Model Based Space Systems and Software Engineering Workshop

-MBSE 2020

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

Authors: Isabelle Conway, Silvana Radu, ESA

Lui Wang, John W. Evans, NASA

Naoki Ishihama, JAXA

Michel Izygon, Tietronix

Arthur Witulski, Vanderbilt University

Martin S. Feather, Jet Propulsion Laboratory, California Institute of Technology

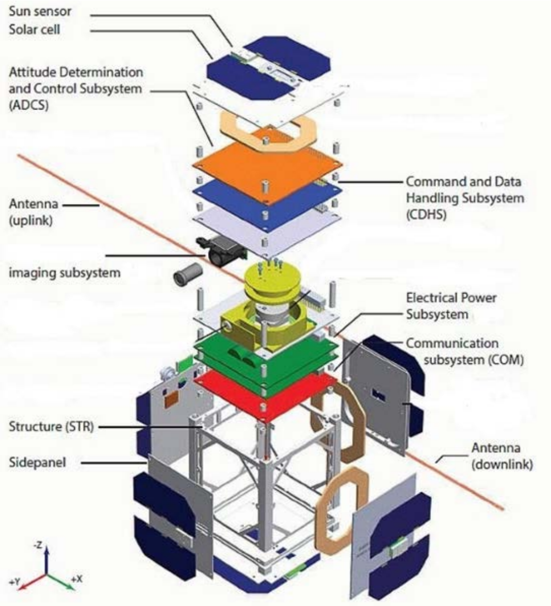
Abstract:

As this workshop attests, Model Based Systems Engineering (MBSE) is moving to the forefront of spacecraft development. The benefits of SysML® as language for the elucidation of the system architecture is well understood and is being demonstrated across programs, such as the NASA Europa Clipper currently in Phase C of the life cycle [1]. Concurrently, the benefits of the evolving development of MBSE for assurance have been recognized and are emerging as Model Based Mission Assurance (MBMA), which promises the development of integral assurance stakeholder views into the model as well as the production of useful products from the model [2,3]. In this regard, the assurance organizations of NASA, ESA and JAXA have setup the MBMA Task Force within the established trilateral Safety Mission Assurance (SMA) working group to explore jointly the potential benefits of MBSE and MBMA in anticipation of future joint projects in which an architecture for a flight mission will be shared in a SysML model. This paper presents the goal and content of this cooperation and reports upon current results.

The cooperative project goal is to develop a model based mission assurance reference model suitable for representing faults and failures and allow automatic generation of Reliability Availability Maintainability and Safety (RAMS) analyses. To ground this effort, the project is using a CubeSat as a target system. Figure 1 represents this CubeSat, dubbed the Trilateral Assurance CubeSat (TACS). The base model for the project was derived from the INCOSE CubeSat standard model built in Magic Draw for demonstration purposes. The project model was derived at Johnson Space Center as the lead organization, with ESA and JAXA as international partners in the design. The preliminary TACS model has been shared among our agencies in order to ensure a common set of requirements, system architecture, functions, and failure modes. Specifically, the Trilateral MBMA Task Force has adopted the ESA ECSS Parts Failure modes Catalog (Annex G - ECSS-Q-ST-30-02C) and generic failures identified in

CubeSats for assigning faults to the system components. The Trilateral Task Force reviewed and refined the model and approach, and came up with an initial mission assurance meta-model.

