



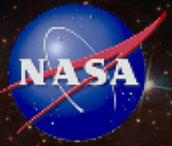
Modeling Off-Nominal Behavior in SysML

**John Day, Kenny Donahue, Mitch Ingham,
Alex Kadesch, Kit Kennedy, Ethan Post**

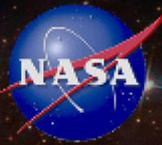
Jet Propulsion Laboratory, California Institute of Technology

AIAA Infotech@Aerospace Conference

June 21, 2012



- **Introduction**
- **Soil Moisture Active-Passive (SMAP) Mission**
- **Capturing Off-Nominal Behavior**
- **Concepts and Relationships**
- **Generation of FM Artifacts**
- **Generation of FMEA from Model**
- **Future Research and Development**
- **Conclusion**



- **Off-nominal behavior is the unintended or unexpected behavior of a system.**
 - Fault Management (FM) is the systems engineering process that assesses and determines the appropriate set of system functions, interfaces and components needed to prevent, mitigate or tolerate off-nominal behavior.
- **While often locally effective, the *ad hoc* methods used in FM result in incomplete assessments of safety, reliability and availability**
 - Further, these assessments are based on time-consuming analyses and design processes that rely on multiple, often implicit, assumptions.
- **As our designed systems grow in capability and complexity, the understanding of emergent behavior in these systems will decrease, leading to systems that are less safe and reliable than systems fielded today.**
 - Only by increasing the rigor with which we consider system behavior as a whole – and off-nominal behavior in particular – can we improve our understanding of these systems, and make significant gains in safety, reliability and availability.
- **Using the Systems Modeling Language (SysML) we show how some basic elements of FM can be performed rigorously, and specific FM artifacts derived from a system model.**

Soil Moisture Active-Passive Mission (SMAP)

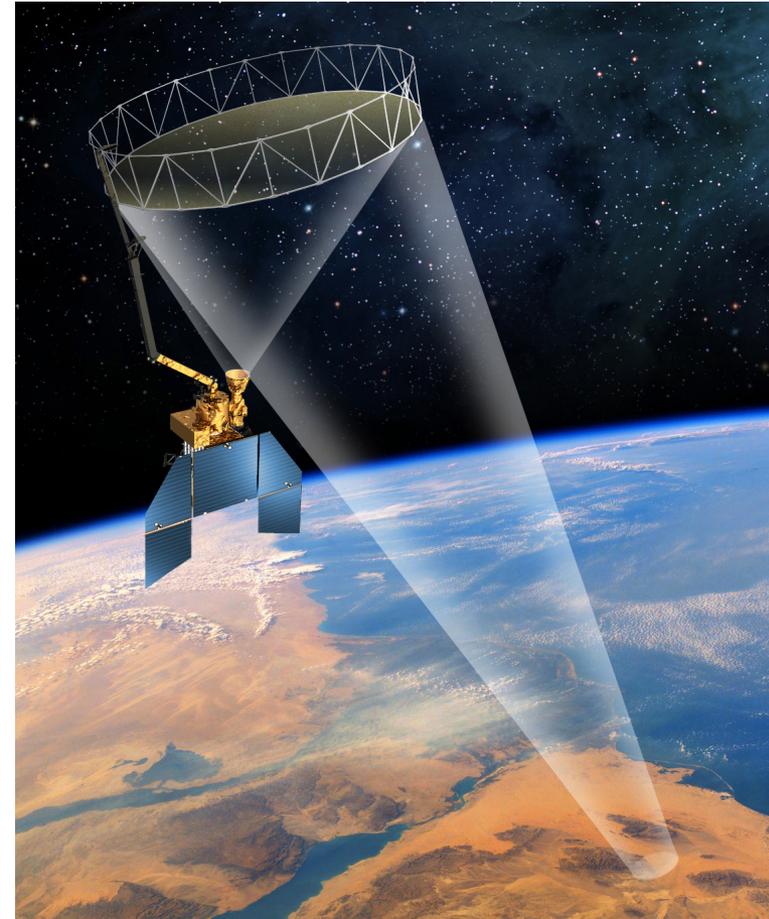


- **SMAP Mission**

- The purpose of the SMAP mission is to determine the moisture content of the Earth's upper soil and its freeze/thaw state.
- This is accomplished using the Instrument, which is composed of a radar, radiometer, and a rotating reflector antenna.
- After separation from the launch vehicle, the Flight System, which is composed of the Instrument and the Spacecraft Bus, must deploy the Instrument and spin up the antenna to the correct spin rate for science data collection.

