

Model-Based Verification and Validation of Spacecraft Avionics

M. Omair Khan

Jet Propulsion Laboratory, California Institute of Technology

Mohammed.O.Khan@jpl.nasa.gov

AIAA Infotech 2012: June 21, 2012

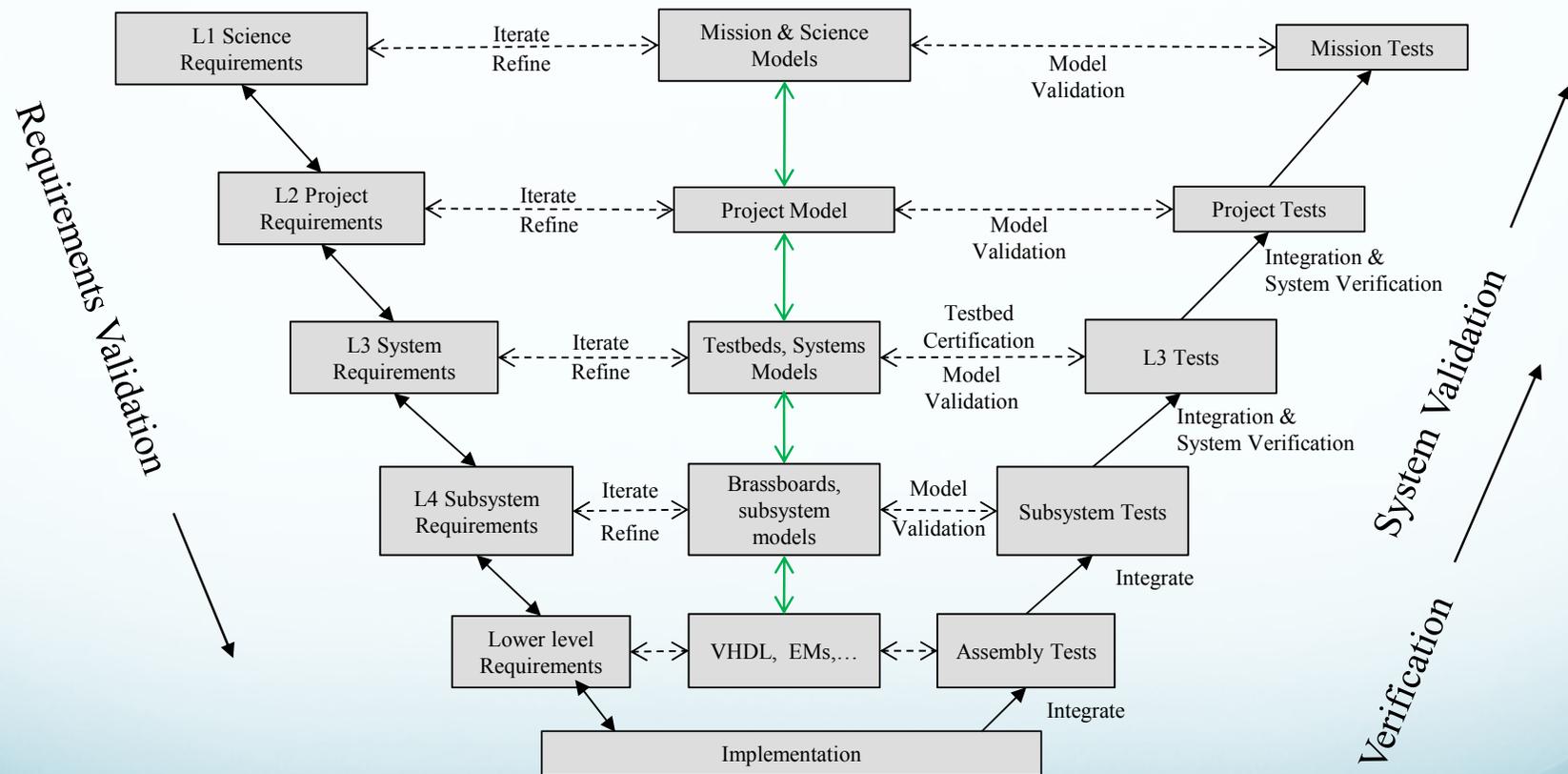
What is Model Based Verification and Validation?

- Model Based Verification and Validation (MBV&V) is the infusion of model based systems engineering into traditional aerospace V&V analysis
- Design Validation asks “Did we build the correct system for the job?”
- Design Verification asks “Did we build the system correctly?”
- MBV&V utilizes SysML to perform:
 - design validation (e.g. formal methods / simulation)
 - design verification (e.g. capture design diagrams and conduct requirements management)
- MBV&V can be applied broadly to the project development cycle

Why MBV&V for Avionics?

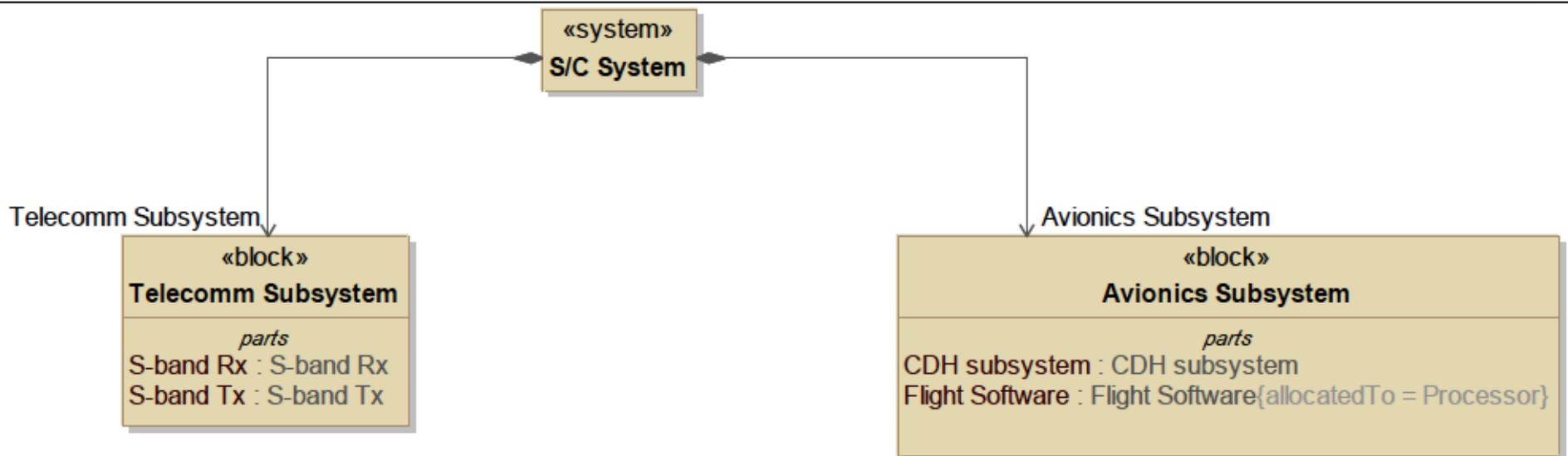
- As ATLO time is staying constant and spacecraft complexity is ever increasing; comprehensive V&V on the flight hardware is not possible
- Just having the system expressed as a formal model makes the V&V issues easier to identify and resolve
- Simulations of models allows for a more thorough understanding of nominal and off-nominal spacecraft behavior
 - Some design validation can take place before any hardware exists

