

A Domain Specific Design Tool for Spacecraft System Behavior

Sravanthi Venigalla, Brandon Eames

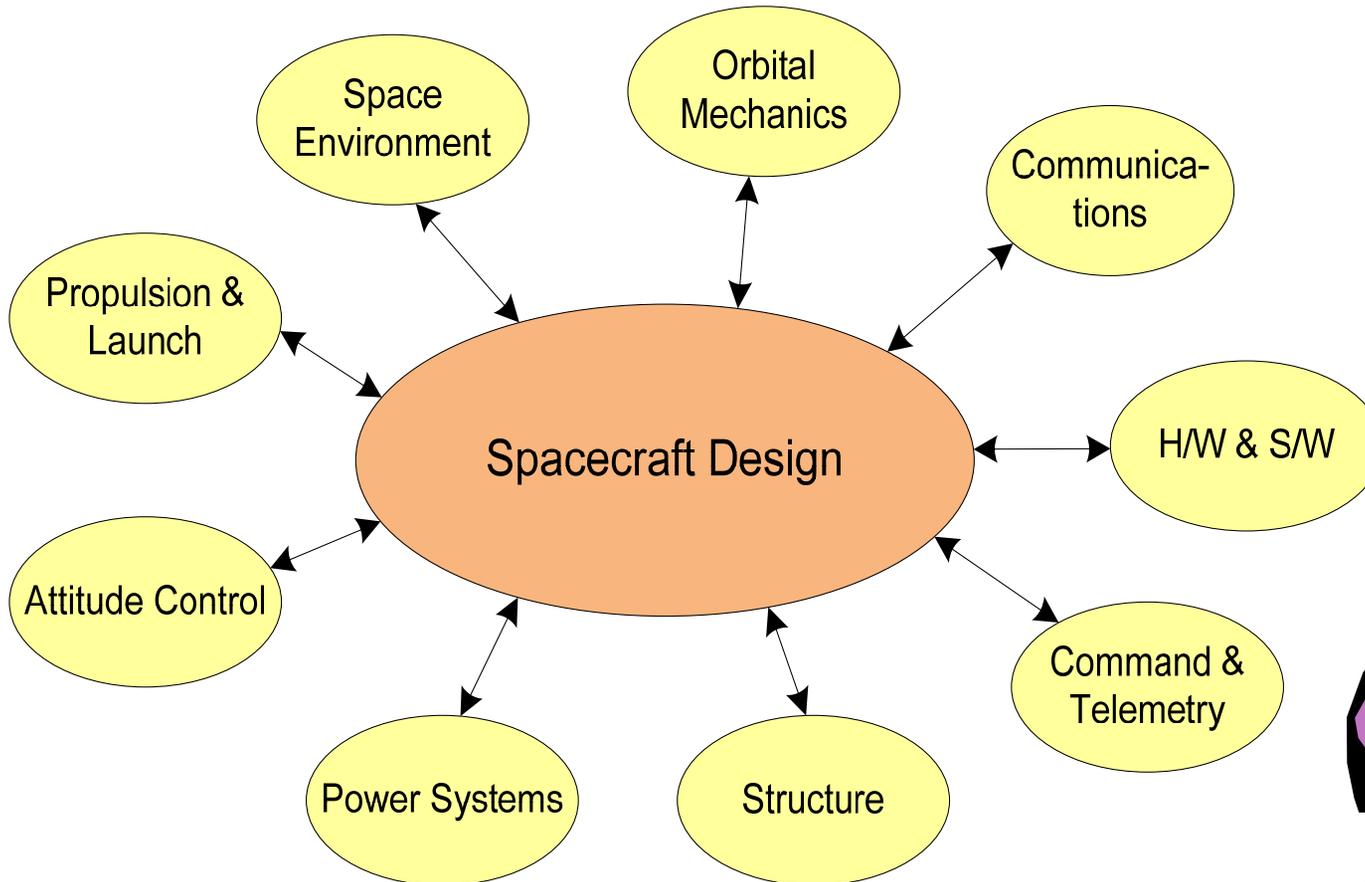
Utah State University, USA

Allan McInnes

University of Canterbury, New Zealand

Domain Specific Modeling Workshop 2008 (DSM'08)

Spacecraft Design

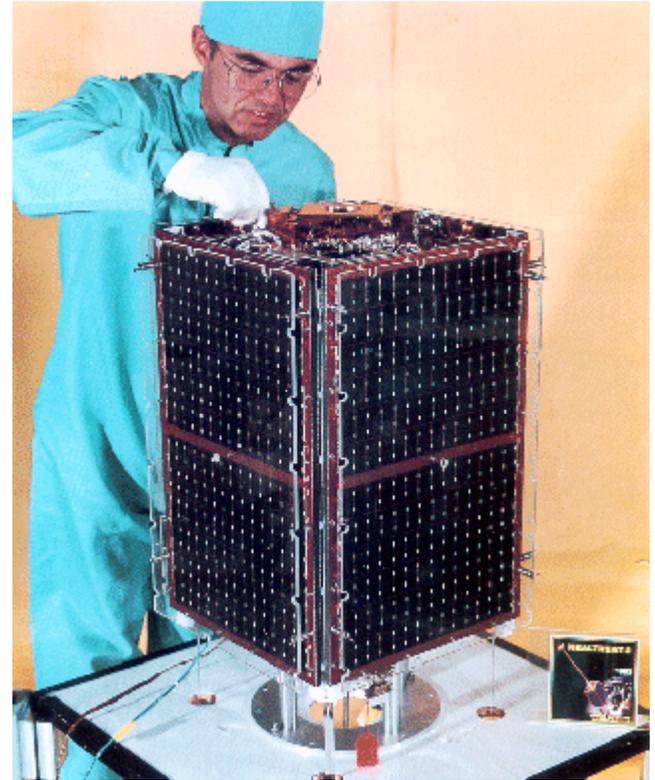


Not an easy task!



Spacecraft vs. Other Systems

- Interdisciplinary
- Limitations & tradeoffs due to space environment
- Lot of interaction for carrying out operations
- Difficult/Not possible to modify after launch
- Failures imply huge loss of money and reputation



A typical small satellite

Fig from Small Satellites Home Page <http://centaur.sstl.co.uk/>

Subsystem view of a Spacecraft

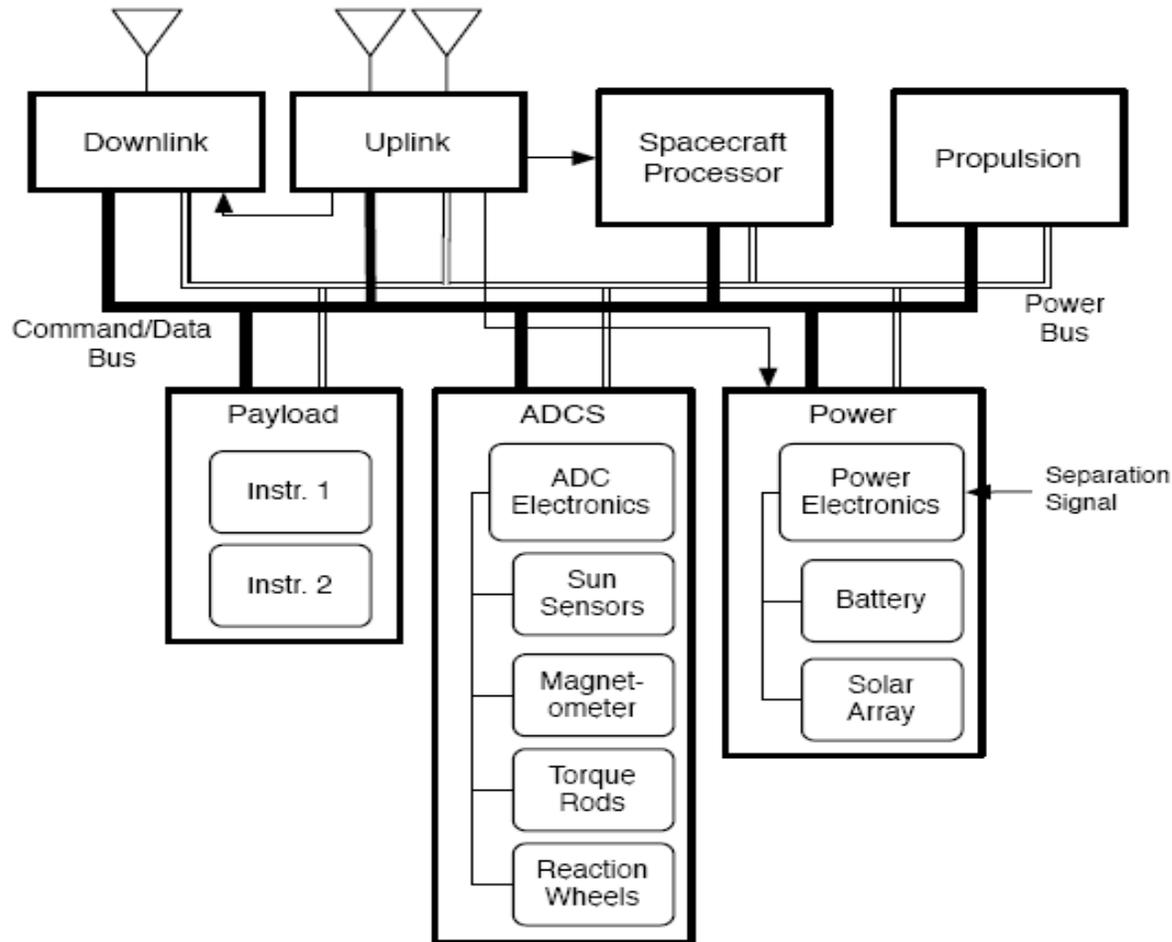
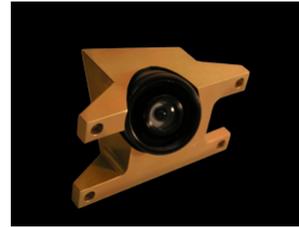