- **Model-based SE Pilot**

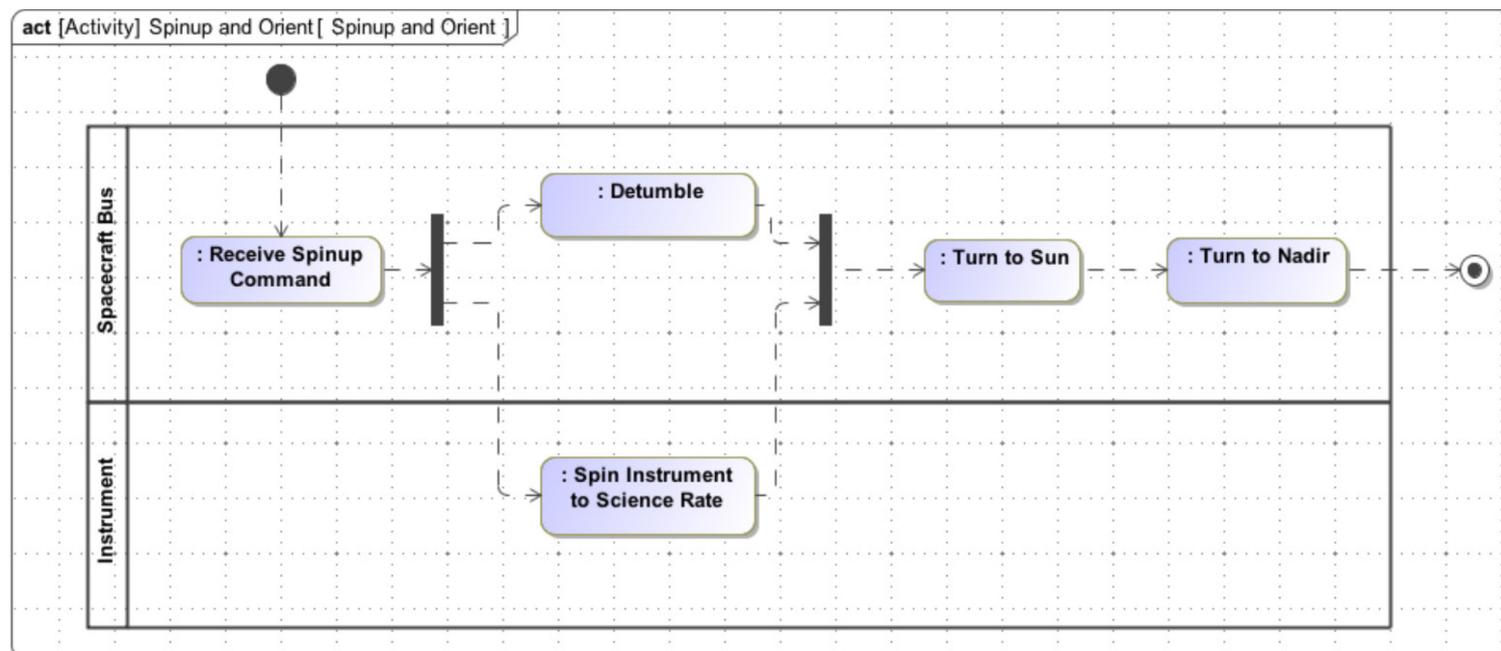
- Our work has focused on modeling the SMAP antenna spin-up behavior in SysML, including the possible off-nominal behaviors of this activity



