AEROSPACE
Assuring Space Mission Success

Application of the Architecture Analysis and Design Language (AADL) to Space System Safety and Reliability Assessment

Myron Hecht, Alex Lam , Chris Vogl,

Presented to
Flight Software 2010 Workshop
Pasadena, CA

November, 2010

© The Aerospace Corporation 2009

Outline

- Introducing AADL
- AADL Error Annex
- Tool Set for Analyzing Risk and Reliability/Availability
- Satellite Example
- FMEA Generation
- Conclusions

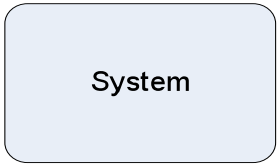
Introducing the Architecture Analysis & Design Language (AADL)

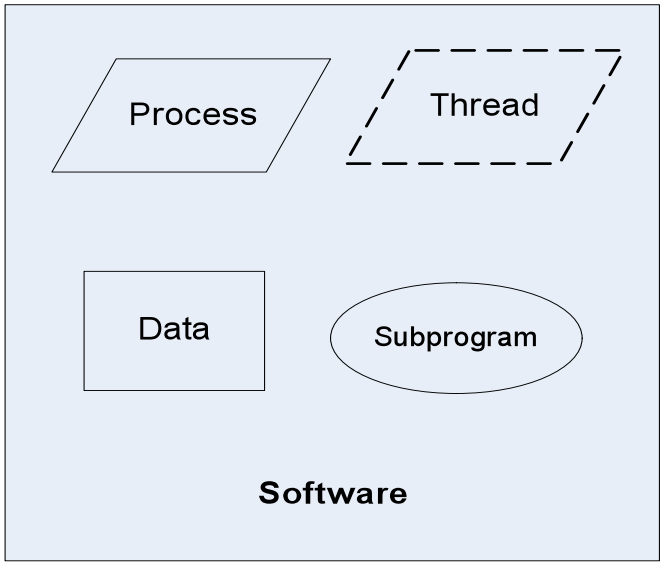
- Society of Automotive Engineers (SAE) Aerospace Standard AS5506 (2004)
  - *Preceded by more than a decade of development under the DARPA Meta-H program*
- Provides a standardized textual and graphical notation for describing software and hardware system architectures and their functional interfaces
  - *architectures (using standard language).*
  - *expected program behavior (using behavior annex)*
  - *Failure and recovery behavior (using error annex)*

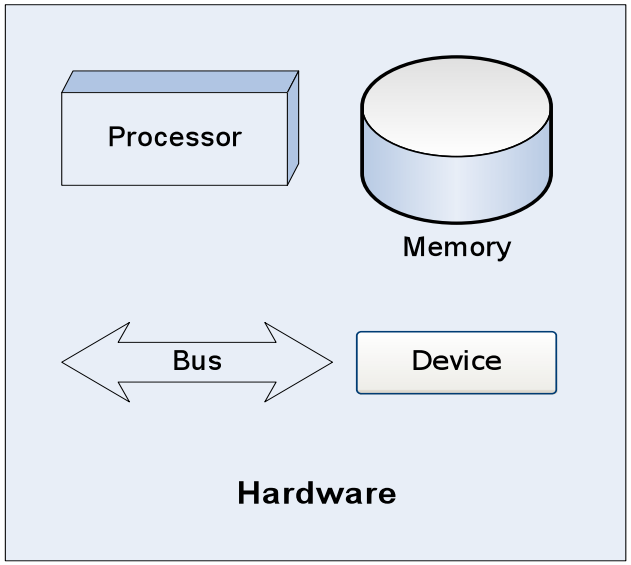
AADL vs. other OMG Languages for Stochastic Analysis of Risk and Reliability

- Advantages
  - *Objects directly represent real-time system hardware and software*
  - *Standard method for incorporation of quantitative attributes*
    - Failure and Recovery Probabilistic Distributions
    - Parameters of those distributions
    - Probabilities and rates for individual transitions
  - *Standard methods for representing propagation of failures across multiple components*
    - Event ports for failure propagations
    - Guards to enable conditional propagations (important for abstractions and reuse)
- Drawbacks
  - *No commercial quality tools*
    - Public domain tools are available and usable – but not bug free

AADL Components (graphical representation)