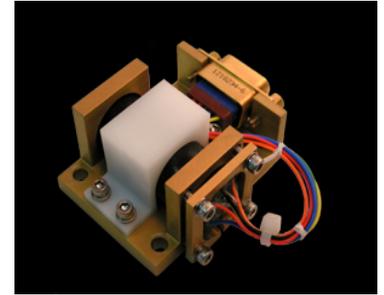
Figure from Allan I. S. McInnes Ph.D. dissertation “A formal approach to specifying and verifying Spacecraft behaviour”

ADCS Subsystem

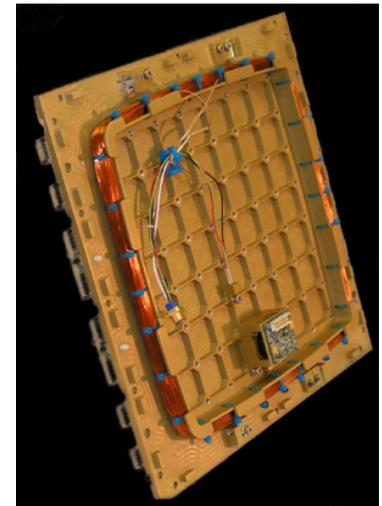
- Concerned with the spacecraft's orientation in space.
- Determines whether science operations can be performed.
- Affects the solar power that can be generated by the spacecraft.



Star camera

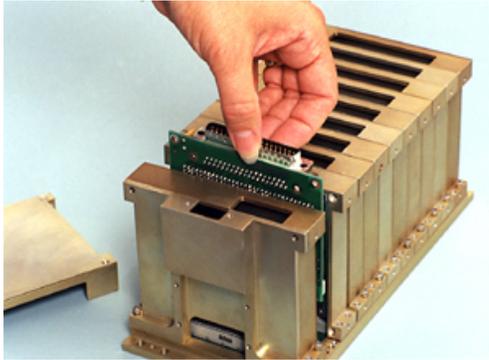


Magnetometer



Actuator

CDH & Power Subsystems



CDH Subsystem



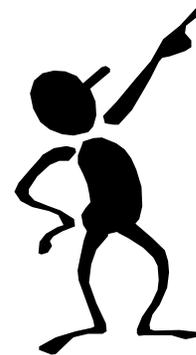
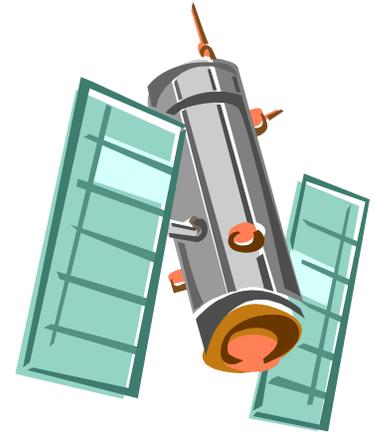
Solar cells

- Consists of hardware & software
- Manages all interactions with ground station

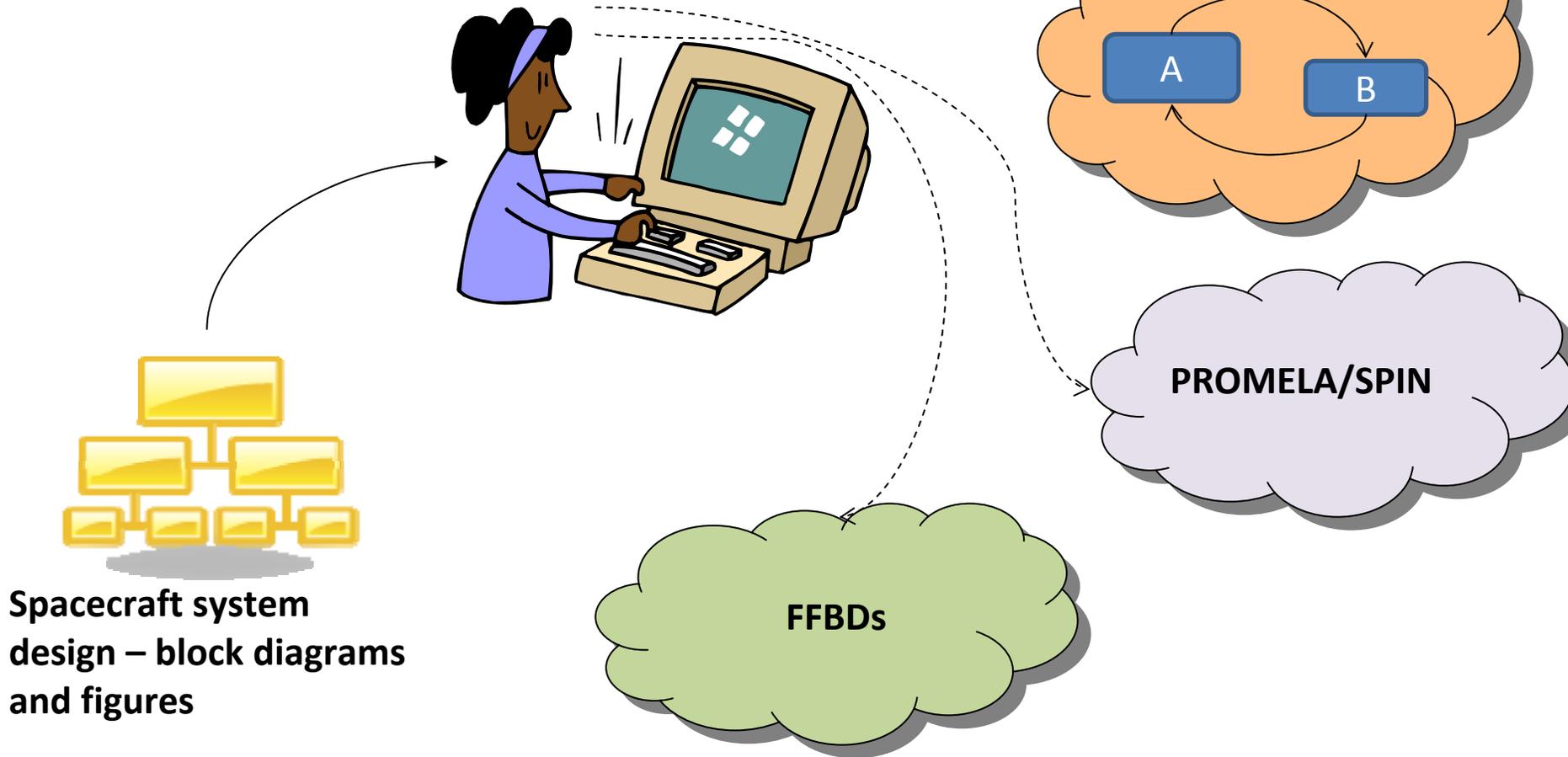
- Consists of sources of power – solar cells and batteries and the wiring to other subsystems.

How to Analyze Spacecraft Behavior?