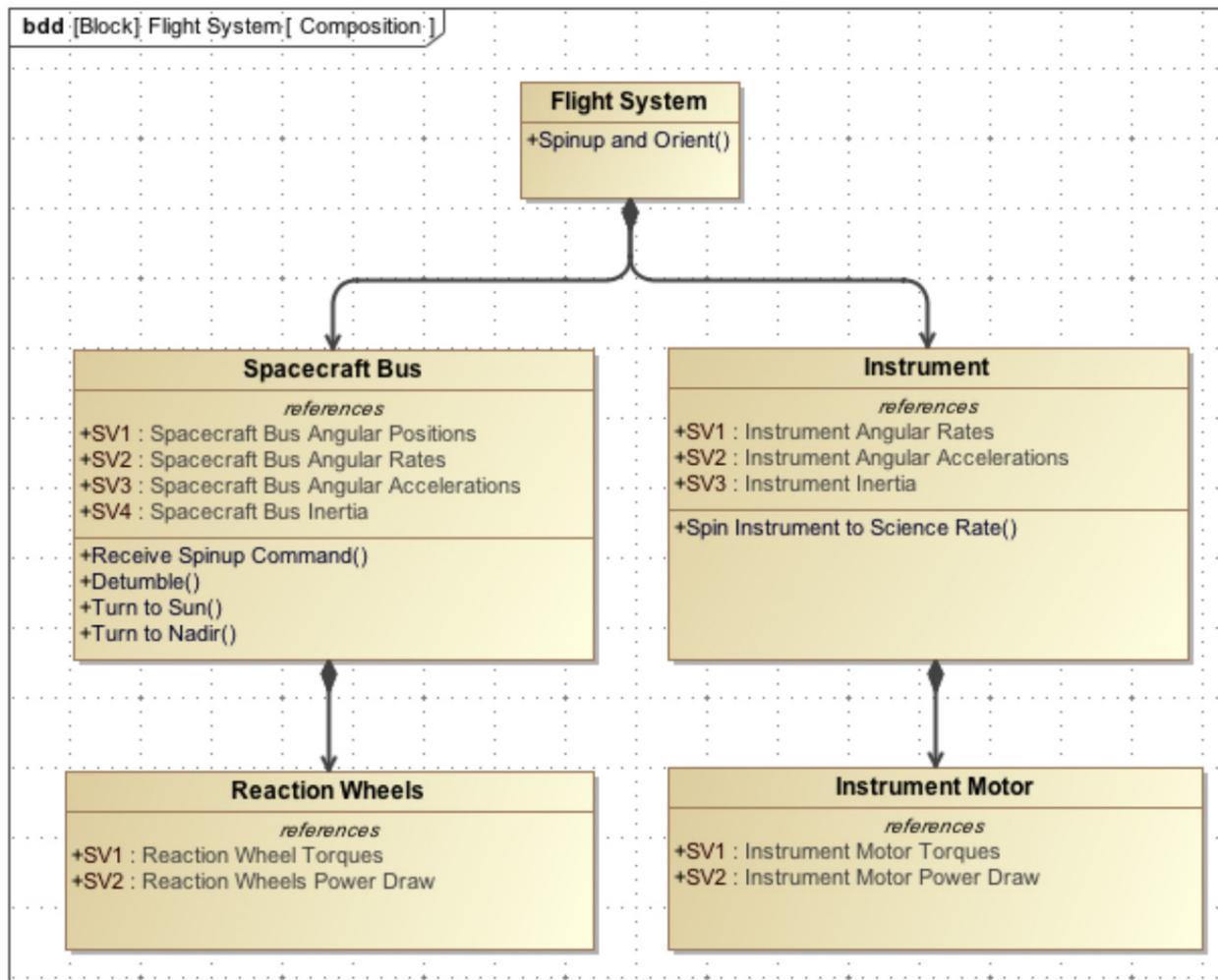
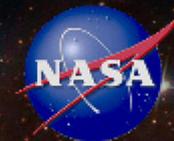
Model of SMAP Spin-up Activity



- Spinup of the SMAP instrument antenna is initiated by ground command
- The change in momentum causes the spacecraft bus to begin spinning in the opposite direction, requiring a detumble activity to null spacecraft rates
- After detumble, the the spacecraft bus first turns to Sun, then to nadir before continuing on to instrument checkout and operation



Model of SMAP Structure





- **Systems are conceived, developed and designed with some defined purpose, expressed as a set of system objectives.**
 - The set of system objectives, over time, can be described as the intended behavior of the system.
- **Developing a system requires an understanding of both the nominal (intended and expected) behavior and the off-nominal behavior.**
 - However, the off-nominal state space is much larger than the nominal state space – capturing this in a way that allows development of appropriate design mechanisms, without losing essential information, is difficult and time-consuming.
- **Development of an integrated system model, has significant benefits that we leverage to effectively address the nominal and off-nominal behavior of a system.**
 - In this conception, engineering artifacts are views derived from the system model

