Automated Generation of Failure Modes and Effects Analyses from AADL Architectural and Error Models

Myron Hecht, Alexander Lam, Russell Howes, and Christopher Vogl,
The Aerospace Corporation

Presented to
Systems and Software Technology Conference
Salt Lake, City, UT
April, 2010

Outline

- Motivation
- Background on FMEAs
- Introduction to AADL
- AADL Error Model Annex
- Tool Set for Analyzing Risk and Reliability/Availability
- Automated FMEA Generation Example
- Additional Discussion
- Conclusions

Motivation

- Failure Modes and Effects Analyses (and related Criticality Analyses) are rigorous and comprehensive reliability and safety design evaluations
  - *Generally required either by industry standards or Government policies*
  - *A fundamental element of defense in many product liability lawsuits*
- When performed manually, FMEAs are usually done only once during the detailed design phase because of cost and schedule constraints
  - *Labor intensive*
  - *Require senior level; analysts*
- If automated, FMEAs would have significant benefits
  - *Multiple iterations from conceptual to detailed design*
  - *Enables early identification of potential problems*
    - Single points of failure
    - Unanticipated effects
  - *Facilitates tradeoff studies and evaluations of alternatives*

Failure Modes and Effects Analysis (FMEA)

- Purpose
  - *To determine the effect of hardware and software failures upon the system and equipment failures.*
    - Classify effects by impact on mission success and personnel/equipment safety.
    - Identify single points of failure
- History
  - *First defined as Military Procedure MIL-P-1629, "Procedures for Performing a Failure Mode, Effects and Criticality Analysis", November 1949.*
  - *Further developed and applied by NASA in the 1960's to improve and verify reliability of space program hardware.*
  - *Since the 1980s, a standard of practice in a wide variety of industries*
    - DoD: MIL-STD-1629A
    - Industrial: IEC 60812 (1985)
    - Aviation: SAE ARP 5580 (2001)
    - Automotive: SAE J1739 (2002)
    - Space: ECSS-Q-30-02A

FMEA Methodology

Conventional	Automated
Define Ground Rules and Assumptions Levels of indenture Components to be considered Failure modes by component category Severity Level Definitions Rules for recovery mechanisms and compensating provisions For Each Component Postulate failure and failure mode Identify immediate effect of failure Identify next higher level effects and “end effects” Identify compensating provisions Evaluate severity level at end effect	• Ground rules and assumptions defined by component properties • Components and failure modes defined in models • Effects identified through graph tracing

FMEA Output

In Either Worksheet or Tabular Format…

- Identification*:* Failure Mode identification.
- Item*:* For software, a process in its context.
- Failure Mode*:*
  - ***Immediate Effect:***
  - ***Intermediate Effect: Second level effect.***
    - Operator
    - External networks
    - Database
    - Recovery
  - ***End Effect:***
    - System Level (e.g., Individual satellites or the constellation through TT&C functions)
    - Payload performance
    - Data to outside users through terrestrial interfaces
- Existing Mitigations*:* Any existing mitigations present in the architecture or design were identified.
- Severity level:
  - *Set under assumption that existing mitigations assumed to work*
- Comments:
  - *Additional comments documenting assumptions and uncertainties.*