- Simulation ?
- Verification
 - At the subsystem level
 - At the system level
- Validation
 - At the system level

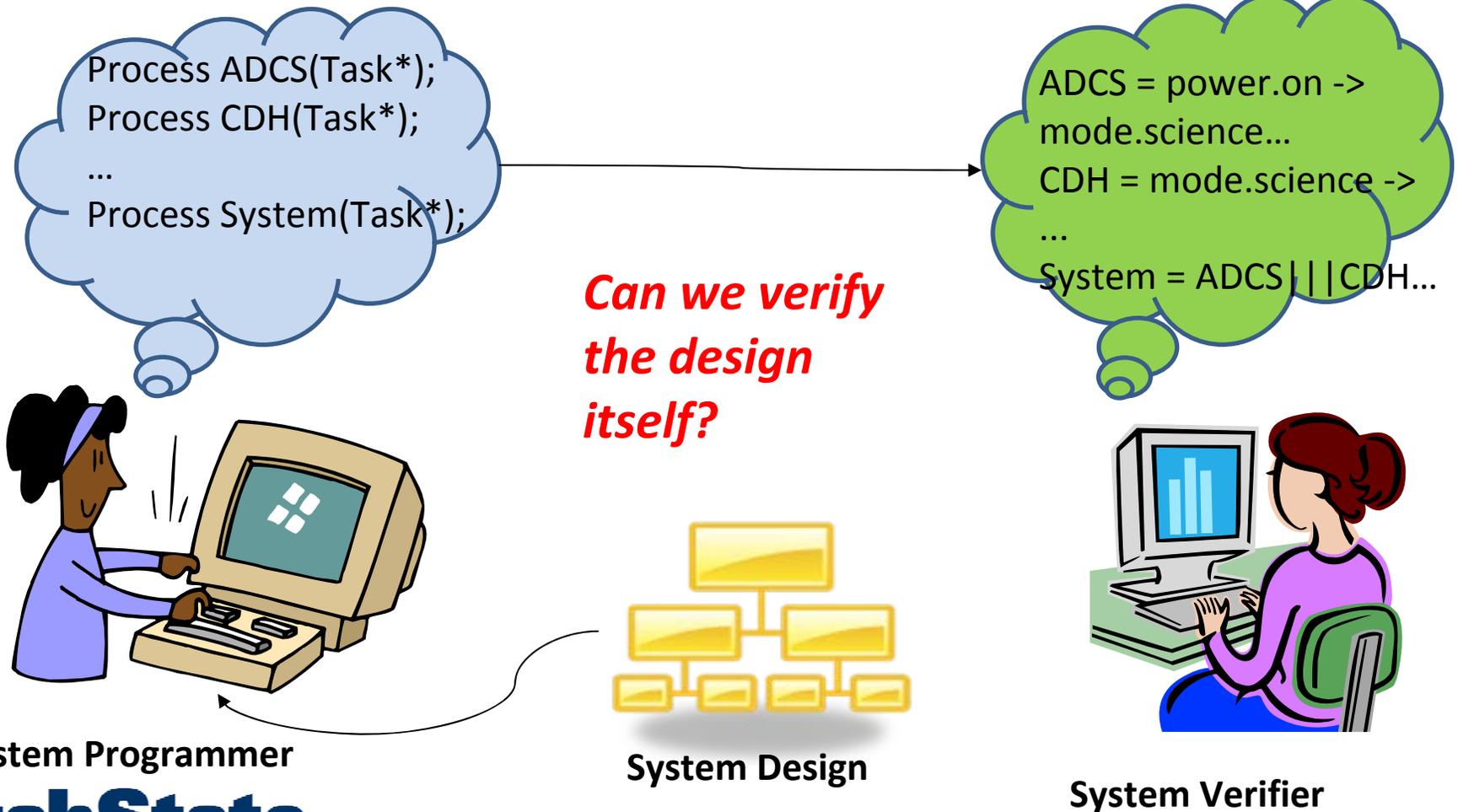


Common Formalisms for modeling Behavior



Spacecraft system design – block diagrams and figures

System Development & Verification



Communicating Sequential Processes (CSP)

- A process algebra used for system verification.
- A system is described in terms of an appropriate combination of processes .
- Each process is described in terms of channels and events.
- Event is an abstract symbolic representation of an interaction.
- Channels are the carriers for events.

CSP contd...

- Operators for alternate actions – $[]$ is for choice exercised by the environment and $|\sim|$ is for non-deterministic choice.
- Generalized Parallel Combination – $P1[|A|]P2$ is for synchronization between processes P1, P2 over the set of events A.
- Interleaved Parallel Combination – $P1 ||| P2$ is for the case when P1 and P2 run independently of each other.

An Example – A packet receiver

channel success, fail

channel response : {0,1}

Proc = recv?packet -> if (checksum = 0)
 then success -> Proc
 else fail -> Proc

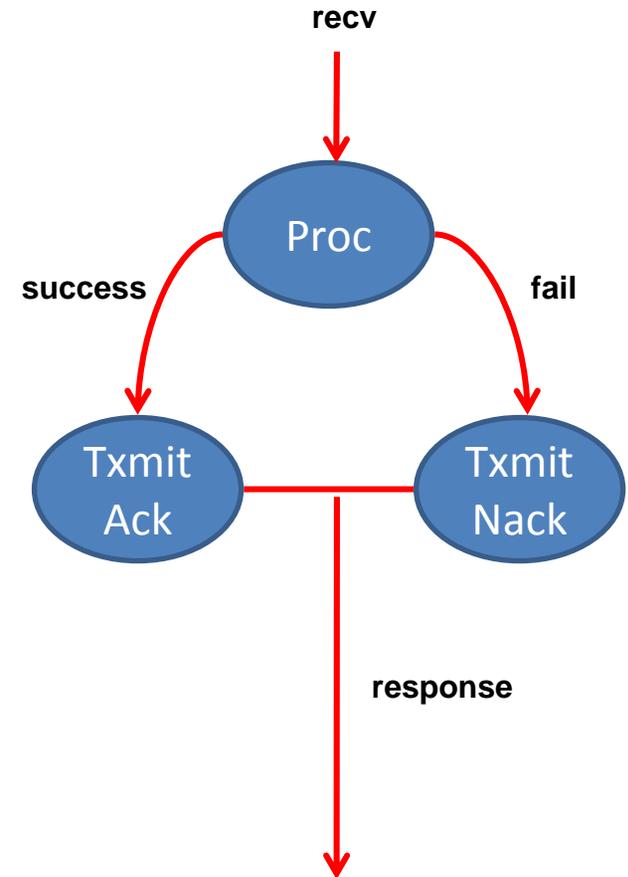
TxmitAck = success -> response!0 -> TxmitAck

TxmitNack = fail -> response!1 -> TxmitNack

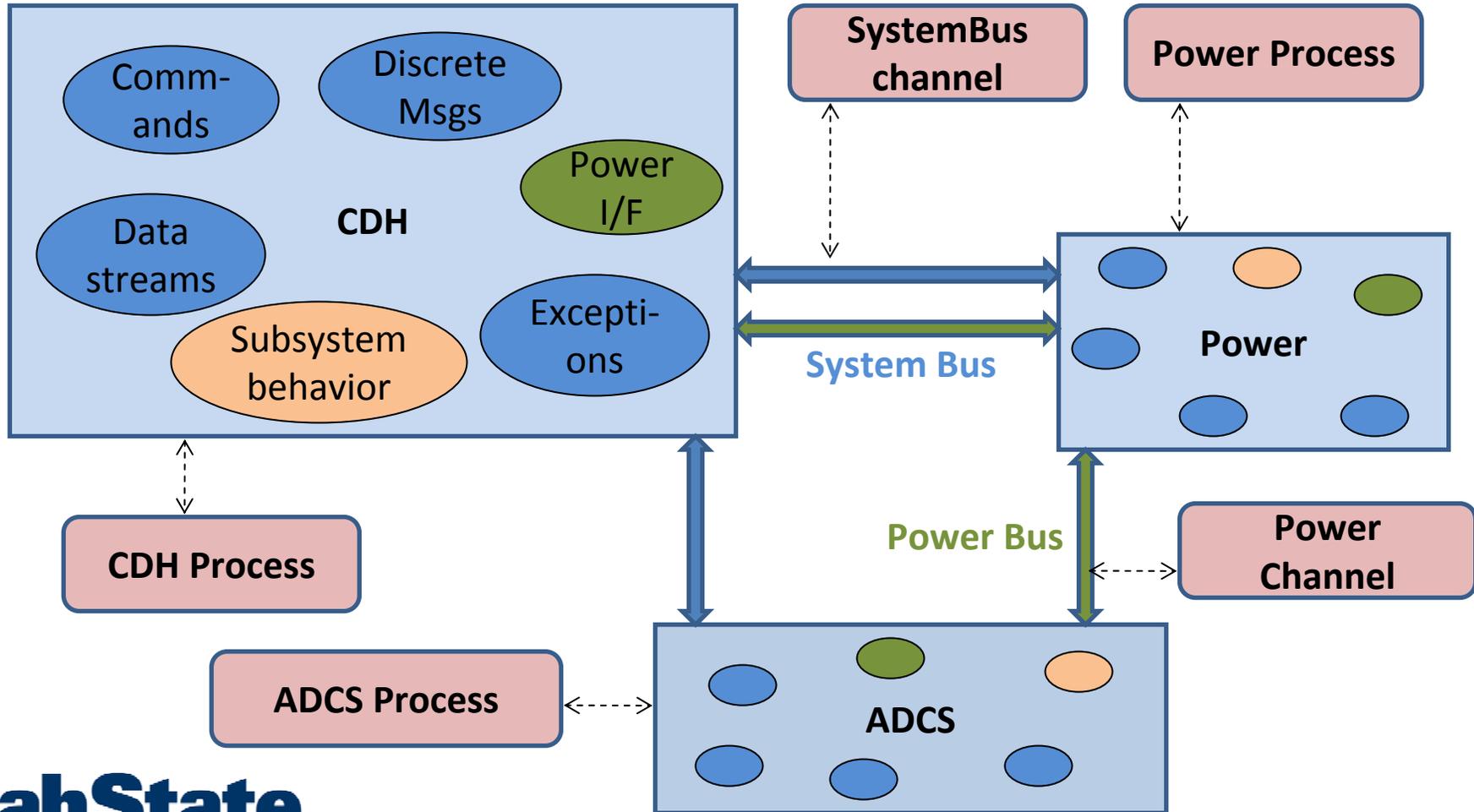
Composite = (TxmitAck ||| TxmitNack)