MBSE infusion into Project Development

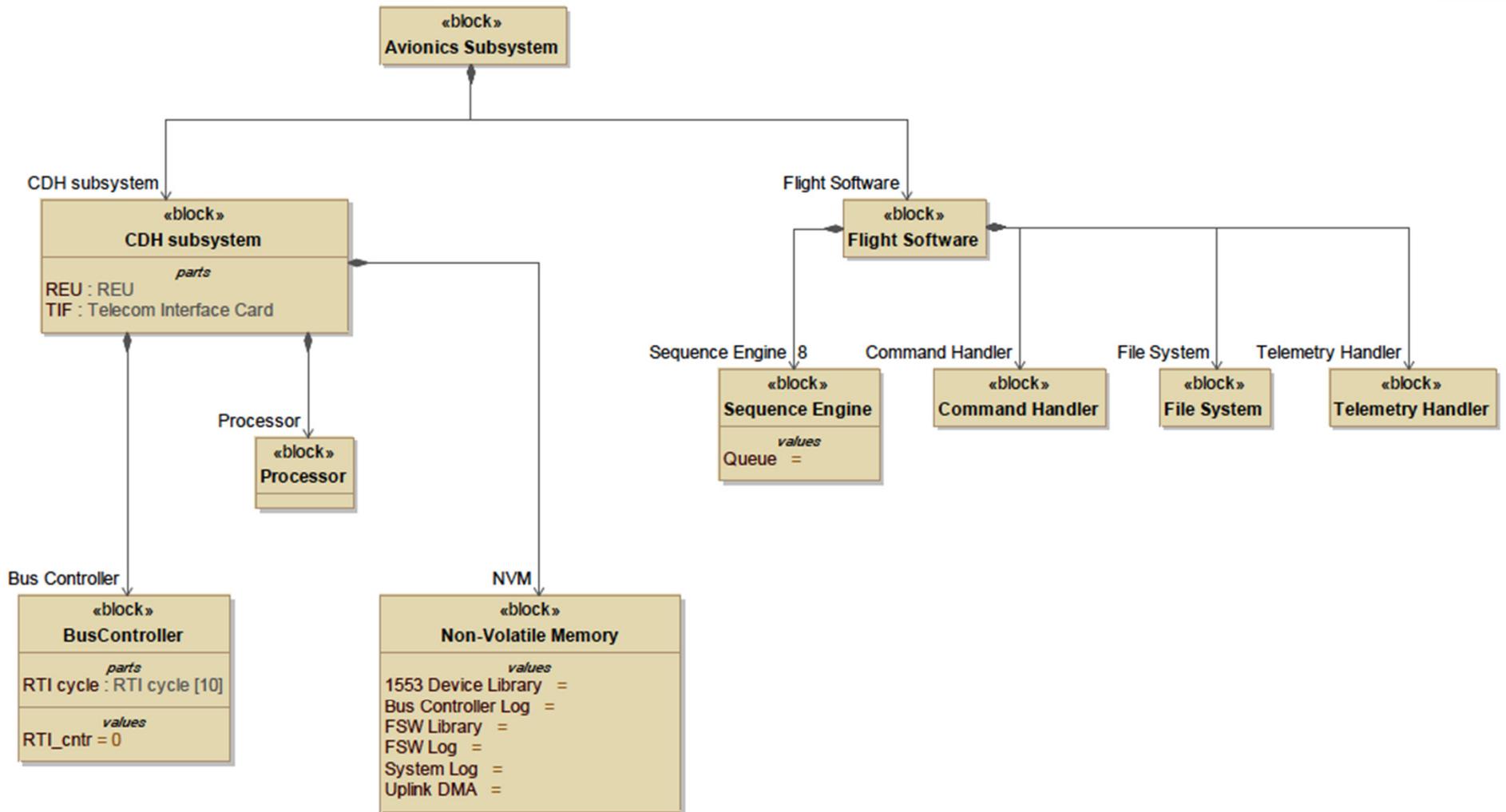


Source: Dr. Mike Sievers
(Jet Propulsion Laboratory)