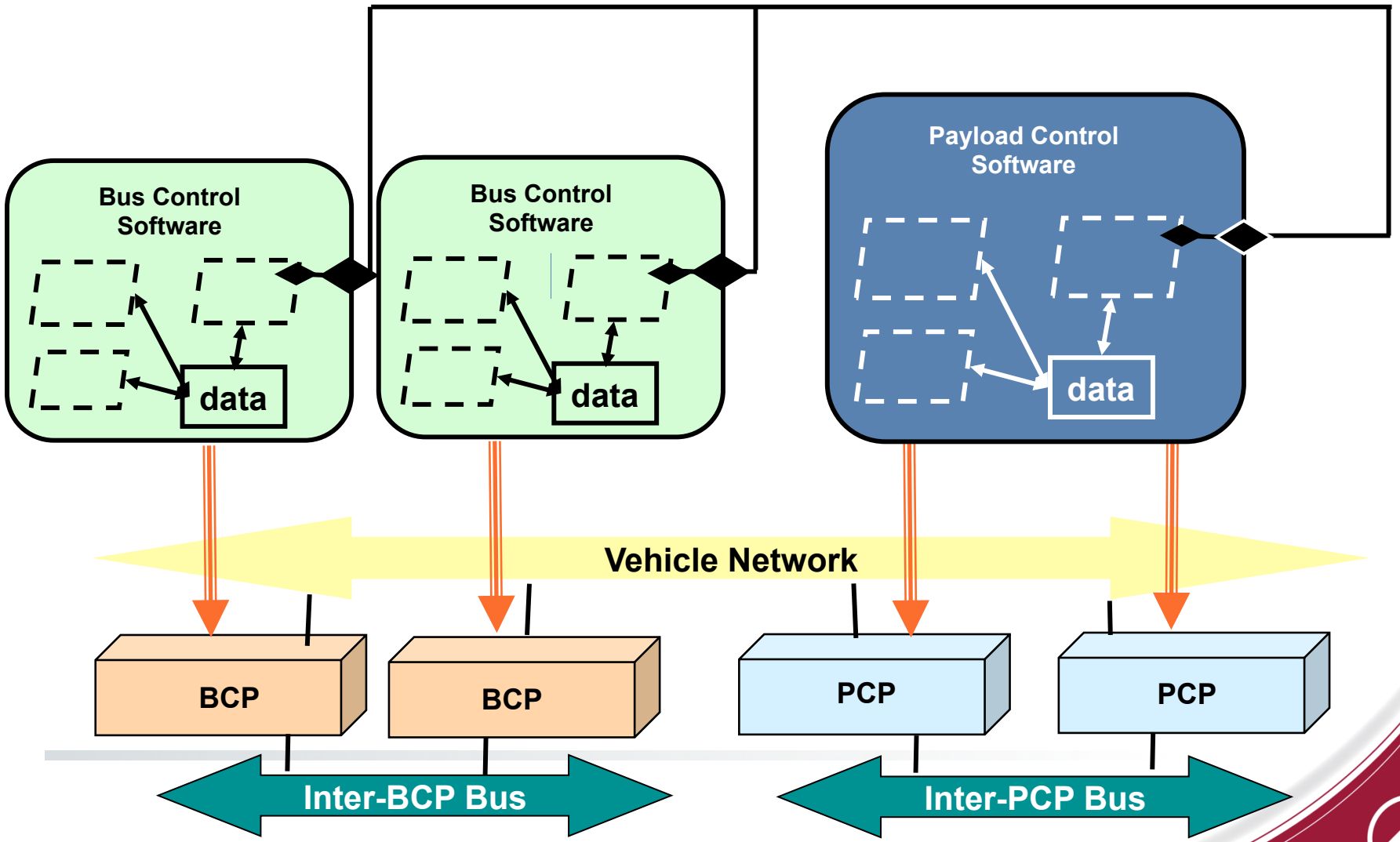






– text and xml representations also defined

AADL Hardware/Software Architecture Representation



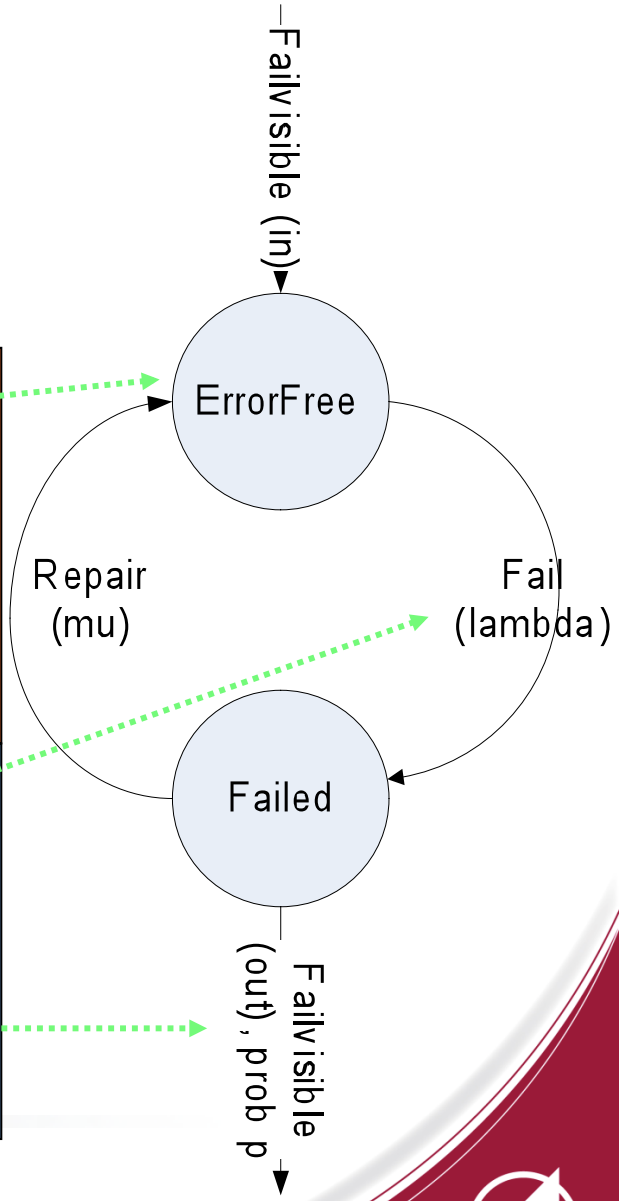
AADL Error Annex

- AADL annex that supports stochastic analysis
- Defines error model
  - *State transition diagram that represents normal and failed states*
  - *Error models can be associated with hardware components, software components, connections, and "system" (composite) components*
- Error model consists of
  - *State definitions*
  - *Propagations from and to other components*
  - *Probability distribution and parameter definitions*
  - *Allowed state transitions and probabilities*

AADL Error Model Example

```
error model example
features
ErrorFree: initial error state;
Failed: error state;
Fail: error event {Occurrence => poisson lambda};
Repair: error event {Occurrence => poisson mu};
Failvisible: in out error propagation {Occurrence => fixed p};
end example;
```

```
error model implementation example.general
transitions
ErrorFree-[Fail]->Failed;
Failed-[Repair]->ErrorFree;
ErrorFree-[in Failvisible]->Failed;
Failed-[out Failvisible]->Failed;
end example.general;
```