 [|success, fail|]

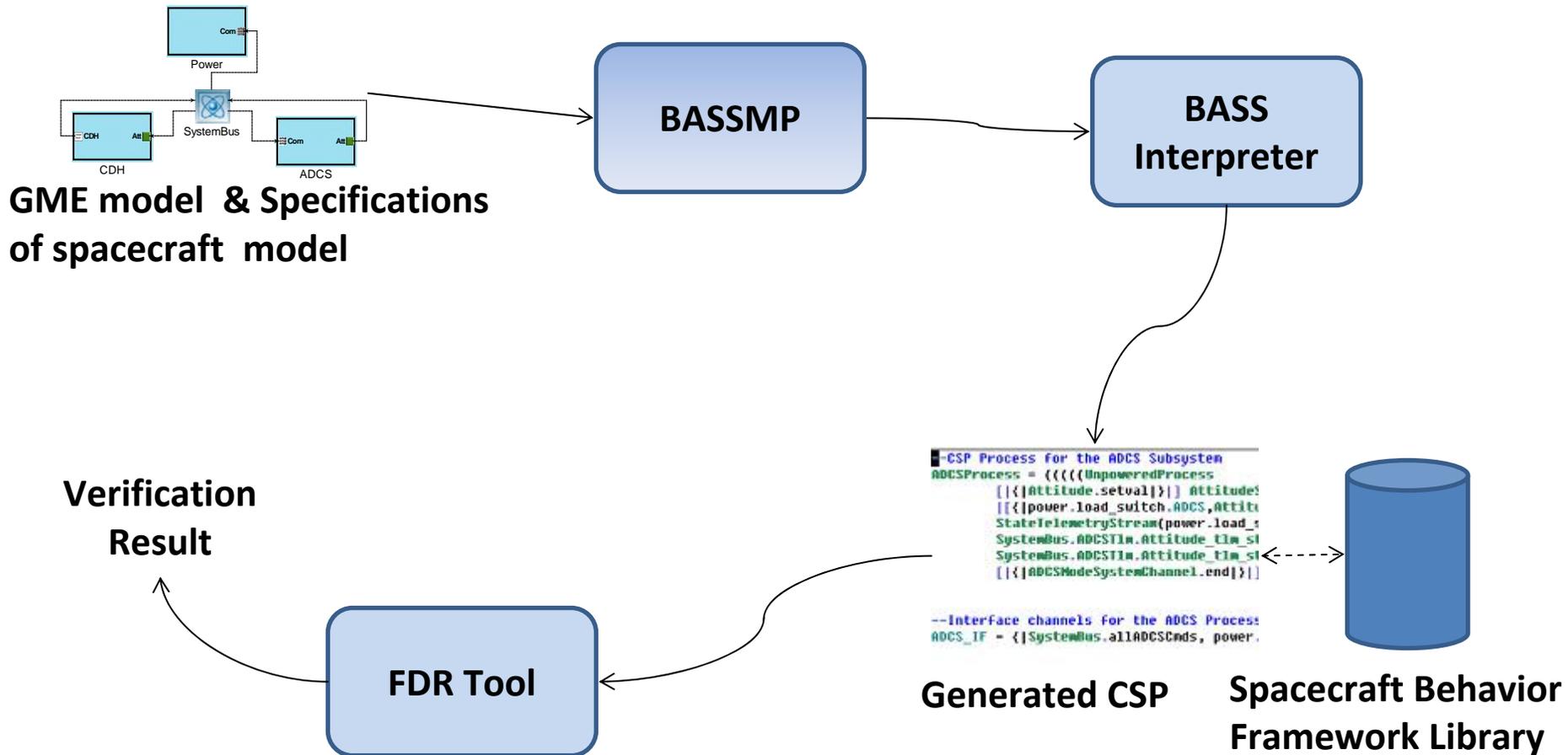
 Proc



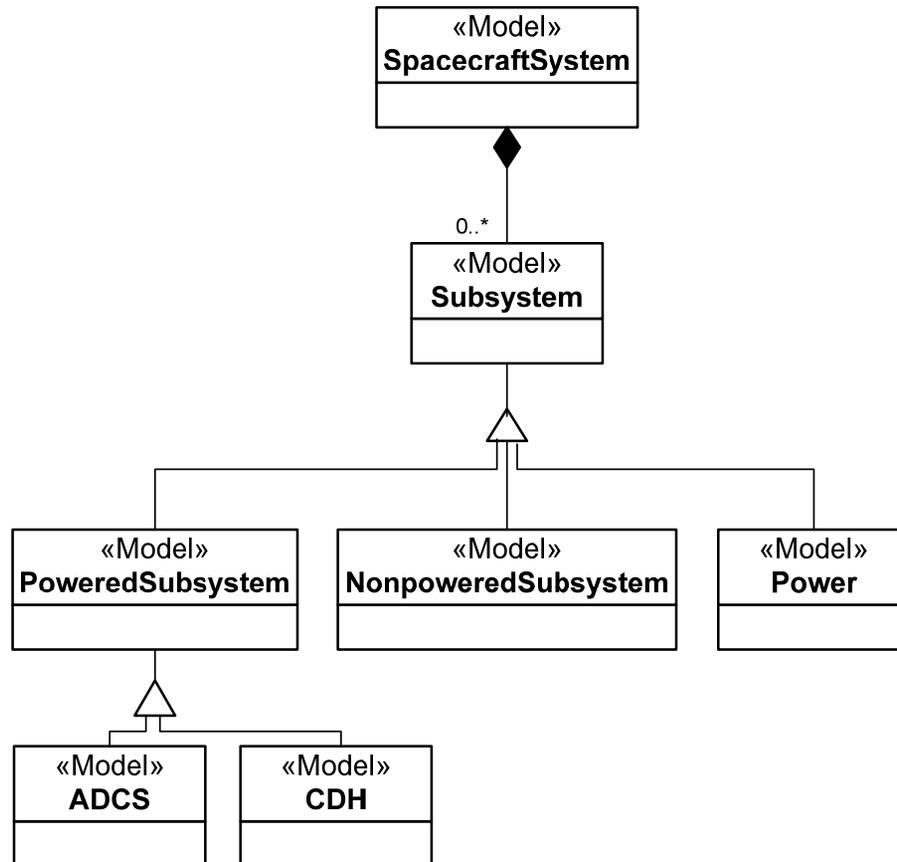
High Level Spacecraft Behavior in CSP



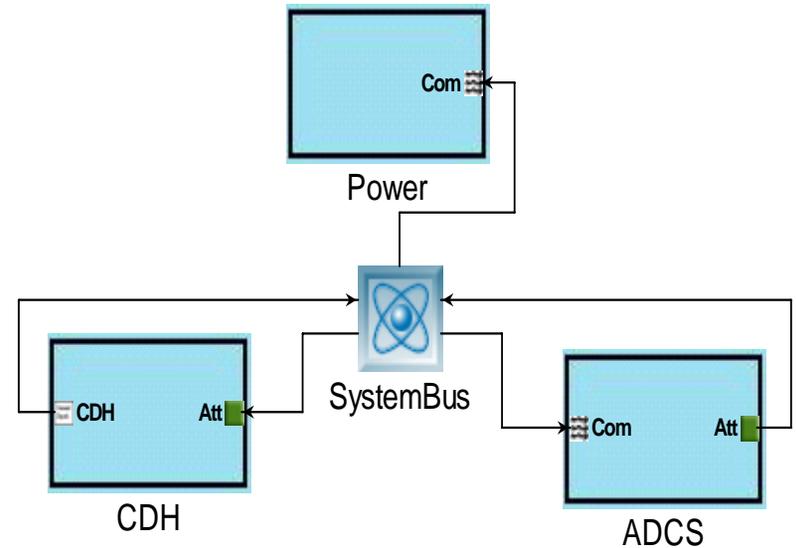