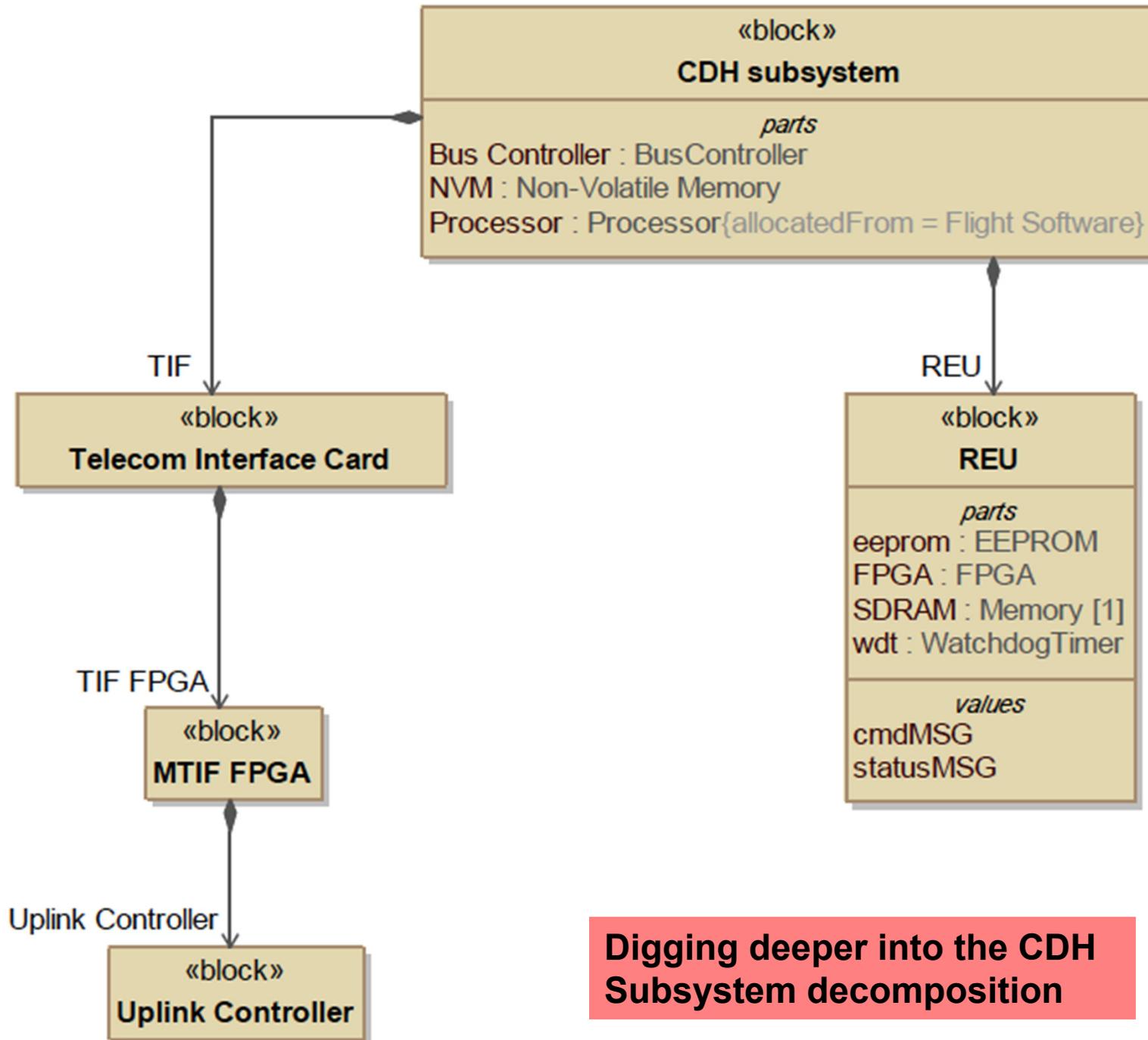
Block Definition Diagrams (BDD)
describe the compositional hierarchy of
the system



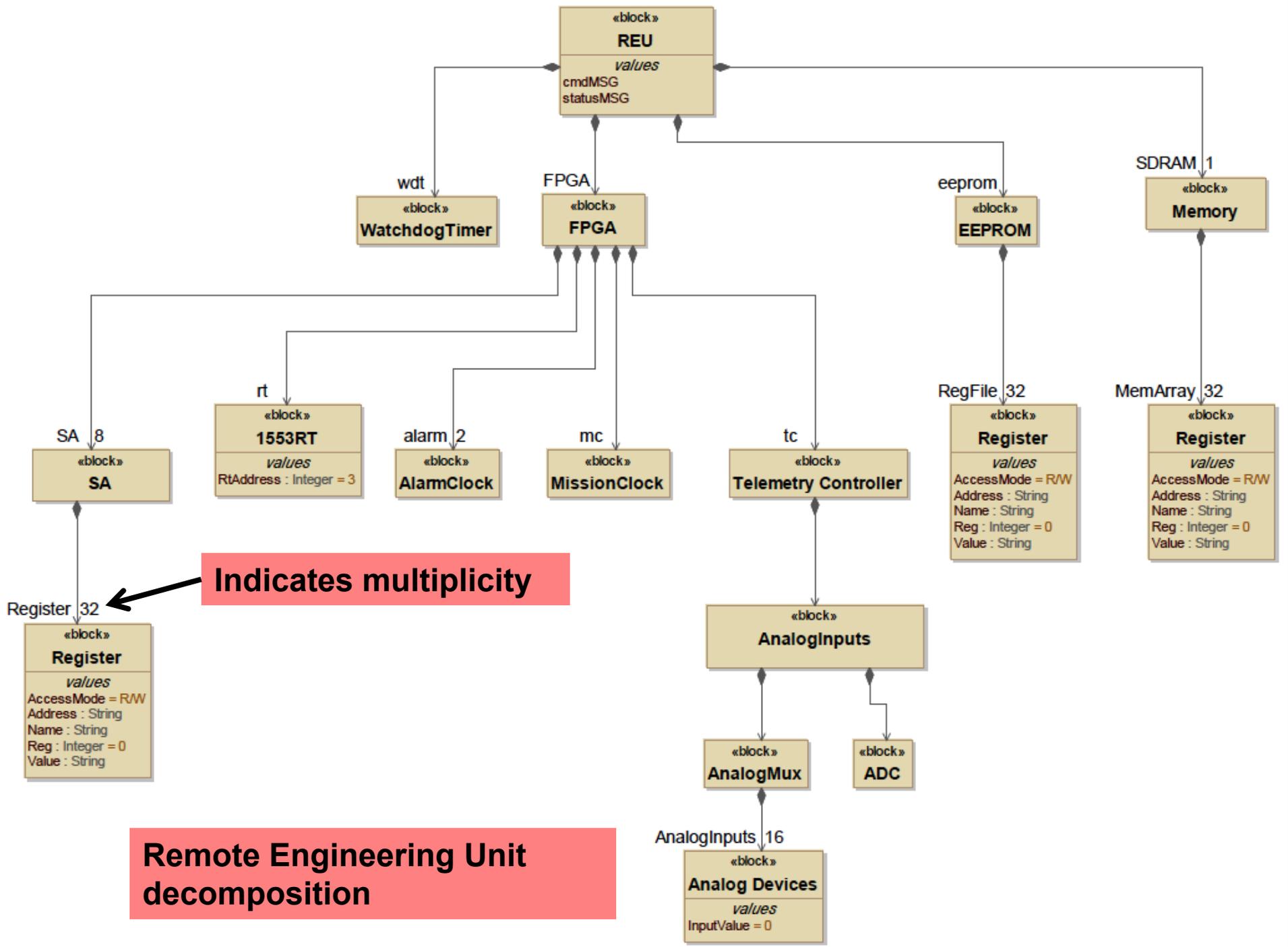
Scope of model and simulation is limited to uplink command processing by the avionics subsystem (e.g. flight software and remote engineering unit)