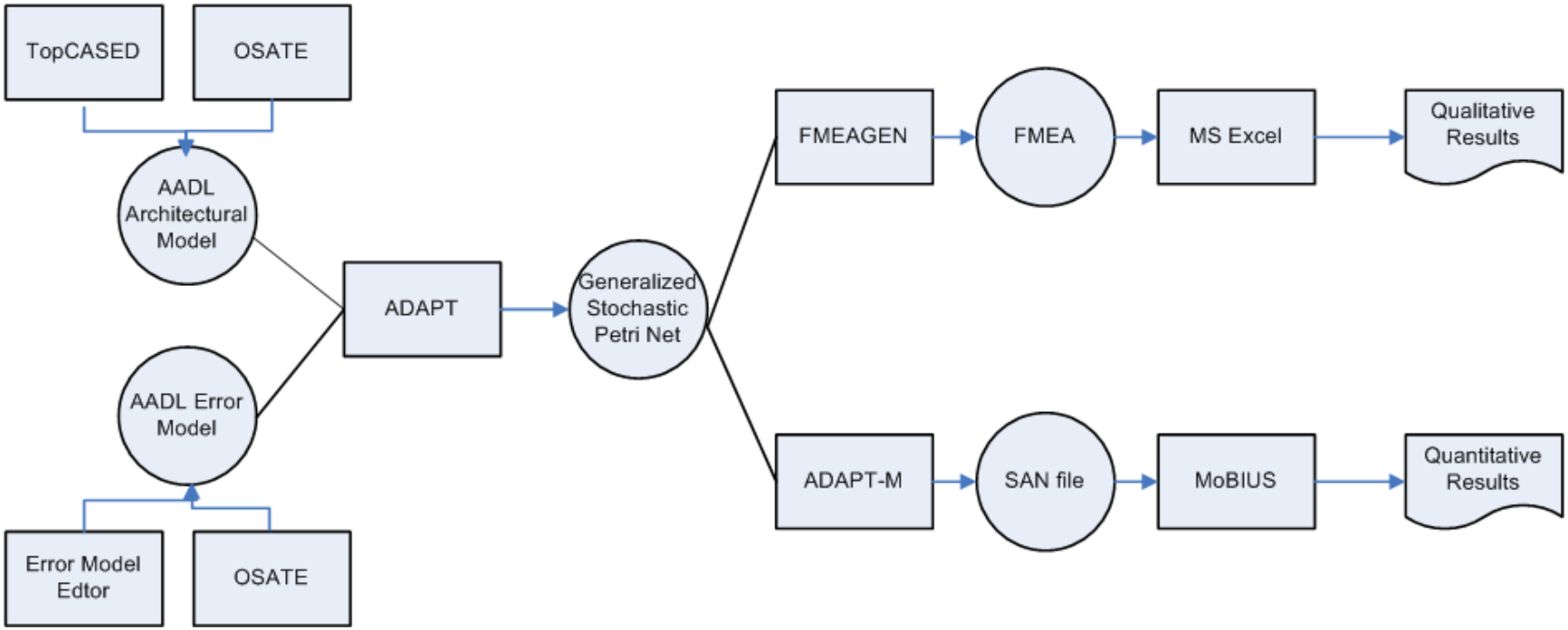


More information: Feiler (2007)

AADL Tool Set

- Eclipse Development Environment (Ganymede) and Eclipse Modeling Framework (EMF)
- Component plug-ins
  - ***TopCASED*** *graphical editor to create AADL architecture diagrams (SEI, Aerospace modifications)*
  - ***Error Model Editor*** *graphical editor to create AADL error model diagrams (Aerospace)*
  - ***OSATE*** *AADL generator (SEI, Aerospace modifications)*
  - ***ADAPT-M*** *Stochastic Petri net to MoBIUS stochastic analysis network tool ((SEI/LAAS Toulouse and Aerospace)*
  - ***MoBIUS*** *Quantitative Dependability modeling and prediction tool (University of Illinois, Champaign Urbana)*
  - ***FMEAGEN*** *FMEA Generator (Aerospace)*

AADL Modeling Tool Set Data Flow



Tool Set Screen Shot

AADL - GeoBus/aaxl/GeoBusArch.aaxldi - Eclipse Platform

File Edit Navigate Search Project OSATE Analyses ADAPT-M Run Window Help

AADL Navigator

- GeoBus
  - aadl
    - GeoBusArch.aadl
    - GeoBusErrorModel.aadl
  - aaxl
    - GeoBusArch_GEObus_impl_Instance.aaxl
    - GeoBusArch_GEObus_impl_Instance.pn
    - GeoBusArch.aaxl
    - GeoBusArch.aaxldi
    - GeoBusErrorModel.aaxl
    - GeoBusErrorModel.aaxldie
  - GeoBusErrorModel.aadl
  - GeoBusErrorModel.aaxl
  - GEOBusFMEA.xls
  - GEOBusFMEA2.xls
  - GEOBusFMEA3.xls
- UpdatedSRS
  - aadl
    - SRS_EM.aadl
    - SRS.aadl
  - aaxl
    - SRS_EM.aaxl
    - SRS_EM.aaxldie
    - SRS_SRS_Simple_Instance.aaxl
    - SRS_SRS_Simple_Instance.pn
    - SRS.aaxl
    - SRS.aaxldi
  - SRS_FMEA.xls
  - SRS_FMEA2.xls
  - SRS_FMEA3.xls
- Plugin_Resources
  - AADL_Project.aadl
  - AADL_Properties.aadl
  - SEI.aadl

SRS_EM.aaxl | SRS.aaxldi | SRS_EM.aaxldie | SRS.aaxl | *GeoBusArch.aaxldi

/GeoBus/aaxl/GeoBusArch.aaxldi

Select
Marquee
Instances
System
Data
Process
Memory
Features
In Data Port
In Event Port
In DataEvent Port
Port Group
Connections
PortGroup
Data
Event
EventData
DataAccess
Modes
Initial Mode
Mode
Mode Transition
Error Annex
Error Subclause
Model Property
Report Property
In Guard