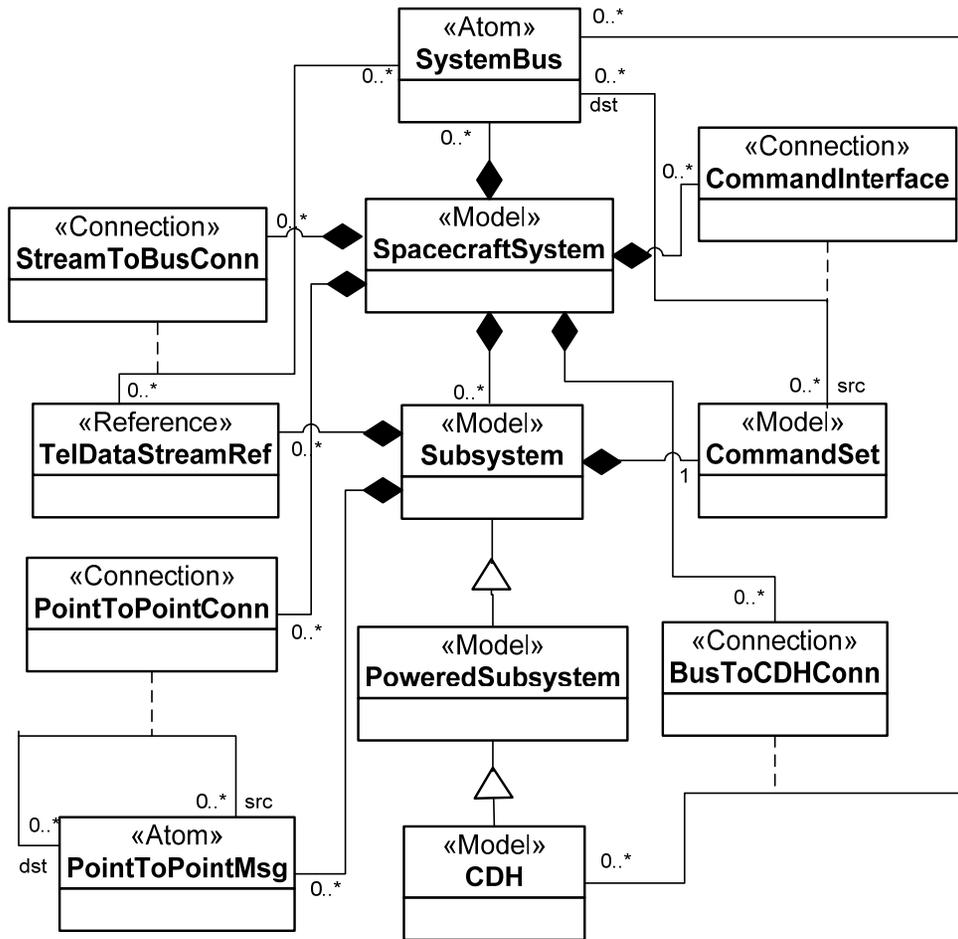
BASS Tool Flow



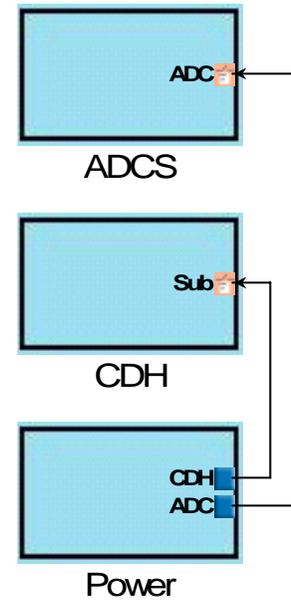
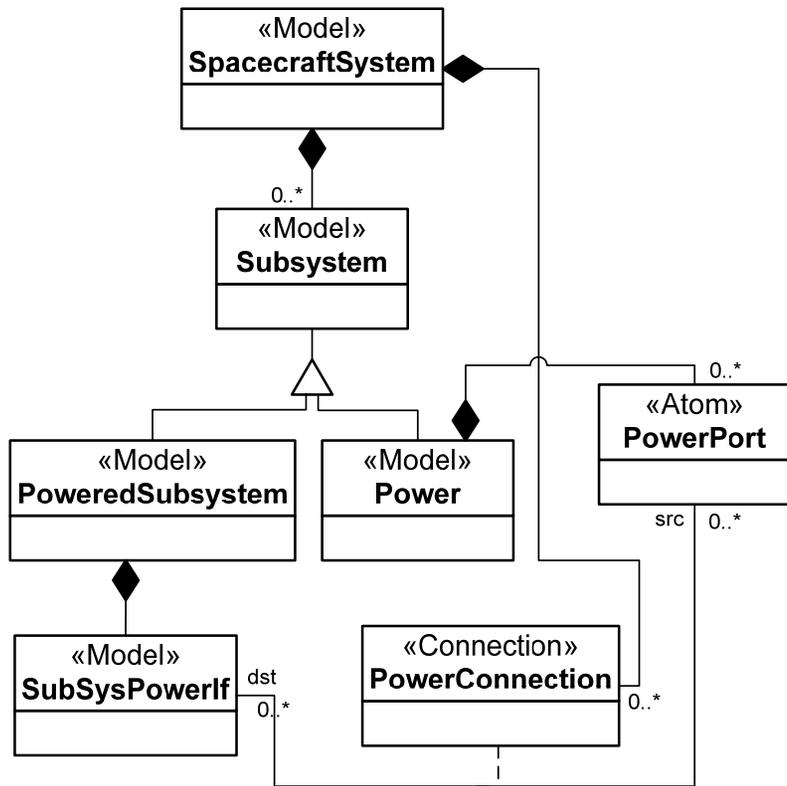
Spacecraft System