Digging deeper into the Avionics Subsystem decomposition



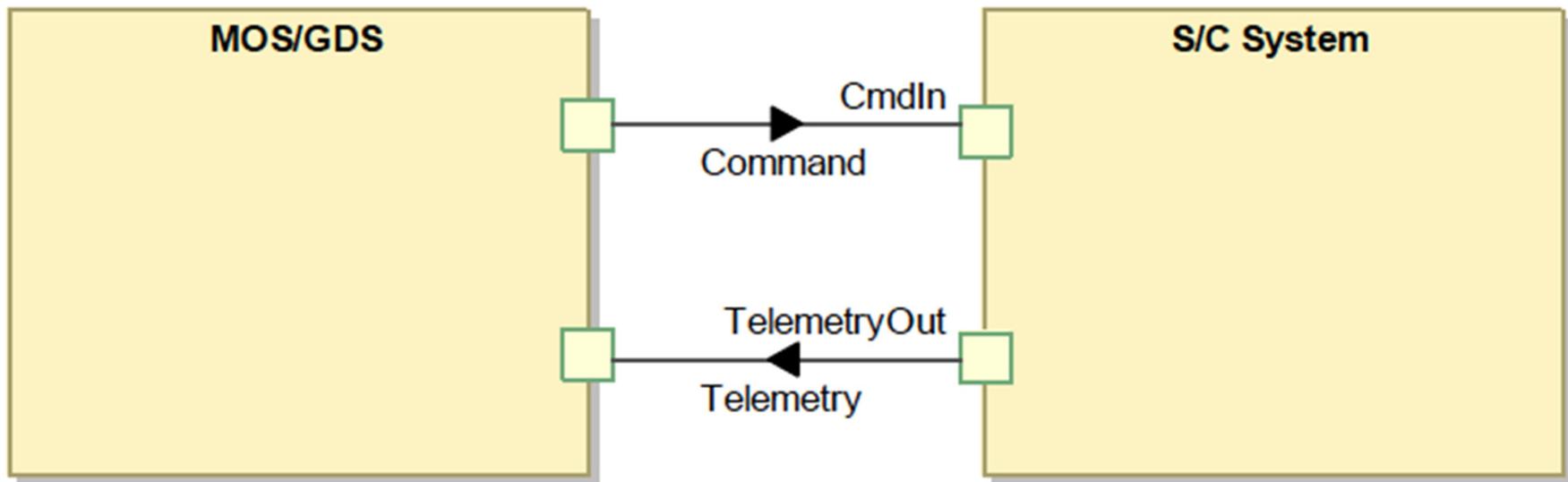
Digging deeper into the CDH Subsystem decomposition



