Automated Generation of Failure Modes and Effects Analyses from AADL Models

Alexander Lam, Christopher Vogl, Myron Hecht, and Chris Dimpfl
The Aerospace Corporation

Presented to
2011 Flight Software Workshop
Applied Physics Laboratory
October 2011

Outline

- Motivation
- Background on FMEAs
- Introduction to AADL
- Automated FMEA Generation Process
- Algorithm Description
- Results
- MDDA Workbench Description
- Discussion
- Conclusions

Failure Modes and Effects Analysis (FMEA) Background

- 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
- A standard of practice in a wide variety of industries: Examples
    - DoD: MIL-STD-1629A (introduced as MIL-P-1629A in the 1960s)
    - Industrial: IEC 60812 (1985)
    - Aviation: SAE ARP 5580 (2001)
    - Automotive: SAE J1739 (2002)
    - Space (ESA): ECSS-Q-30-02A (2001)

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*

Manual vs. Automated Output

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	FAILURE EFFECTS			FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	SEVERITY CLASS	REMARKS
					LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

Format defined in MIL STD 1629A

ID	Item	Initial State	Initial Failure Mode	1st Level Effect	Transition	2nd Level Effect	Transition	3rd Level Effect	Severity	M
1	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Workir
1	Sat_Payload	Working		Working	Bus failure causes payload transition	Standby		Standby	Bus Recovery Causes Payload Transition	Workir
2	Sat_Bus	Working		Working		Working	5			
2	Sat_Payload	Working	Failure	Failed	Recovery	Working	5			

From FMEA Generator and Postprocessor

FMEA Development Method Comparison

Data Item	Generated Manually	Generated Using Automated Tool
Identif-ication	Identification Label or number	Same
Item	Item (un-failed state only)	Item (in un-failed and multiple degraded states – allows for consideration of multiple simultaneous failures
Failure Mode	Description of how the item failed	Name and description of error model transition (description of how failed contained in properties of transition)
Immediate Effect	Manual description of immediate effect	Name and properties of state to which transitioned (description contained in properties of destination state)
Subse-quent Effects	Limited to only two additional levels (immediate and end end effects)	Not limited to only two levels– could be tens or hundreds of effects (subsequent states and transitions)
Detection	Description of any detection methods	Detection is described in the context of subsequent transitions (contained in transition properties)
Compen-sating Provisions	Description of any mitigation methods	Compensating provisions (i.e., recovery) described in the context of subsequent transitions (contained in transition properties)
Severity level:	Assigned at time of analysis	Contained in state property