System Instance Diagram GeoBusArch::GEObus_System.CTU / unnamed

SW_Conn1 SW_Conn3 FMS_Conn SW_Conn2 SW_Conn4

Primary_SU: SW_Conn1, SW_Conn2, FMS_Conn, CPU_Control

Backup_SU: SW_Conn1, SW_Conn2, FMS_Conn, CPU_Control

FMS: FMS_Conn, SW_Conn1, SW_Conn2

Primary_PU: Control, InterBus

Backup_PU: Control, InterBus

CTU_Bus

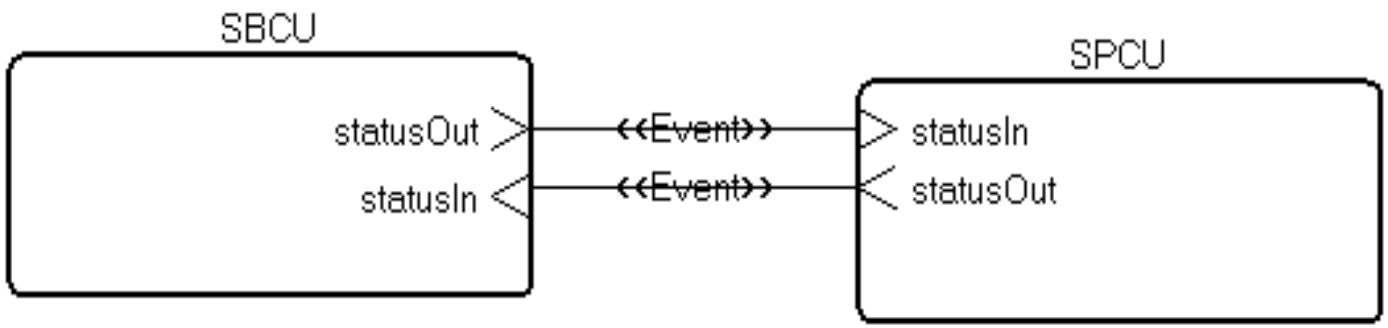
InterBus

<<Data>> <<Event>> <<BusAccess>>

Problems | Properties | Documentation

Example: Simple Satellite

- Bus and Payload Computers
  - *Object names:*
    - SBCU (Spacecraft Bus Computer Unit
    - SPCU (Spacecraft Payload Computer Unit)
  - *Payload relies on the Bus, thus whenever the Bus is in Standby, the Payload goes to Standby.*

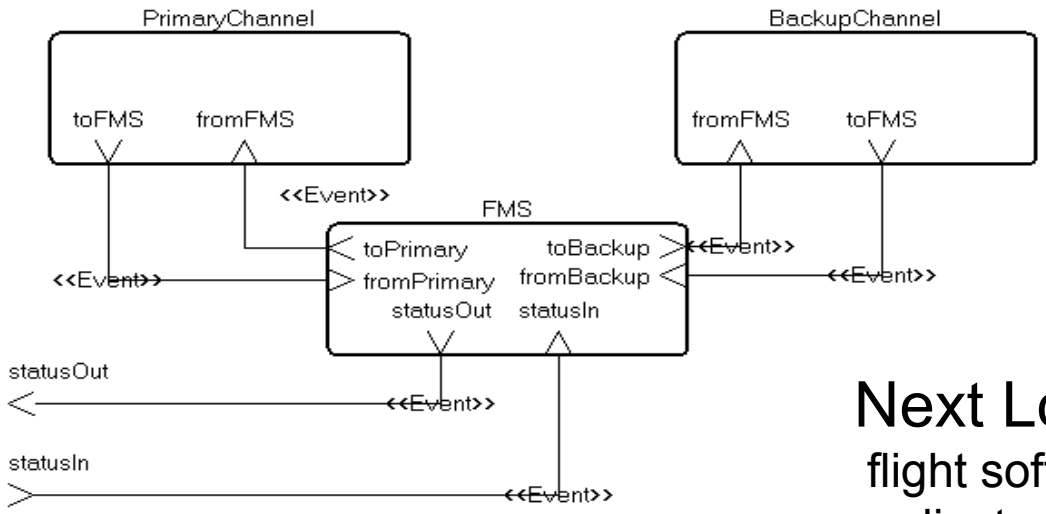


Spacecraft Bus Control Unit (SBCU)

- Architecture Description
  - *Dual redundant Bus Control Processors (BCP)*
  - *Each runs identical copy of bus control software (BCS)*
- Failure Behavior
  - *Permanent Failures (primarily hardware)*
    - A hardware failure results in loss of a processor
    - Two permanent failures result in a mission loss
  - *Transient Failures (primarily software)*
    - Once BCP is active, when it fails control immediately switches to other processor (hot standby)
    - Switching is not always successful (“imperfect switching)
      - *If successful, then a short (“minor failure”) occurs*
      - *If not successful, then a longer (“major failure”) occurs*

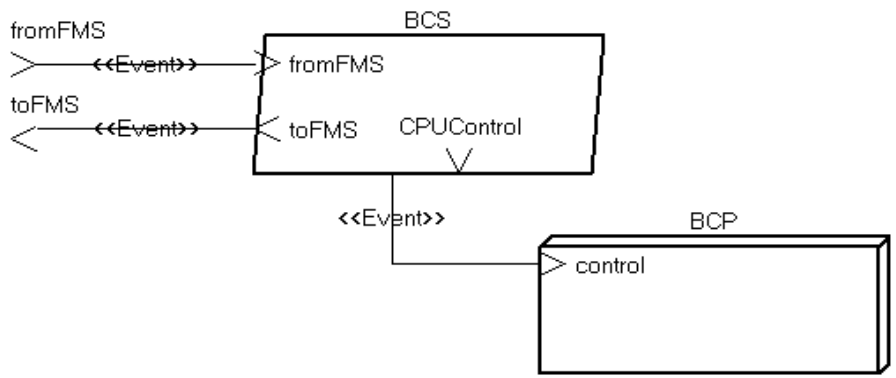
SBCU AADL Architecture Graphical Representation