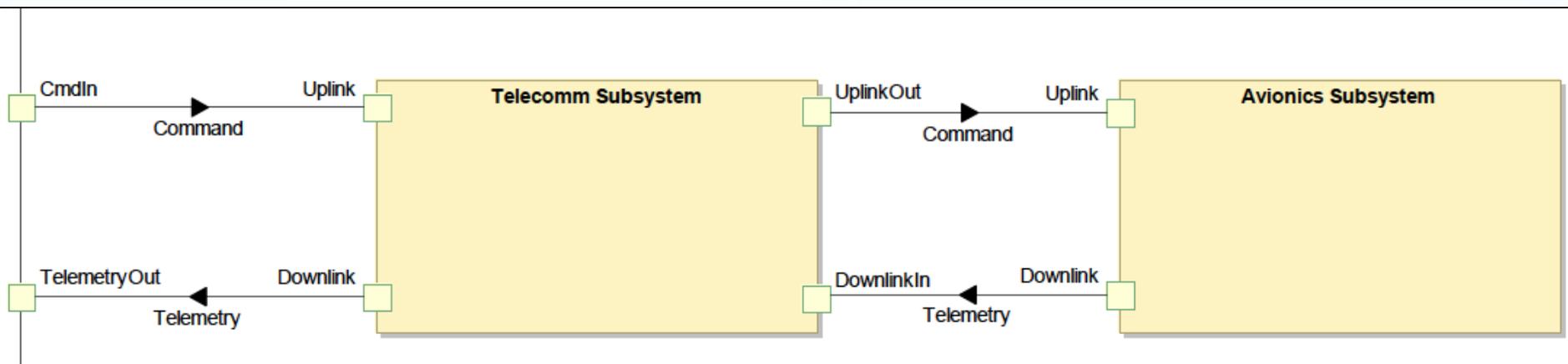
Indicates multiplicity

Remote Engineering Unit decomposition

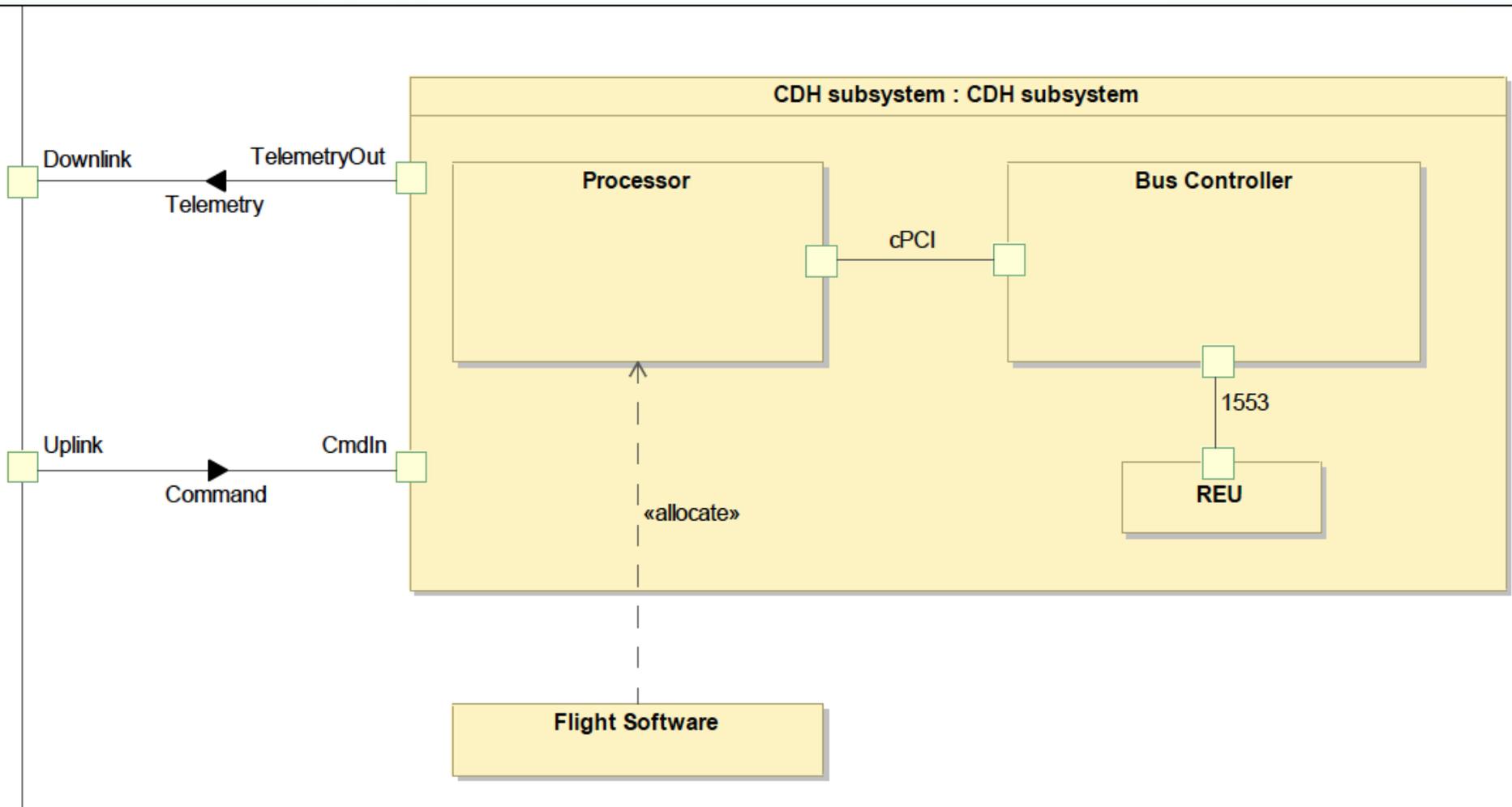
Internal Block Diagrams (IBD) describe the interaction routes for elements within the BDD structure