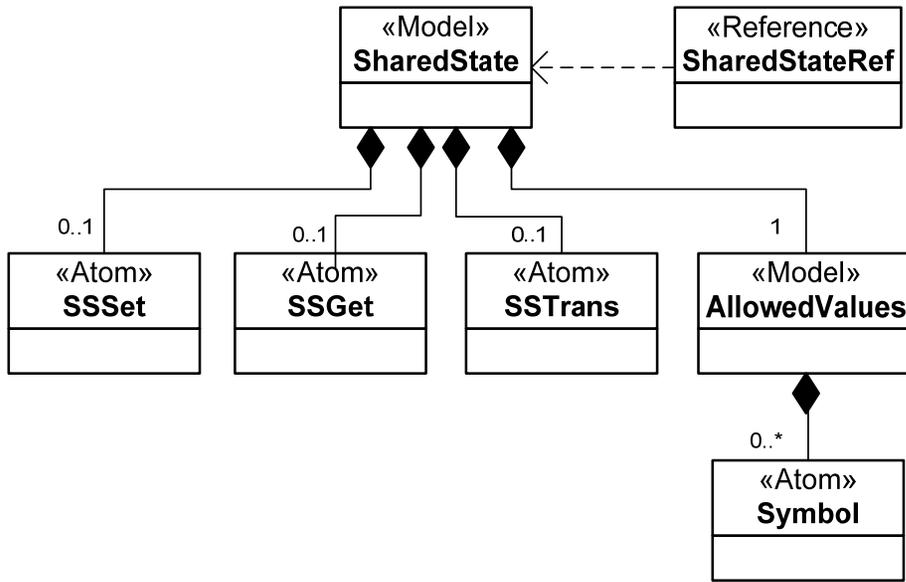
Datacomm Aspect of Spacecraft



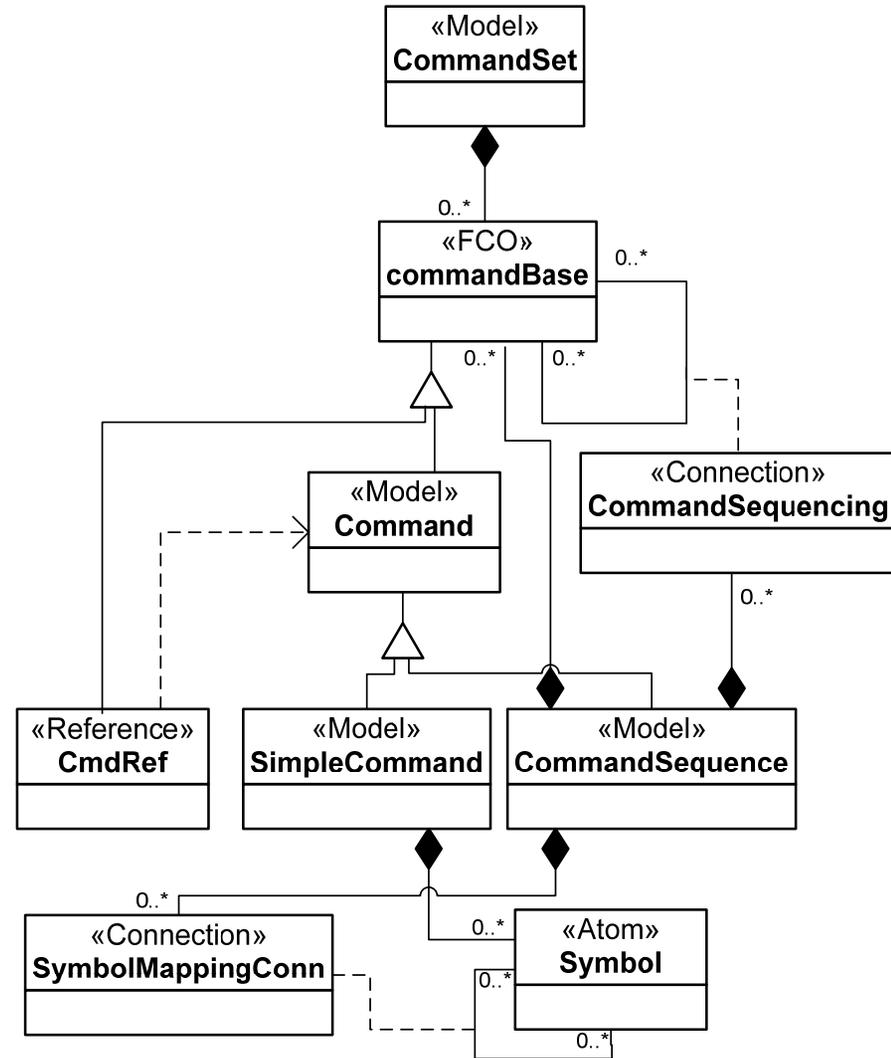
Power Aspect of the Spacecraft



Common Constructs

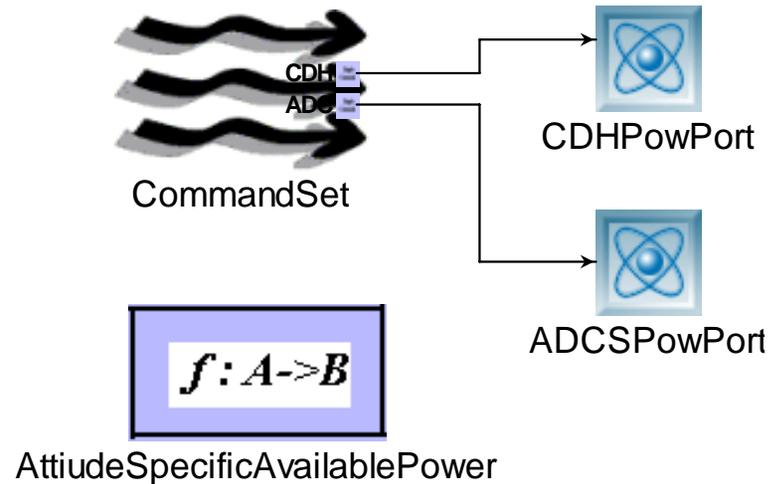
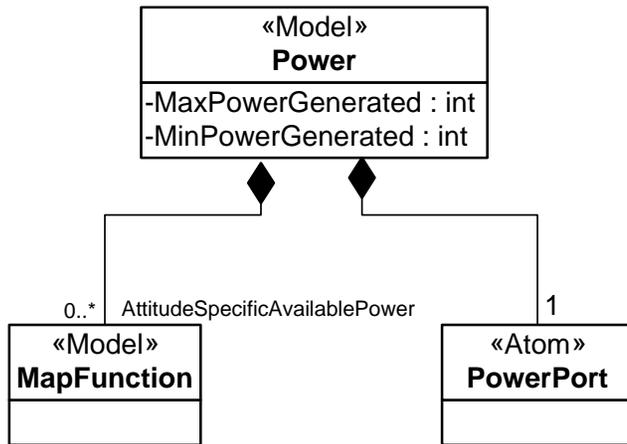


Shared State Object representing a shared variable

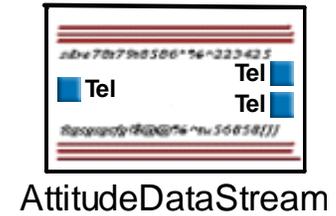
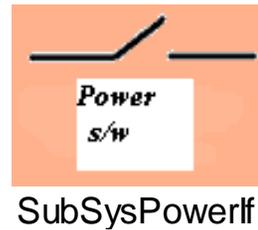
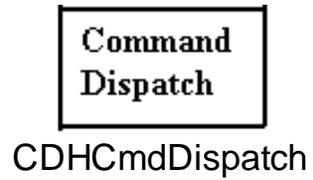
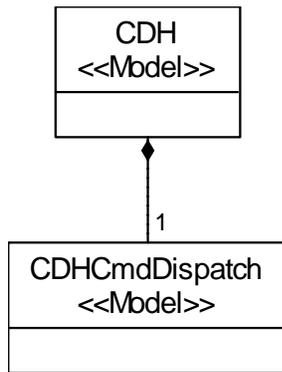


Spacecraft Commands

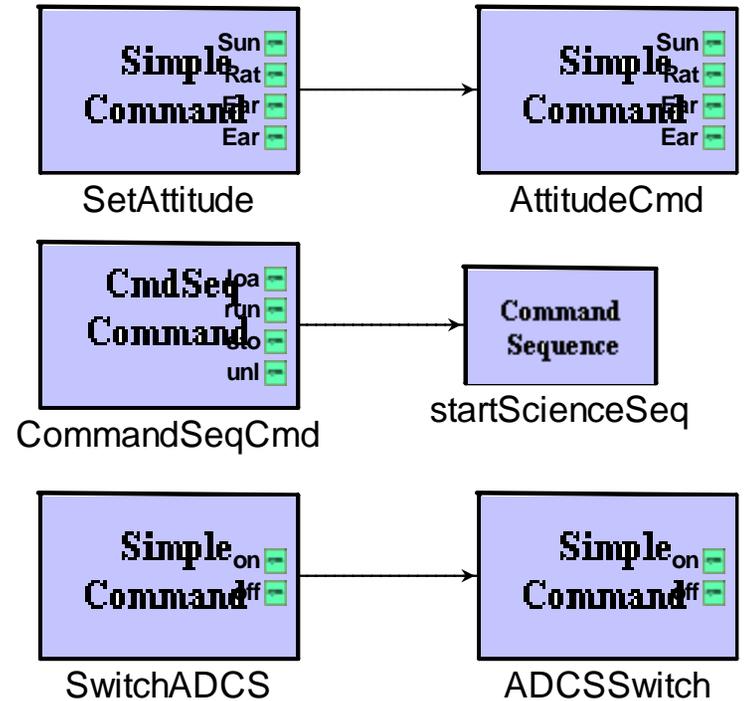
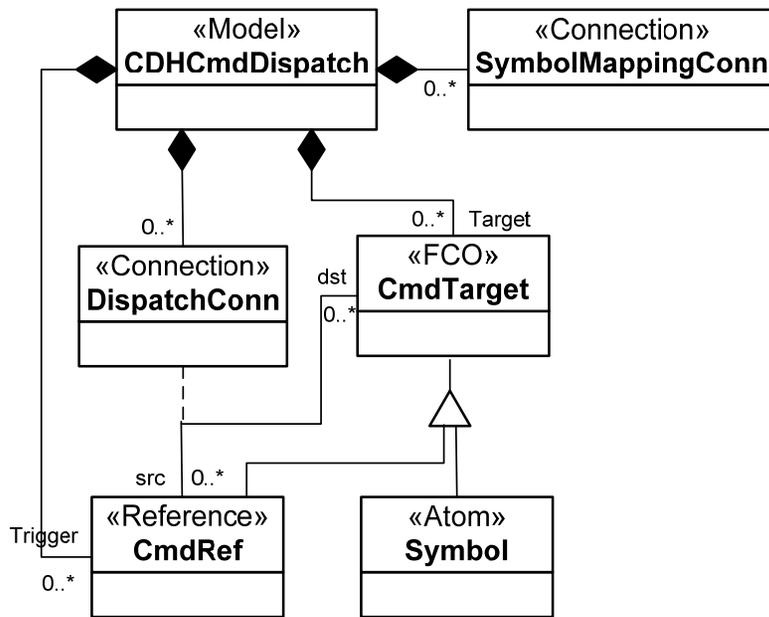
Power Subsystem