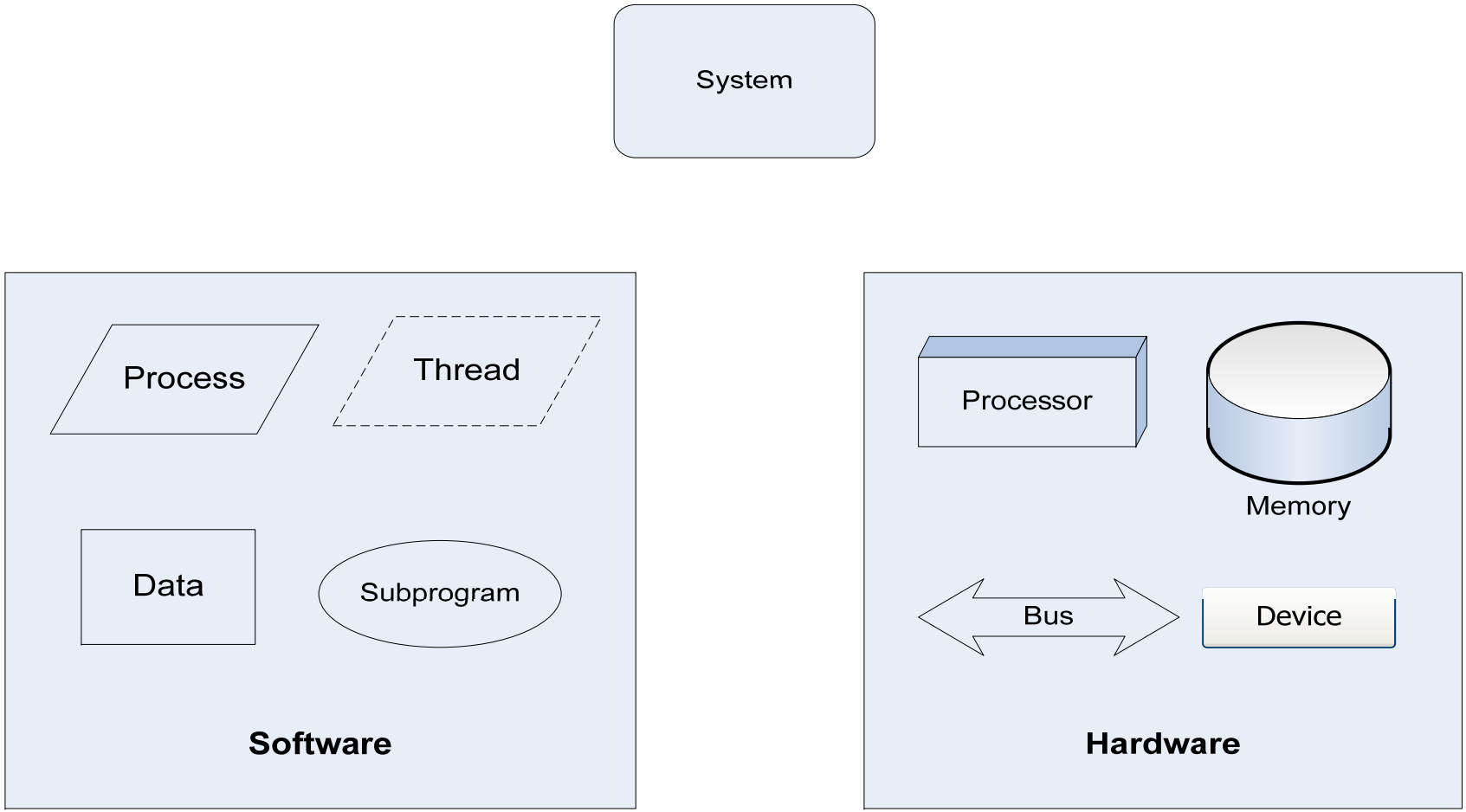
Introduction to the Architecture Analysis & Design Language (AADL)

- 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 Error Model 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*

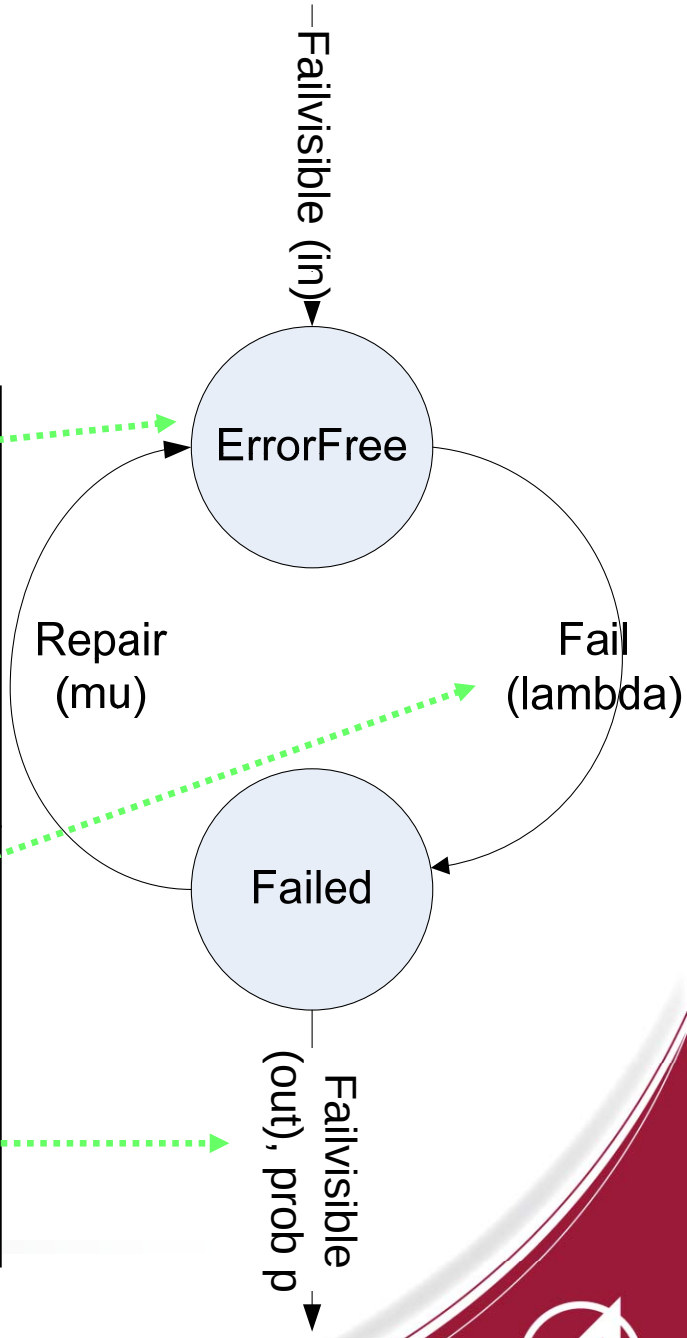
Enabling Features of AADL

- Standard representation of architecture and error models
- Representation of failure propagation through system components
  - *Event Ports*
  - *Guards*
  - *Propagations*
- Error Model properties
  - *Working status of states*
  - *Descriptive information for initial states, effects (subsequent states), and failure modes (transitions)*
  - *Initial states*
  - *Terminal States*