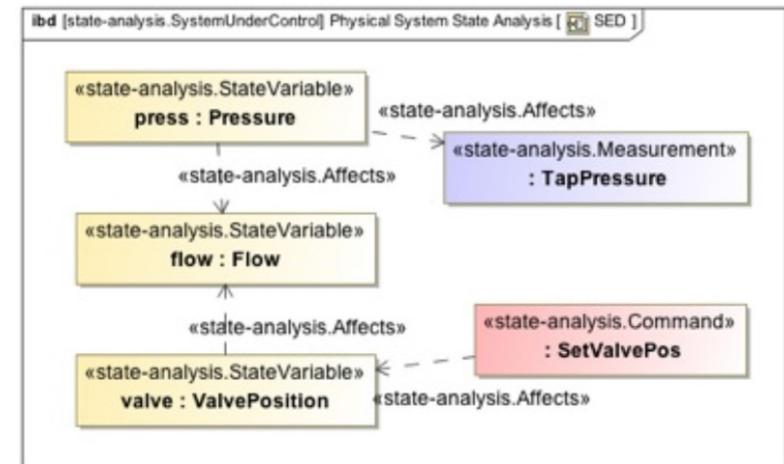
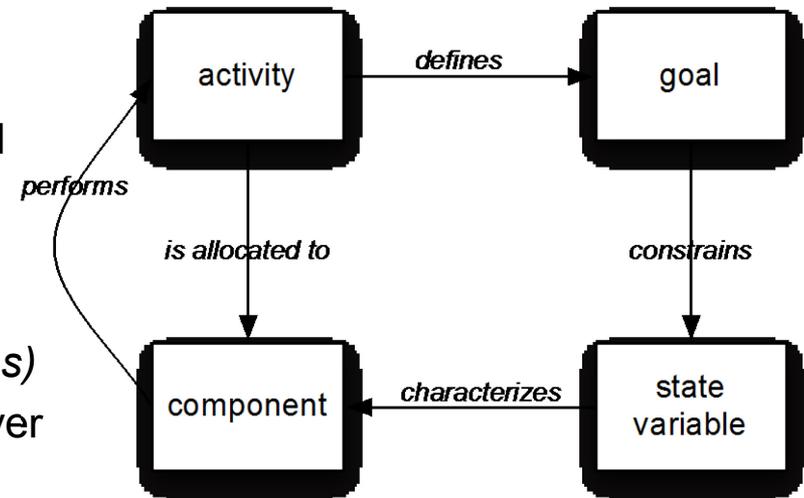


- **Typical FM analysis artifacts (e.g., FMEAs, FTA) rely heavily on system descriptions of structure and behavior.**
 - An integrated system model that defines explicit connections between system descriptions and failure analysis artifacts has the potential to provide exceptional improvement in both the accuracy of the failure analyses and a reduction in the amount of effort necessary to develop and maintain the analyses
- **One beneficial approach is to include the results of failure analysis in the system model.**
 - This allows explicit crosschecks between the failure analyses and the model structure, which significantly improves the ability of engineers to relate the two
- **However, a much more powerful approach is to include the necessary relationships in the system model, and to use these relationships to derive the necessary FM artifacts.**
 - In this way, a FMEA or FTA becomes just another view of the system, and is always current and consistent with the rest of the model. This approach enables significant improvements in both the accuracy and development time required

Concepts, Relationships and Views



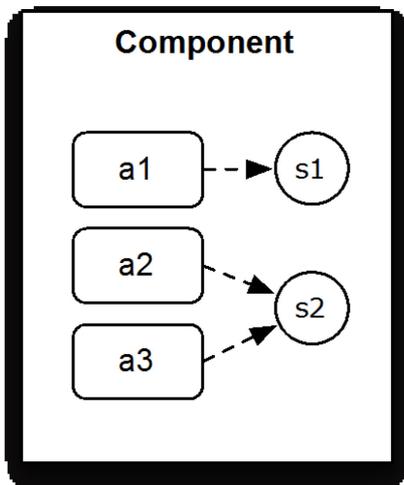
- **We utilize four basic concepts, and define their relationships:**
 - Activity: actions that describe the intended behavior of the system
 - Component: system elements at a given level of abstraction
 - *components perform functions (activities)*
 - Goal: intended value of a state variable over some period
 - *each activity has a single goal associated with it, but there may be multiple goals associated with each state variable*
 - State Variable: a characteristic of a system component
- **System views:**
 - Use typical SysML diagrams (activity, block definition, etc.)
 - Plus a “state effects diagram” (SED) that shows which state variables affect other state variables



Generation of FMEA from Model



- In our model, every nominal activity is allocated to a component
- Each activity specifies an intended outcome, and the inability to perform that activity is used as the defining characteristic of a failure mode
 - Failure modes are the “inverse of intent”
 - Intent may come from different sources, and may contribute to confusion in this area



Component	State Variable	Failure Mode	Causes	Effects
C1	SV1	a1 failure		
C1	SV2	a2 failure		
C1	SV2	a3 failure		
...		

