International Cooperation on Model Based Development for Spaceflight Assurance: The TACS Test Case

Isabelle Conway – ESA
Lui Wang – NASA
Naoki Ishihama - JAXA

Introduction

- **In 2009, the WG for Safety Mission Assurance (SMA) was setup by ESA-JAXA-NASA to foster cooperation in the space SMA field**

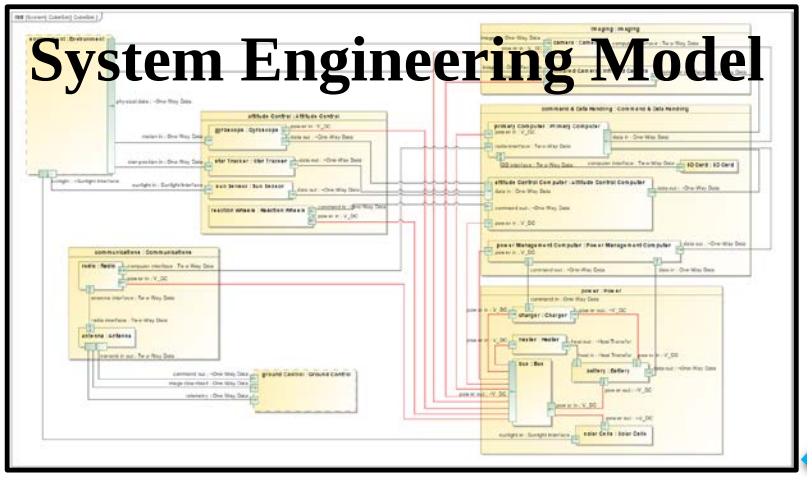
- **In 2018, a Task Force was setup to focus on SMA activities linked to MBSE: the MBMA Task Force led by John Evans (NASA) and Isabelle Conway (ESA)**

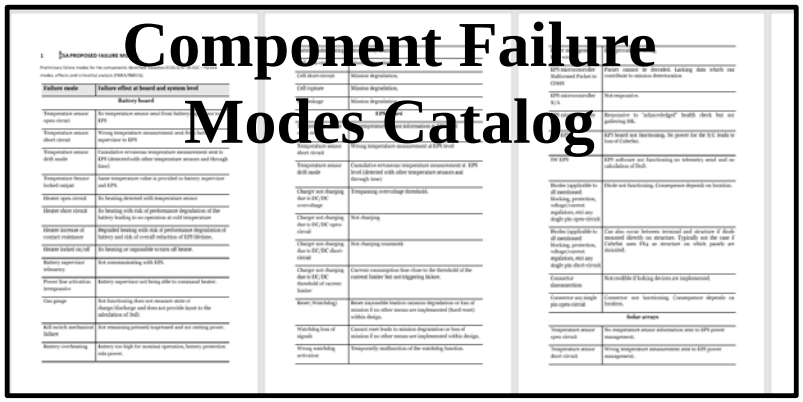
- **MBMA Task Force main objective is to develop a model based mission assurance reference model suitable for representing faults and failures and allow automatic generation of Failure Mode and Reliability artifacts.**

Project Approach

- **Share a common demonstration project**
  - Trilateral Assurance CubeSat (TACS) - derived from INCOSE CubeSat standard model
- **Share a systems engineering model of TACS**
  - Tailored to include all interests
  - Modeled in SysML®; for convenience, same modeling tool used
- **Identify illustrative TACS failures**
  - Derived from ESA's Parts Failure Modes Catalog (Annex G - ECSS-Q-ST-30-02C)
  - Derived from typical failure modes identified in CubeSats
  - Represent failures and (local) effects
  - Agree on a representation to be added to the model
- **Apply automation to generate assurance artifacts**
- **Work toward standardization of the methodology across agencies**

Process Flow





1 Add to this model component failures' local effects on the functions they perform

2 Propagate the effects through the system model to determine impacts on system requirements

3 Generate Mission Assurance Artifacts

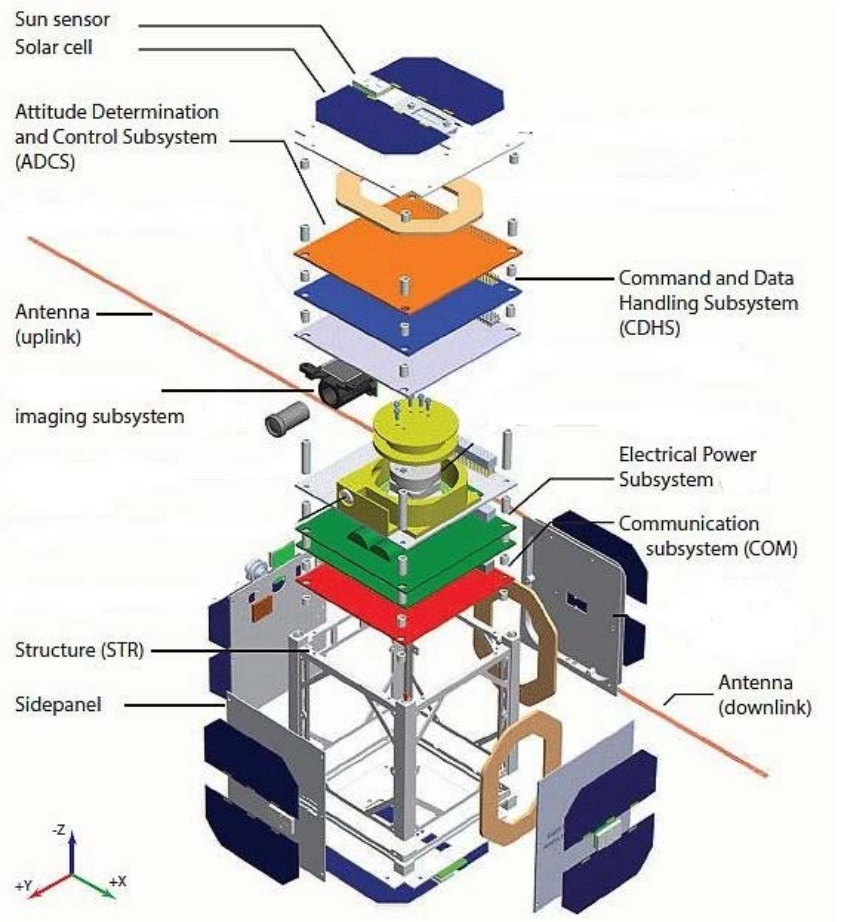
Fault Trees, FMECAs, Probabilistic Risk Assessments

If 1 is done in a standard way, 2 & 3 are automatable

Trilateral Assurance CubeSat (TACS)

Simple CubeSat Subsystems

- Power
- Communication
- C&DH
  - Computer
  - Software
- Imaging
- Attitude Control