**Project level 2 interactions:
Inter-system communication**

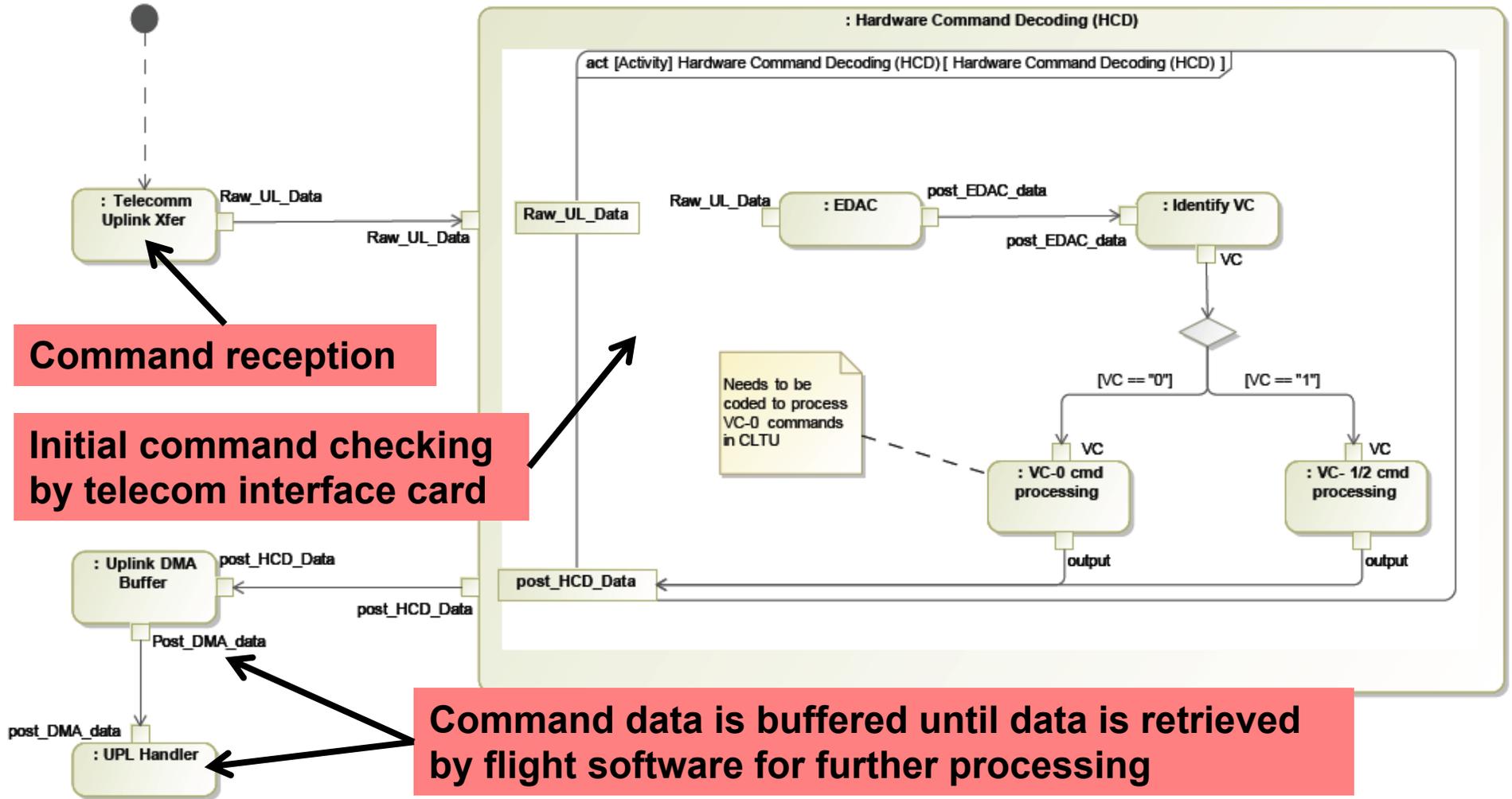


**Project level 3/4 interactions:
Intra-S/C and subsystem communication**

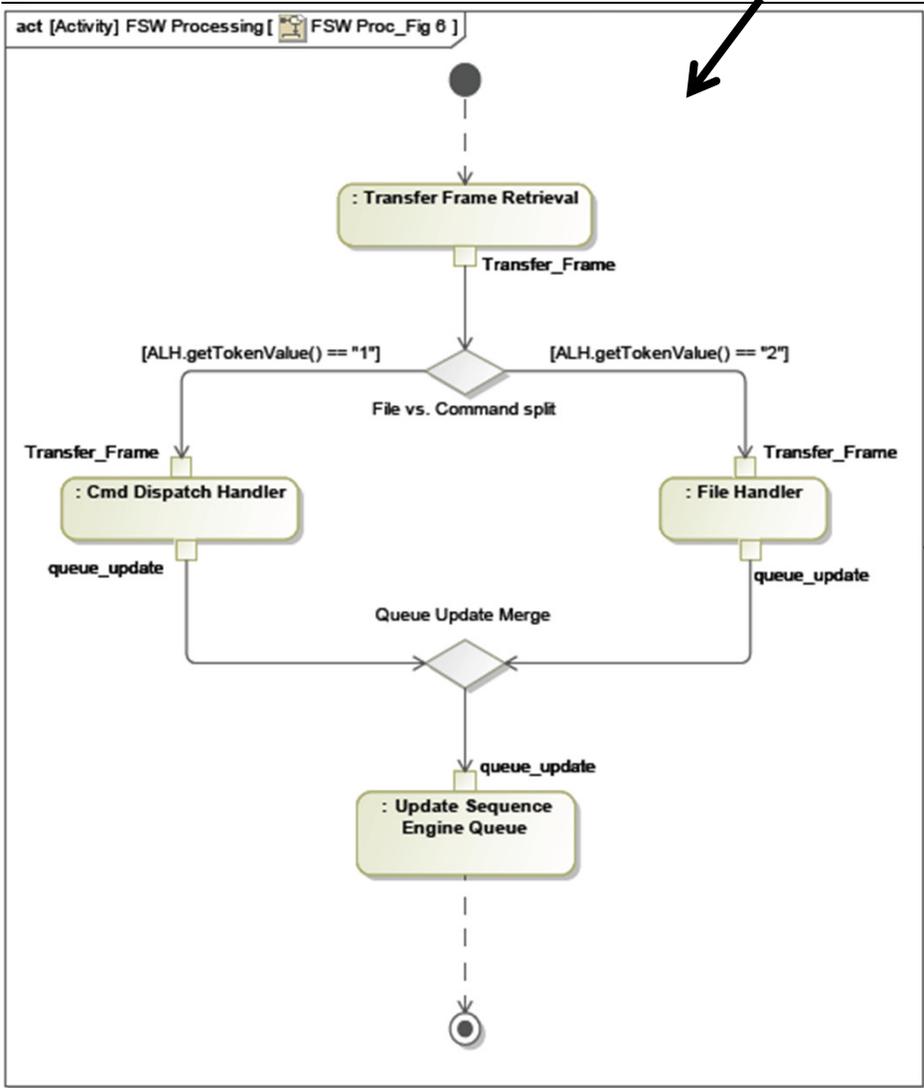


**Project level 5 interactions:
Intra-subsystem / device level communication**

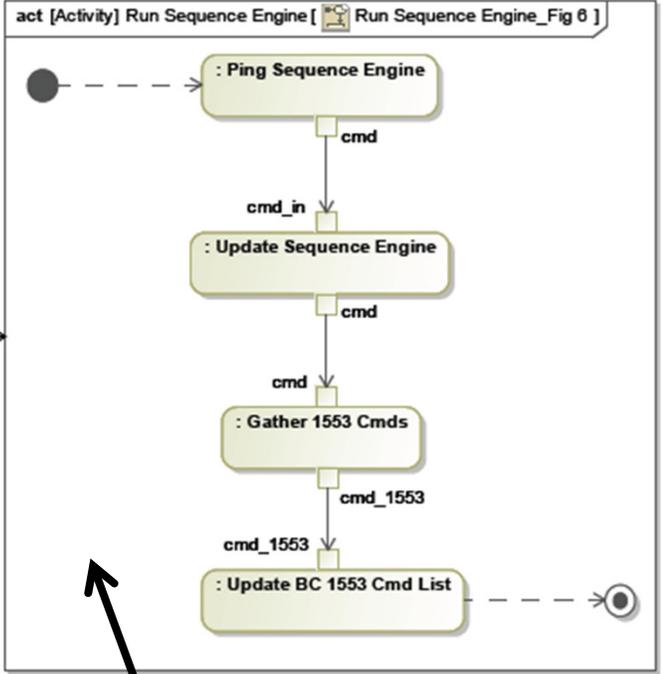
Activity Diagrams describe the behavior and functional interaction of elements within the BDD and IBD



