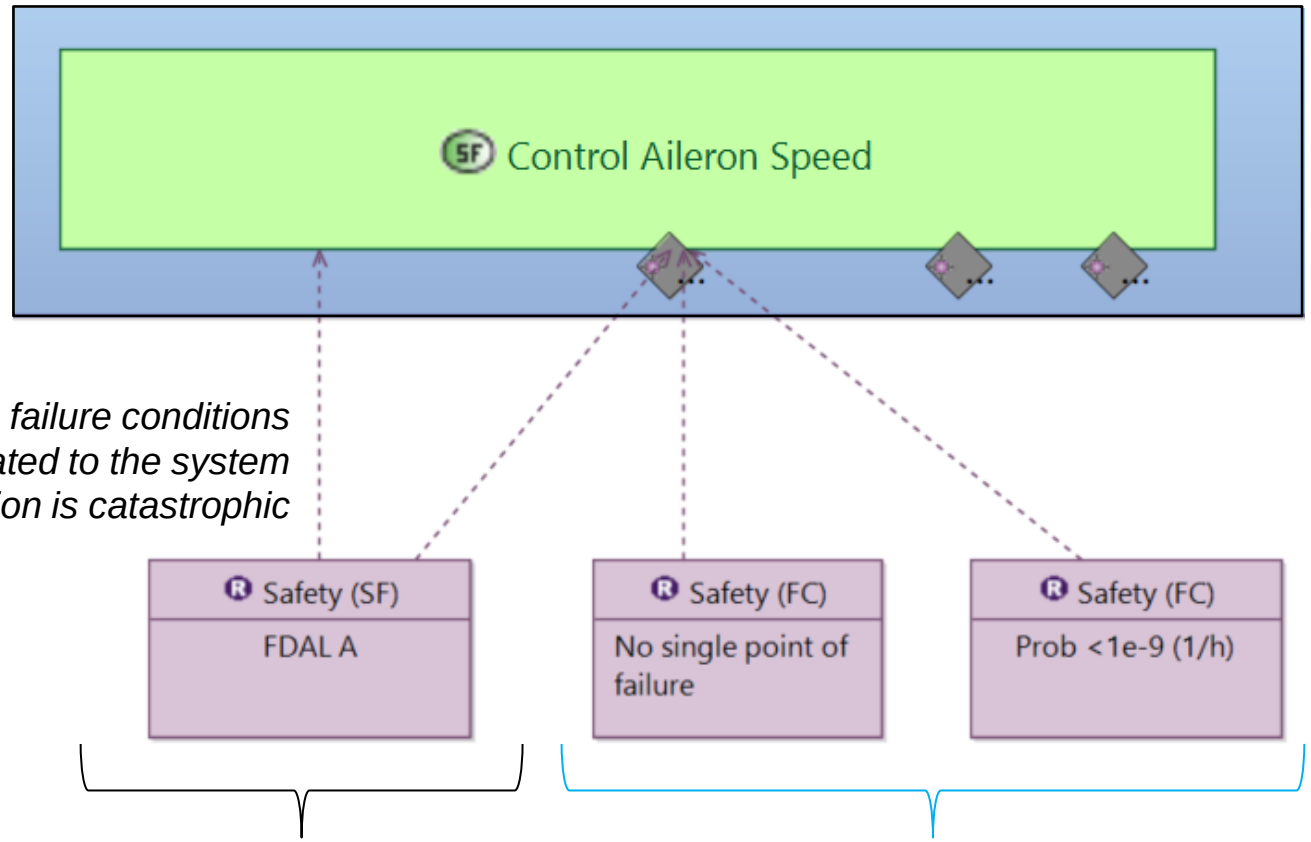
Table A-7 - AFHA Format Example

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	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

ATICA4Capella & Requirements Viewpoint

ATICA
Digital engineering for complex systems

Function Development Assurance Level (F-DAL) assignment based on FHA results



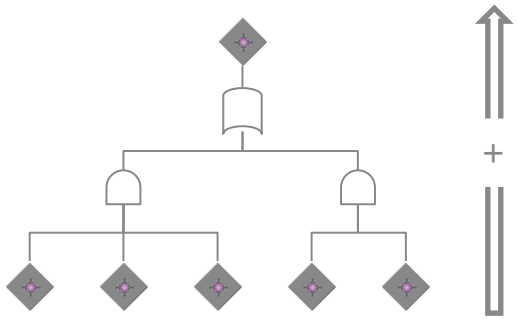
One of the failure conditions associated to the system function is catastrophic

Requirements associated to the system function, to be considered during the design

Requirements impacting the failure condition, to be verified by safety analysis

Requirements associated to the system function, to be considered for during the design