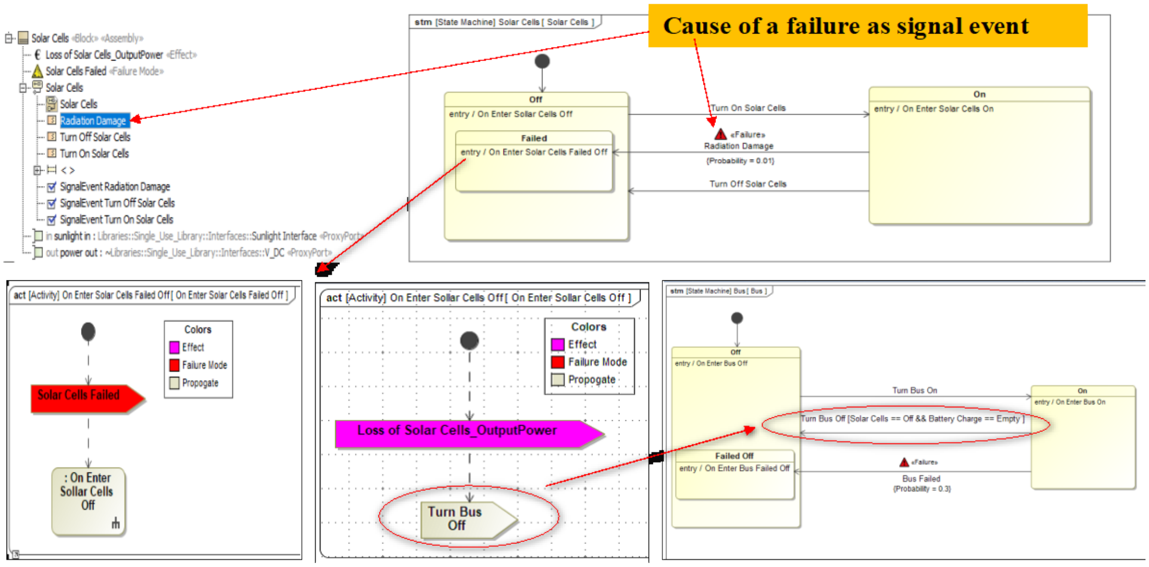
It has long been recognized that useful system products are forthcoming from SysML. The emphasis in this project is on the generation of fault management and reliability artifacts. These include Failure Modes and Effects Analysis (FMEA) and Fault Trees (FTA) based on early mission design, using TACS as an example. Leveraging on a consistent SysML model developed by the system design team using a NASA SysML Profile, the MBMA modeling framework extends the nominal system models and behaviors by adding failure modes and effects using a combination of SysML state machine and activity diagrams representations.



Sun sensor
Solar cell
Attitude Determination and Control Subsystem (ADCS)
Antenna (uplink)
imaging subsystem
Command and Data Handling Subsystem (CDHS)
Electrical Power Subsystem
Communication subsystem (COM)
Structure (STR)
Sidepanel
Antenna (downlink)
-Z
+Y
+X

Figure 1, TACS CubeSat - adapted from ESTCube-1.

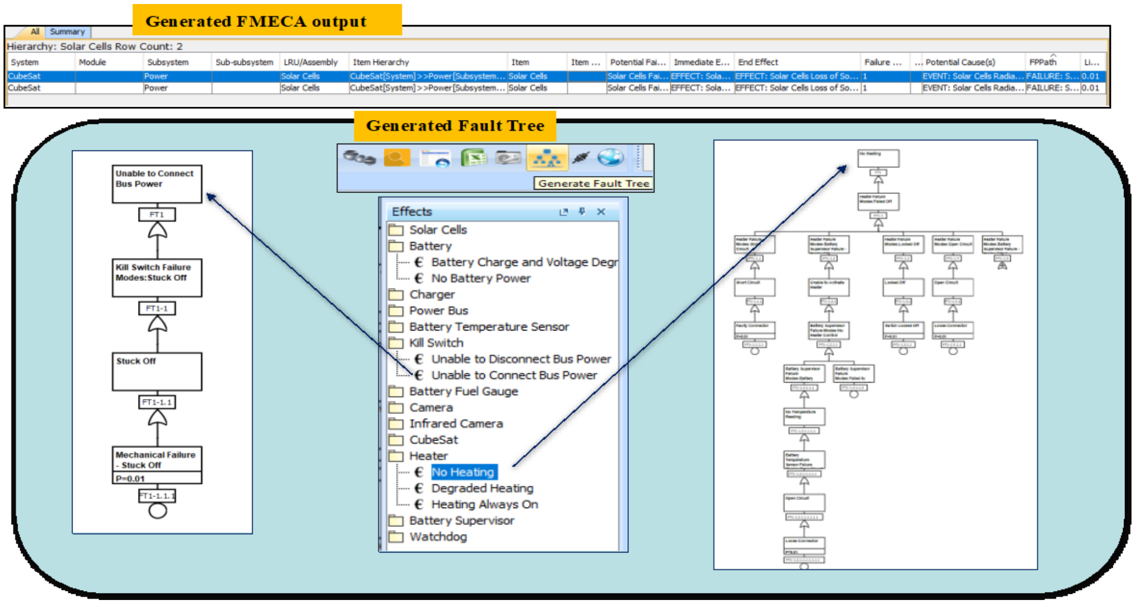
In this approach, state machine diagrams represent the possible transitions between nominal and faulty states of the system's components, together with the effects those faults have upon the components' functions. Figure 2 illustrates interactions among state machines that capture the transitions between the nominal <ON> state to off-nominal <Failed> states using a combination of Signals, Activity and Guard Conditions.