SBCU Top Level Diagram

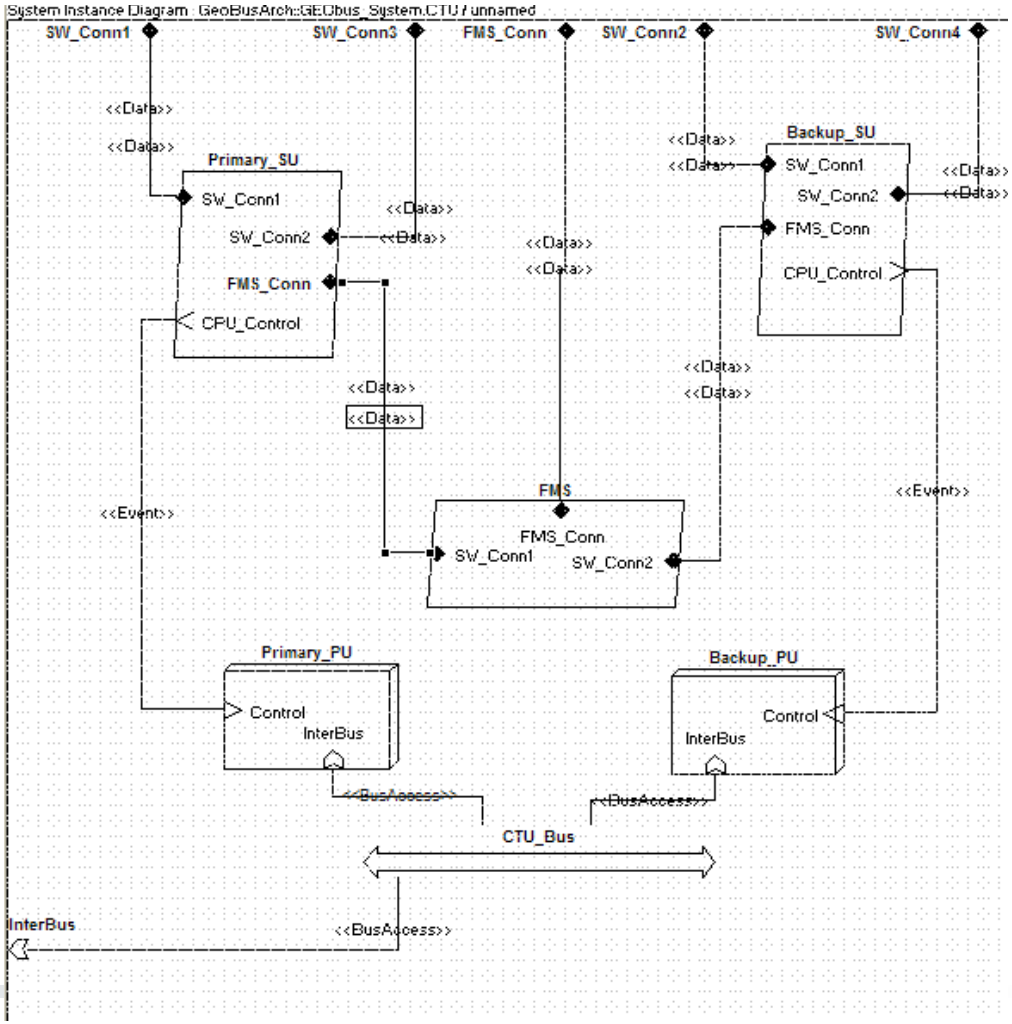


Next Lower level:

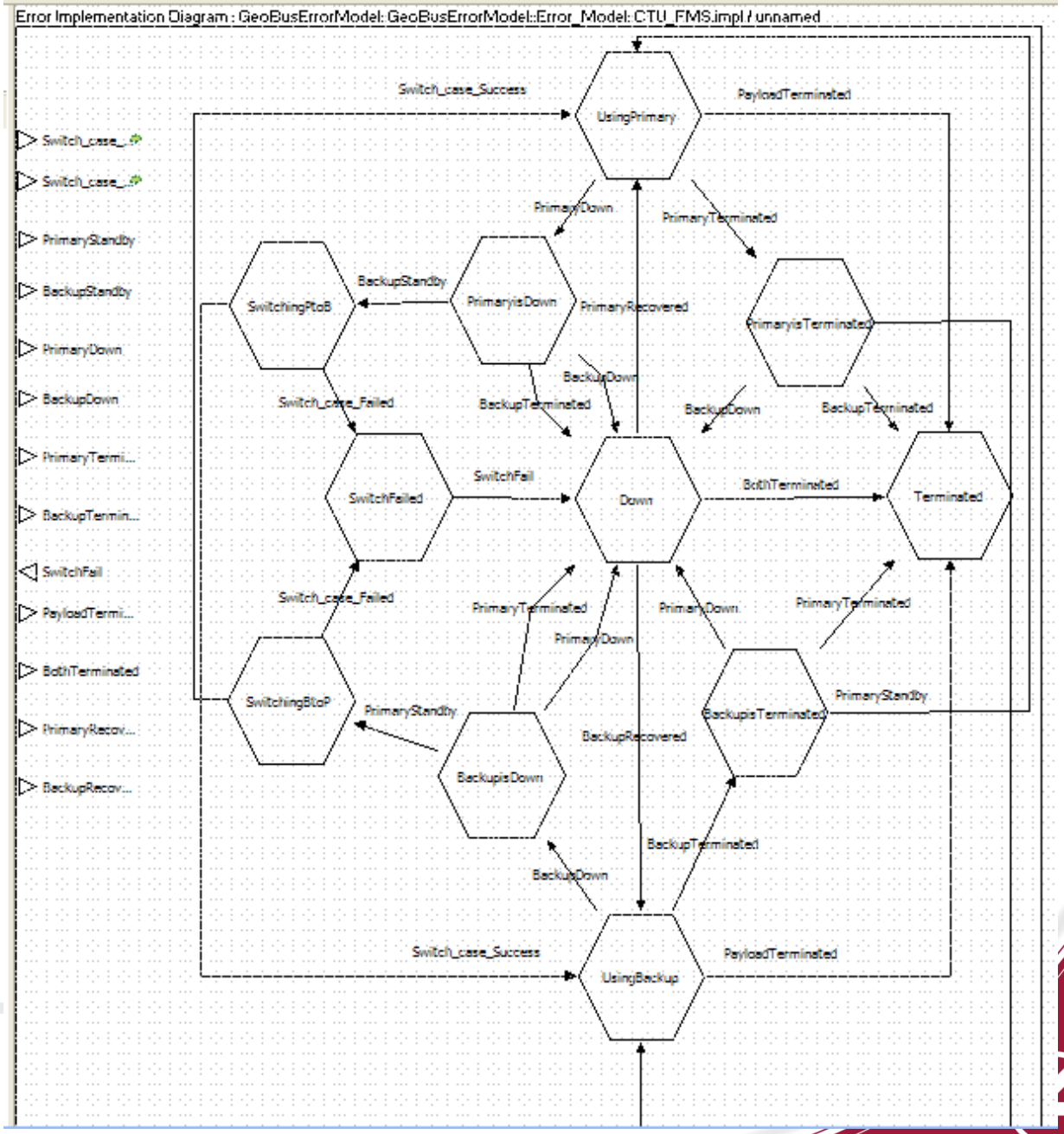
flight software running on one of two replicated processors