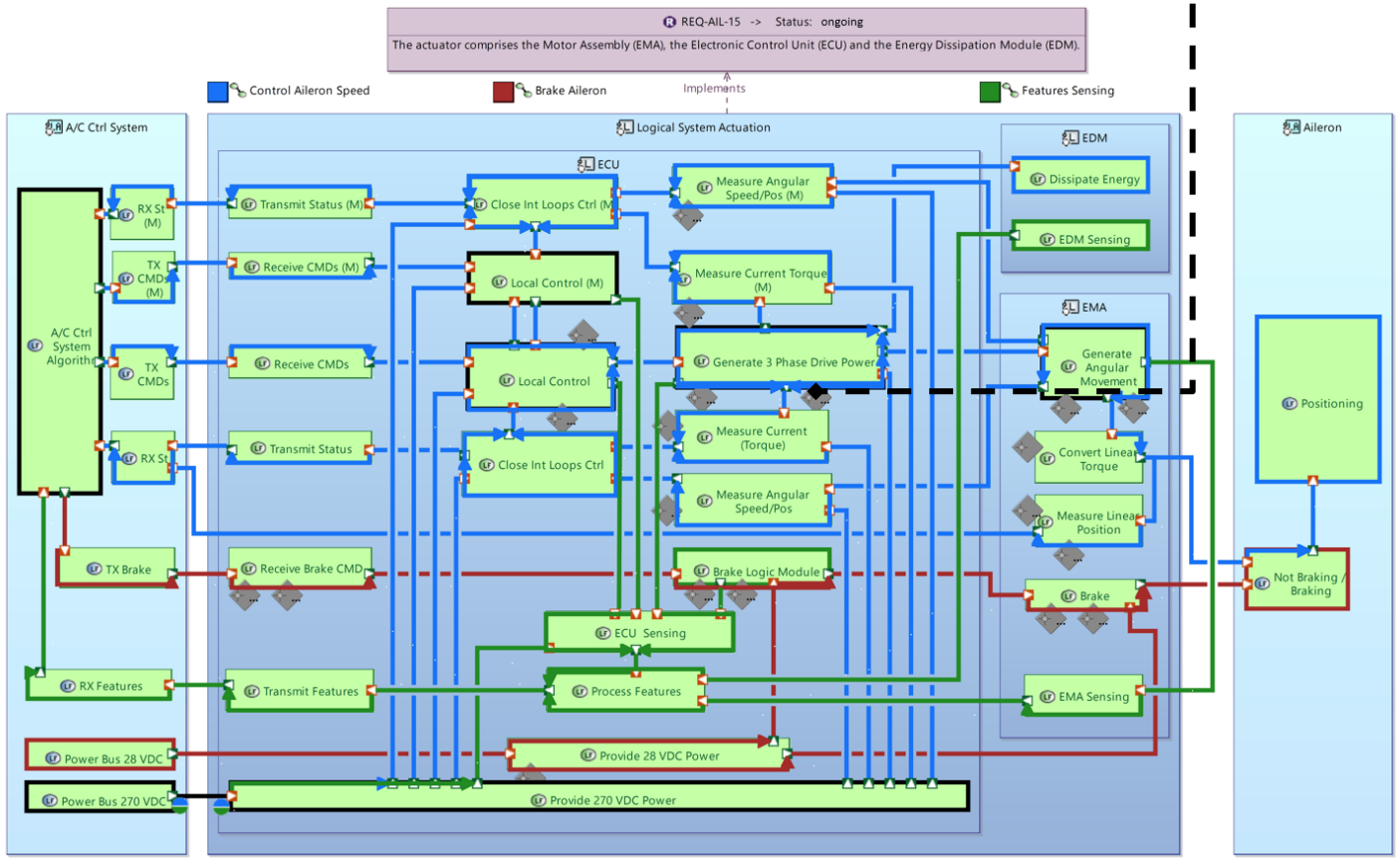
ATICA will assist the modelling process providing warnings when conditions associated to certain requirements are not met