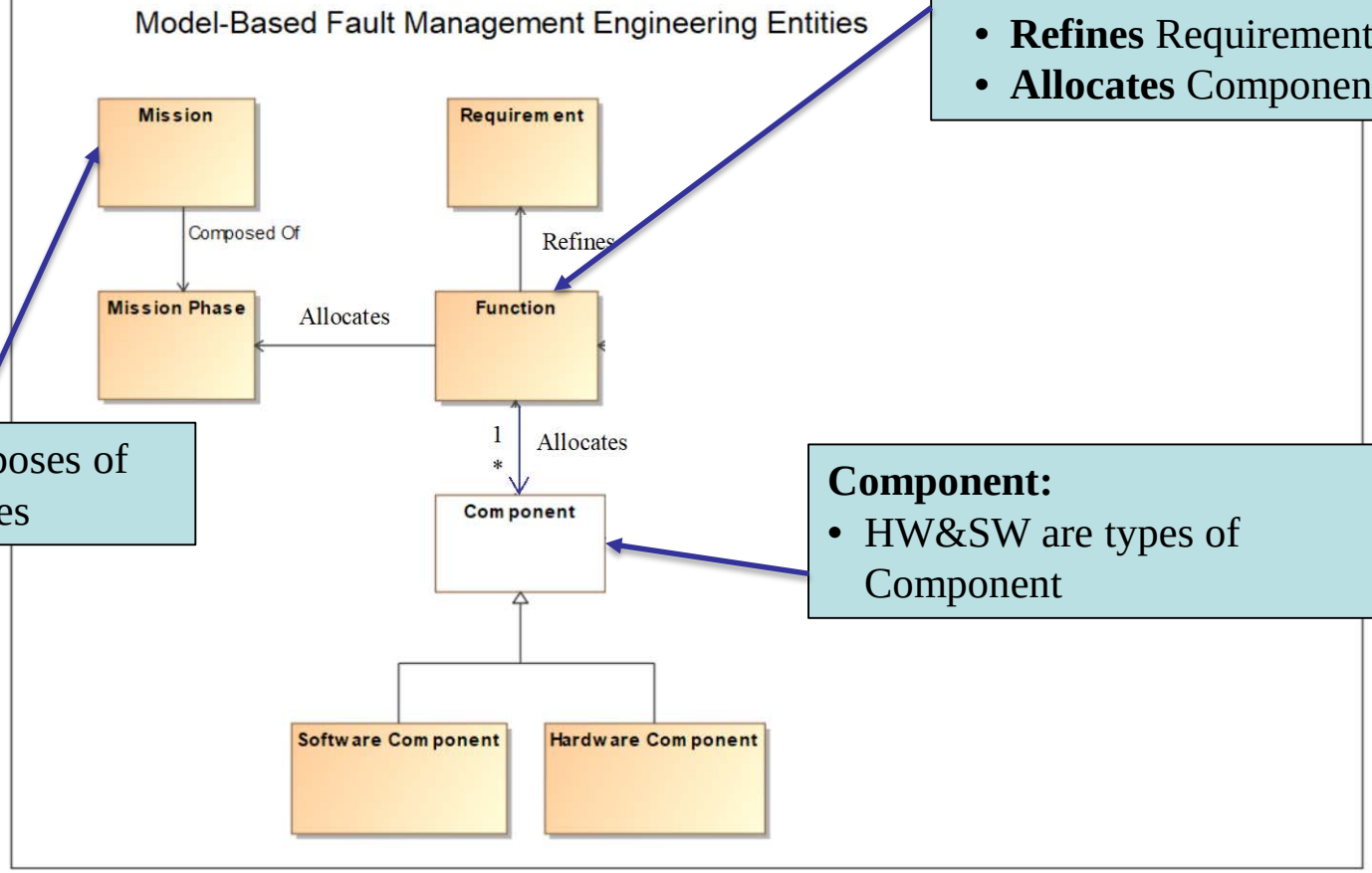
Adapted and Modified from ESTCube-1

Catalogue Failure Examples

Component	Failure Mode	Effect
Heater	Open circuit	No heating
	Short circuit	No heating
	Locked ON	Heating always ON
	Locked OFF	Heating always OFF
Battery temperature sensor	Open circuit	No temperature reading
	Short circuit	Incorrect temperature reading
Battery	Open circuit	Battery charge and voltage degradation

MBMA Modeling Representation

MBMA Meta-model



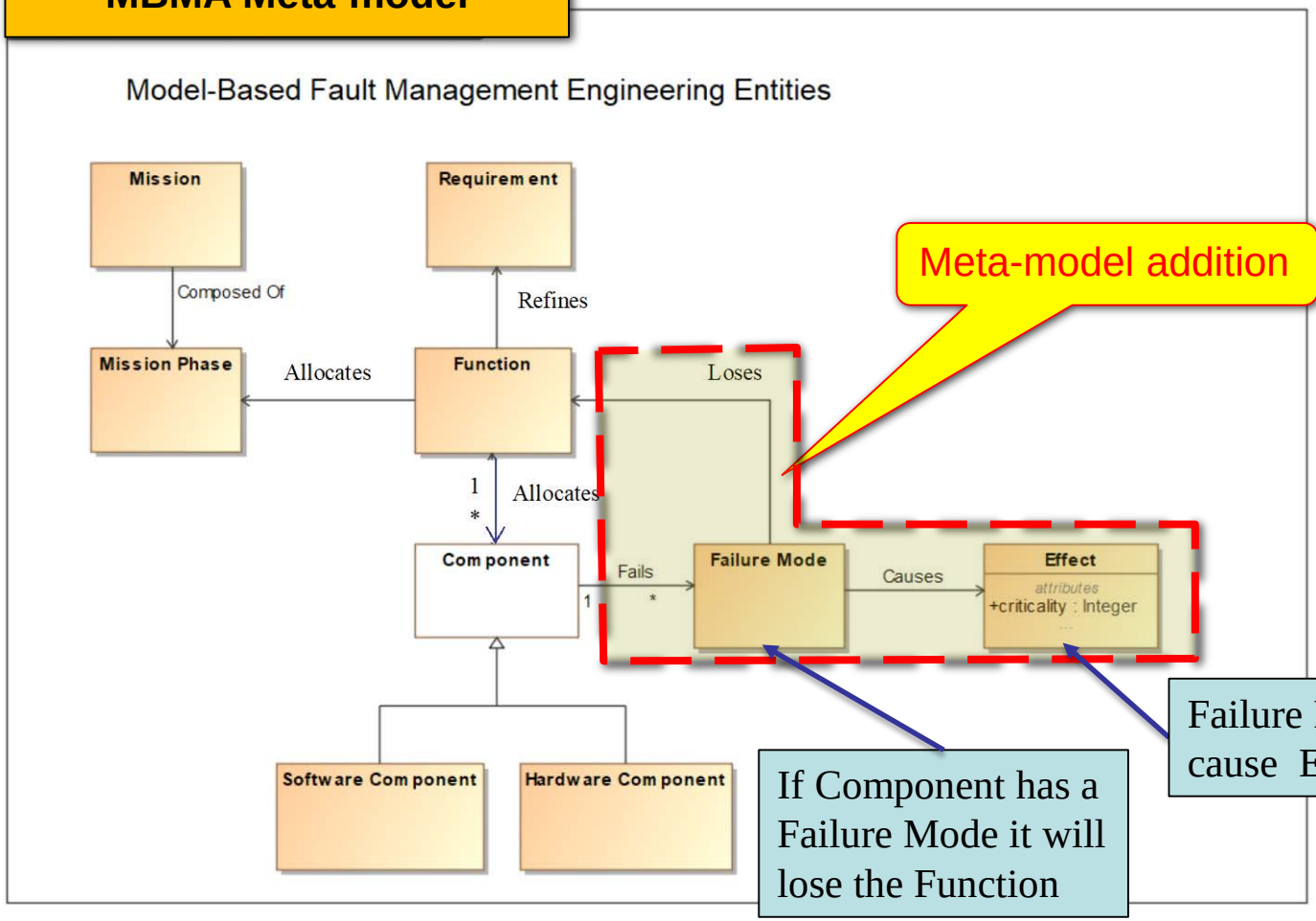
Function:
- **Allocates** Mission Phases
- **Refines** Requirements
- **Allocates** Components