FSW further processes command data



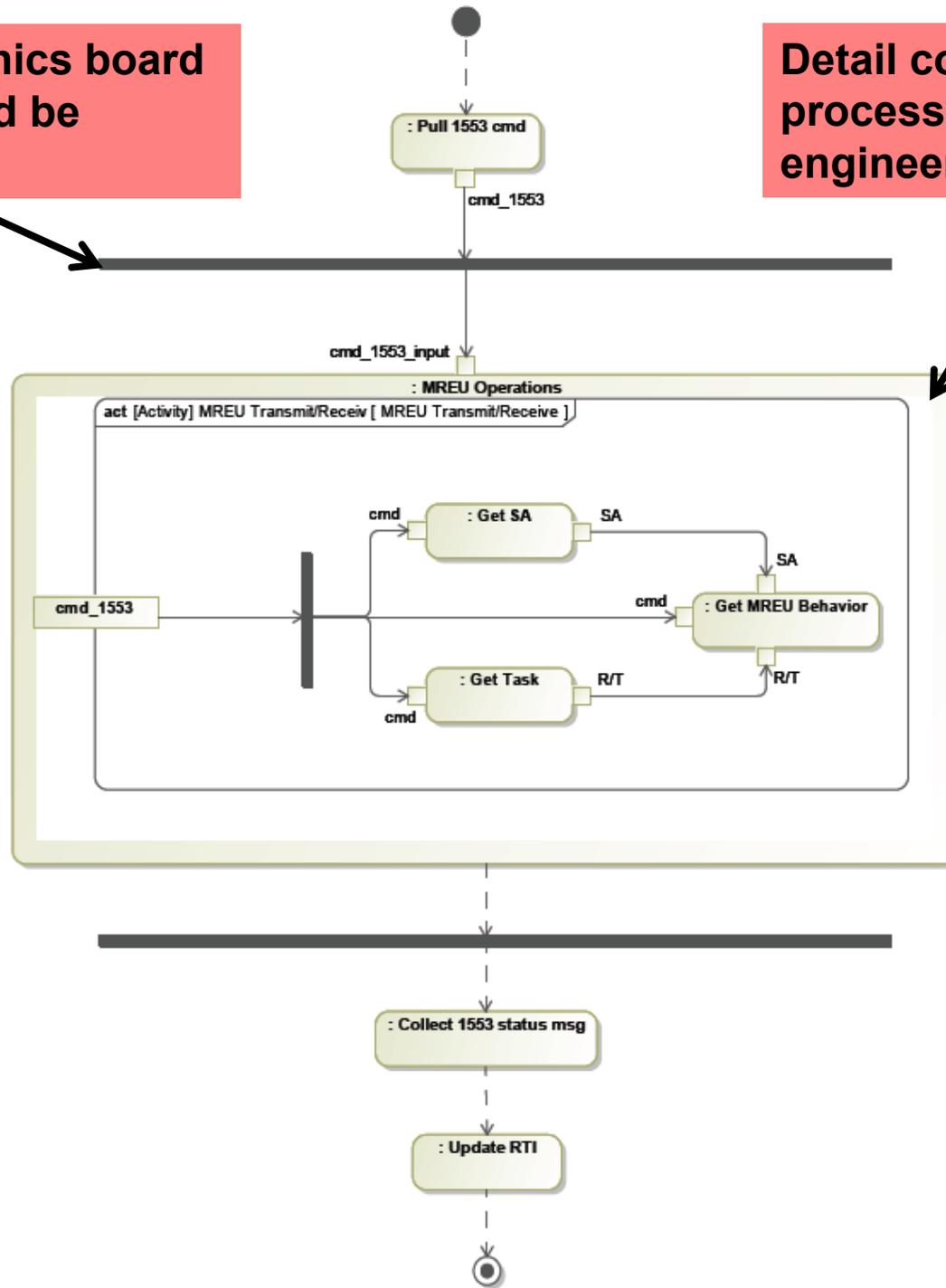
Runs after "FSW processing" activity is complete