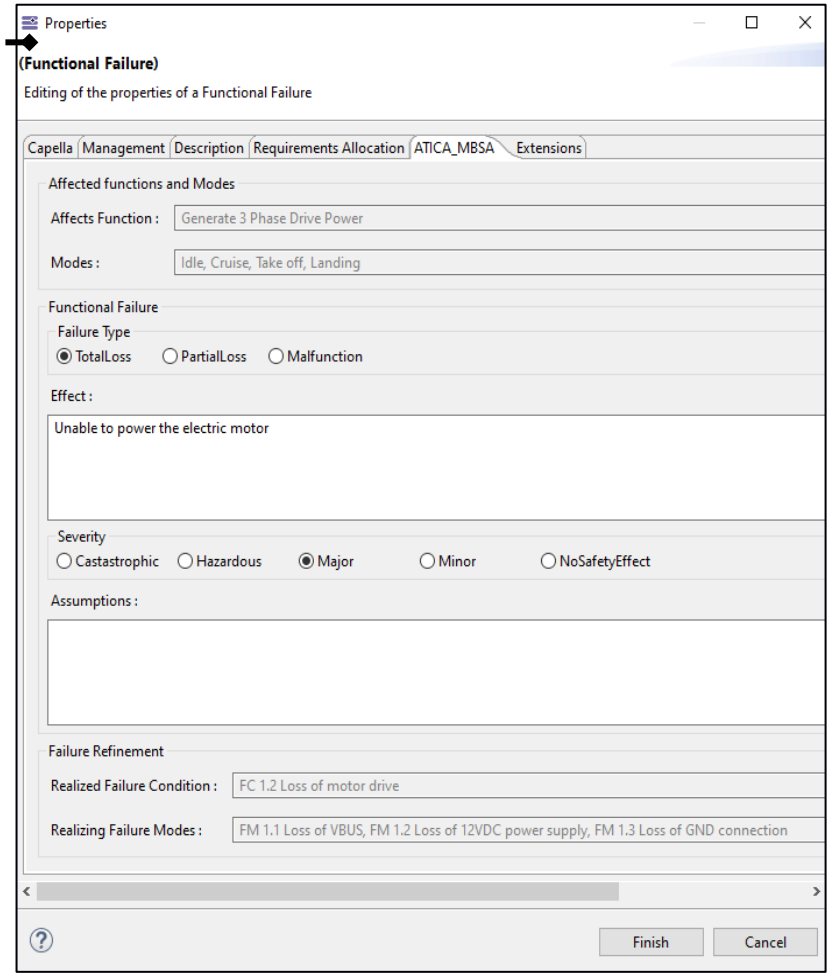


New Feature
Under consolidation

ATICA4Capella | Model Based Safety Analysis

Logical level

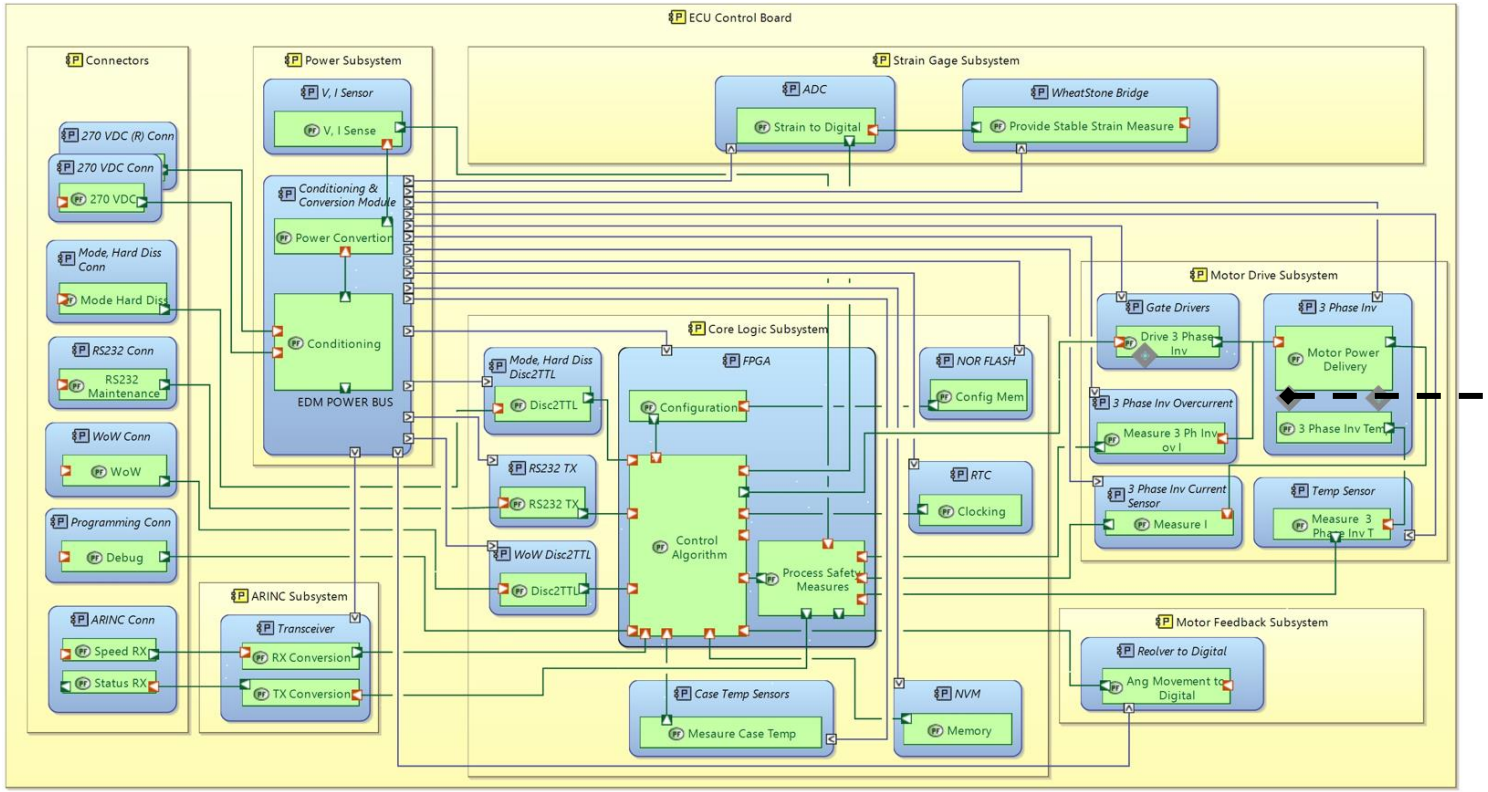