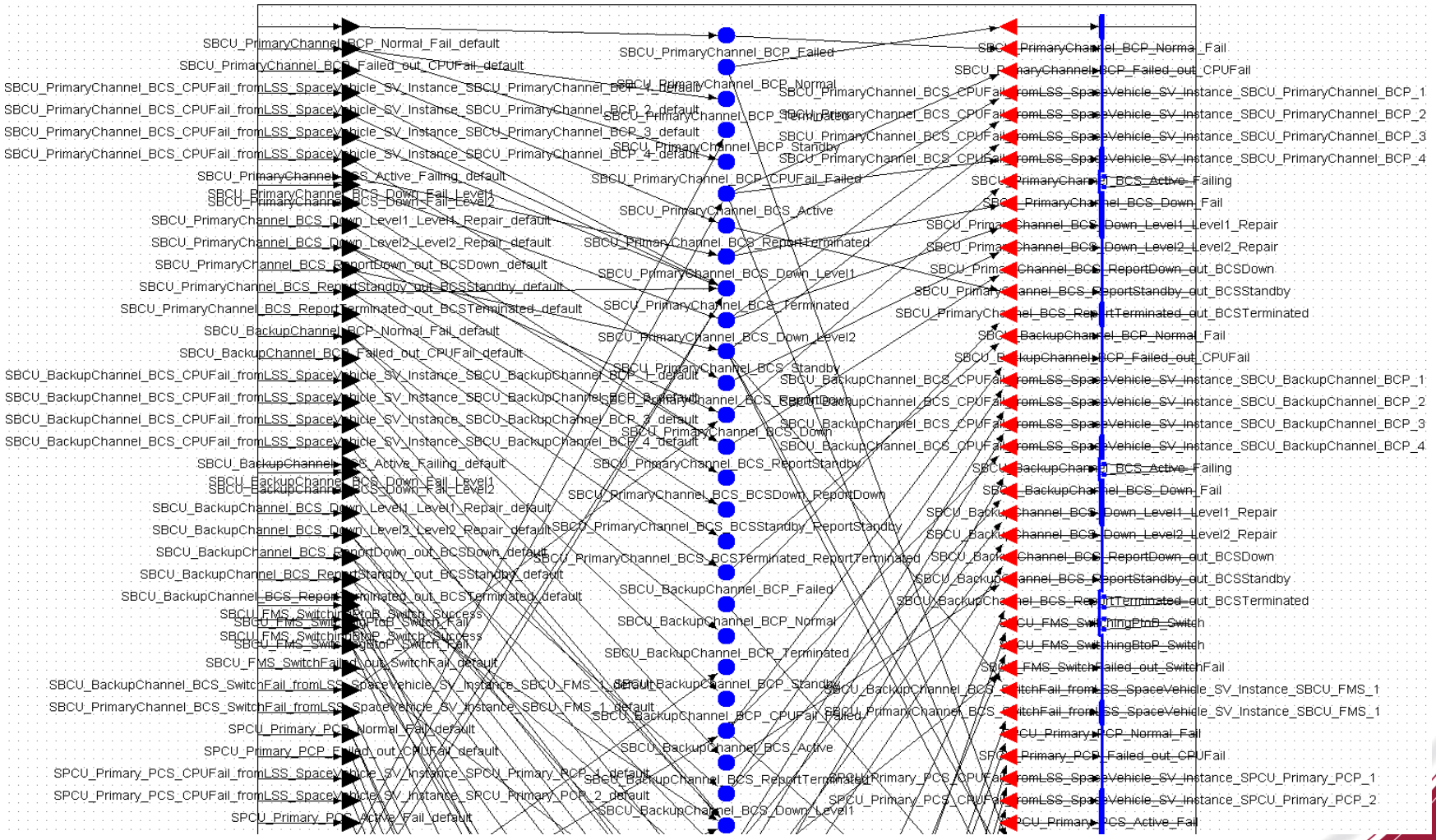
Reusable AADL Representation of SBCU



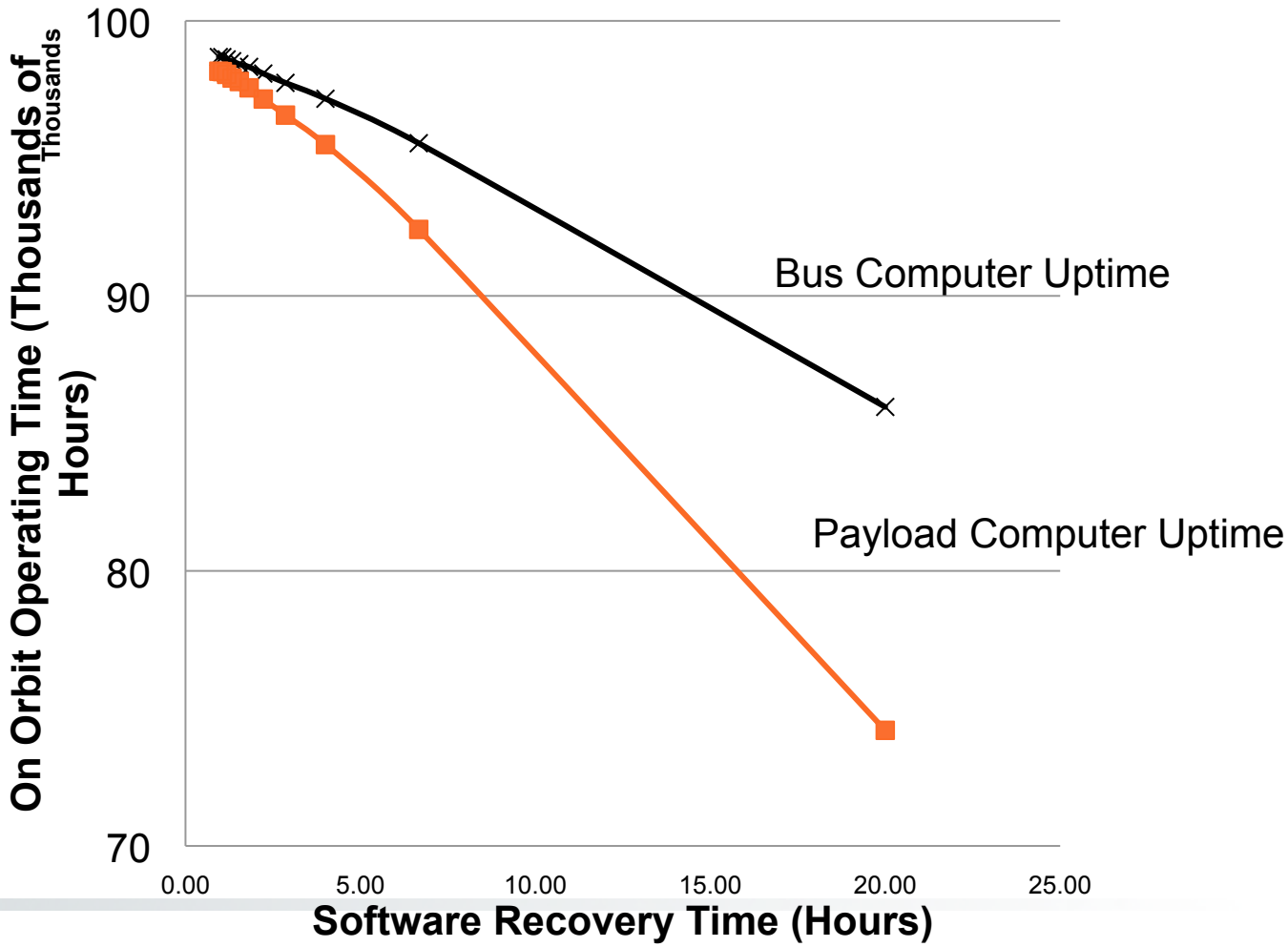
SBCU Error Model