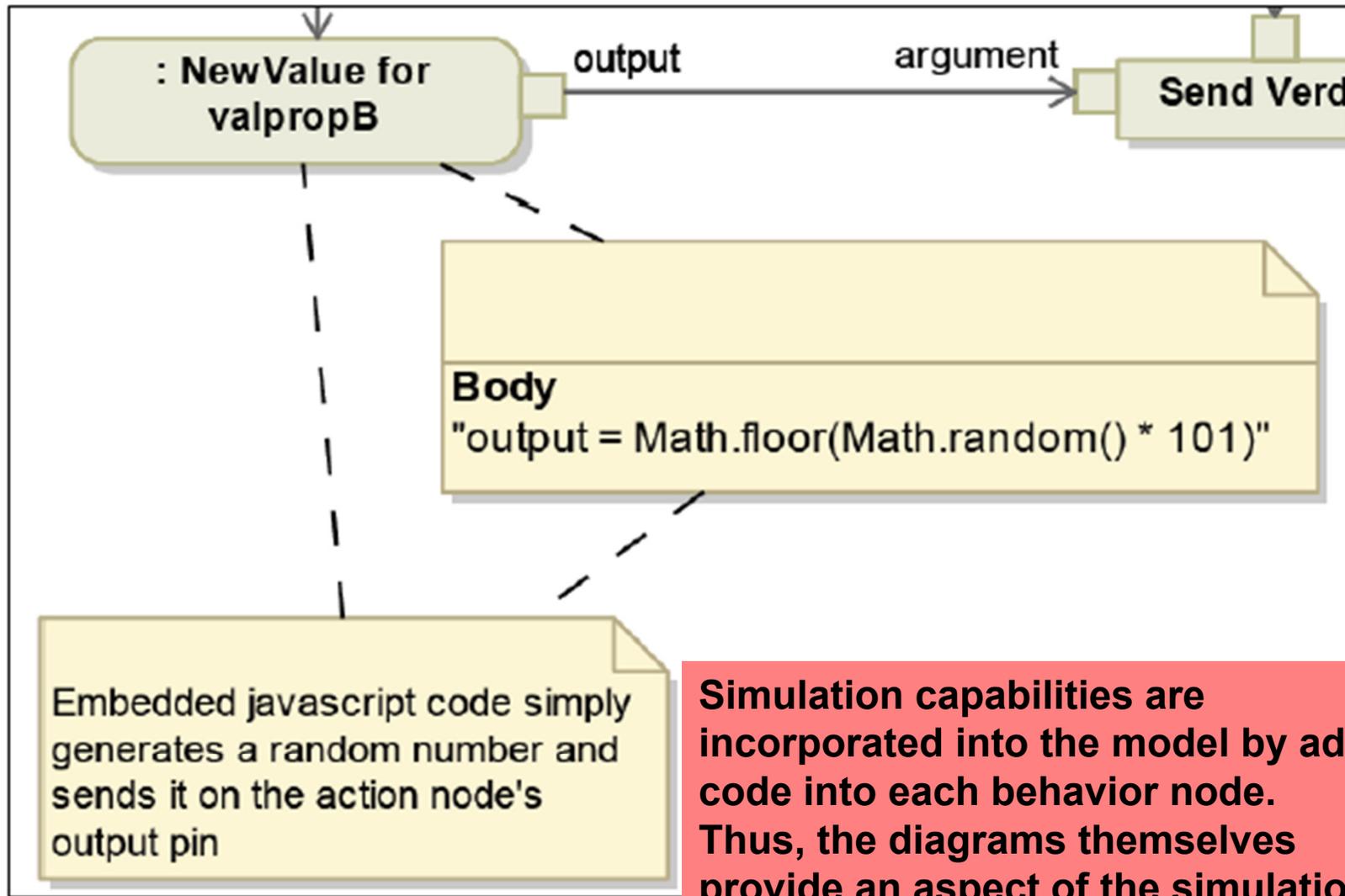


Commands are placed into sequence engines for eventual activation

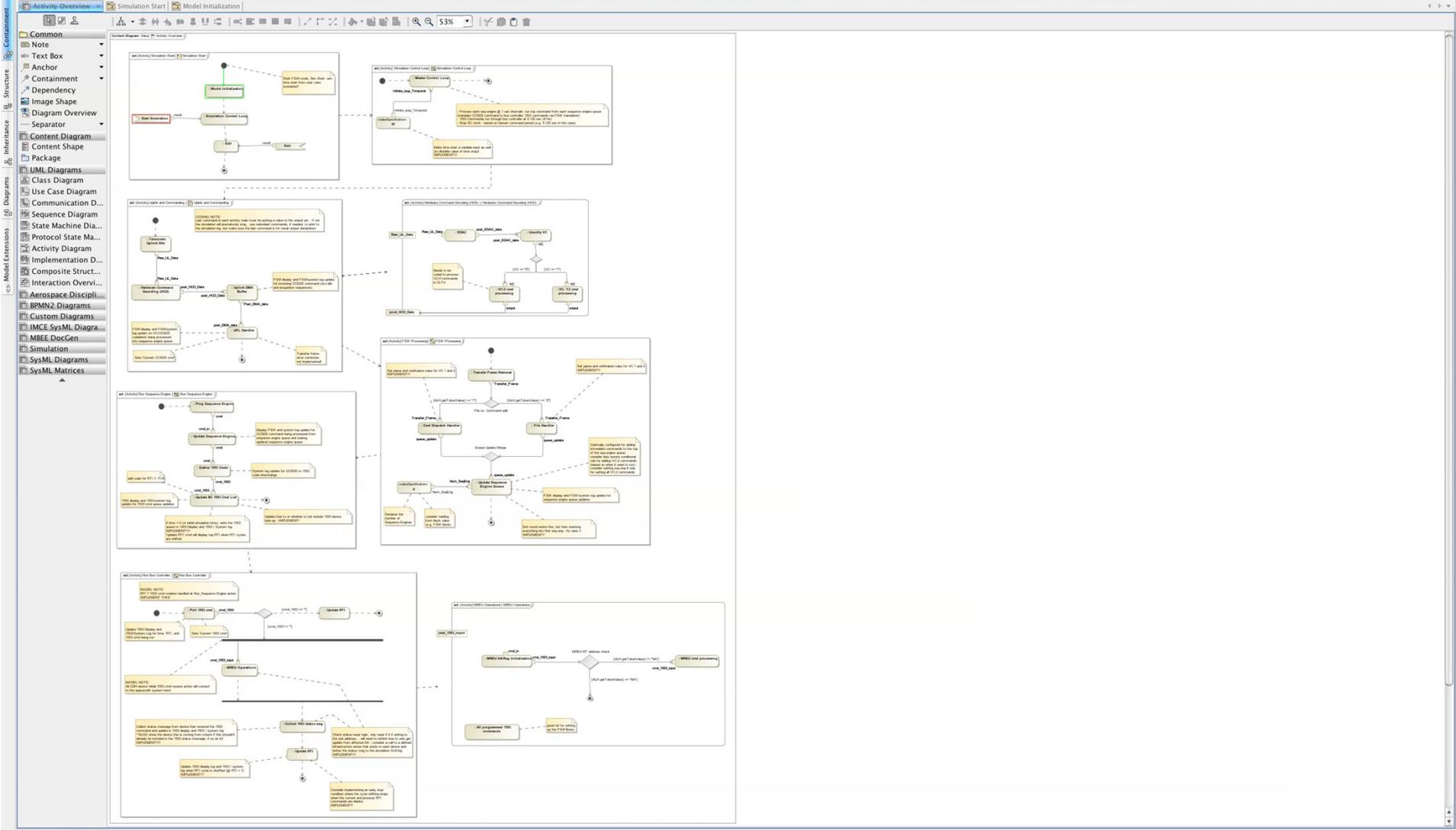
Additional avionics board behaviors would be integrated here

Detail command processing by the remote engineering unit





Simulation capabilities are incorporated into the model by adding code into each behavior node. Thus, the diagrams themselves provide an aspect of the simulation coding architecture (e.g. logic pathways)



Summary

- Our simulation was able to mimic the results of 30 tests on the actual hardware
 - This shows that simulations have the potential to enable early design validation – well before actual hardware exists
- Although simulations focused around data processing procedures at subsystem and device level, they can also be applied to system level analysis to simulate mission scenarios and consumable tracking (e.g. power, propellant, etc.)
- Simulation engine plug-in developments are continually improving the product, but handling time for time-sensitive operations (like those of the remote engineering unit and bus controller) can be cumbersome