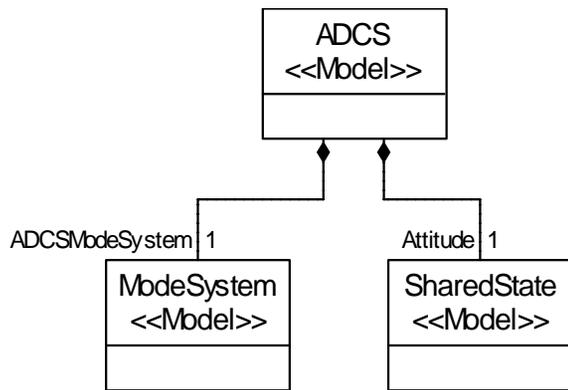
CDH Subsystem



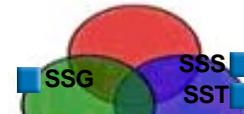
CDH Command Dispatch



ADCS Subsystem



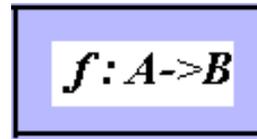
CommandSet



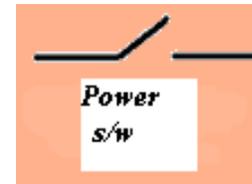
Attitude



ADCSModeSystem



ADCSModePower

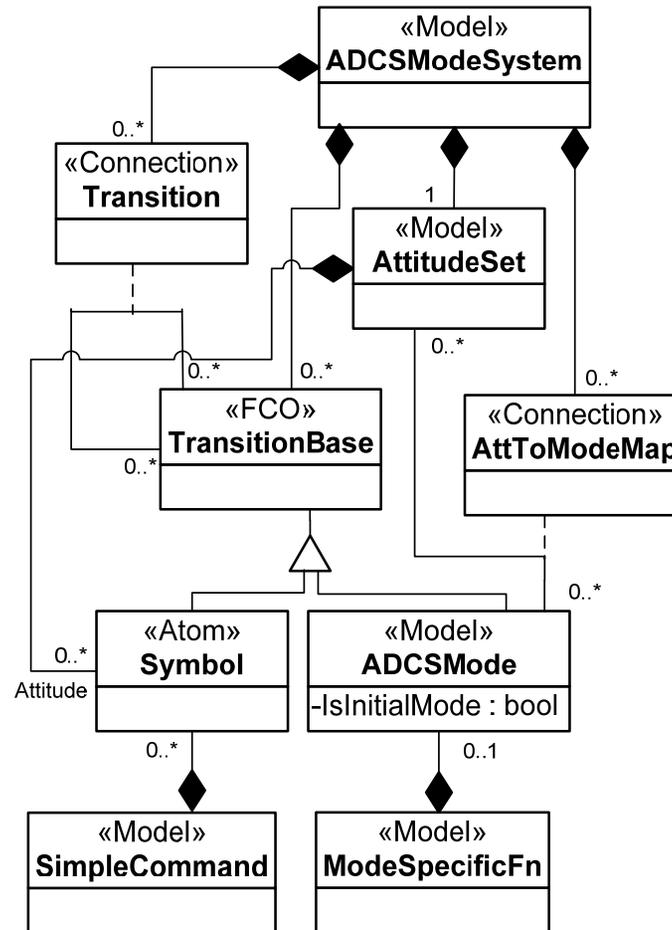


ADCSPowerlf

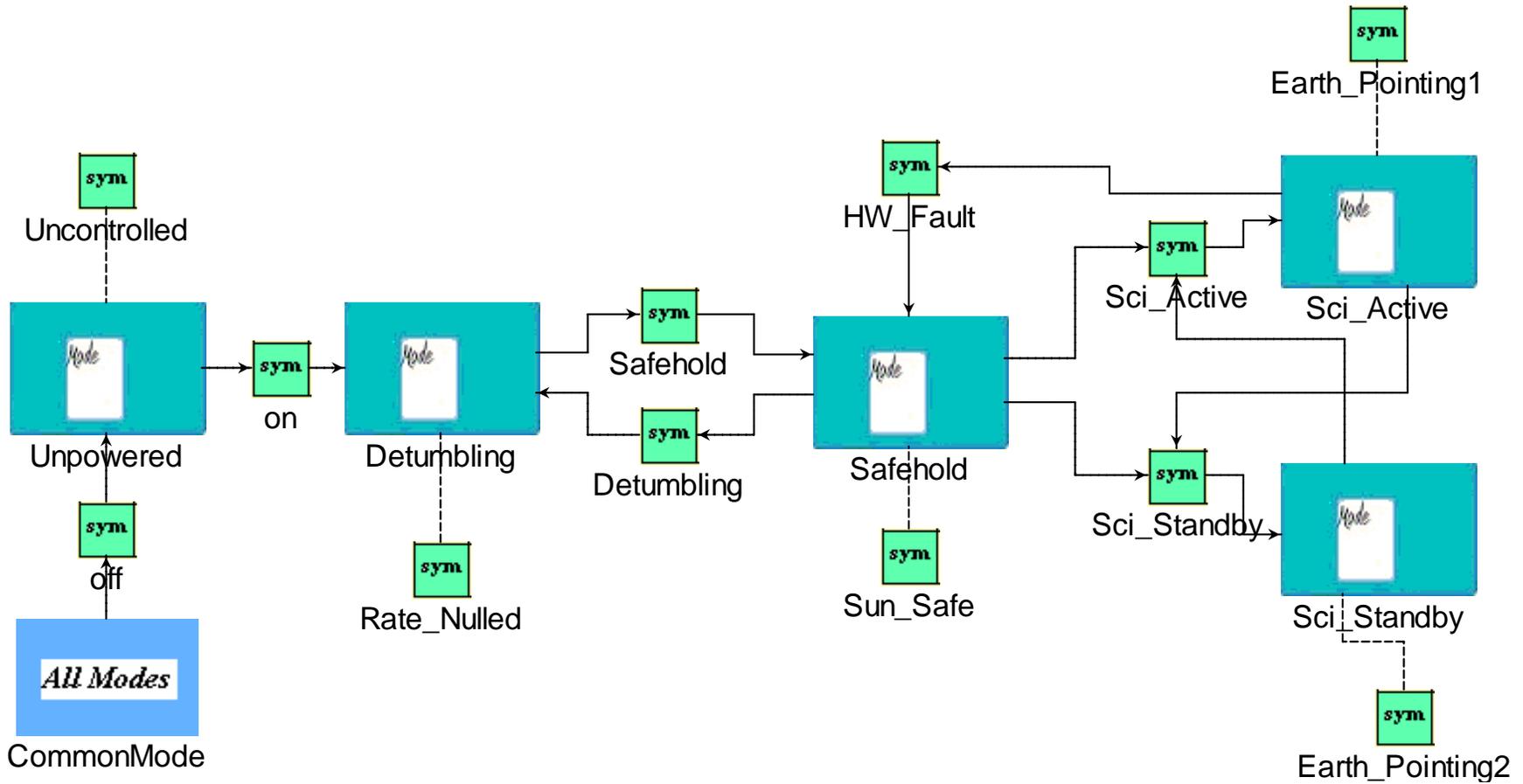


AttitudeDataStream

ADCS Modesystem

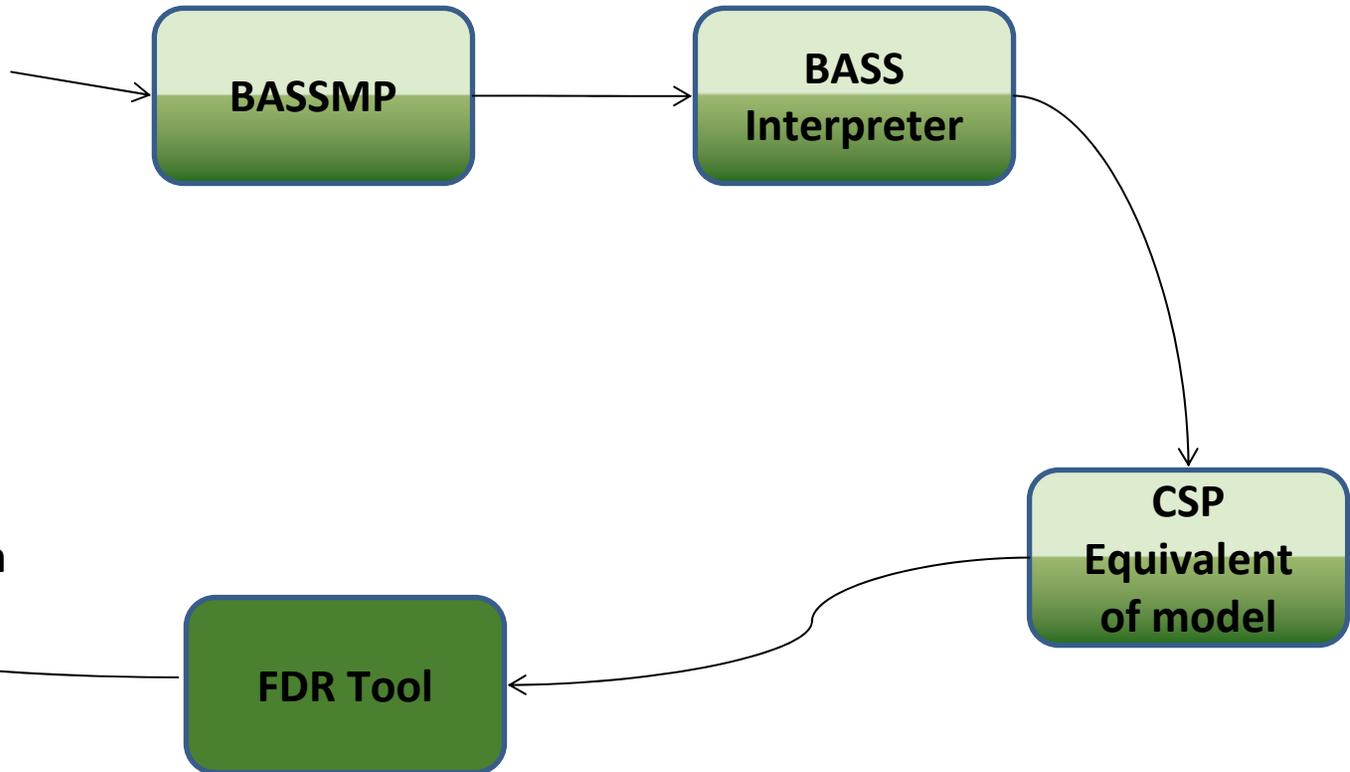


ADCS ModeSystem



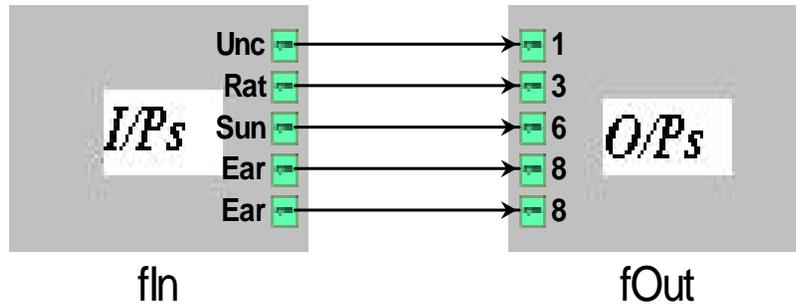
Work Done Thus Far...

GME model &
Specifications
of spacecraft
model

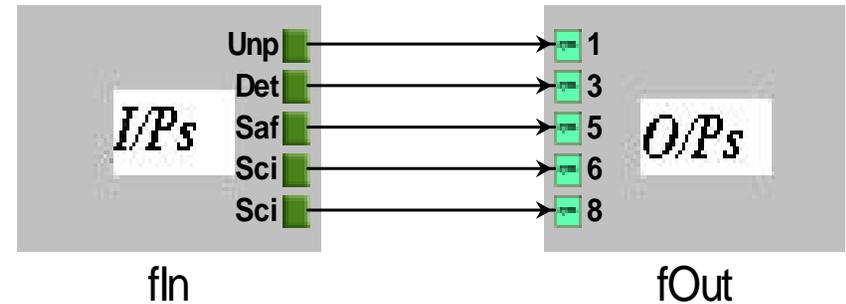


Power sufficiency Check

- The amount of power generated depends on the Attitude and is represented by the function AttitudeSpecificAvailablePower in the Power Subsystem