Mission composes of Mission Phases

Component:
- HW&SW are types of Component

MBMA FM Meta Model

MBMA Meta-model



MBMA Component Meta-Model

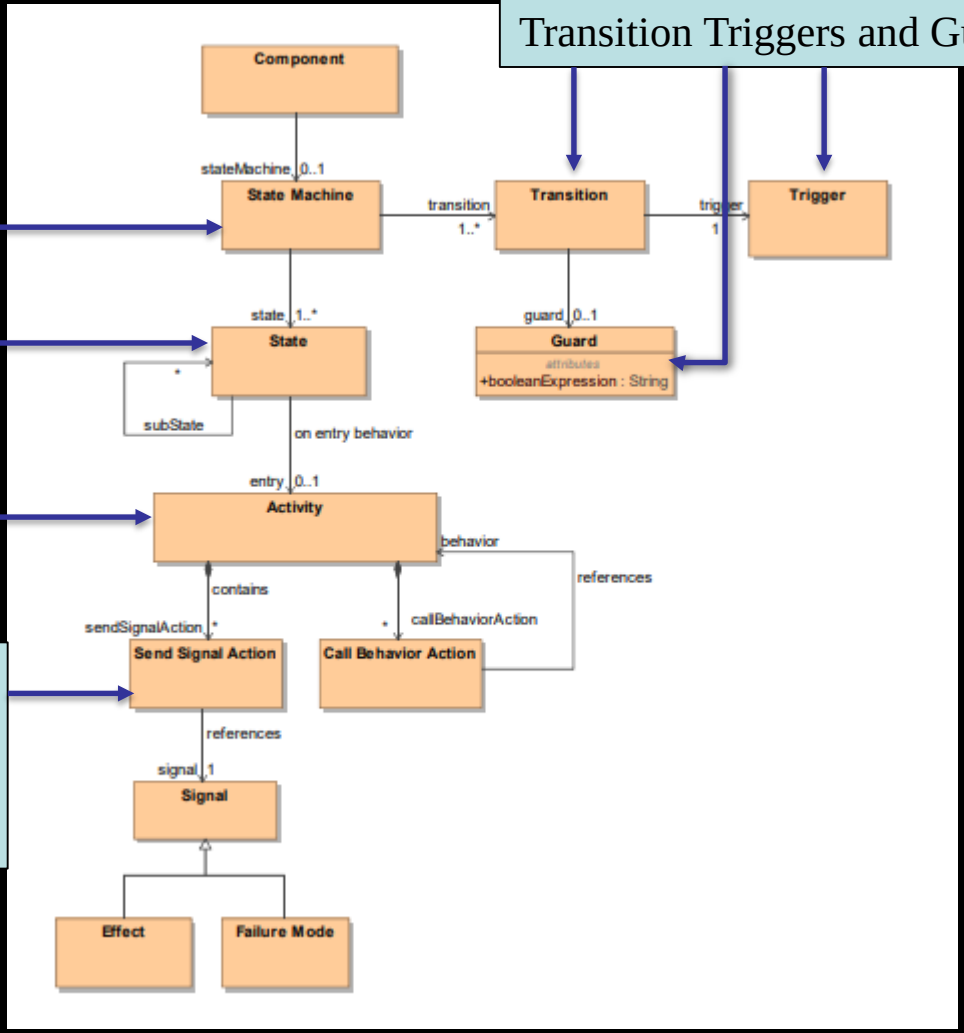
Each State Machine has Transition Triggers and Guards

Captures the behavior of a component

State Machine can have one or more states

Each state has Activity on entering the state

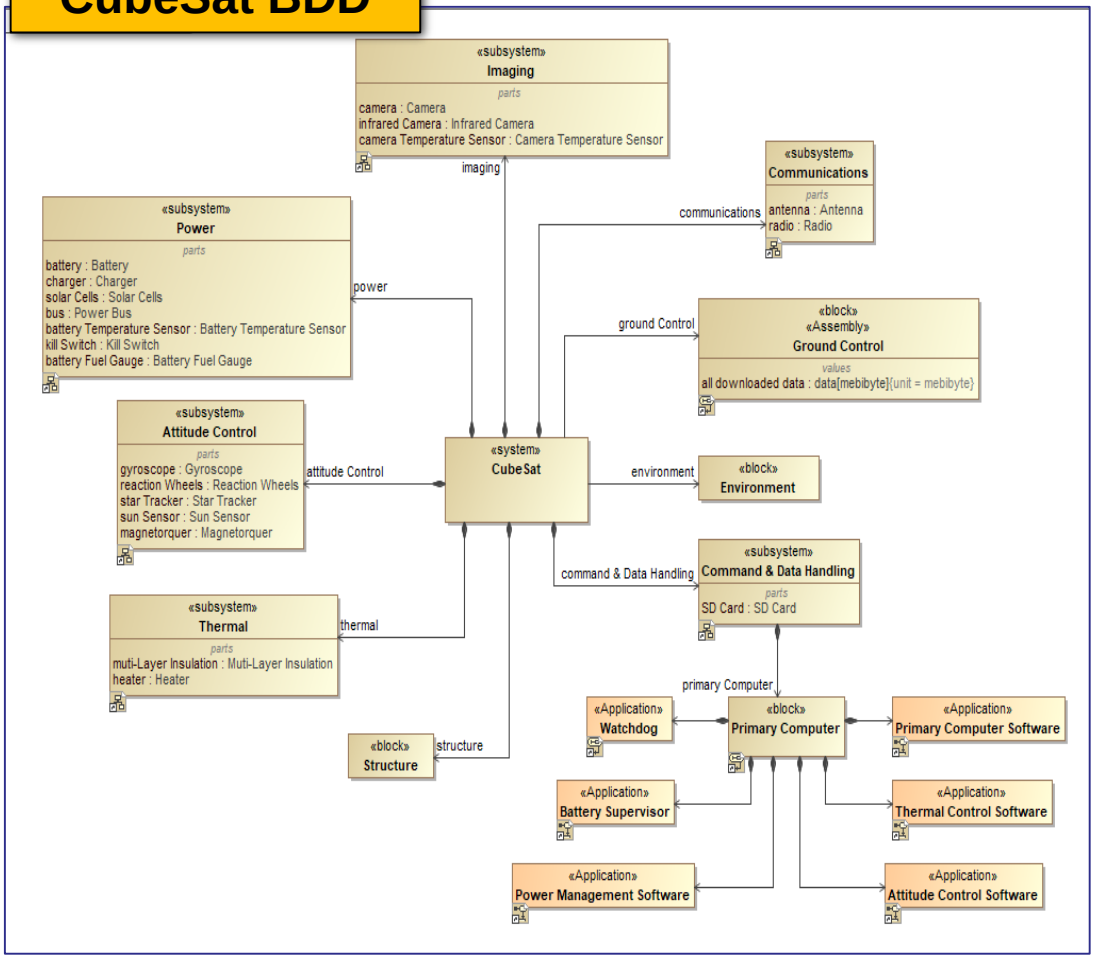
Use Send-Signal-Action to send either Failure Mode, Effect or Nominal State Transition Signal



TACS (Components & Functions)