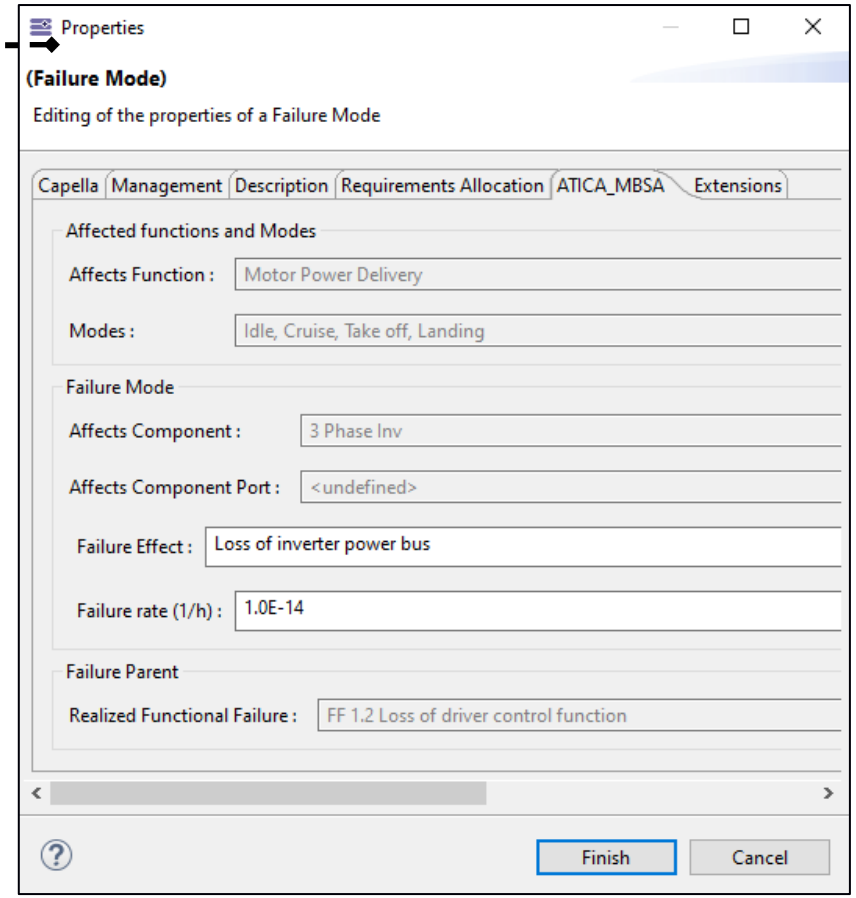


ATICA4Capella | Model Based Safety Analysis

Physical level

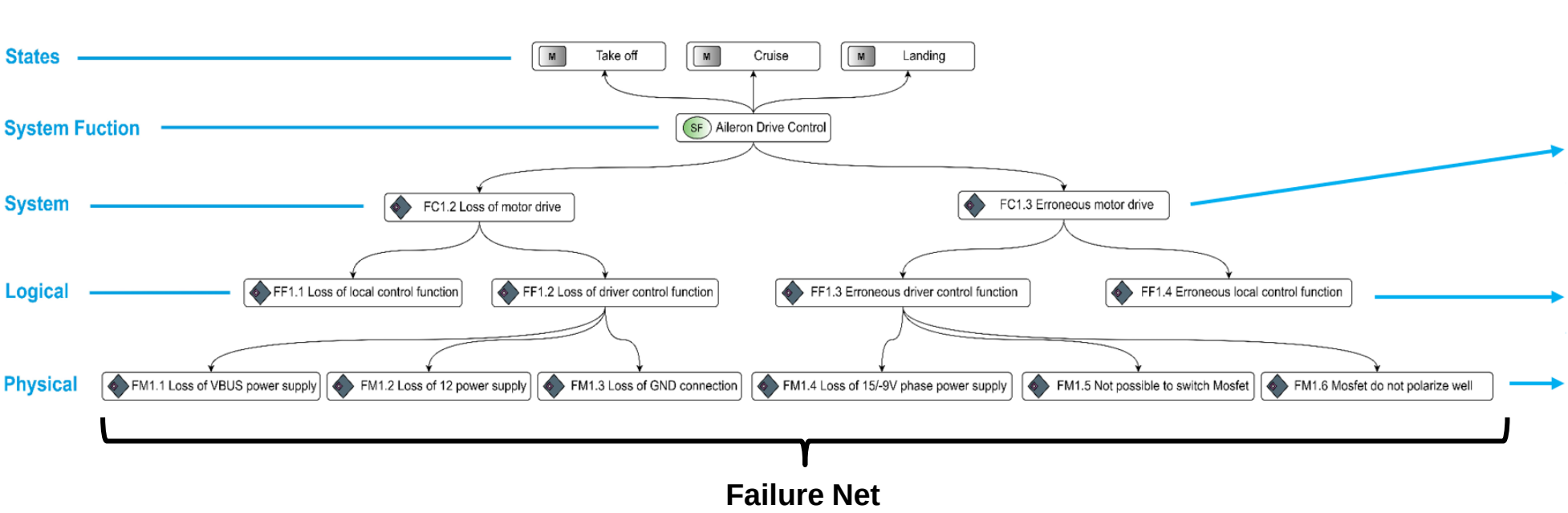
ATICA
Digital engineering for complex systems