Cause of a failure as signal event
Solar Cells «Block» «Assembly»
Loss of Solar Cells_OutputPower «Effect»
Solar Cells Failed «Failure Mode»
Solar Cells
Solar Cells
Radiation Damage
Turn Off Solar Cells
Turn On Solar Cells
< >
SignalEvent Radiation Damage
SignalEvent Turn Off Solar Cells
SignalEvent Turn On Solar Cells
in sunlight in : Libraries::Single_Use_Library::Interfaces::Sunlight Interface «ProxyPort»
out power out : ~Libraries::Single_Use_Library::Interfaces::V_DC «ProxyPort»
stm [State Machine] Solar Cells [Solar Cells]
Off
entry / On Enter Solar Cells Off
Failed
entry / On Enter Solar Cells Failed Off
Turn On Solar Cells
«Failure» Radiation Damage
{Probability = 0.01}
Turn Off Solar Cells
On
entry / On Enter Solar Cells On
act [Activity] On Enter Solar Cells Failed Off[On Enter Solar Cells Failed Off]
Colors
Effect
Failure Mode
Propogate
Solar Cells Failed
: On Enter Sollar Cells Off
act [Activity] On Enter Sollar Cells Off[On Enter Sollar Cells Off]
Colors
Effect
Failure Mode
Propogate
Loss of Solar Cells_OutputPower
Turn Bus Off
stm [State Machine] Bus [Bus]
Off
entry / On Enter Bus Off
Turn Bus On
On
entry / On Enter Bus On
Turn Bus Off [Solar Cells == Off && Battery Charge == Empty]
Failed Off
entry / On Enter Bus Failed Off
«Failure»
Bus Failed
{Probability = 0.3}

Figure 2, Electrical Power System (EPS)-Solar Cells State Machine & Activity Diagrams of failure due to Radiation

After enhancing the nominal system model with the failure information, FMECAs and FTAs can be generated automatically from the enhanced SysML model. Figure 3 illustrates the FMECA and FTA outputs and different failure effects can be interactively selected from a system component hierarchy and displayed in a graphical user interface within the MagicDraw® application.



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
Generate Fault Tree
Unable to Connect Bus Power
FT1
Kill Switch Failure Modes:Stuck Off
FT1-1
Stuck Off
FT1-1.1
Mechanical Failure - Stuck Off
P=0.01
FT1-1.1.1
No Heating
Heater Failure Modes:Failed Off

Effects
- Solar Cells
- Battery
  - € Battery Charge and Voltage Degr
  - € No Battery Power
- Charger
- Power Bus
- Battery Temperature Sensor
- Kill Switch
  - € Unable to Disconnect Bus Power
  - € Unable to Connect Bus Power
- Battery Fuel Gauge
- Camera
- Infrared Camera
- CubeSat
- Heater
  - € No Heating
  - € Degraded Heating
  - € Heating Always On
- Battery Supervisor
- Watchdog

Figure 3, TACS EPS FMECA & FTA Output

This modeling approach has been demonstrated by NASA on projects such as NASA Cascade Distiller System [4] and has been the basis for some efforts on the NASA Europa Clipper [5].

The plan for this effort is to present the recommendation of a meta-model for the representation of faults and failures at the Trilateral Safety and Mission Assurance Conference (TRISMAC) in June 2021 in Tokyo and to work towards standardization of the framework across agencies.

References

1. T. Bayer et al., "Europa Clipper Mission: Preliminary Design Report," 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2019, pp. 1-24, doi: 10.1109/AERO.2019.8741777.
2. J. Evans, S. Cornford and M. S. Feather, "Model based mission assurance: NASA's assurance future," 2016 Annual Reliability and Maintainability Symposium (RAMS), Tucson, AZ, 2016, pp. 1-7, doi: 10.1109/RAMS.2016.7448047.
3. M. Izygon, H. Wagner, S. Okon, L. Wang, M. Sargusingh and J. Evans, "Facilitating R&M in spaceflight systems with MBSE," 2016 Annual Reliability and Maintainability Symposium (RAMS), Tucson, AZ, 2016, pp. 1-6, doi: 10.1109/RAMS.2016.7448031.
4. M.J. Sargusingh, M.R. Callahan, S. Okon, “Cascade Distillation System Design for Safety and Mission Assurance,” 45th Int. Conf. on Environmental Systems, Bellevue, Washington, 2015.
5. Castet, J.F., Bareh, M., Nunes, J., Okon, S., Garner, L., Chacko, E. and Izygon, M., 2018, March. Failure analysis and products in a model-based environment. In 2018 IEEE Aerospace Conference (pp. 1-13). IEEE.

Acknowledgements: this research was carried out at ESA, NASA, JAXA, Tietronix, Vanderbilt University, and the Jet Propulsion Laboratory, California Institute of Technology under a contract with the National Aeronautics and Space Administration.