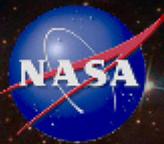
Simple FMEA for SMAP Flight System



- To build a FMEA for the SMAP Flight System we collected the set of activities allocated to it
- By using the logical negation of each activity (“Failure to Spin-up” instead of “Spin-up”) we develop the set of failure modes for the flight system
 - Each row lists the component of interest followed by a state variable then a failure mode
 - The set of failure modes is limited to the spin-up activity

Component	State Variable	Failure Mode
Spacecraft Bus	(undefined in model)	Failure to receive spinup command
Spacecraft Bus	Spacecraft Bus Angular Rates	Failure to detumble
Spacecraft Bus	Spacecraft Bus Angular Positions	Failure to turn to sun
Spacecraft Bus	Spacecraft Bus Angular Positions	Failure to turn to nadir
Instrument	Instrument Angular Rates	Failure to spin instrument to transition rate

Full FMEA for SMAP Flight System



- The information contained within a FMEA is more accurate for immediate failure effects or failure symptoms, but often becomes progressively more inaccurate the further away the effect is from the originating component
- We use the relations captured in the SED to determine a rigorous set of causes and effects of the failure modes in our FMEA

Component	State Variable	Failure Mode	Causes	Effects
Spacecraft Bus	(undefined in model)	Failure to receive spinup command	(none for this example)	-RW unable to draw power -RW unable to provide sufficient torque -SCB unable to accelerate sufficiently
Spacecraft Bus	Spacecraft Bus Angular Rates	Failure to detumble	-SCB unable to provide necessary acceleration -SCB Inertia not sufficiently known -RW's unable to provide necessary torque -Instrument unable to accelerate nominally	-SCB unable to control angular position sufficiently
Spacecraft Bus	Spacecraft Bus Angular Positions	Failure to turn to sun	-SCB unable to provide necessary rates -SCB unable to provide necessary acceleration -SCB Inertia not sufficiently known -RW's unable to provide necessary torque -Instrument unable to accelerate nominally	(none for this example)
Spacecraft Bus	Spacecraft Bus Angular Positions	Failure to turn to nadir	-SCB unable to provide necessary rates -SCB unable to provide necessary acceleration -SCB Inertia not sufficiently known -RW's unable to provide necessary torque -Instrument unable to accelerate nominally	(none for this example)
Instrument	Instrument Angular Rates	Failure to spin instrument to transition rate	-Instrument unable to provide necessary acceleration -Instrument Inertia not sufficiently known -Instrument Motor unable to provide necessary torque -SCB unable to provide necessary acceleration	-Instrument unable to move nominally



- **This work described here only scratches the surface of the possible applications of modeling off-nominal behavior.**
 - Determination of the relevant concepts and relationships needed to derive a FMEA required only a small set of relevant concepts and relationships.
- **Other typical FM artifacts, and the ability to perform other analyses, require additional concepts and relationships to be defined.**
 - In particular, we are interested in generation of fault trees, success trees and reliability block diagrams directly from the system model, and querying the information in the model to assess the completeness and effectiveness of the FM functionality.
- **Ultimately, we intend to develop a SysML profile that captures these concepts and relationships and allows effective and consistent application within a system model.**



- **Fault Management is an essential part of the system engineering process that is limited in its effectiveness by the *ad hoc* nature of the applied approaches and methods.**
 - Providing a rigorous way to develop and describe off-nominal behavior is a necessary step in the improvement of fault management, and as a result, will enable safe, reliable and available systems even as system complexity increases.
- **The basic concepts described in this paper provide a foundation to build a larger set of necessary concepts and relationships for precise modeling of off-nominal behavior, and a basis for incorporating these ideas into the overall systems engineering process.**
- **The simple FMEA example provided applies the modeling patterns we have developed and illustrates how the information in the model can be used to reason about the system and derive typical fault management artifacts.**
- **A key insight from the FMEA work was the utility of defining failure modes as the “inverse of intent”, and deriving this from the behavior models.**
- **Additional work is planned to extend these ideas and capabilities to other types of relevant information and additional products**



Backup Slides

Simplified State Effects Diagram