Subsystem	Name	Function
Attitude Control	Gyroscope	Determine Attitude and Position
Attitude Control	Magnetorquer	Desaturate Reaction Wheels
Attitude Control	Reaction Wheels	Adjust Attitude and Rotation Rate
Attitude Control	Star Tracker	Determine Attitude and Position
Attitude Control	Sun Sensor	Determine Attitude and Position
C&DH	Computer	Run CubeSat Software
C&DH	SD Card	Store Images
Communications	Antenna	Communicate and Transfer Data
Communications	Radio	Communicate and Transfer Data
Imaging	Camera	Capture Images
Imaging	Camera Temperature Sensor	Provide Camera Temperature
Imaging	Infrared Camera	Capture IR Images
Power	Battery	Provide Power Store Power
Power	Battery Fuel Gauge	Provide Battery DoD
Power	Battery Temperature Sensor	Provide Battery Temperature
Power	Charger	Charge Battery
Power	Kill Switch	Activate Power
Power	Power Bus	Provide Electrical Interfaces
Power	Solar Cells	Provide Power
Computer	Attitude Control Software	Control Attitude Control Subsystem
Computer	Battery Supervisor	Control Battery Health
Computer	Power Management Software	Control Power Usage
Computer	Primary Computer Software	Control Image Capture and Storage
Computer	Thermal Control Software	Control Temperature
Computer	Watchdog	Reset System
Thermal	Heater	Provide Heating
Thermal	Muti-Layer Insulation	Provide Insulation

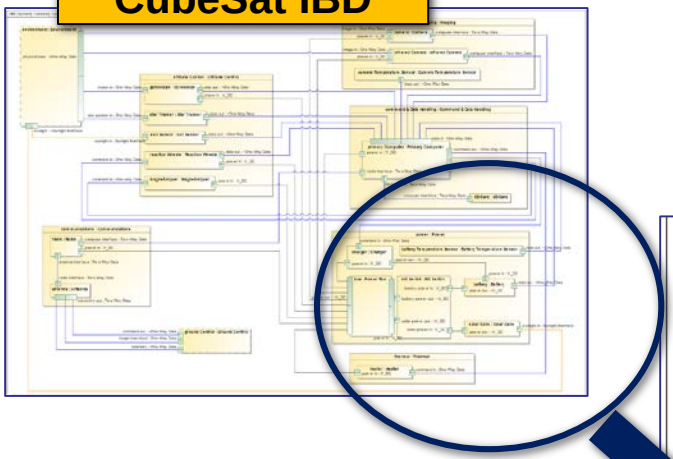
CubeSat BDD



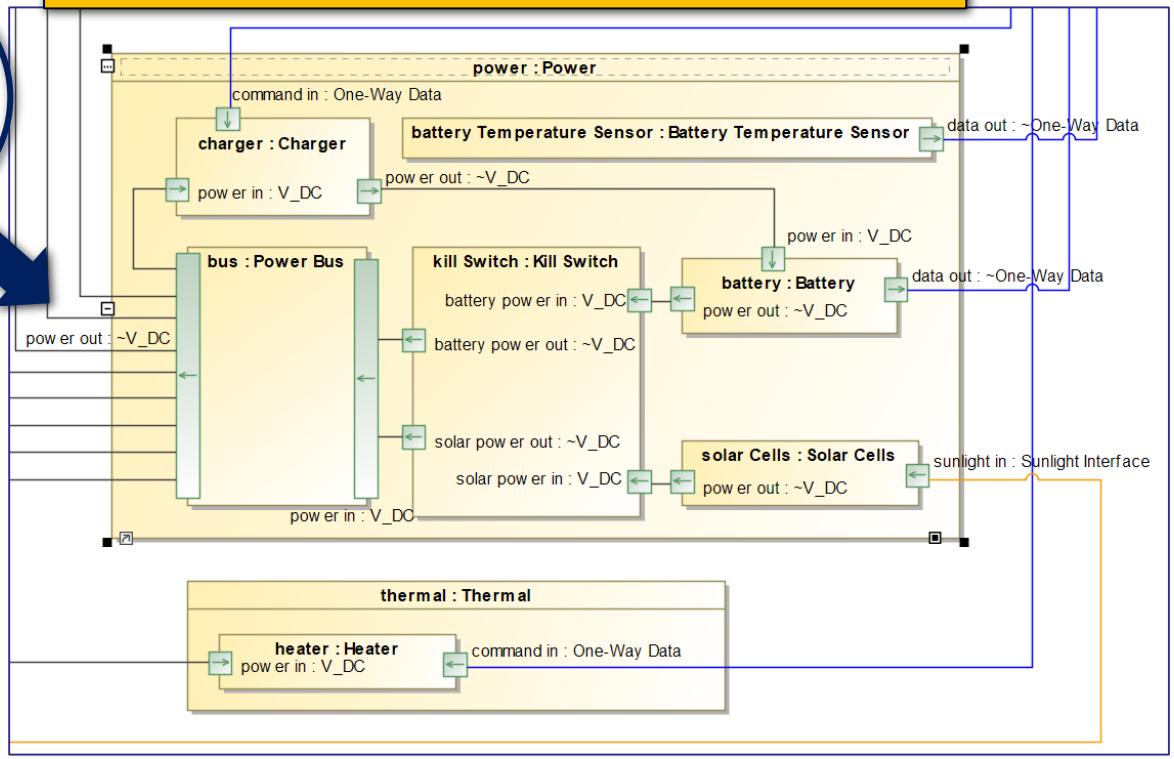
Adapted and Modified from ESTC[illegible]-1