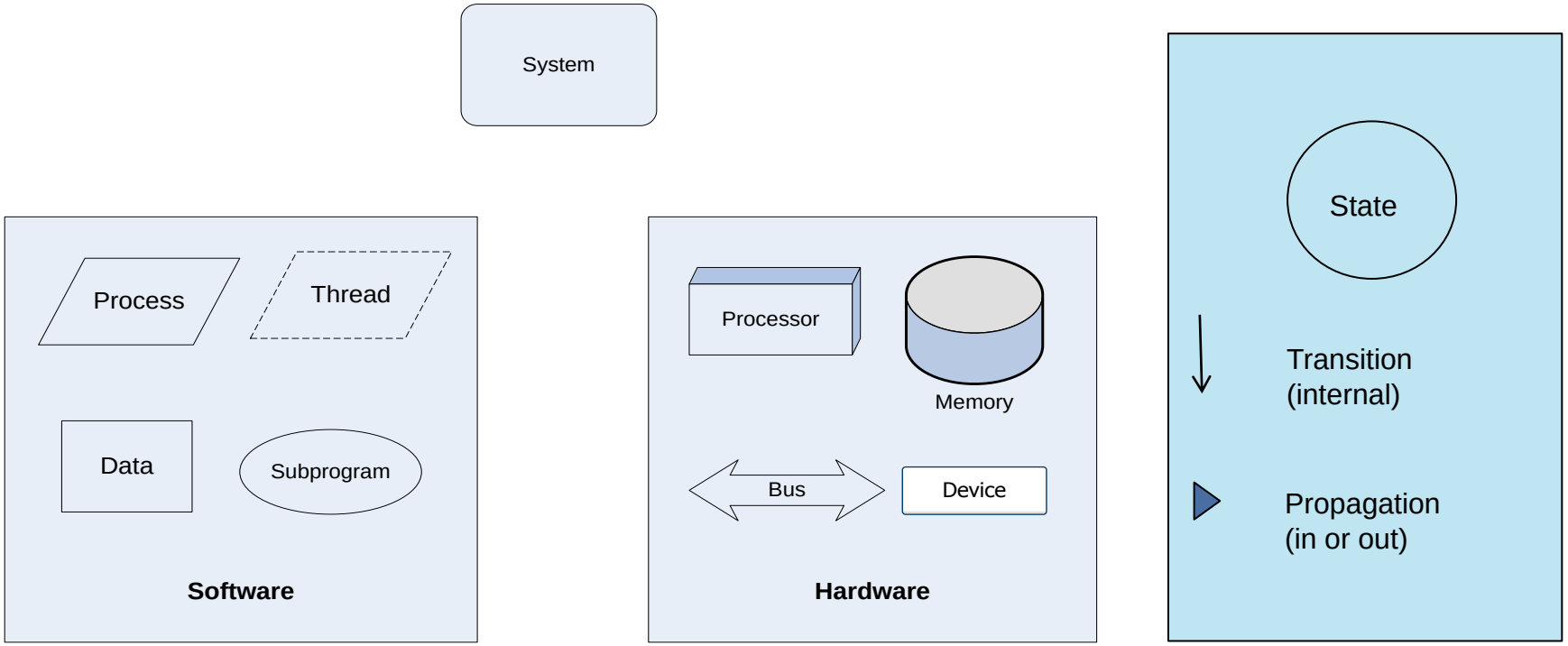
Architecture Analysis & Design Language (AADL)

- Society of Automotive Engineers (SAE) Aerospace Standard AS5506 (2006 for v 2)
- 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)*
- Representation of failure propagation through system components
  - *Event Ports*
  - *Guards*
  - *Propagations*

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*
- Error Model properties
  - *Working status of states*
  - *Descriptive information for initial states, effects (subsequent states), and failure modes (transitions)*
  - *Initial states*
  - *Terminal States*

AADL Components (graphical representation)



Architecture Model

Error Model

AS 5506 Annex A describes the graphical notation

Automated FMEA Generation Process

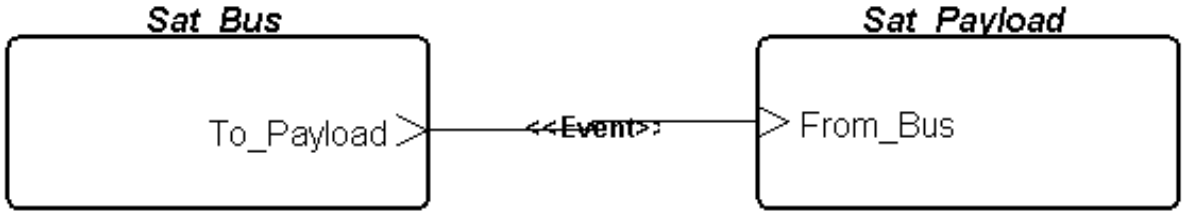
- Create AADL System Architecture and Error Models
  - *The Aerospace Corporation's Model Driven Design and Analysis (MDDA) Workbench which is described later in this presentation*
- Transform the AADL Models into a Petri Net
  - *A Petri Net generation model generator component of the MDDA Workbench generates the Petri Net automatically*
- Produce a "raw" FMEA by tracing the Transitions in the Petri Net and creating a tree of these traces ("Petri Tree)
  - *An FMEA generator component of the MDDA Workbench performs this automatically*
- Filter the FMEA to extract rows of relevance using a post-processing tool
  - *An FMEA post-processor component of the MDDA Workbench is an interactive tool for performing this process*