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;
```

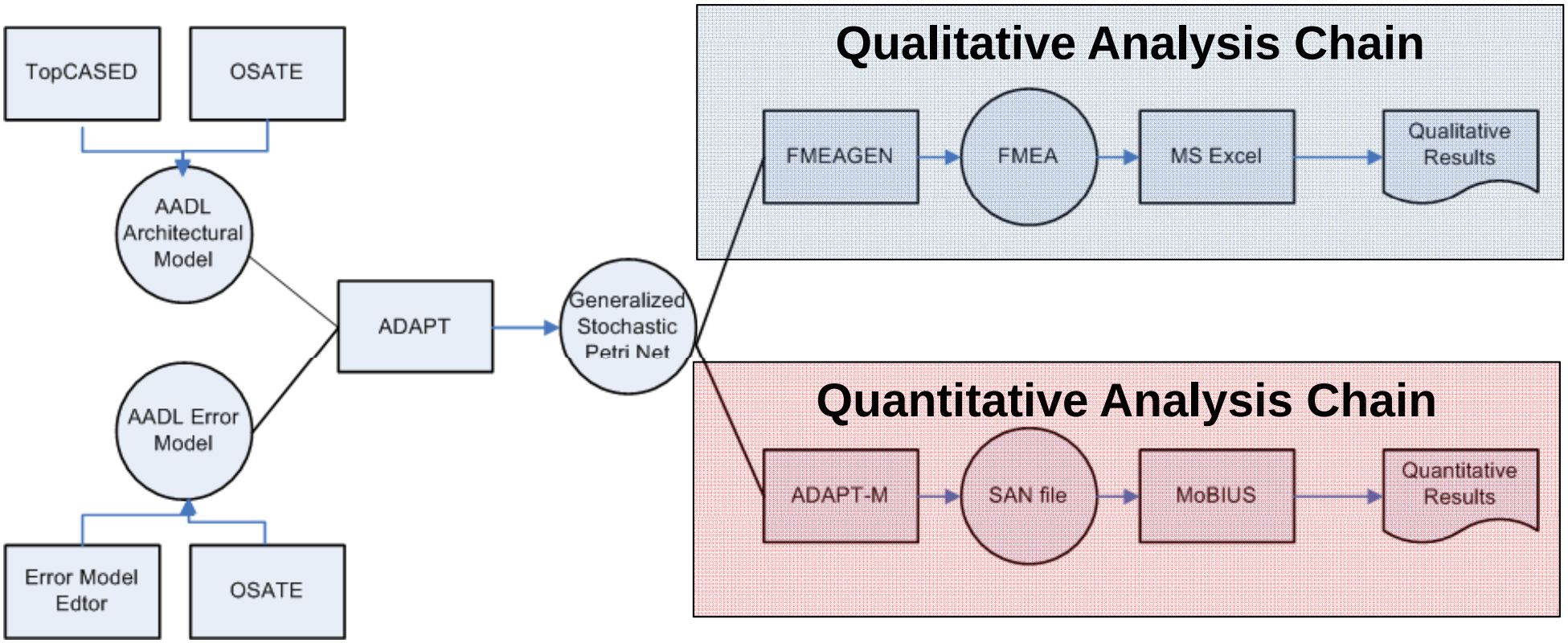


More information: Feiler (2007)

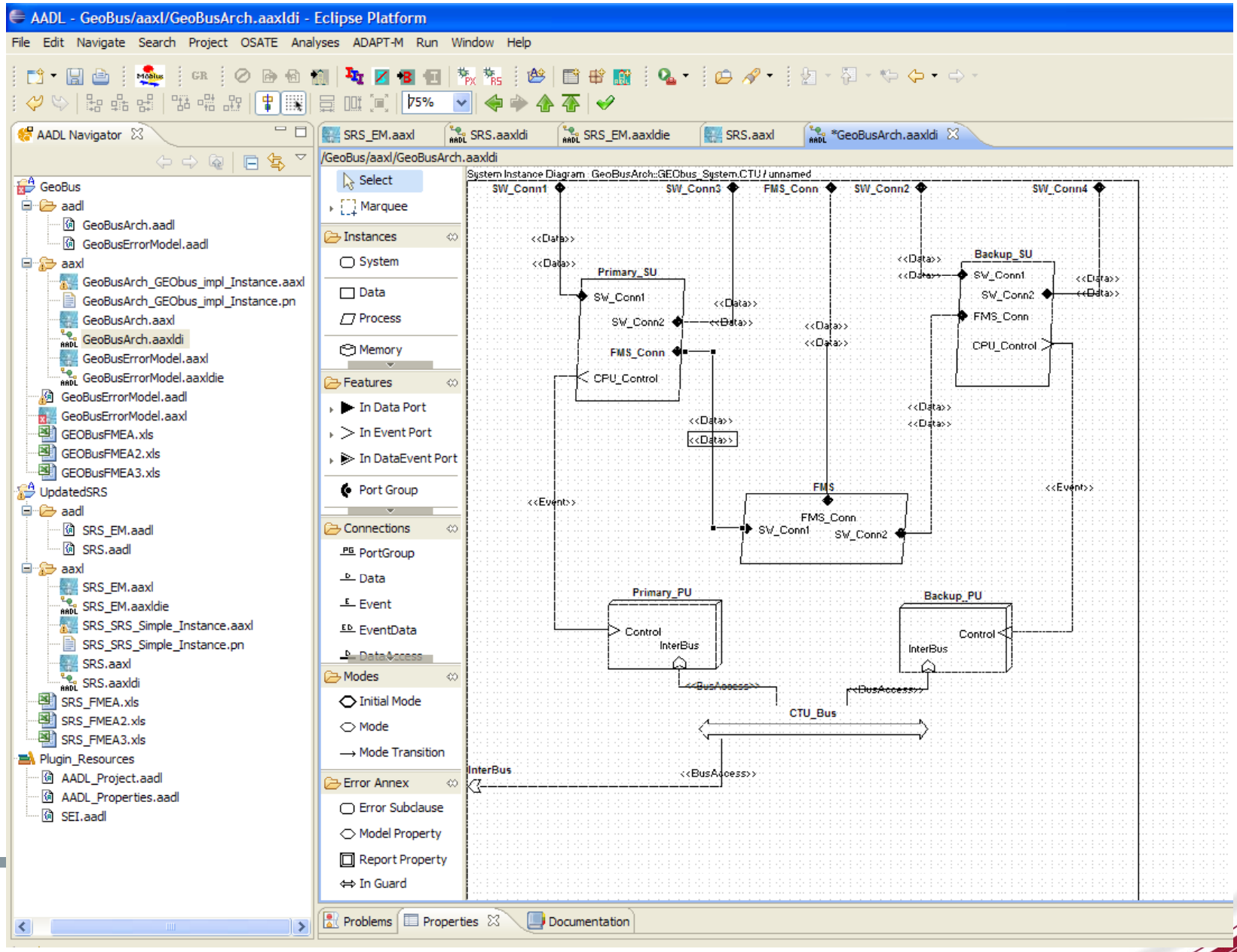
AADL Tool Set

- 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 (The Aerospace Corporation newly developed)*
  - ***OSATE*** *AADL generator (SEI, The Aerospace Corporation modifications)*
  - ***ADAPT-M*** *Stochastic Petri net to MoBIUS stochastic analysis network tool ((SEI/LAAS Toulouse and The Aerospace Corporation)*
  - ***MoBIUS*** *Quantitative Dependability modeling and prediction tool (University of Illinois, Champaign Urbana)*
  - ***FMEAGEN*** *FMEA Generator (The Aerospace Corporation newly developed)*

AADL Modeling Tool Chain Data Flow



Tool Set Screen Shot

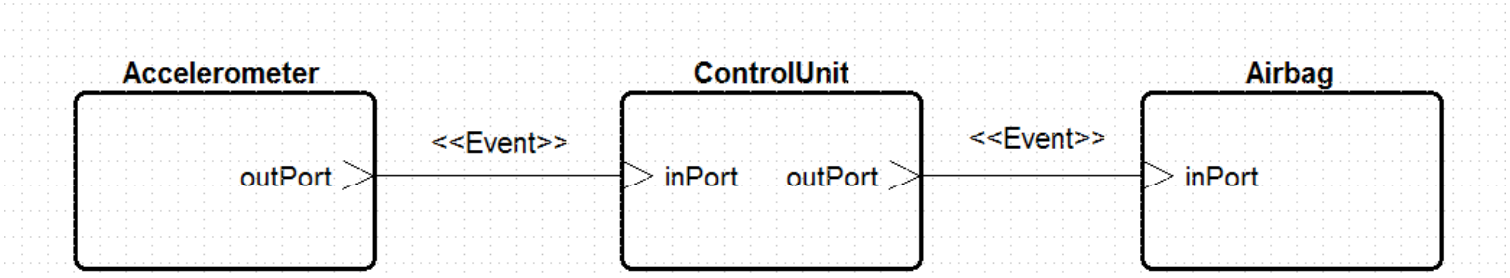