TACS EPS IBD

CubeSat IBD



CubeSat IBD – PWR Sub-System Closeup



CubeSat power subsystem was selected for failure mode analysis

FMECA and Fault Tree Interactive Display Output

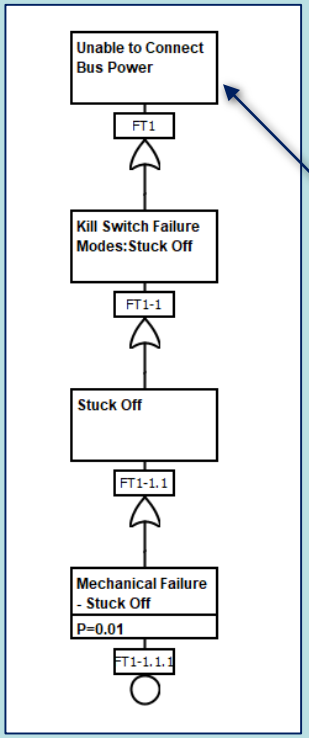
Generated FMECA output

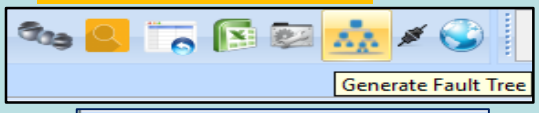
All | Summary

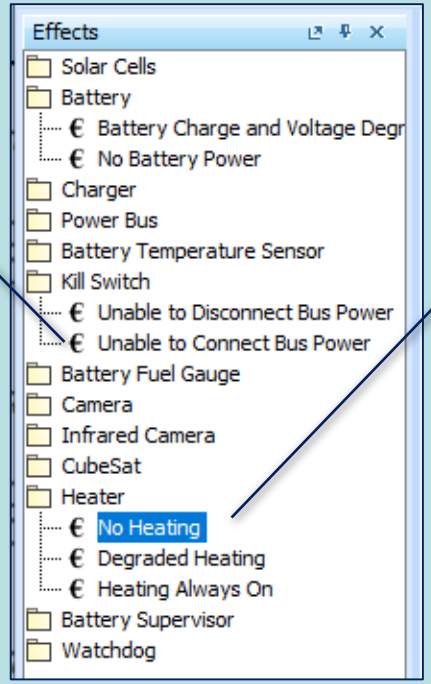
Hierarchy: Solar Cells Row Count: 2

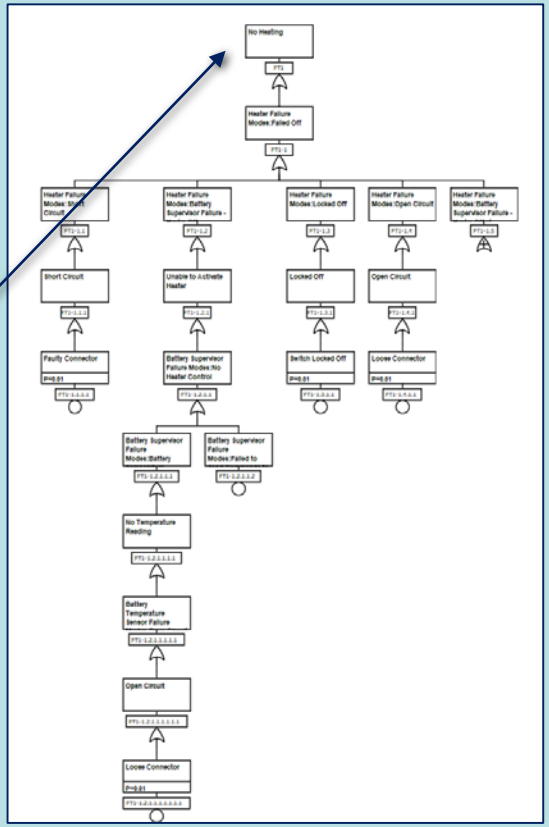
System	Module	Subsystem	Sub-subsystem	LRU/Assembly	Item Hierarchy	Item	Item ...	Potential Fai...	Immediate E...	End Effect	Failure ...	...	Potential Cause(s)	FPPath	Li...
CubeSat		Power		Solar Cells	CubeSat[System]>>Power[Subsystem...	Solar Cells		Solar Cells Fai...	EFFECT: Sola...	EFFECT: Solar Cells Loss of So...	1		EVENT: Solar Cells Radia...	FAILURE: S...	0.01
CubeSat		Power		Solar Cells	CubeSat[System]>>Power[Subsystem...	Solar Cells		Solar Cells Fai...	EFFECT: Sola...	EFFECT: Solar Cells Loss of So...	1		EVENT: Solar Cells Radia...	FAILURE: S...	0.01