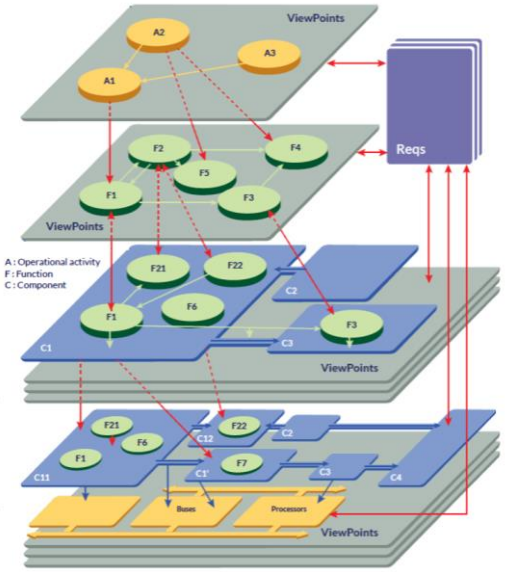




ATICA4Capella | Model Based Safety Analysis

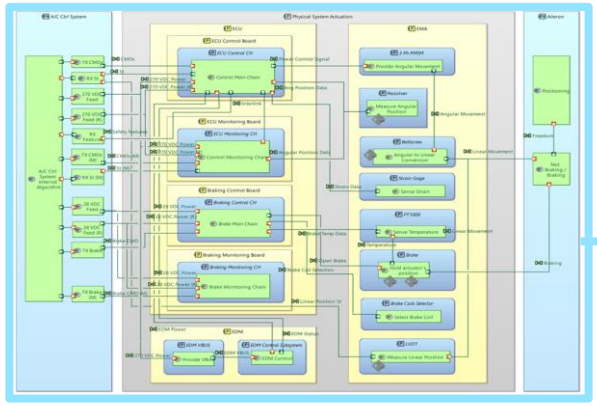
ATICA
Digital engineering for complex systems