FMEA Generation Algorithm Features

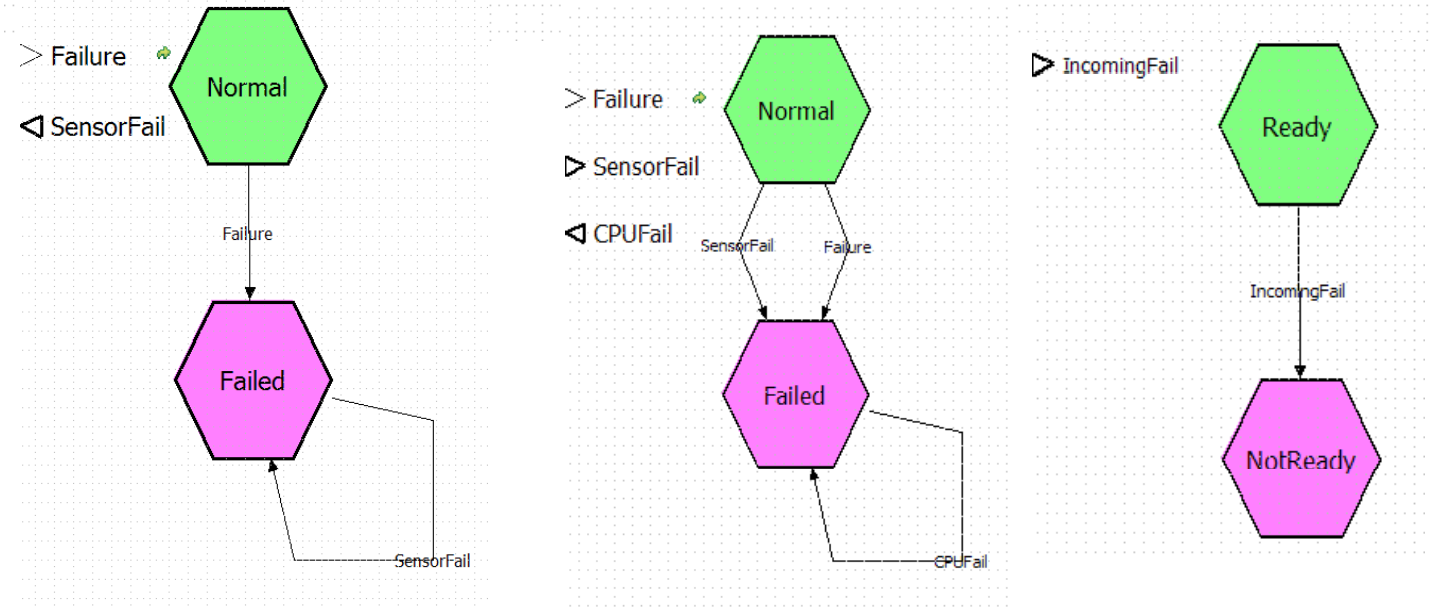
- Automatically traces from all working states to failure states
  - *Terminates when trace detects a restoration condition or a failure condition*
- Not limited to only 3 levels of effects
- Checks to prevent repeated visits to same states
  - *Ensures termination*
  - *Of particular importance for recoverable systems*

Example: Supplemental Restraint System

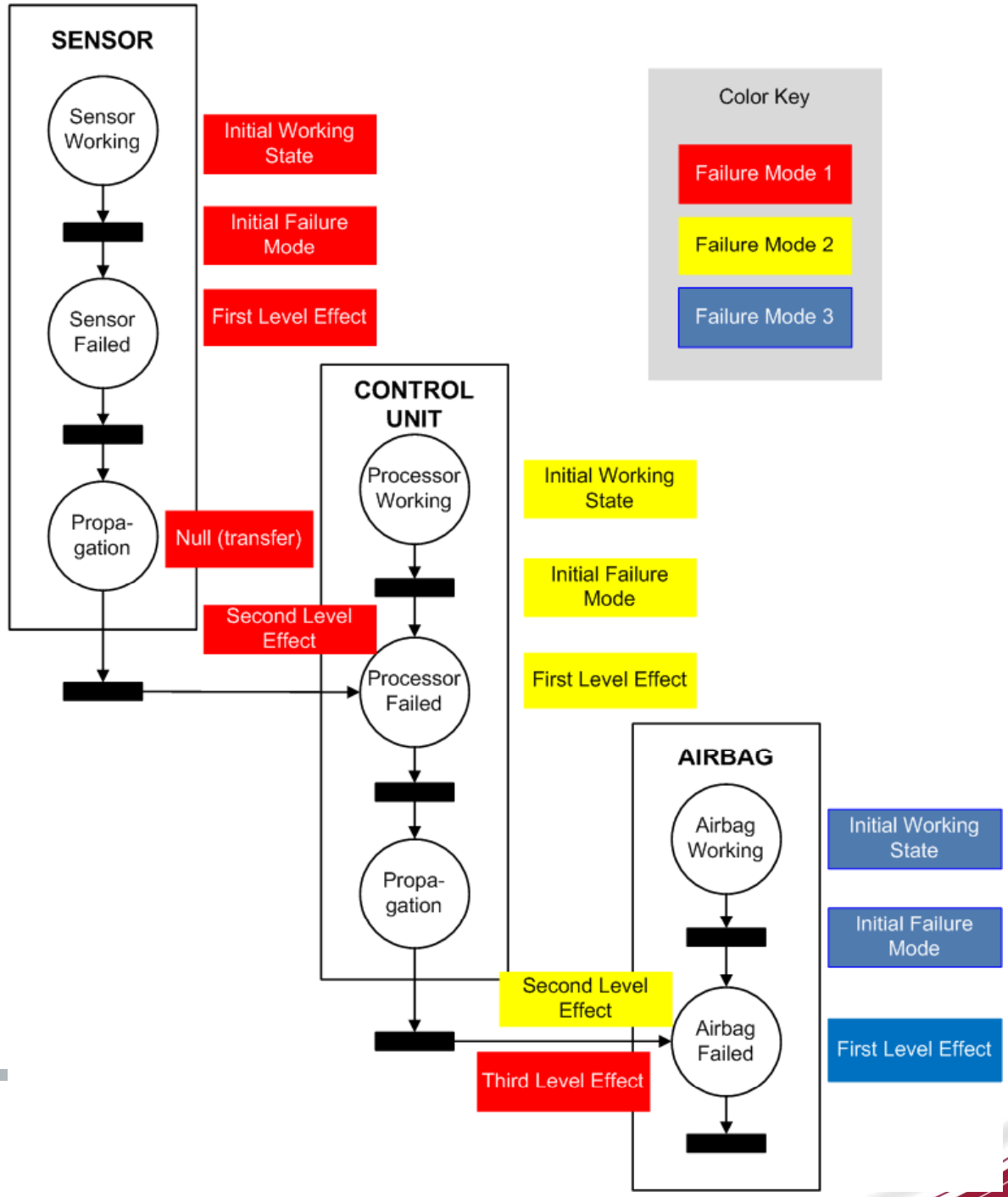
Architectural Model



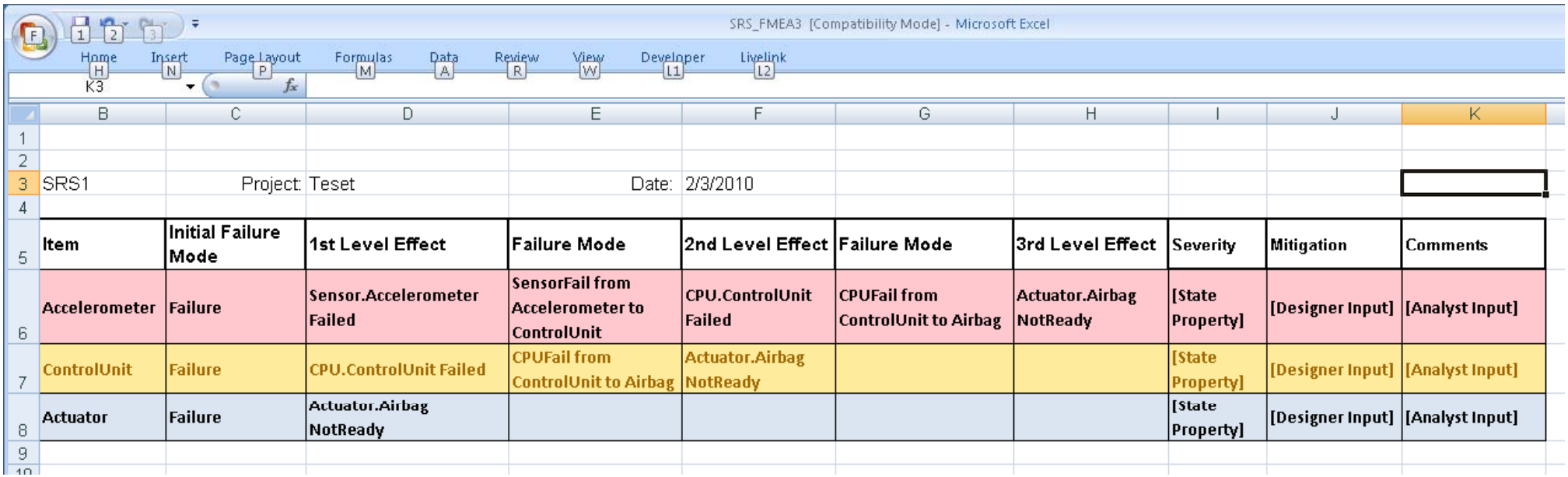
Error Models



Generation of FMEA from Petri Net of Error Models



Results: Automatically Generated FMEA

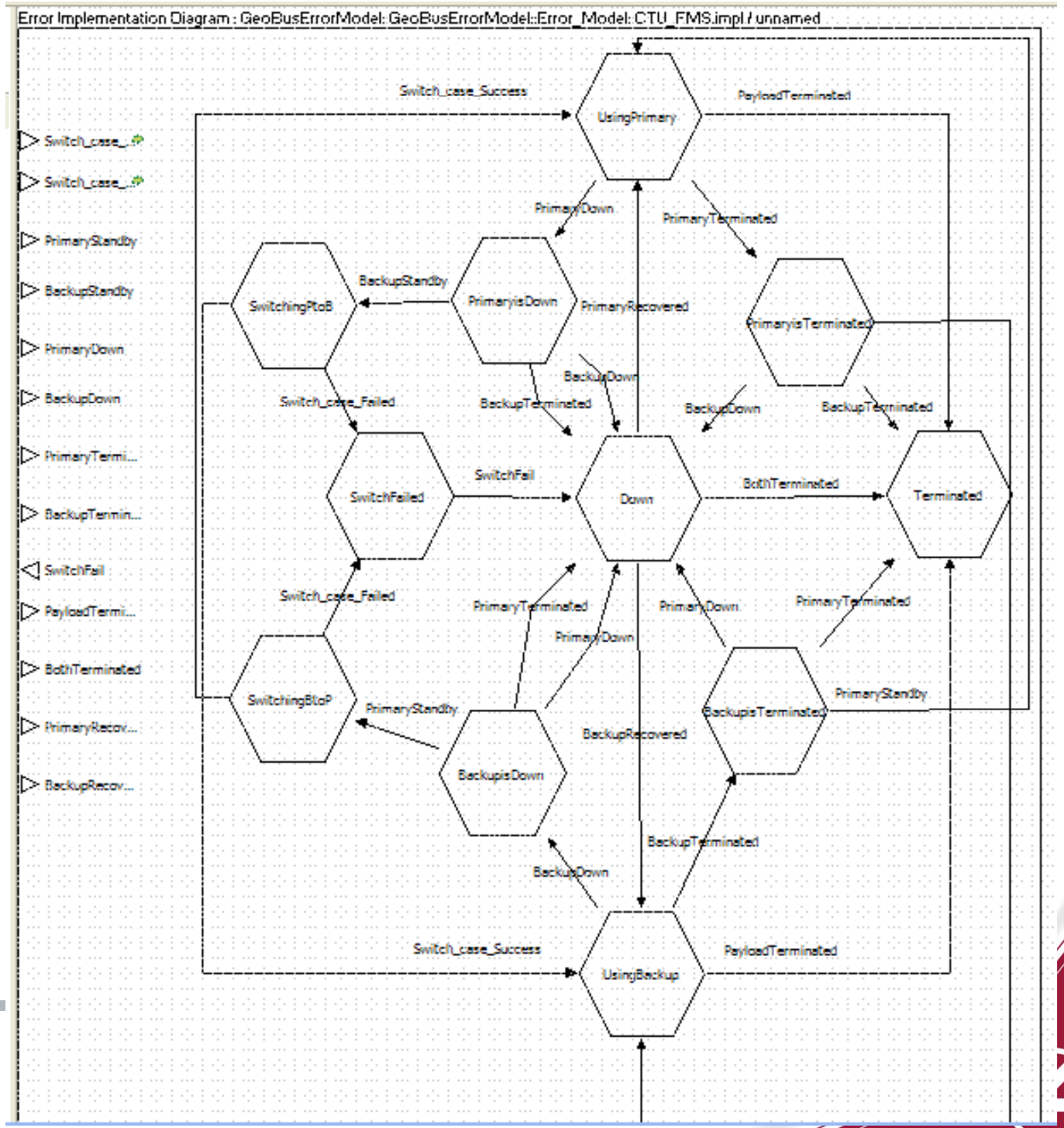


SRS1 Project: Teset Date: 2/3/2010