Generated Fault Tree



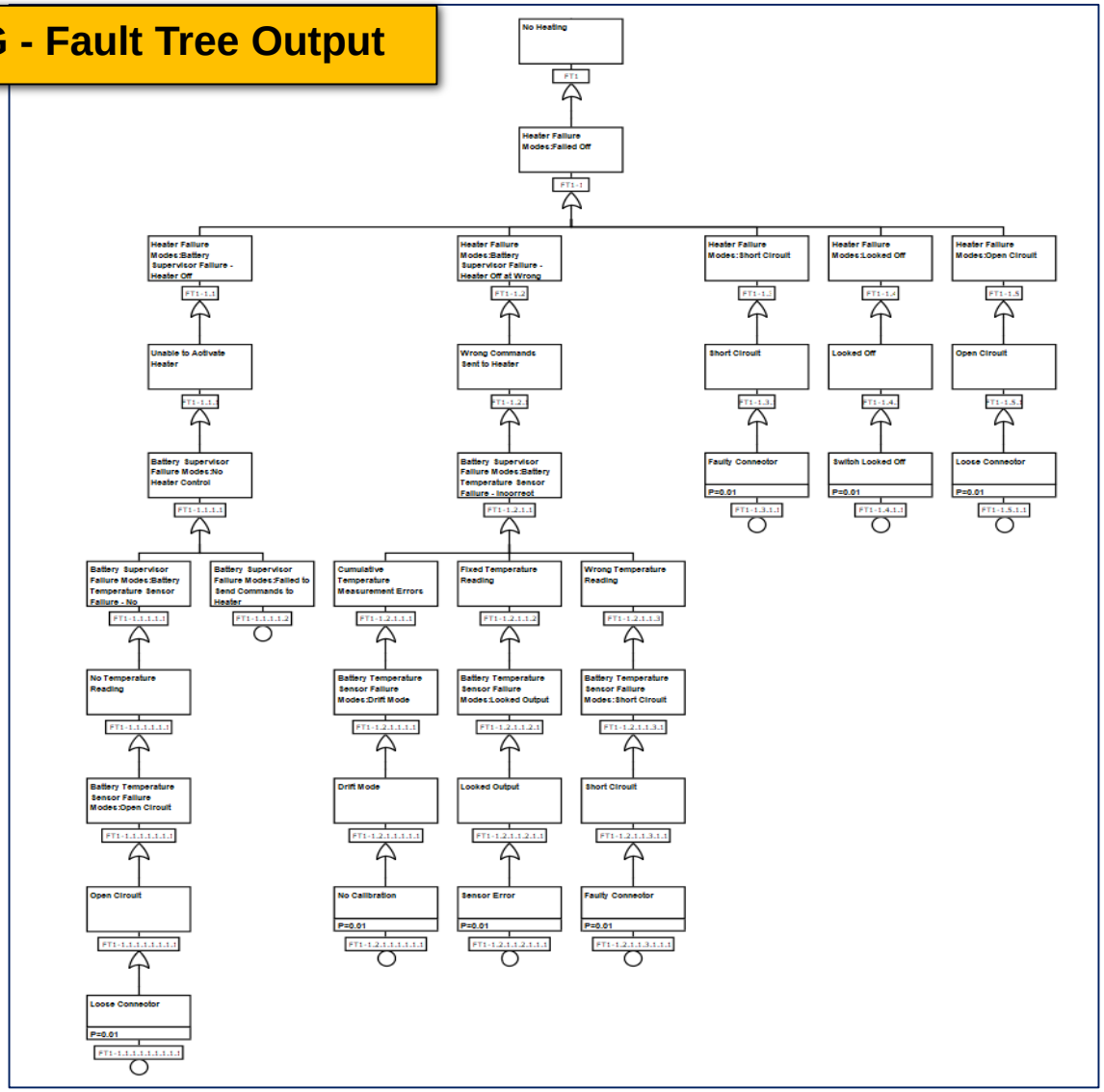






Fault Tree Output

SVG - Fault Tree Output



FMECA Matrix Output

CSV - FMECA Output

System	Subsystem	Item	Potential Failure Mode	Immediate Effect	End Effect	Failure Count	Other Independent Failures	Potential Cause(s)	FPPath	Likelihhod
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Open Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Loose Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Short Circuit	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Faulty Connector	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery No Battery Power	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Leakage	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Leaking Cell	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery No Battery Power	EFFECT: CubeSat Mission Degradation	1		EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Mission	1		EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery Battery Charge and Voltage Degradation	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Battery	Cell Ruptured	EFFECT: Battery No Battery Power	EFFECT: CubeSat Loss of Spacecraft	2	Solar Cells Open Circuit	EVENT: Battery Cell Rupture	FAILURE: Batt	0.01
CubeSat	Power	Charger	Open Circuit	EFFECT: Charger Unable to Charge Battery	EFFECT: Charger Unable to Charge Battery	1		EVENT: Charger Loose Connector	FAILURE: Char	0.01
CubeSat	Power	Charger	Short Circuit	EFFECT: Charger Degraded Charging Ability	EFFECT: Charger Degraded Charging Ability	1		EVENT: Charger Faulty Connector	FAILURE: Char	0.01
CubeSat	Power	Charger	Overvoltage	EFFECT: Charger Degraded Charging Ability	EFFECT: Charger Degraded Charging Ability	1		EVENT: Charger Voltage Above Th	FAILURE: Char	0.02
CubeSat	Power	Charger	Overcurrent	EFFECT: Charger Degraded Charging Ability	EFFECT: Charger Degraded Charging Ability	1		EVENT: Charger Current Above Th	FAILURE: Char	0.01
CubeSat	Power	Power Bus	Bus Failed	EFFECT: Power Bus No Bus Power	EFFECT: CubeSat Loss of Spacecraft	1		EVENT: Power Bus Failure in Bus H	FAILURE: Pow	0.01
CubeSat	Power	Kill Switch	Stuck On	EFFECT: Kill Switch Unable to Disconnect Bus Power	EFFECT: CubeSat Mission Degradation	1		EVENT: Kill Switch Mechanical Fai	FAILURE: Kill S	0.02
CubeSat	Power	Kill Switch	Stuck Off	EFFECT: Kill Switch Unable to Connect Bus Power	EFFECT: CubeSat Loss of Spacecraft	1		EVENT: Kill Switch Mechanical Fai	FAILURE: Kill S	0.01

Benefits

Automated support for the generation of reliability artifacts offers the following benefits:

- **Speed –** reliability artifacts can be rapidly produced, and thus the results of reliability studies and analyses can be fed back to system engineers in a timely manner
- **Correctness** – automatic derivation of the artifacts directly from system models ensures they are correct and complete with respect to those models
- **Expertise –** by relieving reliability engineers from manual construction of reliability artifacts, their time and effort can be put to valued use to provide insights and guidance to system engineers

Conclusion

Theme: Working toward standardization to integrate the MBMA methodology for ESA, NASA and JAXA

- Completed an integrated assessment of MBMA CubeSat Model with Failure modes
- Today we have shown a sample CubeSat example
- Plan to present the final results at the Trilateral Safety and Mission Assurance Conference (TRISMAC) in June 2021 in Tokyo. (hope to see you there ☺)

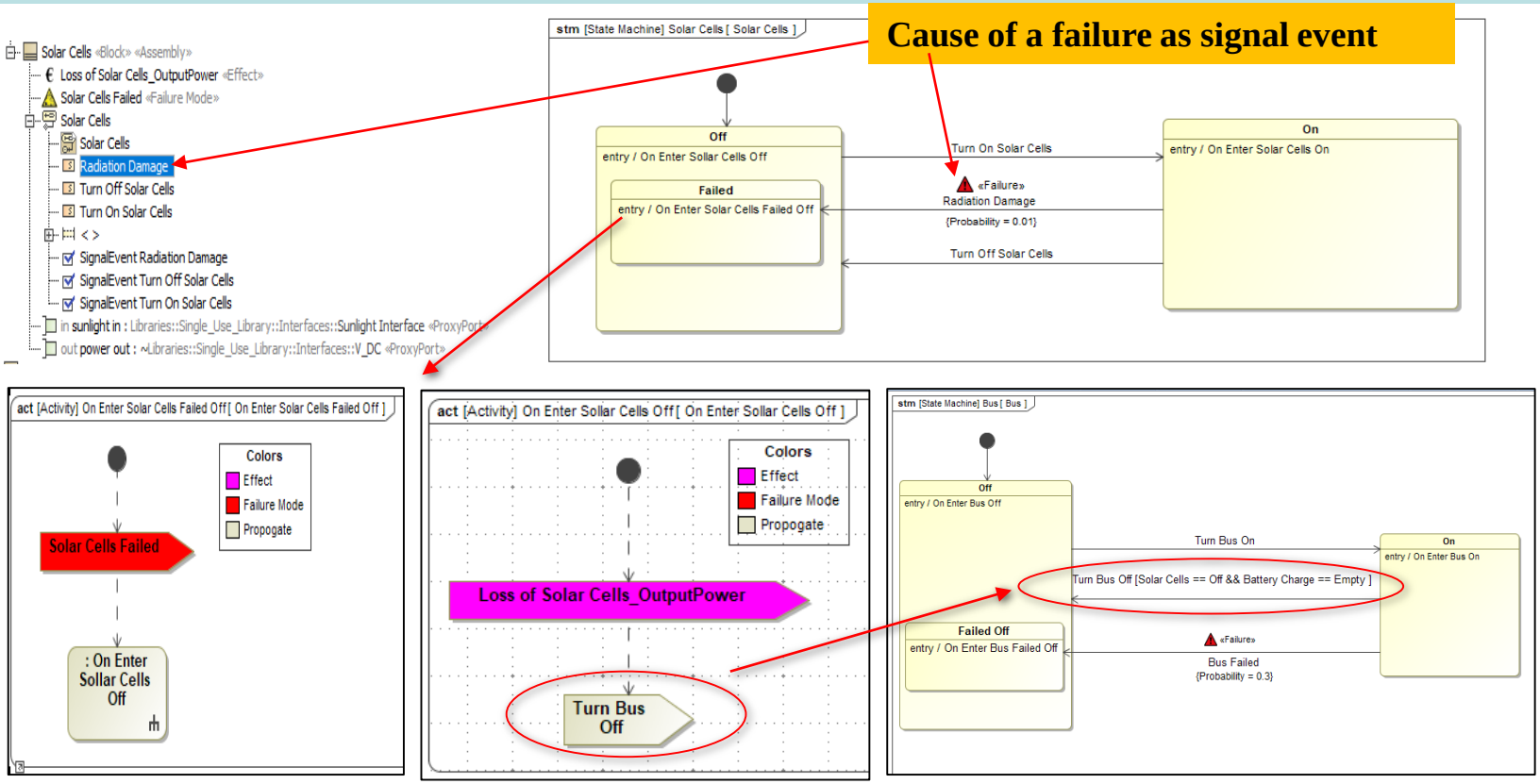
Future Work

- **Explore redundancy mission phases and scalable modeling approach**
- **Investigate methods to create reusable spacecraft related models across organizations**
- **Generate additional Reliability Products**
- **Apply the MBMA methodology to enterprise programs for ESA, JAXA and NASA**