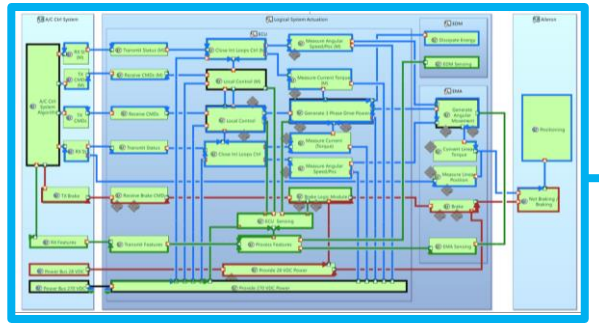


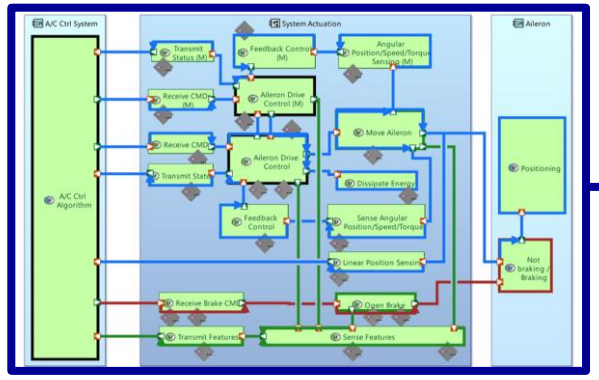


Failure net / FMES generation

ATICA
Digital engineering for complex systems

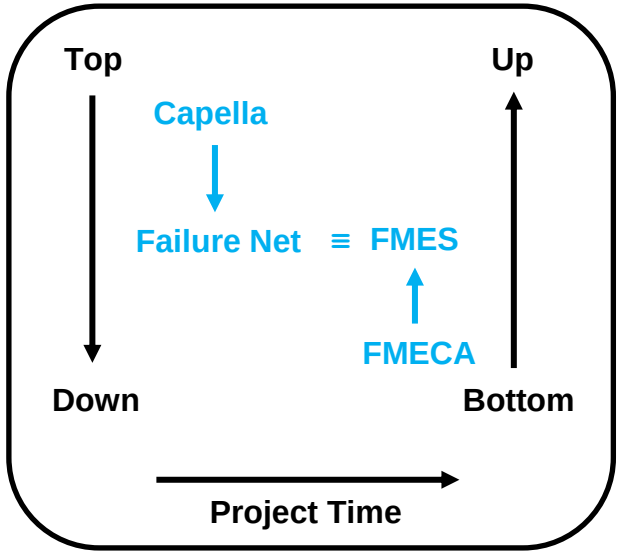


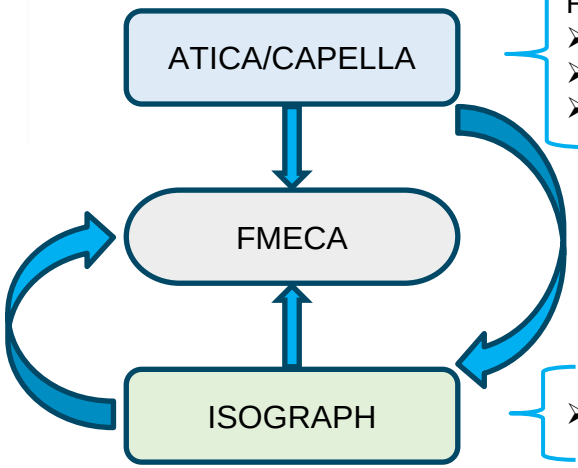




- Failure Net
  - [1.201.104:Schottky Diode - Mosfets Protection] Fail short
    - [1.201.100:3_Phase_Inverter] Loss of VBUS power supply
    - [1.200:BLDC270] Loss of driver control function
    - [1:Control Board] Loss of motor drive
  - [1.201.104:Schottky Diode - Mosfets Protection] Fail open
    - [1.201.100:3_Phase_Inverter] Loss of the path for return current
    - [1.200:BLDC270] No immediate effect
    - [1:Control Board] No immediate effect
  - [1.201.104:Schottky Diode - Mosfets Protection] Parameter change
    - [1.201.100:3_Phase_Inverter] More sensitive to noise
    - [1.200:BLDC270] No immediate effect
    - [1:Control Board] No immediate effect

Failure Modes (03 Physical Arch)
Functional Failures (02 Logical Arch)
Failure Conditions (01 System Arch)





Failure Net:
- Component Level
- Board Level
- System Level

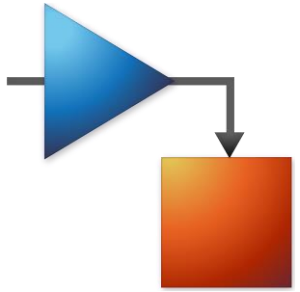
- Basic Failure Modes

New Feature
Under consolidation

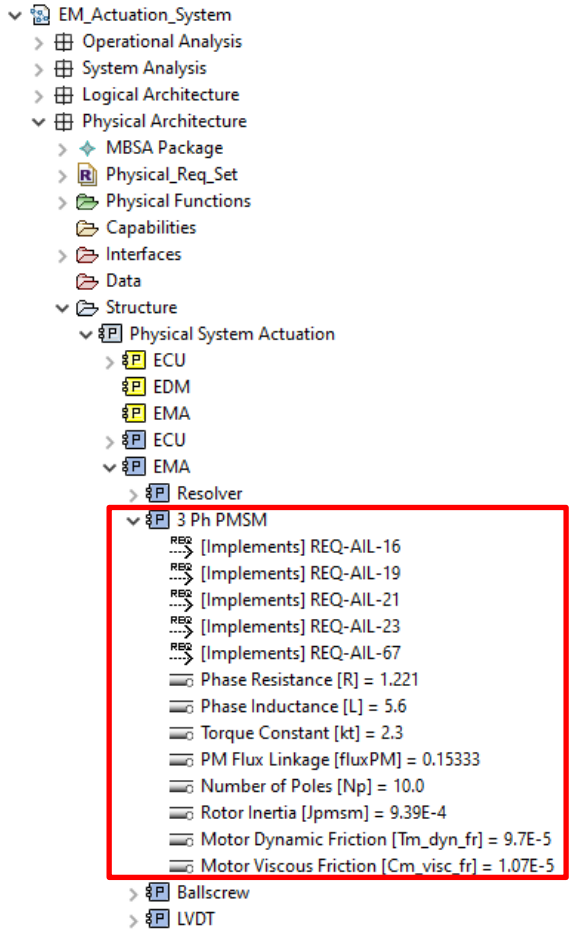
Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps

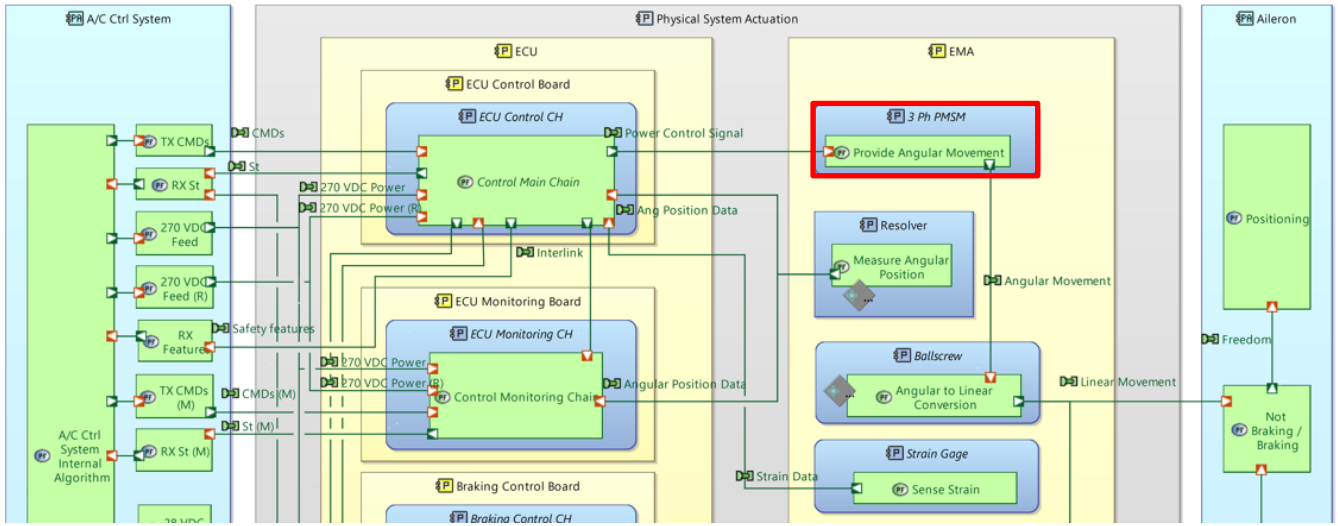
Interoperability



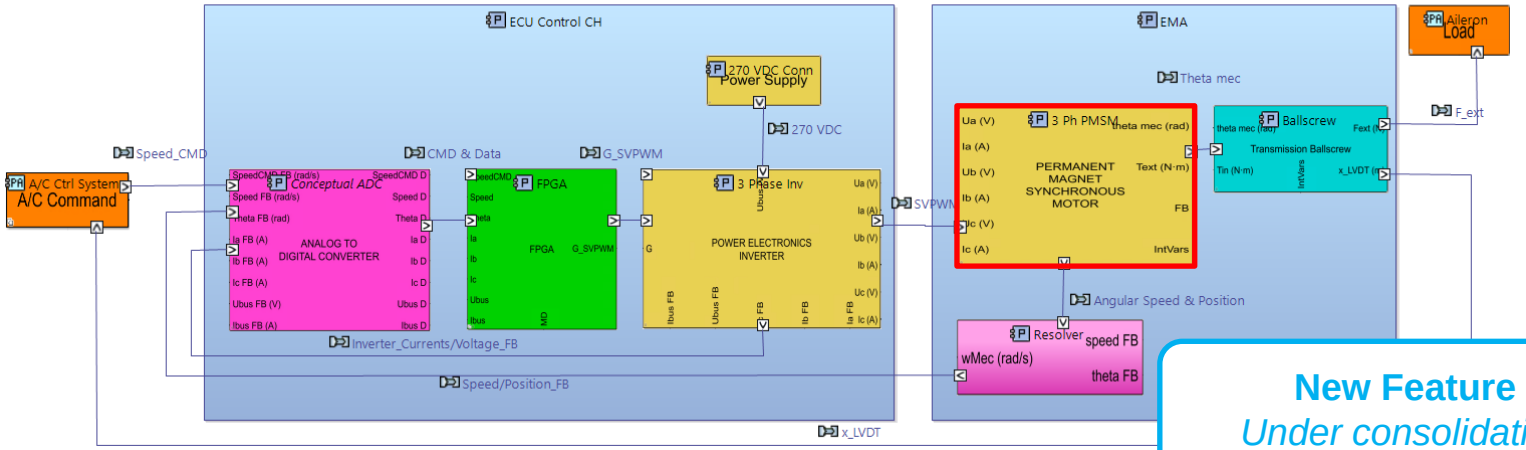
Connection with Simulink



same componet, several representations

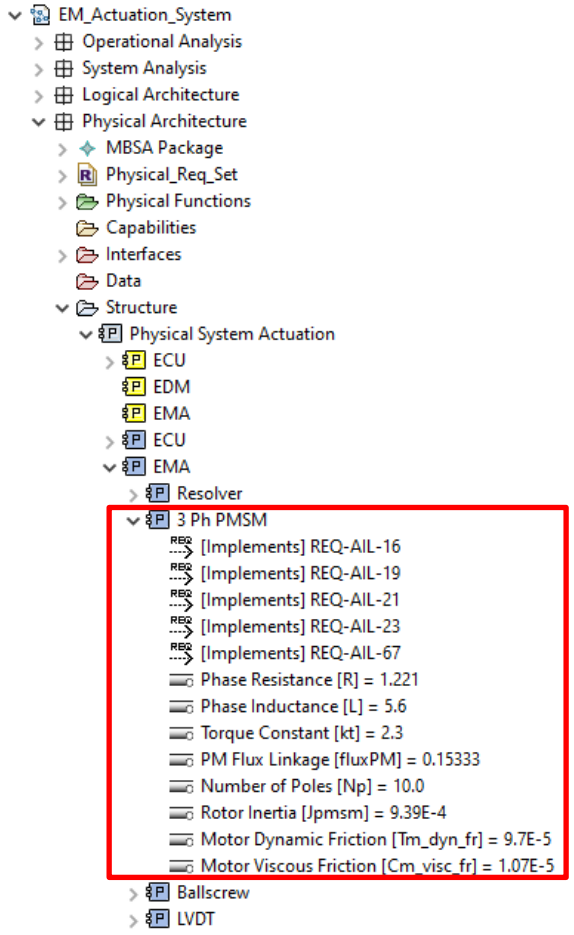


Simulink View



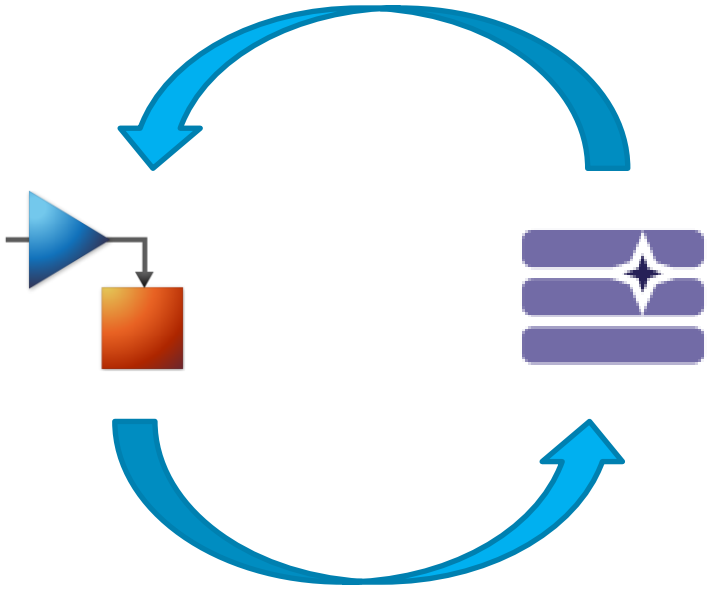
New Feature
Under consolidation

Connection with Simulink



same componet, several representations

Interoperability through excel

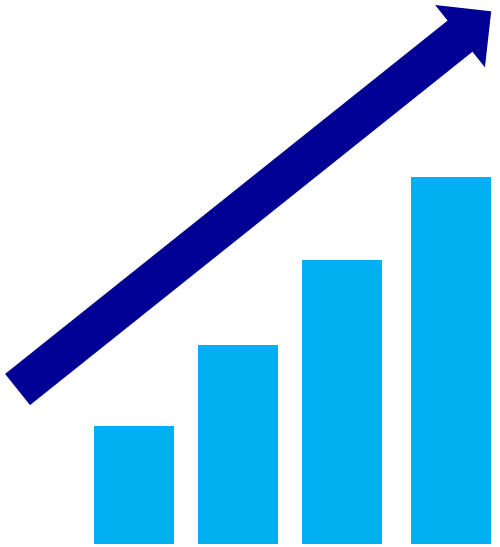


Interoperability through excel

New Feature
Under consolidation

Outline

- Project scope
- Electromechanical actuation system
- MBSE tools trade-off
- Digital engineering framework
- Requirements Management
- System Model
- ATICA4Capella
- Connection with Simulink
- Next steps



Conclusions

- Main conclusions from Héroux Devtek Spain / CESA point of view:
  - Great utility for complex and highly integrated systems and equipment
  - MBSA enriches the model and increases the awareness of the safety aspects
  - Test effectiveness to foster coordination between multidisciplinary teams and manage project information
  - Evaluate the initial learning curve versus the final benefits

Next Steps

- Future work:
  - Implement MBSE including MBSA as a new systems development methodology at Héroux Devtek Spain / CESA. Collaborate with ANZEN to expand ATICA functionality:
    - Analysis of hidden failures
    - Analysis of redundancies
    - Cut sets analysis
    - Fault Tree Analysis

CapellaDays
ONLINE 2023

7th edition
Session #1
I'm speaking at!

Talk

Model-driven Design and Development of an Electromechanical Actuation System

Tuesday
14th NOVEMBER, 2023
5:15 pm UTC+1

Speaker
Elena García Llorente
CESA - Heroux Devtek
elena.garcia@herouxdevtek.com

Speaker
Luis Cárdenas González
Anzen Engineering
luiscardenas@anzenengineering.com