Item	Initial Failure Mode	1st Level Effect	Failure Mode	2nd Level Effect	Failure Mode	3rd Level Effect	Severity	Mitigation	Comments
Accelerometer	Failure	Sensor.Accelerometer Failed	SensorFail from Accelerometer to ControlUnit	CPU.ControlUnit Failed	CPUFail from ControlUnit to Airbag	Actuator.Airbag NotReady	[State Property]	[Designer Input]	[Analyst Input]
ControlUnit	Failure	CPU.ControlUnit Failed	CPUFail from ControlUnit to Airbag	Actuator.Airbag NotReady			[State Property]	[Designer Input]	[Analyst Input]
Actuator	Failure	Actuator.Airbag NotReady					[State Property]	[Designer Input]	[Analyst Input]

Enhanced formatting for presentation purposes

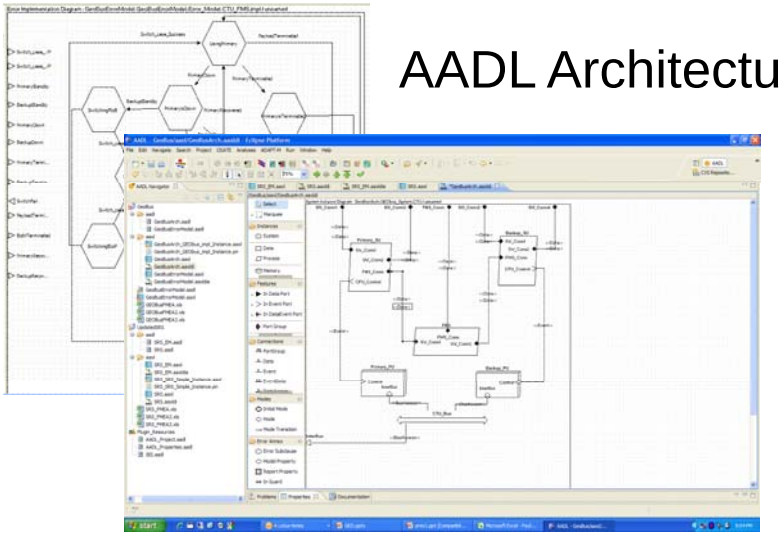
More Complex Error Model



Results: Automatically Generated FMEA

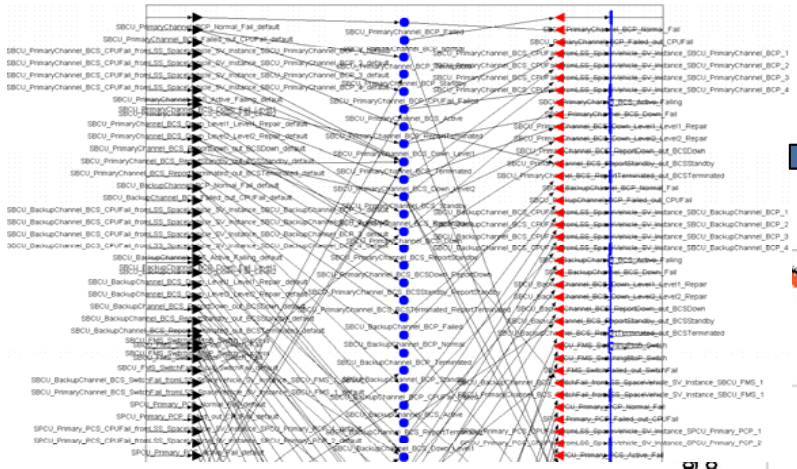