Backup

Modelling Hardware Failures and Effect

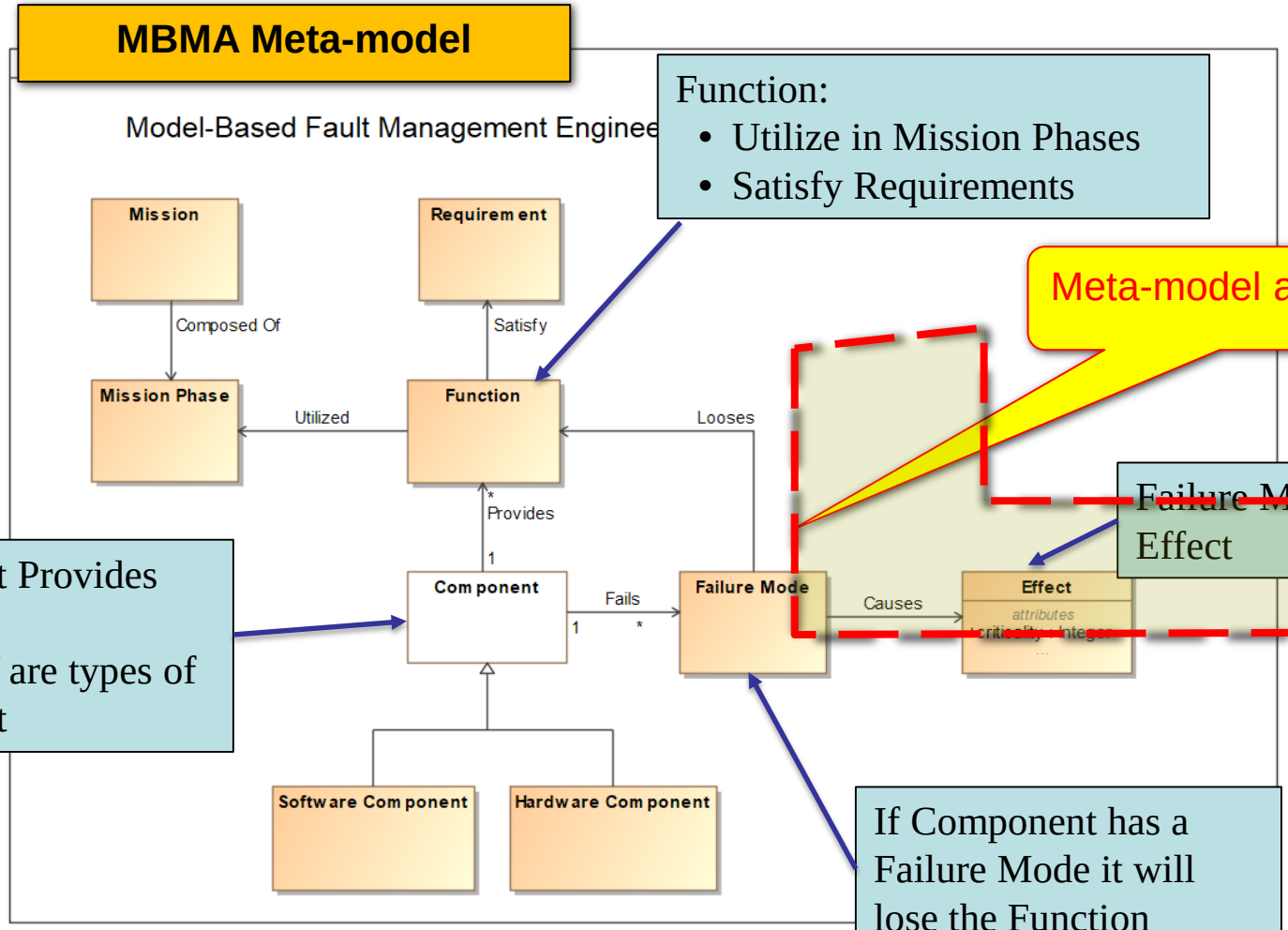
- Solar Cells SM diagram shows nominal states and a Failed State “On Enter Solar Cells Failed off”. Cause of a failure is a “Radiation Damage”.
- Solar Cells activity diagram declares a Failure Mode. Solar Cells Failed and On Enter Solar Cells off.
- On Enter Solar Cells Off activity diagram declares the result of the Solar Cells failure. Loss of Solar Cells Output power – Turn Buss off
- Bus SM – the result of failure – on Enter Bus off.



ESA Catalogue Failure Modes

HW	SW	ESA Catalogue Failure Mode	ESA Catalogue Effect
Battery		Open circuit	Mission degradation
		Short circuit	Mission degradation
		Cell rupture	Mission degradation
		Cell leakage	Mission degradation
Charger		Charger not charging due to DC/DC short-circuit	Not charging constantly
		Charger not charging due to DC/DC open-circuit	Not charging
		Charger not charging due to DC/DC overvoltage	Trespassing overvoltage threshold.
		Charger not charging due to DC/DC threshold of current limiter	Current consumption bine close to the threshold of the current limiter but not triggering failure.
Battery Fuel Gauge		Gas gauge	Not functioning does not measure state of charge/discharge and does not provide input to the calculation of DoD.
Battery Temperature Sensor		Temperature sensor open circuit	No temperature sensor send from battery supervisor to EPS
		Temperature sensor short circuit	Wrong temperature measurement sent from battery supervisor to EPS
		Temperature sensor drift mode	Cumulative erroneous temperature measurement sent to EPS (detected with other temperature sensors and through time)
		Temperature Sensor locked output	Same temperature value is provided to battery supervisor and EPS
Solar Cells		Solar cell short circuit	Partial Surface loss
		Solar cell open circuit	Total surface loss
		Damaged cell/connector	No or low voltage, solar panels not providing sufficient power
		MPPT malfunctioning	Low voltage output
		Damaged diodes	No or low current, solar panels not providing sufficient power
Kill Switch		Kill Switch mechanical failure	Not remaining pressed/unpressed and not cutting power.
Heater		Heater open circuit	No heating detected with temperature sensor
		Heater short circuit	No heating with risk of performance degradation of the battery leading to no operation at cold temperature
		Heater increase of contact resistance	Degraded heating with risk of performance degradation of battery and risk of overall reduction of EPS lifetime.
		Heater locked on/off	No heating or impossible to turn off heater.
Primary Computer	**Battery supervisor**	Power line activation irresponsive	Battery supervisor not being able to command heater.
		Battery supervisor telemetry	Not communicating with EPS.
	Watchdog	Reset (Watchdog)	Reset impossible leads to mission degradation or loss of mission if no other means are implemented (hard reset) within design.
		Wrong watchdog activation	Temporarily malfunction of the watchdog function.
		Watchdog loss of signals	Cannot reset leads to mission degradation or loss of mission if no other means are implemented within design.

