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

Propulsion & Launch
Space Environment
Orbital Mechanics
Communications
HW & SW
Command & Telemetry
Power Systems
Structure

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.

Figs from USU Small Satellite Program  http://ususat.usu.edu/
CDH & Power Subsystems

- 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.

Figs from USU Small Satellite Program  http://ususat.usu.edu/
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

- State charts
- PROMELA/SPIN
-FFBDs

Spacecraft system design – block diagrams and figures
System Development & Verification

Process ADCS(Task*);
Process CDH(Task*);
...
Process System(Task*);

ADCS = power.on -> mode.science...
CDH = mode.science -> ...
System = ADCS || | CDH...

Can we verify the design itself?

System Programmer
System Design
System Verifier
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 : \(\{0, 1\}\)

\[
\text{Proc} = \text{recv}\?\text{packet} \rightarrow \text{if } (\text{checksum} = 0) \\
\quad \text{then } \text{success} \rightarrow \text{Proc} \\
\quad \text{else } \text{fail} \rightarrow \text{Proc}
\]

\[
\text{TxmitAck} = \text{success} \rightarrow \text{response!0} \rightarrow \text{TxmitAck}
\]

\[
\text{TxmitNack} = \text{fail} \rightarrow \text{response!1} \rightarrow \text{TxmitNack}
\]

Composite = (TxmitAck ||| TxmitNack)

[ [success, fail] ]

Proc
High Level Spacecraft Behavior in CSP

- CDH
  - Commands
  - Discrete Msgs
  - Power I/F
  - Exception
- Data streams
- Subsystem behavior
- SystemBus channel
- Power Process

- System Bus
- Power Bus
- Power Channel

- CDH Process
- ADCS Process
BASS Tool Flow

1. **GME model & Specifications of spacecraft model**
2. **BASSMP**
3. **BASS Interpreter**
4. **Generated CSP**
5. **Spacecraft Behavior Framework Library**
6. **Verification Result**

- **FDR Tool**
- **BASSMP**
- **BASS Interpreter**
- **Generated CSP**
- **Spacecraft Behavior Framework Library**
Spacecraft System

- SpacecraftSystem
  - Subsystem
    - PoweredSubsystem
      - ADCS
    - NonpoweredSubsystem
    - Power
      - CDH
Datacomm Aspect of Spacecraft

Diagram showing the integration of various components such as SystemBus, CommandInterface, CommandSet, Power, SystemBus, CDH, and ADCS.
Power Aspect of the Spacecraft
Common Constructs

Shared State Object representing a shared variable

Spacecraft Commands
Power Subsystem

```
«Model»
- Power
  - MaxPowerGenerated : int
  - MinPowerGenerated : int

«Model»
- MapFunction

«Atom»
- PowerPort

0..* AttitudeSpecificAvailablePower

0..1 CDH

1 CDHPowPort

CommandSet

ADC

ADCSPowPort

\[ f : A \rightarrow B \]

AttitudeSpecificAvailablePower
```
CDH Subsystem
CDH Command Dispatch
ADCS Subsystem

ADCS <<Model>>

ADCSModeSystem 1

ModeSystem <<Model>>

ADCSModePower

Attitude 1

SharedState <<Model>>

CommandSet

SSG

SSS

SST

Attitude

ADCSModeSystem

f: A→B

Power s/w

ADCSPowerIf

AttitudeDataStream
ADCS Modesystem

ADCSModeSystem

Transition

Model
ADCSModeSystem

Connection
TransItion

Model
AttitudeSet

FCO
TransitionBase

Connection
AttToModeMap

Atom
Symbol

Model
ADCSMode

-IsInitialMode : bool

Model
SimpleCommand

Model
ModeSpecificFn
Work Done Thus Far...

GME model & Specifications of spacecraft model

BASSMP → BASS Interpreter

Verification Result

FDR Tool → CSP Equivalent of 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`.

```
I/Ps

<table>
<thead>
<tr>
<th>Unc</th>
<th>Rat</th>
<th>Sun</th>
<th>Ear</th>
</tr>
</thead>
<tbody>
<tr>
<td>fIn</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>fOut</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

O/Ps

<table>
<thead>
<tr>
<th>Unp</th>
<th>Det</th>
<th>Saf</th>
<th>Sci</th>
</tr>
</thead>
<tbody>
<tr>
<td>fIn</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>fOut</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>
```

`AttitudeSpecificAvailablePower`  `ADCSModePower`
Check loaded into FDR

Positive Result
Check Loaded into FDR

Negative Result
Summary

• System-level spacecraft design lacks formality
  – Behavior implicity 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