ID	Item	Initial Failure Mode	1st Level Effect	Transition	2nd Level Effect	Transition	3rd Level Effect	Transition	4th Level Effect	Transition	5th Level Effect
1.1	SBCU.Primary_SU	Failure	SU.SBCU_Primary ReportDown	SBCUSdown from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary Down	Failure_case_Minor 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						

Tool Set Capabilities for Quantitative Evaluation

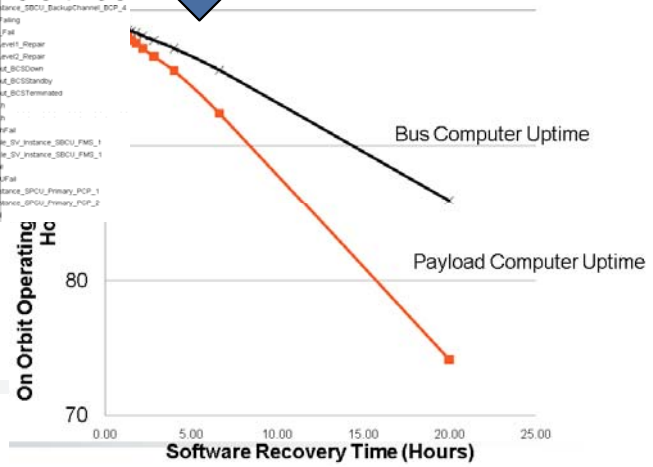


AADL Architecture and Error Models

Mobius Stochastic Analysis Network Model



Results



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*
- Automated Generation of FMEA/CA enables multiple iterations analyses throughout all stages of the design
  - *Allows design alternatives to be evaluated*
    - Strategies for recovering from computing disruptions