Representation using Graphical Editor



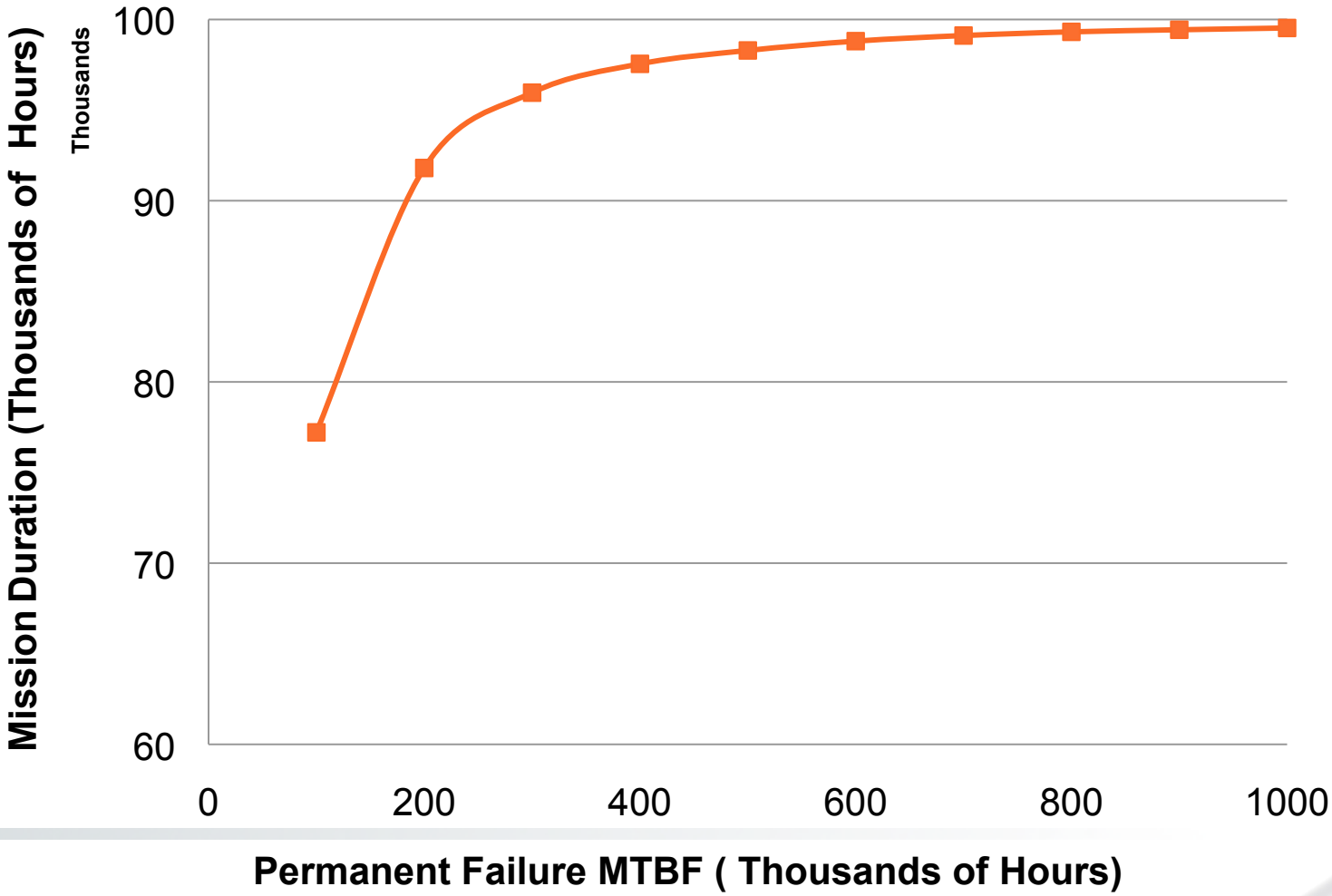
Stochastic Analysis Representation (product of ADAPT-M conversion)