- The amount of power consumed depends on the mode in which a subsystem is and is represented by the function SubsysModePower



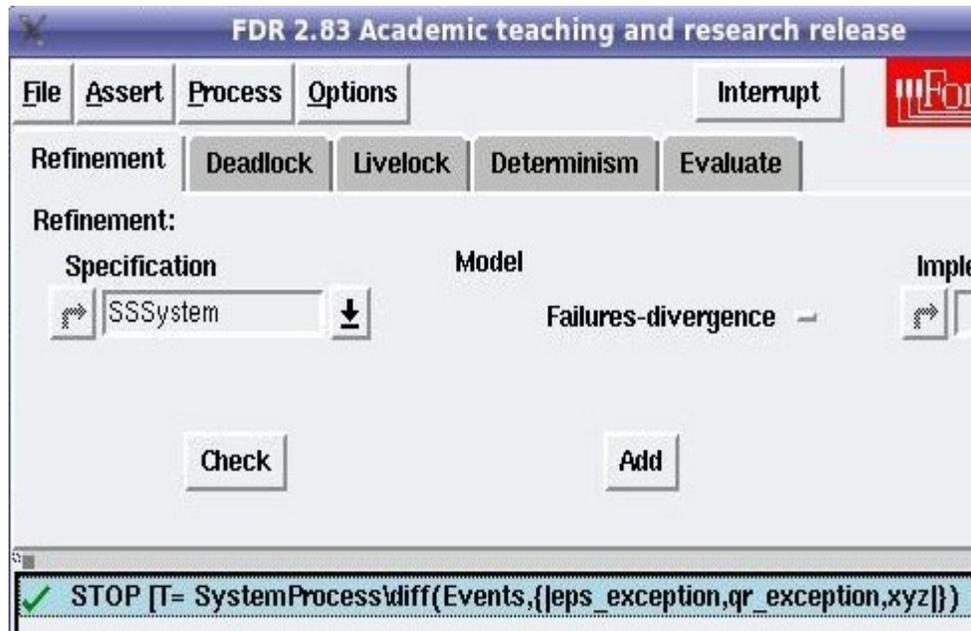
AttitudeSpecificAvailablePower



ADCSModePower

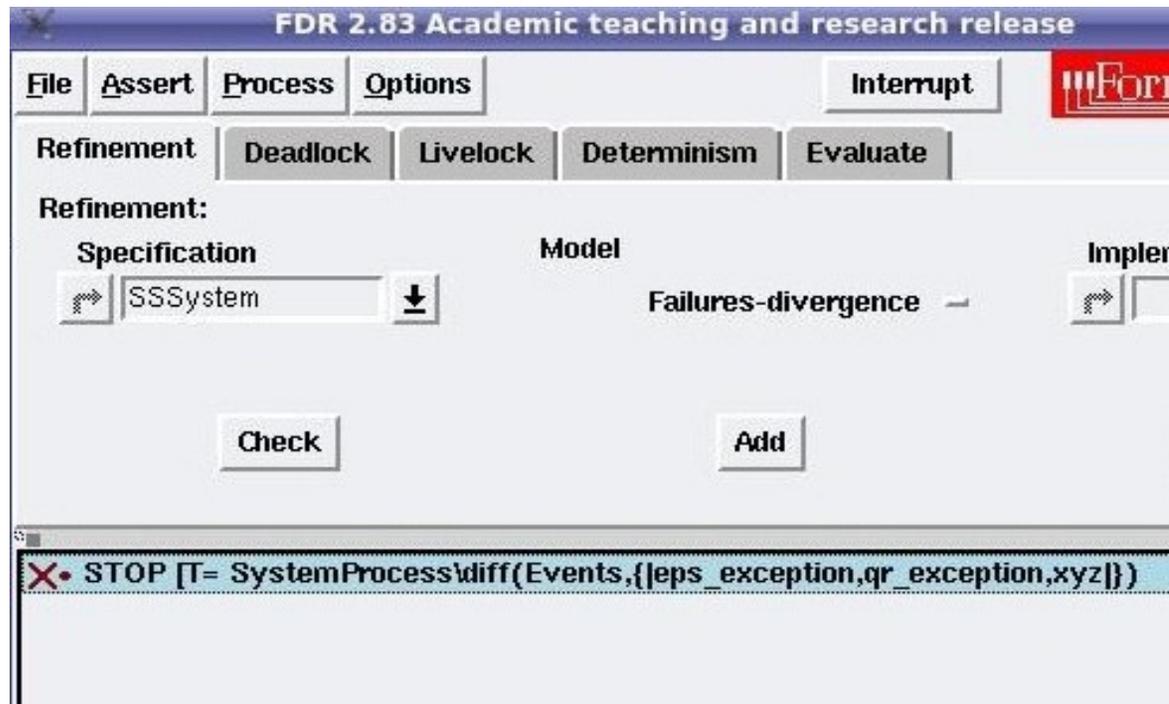
Check loaded into FDR

Positive Result



Check Loaded into FDR

Negative Result



Summary

- System-level spacecraft design lacks formality
 - Behavior implicitly defined and discussed in documentation
 - Little to no analysis performed at system level
- BASS offers a domain-specific visual modeling language for capturing spacecraft behavior
 - Constructs phrased in terms common to spacecraft systems engineers
- Formal Behavioral Analysis
 - CSP used for underlying semantic model
 - Model checking used to prove/analyze properties of the spacecraft