    - Handling failure propagation and common mode failures
  - *Enables safety and reliability problems to be identified early*
    - Of critical importance to all users and stakeholders
    - Significant economic value where products liability is an issue because of conforming and exceeding standard of care

Acronyms

ADAPT: AADL Architectural models to stochastic Petri nets through model Transformation,

AADL: Architecture Analysis & Design Language

FMEA: Failure Mode and Effects Analysis

FMEA/CA: FMEA /Criticality Analysis

OSATE: Open Source AADL Tool Environment (Software tool integrated into Eclipse)

SAE: Society of Automotive Engineers

SAN: Stochastic Analysis Network

TOPCASED: Toolkit In OPen source for Critical Applications & SystEms Development

References

- 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.
- IEC 60812 (1985) Analysis techniques for system reliability - Procedures for failure mode and effect analysis (FMEA) , International Electrotechnical Commission,
- SAE AS5506 (2004), Aerospace Standard: Architecture Analysis and Design Language available online from www.sae.org
- SAE ARP 5580 (2001) Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications, Society of Automotive Engineers, available online from www.sae.org
- SAE J1739 (2002) Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA) , Society of Automotive Engineers, available online from www.sae.org
- SEMATECH (1992) “Failure Modes and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry”, Technology Transfer #92020963B-ENG, available online at http://www.ismi.sematech.org/docubase/abstracts/92020963B-ENG.htm