Results: Uptime vs. Recovery Time



Results: Mission Duration vs. Processor Reliability



Automatically Generated FMEA Features

- Automatically Generated
  - *Utilizes information in petri nets and error models*
  - *Automation enables analyses to be performed repeatedly*
    - Manual analyses are constrained because of cost (typically done only once)
- No limit to number of effect levels
  - *Conventional manually generated FMEAs are done to 3 levels (immediate, next level, end effect)*
  - *Propagations are traced across components*
- Editable
  - *Output Generated in MS Excel*

Results: Automatically Generated FMEA

ID	Item	Initial Failure Mode	1st Level Effect	Transition	2nd Level Effect	Transition	3rd Level Effect	Transition	4th Level Effect	Transition	5th Level Effect
1.1	SBCU.Primary_SU	Failure	SU.SBCU_Primary ReportDown	SBCUSdown from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary Down	Failure_case_Minor from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary DownMinor	RecoverMinor from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary ReportRecover	SBCUSrecover from SBCU.Primary_SU to SBCU.Primary_SU SBCUSrecover from SBCU.Primary_SU to SBCU.FMS	SU.SBCU_Primary HotStandby FMS.SBCU UsingPrimary
1.2.1						SBCU.FMS guardin PrimaryDown from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisDown				
1.2.2.1						Failure_case_Major from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary DownMajor	RecoverMajor from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary ReportRecover	SBCUSrecover from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary HotStandby
1.2.2.2										SBCUSrecover from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU UsingPrimary
1.3						SBCU.FMS guardin PrimaryDown from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisDown				
2.1.1	SBCU.Backup_SU	Failure	SU.SBCU_Backup ReportDown	SBCUSdown from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup Down	Failure_case_Minor from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup DownMinor	RecoverMinor from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup ReportRecover	SBCUSrecover from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup HotStandby
2.1.2										SBCUSrecover from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU UsingBackup
2.2						SBCU.FMS guardin BackupDown from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down				
2.3						SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus				
2.4						SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby				
2.5.1						Failure_case_Major from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup DownMajor	RecoverMajor from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup ReportRecover	SBCUSrecover from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup HotStandby
2.5.2										SBCUSrecover from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU UsingBackup
2.6						SBCU.FMS guardin BackupDown from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down				
2.7						SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus				
2.8						SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby				
3.1	SBCU.Primary_PU	Failure	PU.SBCU Terminated	CPUfail from SBCU.Primary_PU to SBCU.Primary_SU	SU.SBCU_Primary Terminated						
3.2				SBCU.FMS guardin PrimaryTerminated from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisTerminated						
4.1	SBCU.Backup_PU	Failure	PU.SBCU Terminated	CPUfail from SBCU.Backup_PU to SBCU.Backup_SU	SU.SBCU_Backup Terminated						
4.2				SBCU.FMS guardin BackupTerminated from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down						
4.3				SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus						
4.4				SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby						
5.1	SPCU.Primary_SU	Failure	SU.SPCU_Primary ReportDown	SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary Down	Recover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ReportRecover	SPCUSrecover from SPCU.Primary_SU to SPCU.Primary_SU SPCUSrecover from SPCU.Primary_SU to SPCU.FMS	SU.SPCU_Primary ColdStandby FMS.SPCU UsingPrimary		
5.2				SPCU.FMS guardin PrimaryDown from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU Down						
6	SPCU.Backup_SU	Failure	SU.SPCU_Backup ReportDown	SPCUSdown from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup Down	Recover from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup ReportRecover	SPCUSrecover from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup ColdStandby		
7.1	SPCU.Primary_SU	Failure	SU.SPCU_Primary ReportDown	SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary Down	Recover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ReportRecover	SPCUSrecover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby		
7.2				SPCU.FMS guardin BackupDown from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						
8.1	SPCU.Primary_PU	Failure	PU.SPCU Terminated	CPUfail from SPCU.Primary_PU to SPCU.Primary_SU	SU.SPCU_Primary Terminated						
8.2				SPCU.FMS guardin PrimaryTerminated from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU PrimaryisTerminated						
8.2				CPUfail from SPCU.Primary_PU to SPCU.Primary_SU	SU.SPCU_Primary Terminated						
8.4				SPCU.FMS guardin PrimaryTerminated from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU PrimaryisTerminated						
9.1	SPCU.Backup_PU	Failure	PU.SPCU Terminated	CPUfail from SPCU.Backup_PU to SPCU.Backup_SU	SU.SPCU_Backup Terminated						
9.2				SPCU.FMS guardin BackupTerminated from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						
9.3				CPUfail from SPCU.Backup_PU to SPCU.Backup_SU	SU.SPCU_Backup Terminated						
9.4				SPCU.FMS guardin BackupTerminated from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						

Conclusions

- A new generation tool set for quantitative stochastic analysis and qualitative Failure Modes and Effects Analysis (FMEAs) for space systems is under development
  - *Based on use of the Architecture Analysis and Design Language (AADL)*
  - *Graphically oriented*
  - *Modularized with reusable components*
- Results will be able to support decisions from concept development through detailed design
  - *Extent and type of redundancy*
  - *Tradeoffs of reliability vs. Weight, power, and functional capability*
  - *Failure rate and recovery time requirements*
  - *Strategies for recovering from computing disruptions*
  - *Handling failure propagation and common mode failures*

References

- Society of Automotive Engineers (SAE) Aerospace Standard AS5506 (2004)
- A. Rugina, K. Kanoun, M Kaaniche, “The ADAPT Tool: From AADL Architectural Models to Stochastic Petri Nets through Model Transformation,” *7th European Dependable Computing Conference (EDCC),* Kaunas : Lituanie (2008)
- Peter Feiler and Anna Rugina, Dependability Modeling with the Architecture Analysis & Design Language (AADL), Software Engineering Institute report CMU/SEI-2007-TN-043, July 2007, available from www.sei.cmu.edu
- D. D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, and P. G. Webster, “The Mobius framework and its implementation,” IEEE Trans. on Soft. Eng., vol. 28, no. 10, pp. 956–969, October 2002.