MBMA Modeling Representation



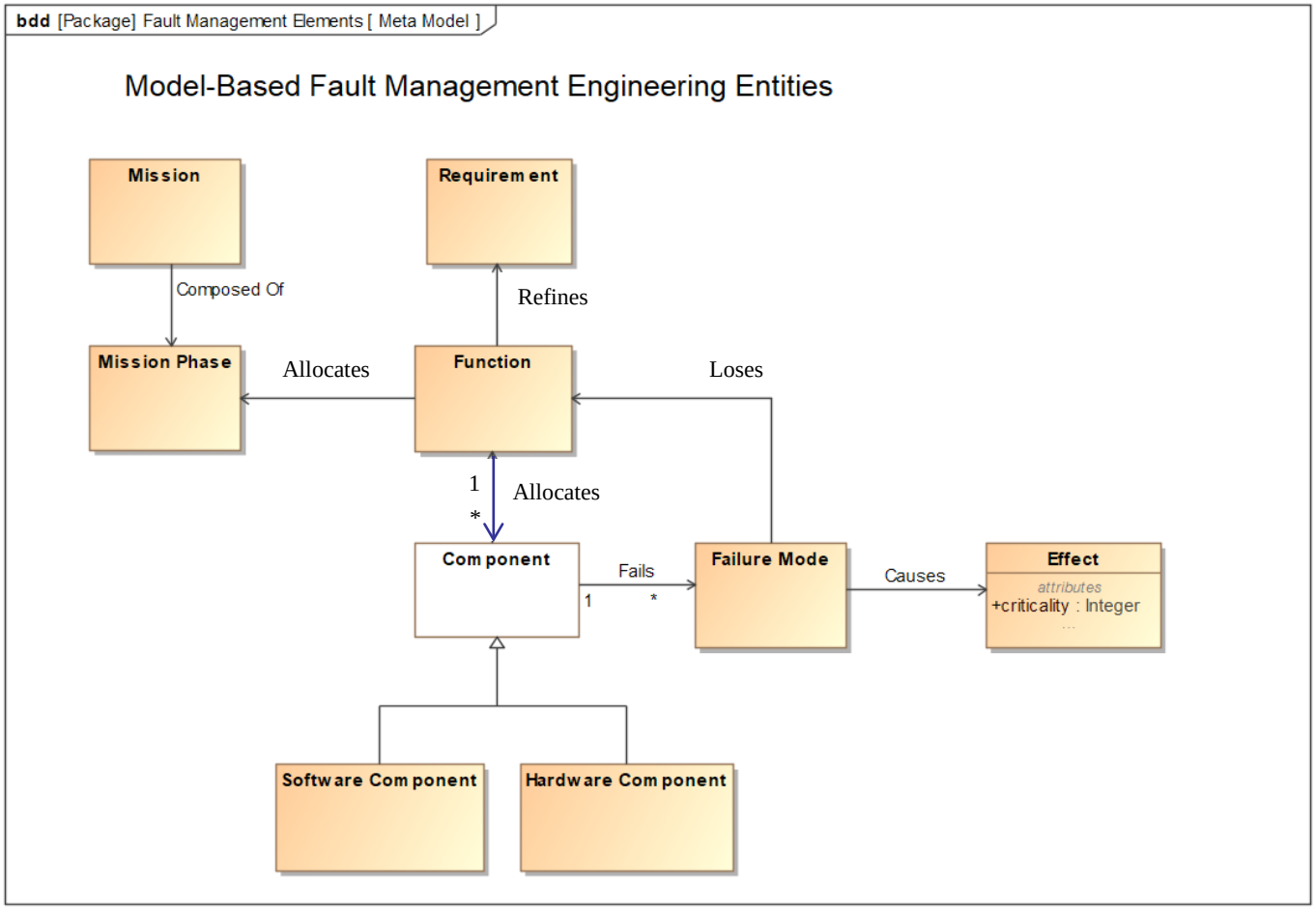
Function:
- Utilize in Mission Phases
- Satisfy Requirements

Meta-model addition

Failure Mode will cause Effect

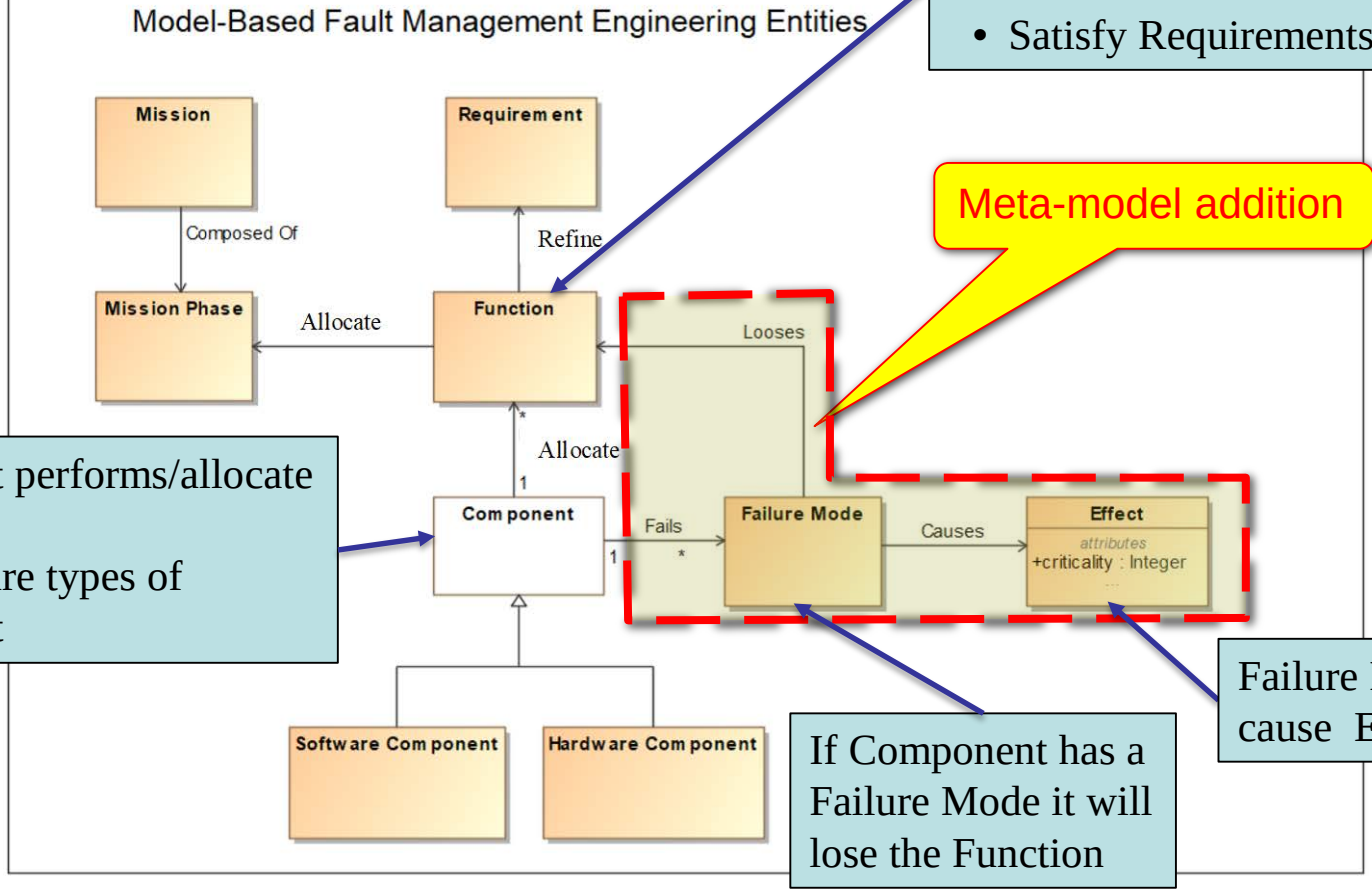
- Component Provides Function
- SW or HW are types of Component

If Component has a Failure Mode it will lose the Function


bdd [Package] Fault Management Elements [Meta Model]
Model-Based Fault Management Engineering Entities
Mission
Requirement
Composed Of
Refines
Mission Phase
Allocates
Function
Loses
1
*
Allocates
Component
Fails
1
*
Failure Mode
Causes
Effect
attributes
+criticality : Integer
Software Component
Hardware Component

MBMA Modeling Representation

MBMA Meta-model



Function:
- Utilize in Mission Phases
- Satisfy Requirements

Meta-model addition

- Component performs/allocate Function
- HW&SW are types of Component

If Component has a Failure Mode it will lose the Function

Failure Mode will cause Effect

Conclusion

Theme: Working toward standardization to integrate the MBMA methodology for ESA, NASA and JAXA

- Completed an integrated assessment of MBMA CubeSat Model with Failure modes
- Today we have shown a sample CubeSat example
- Plan to present the final results at the Trilateral Safety and Mission Assurance Conference (TRISMAC) in June 2021 in Tokyo. (hope to see you there ☺)

Future Work

- **Explore redundancy mission phases and scalable modeling approach**
- **Investigate methods to create reusable spacecraft related models across organizations**
- **Generate additional Reliability Products**
- **Apply the MBMA methodology to enterprise programs for ESA, JAXA and NASA**