Overview of the FMEA Generation Algorithm

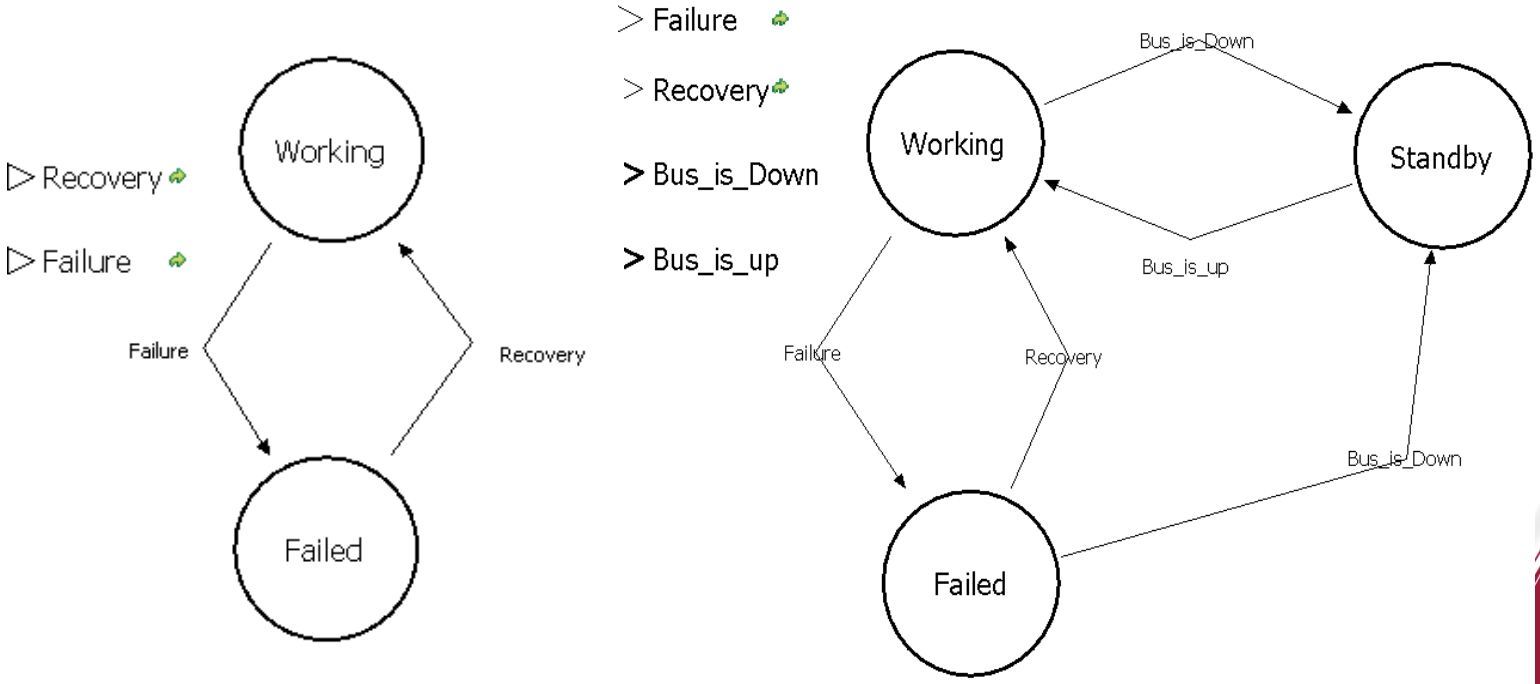
- Sample System in AADL
- Petri Net
- Generation of the Petri tree
- Final results

Sample System

Architecture Model



Error Model

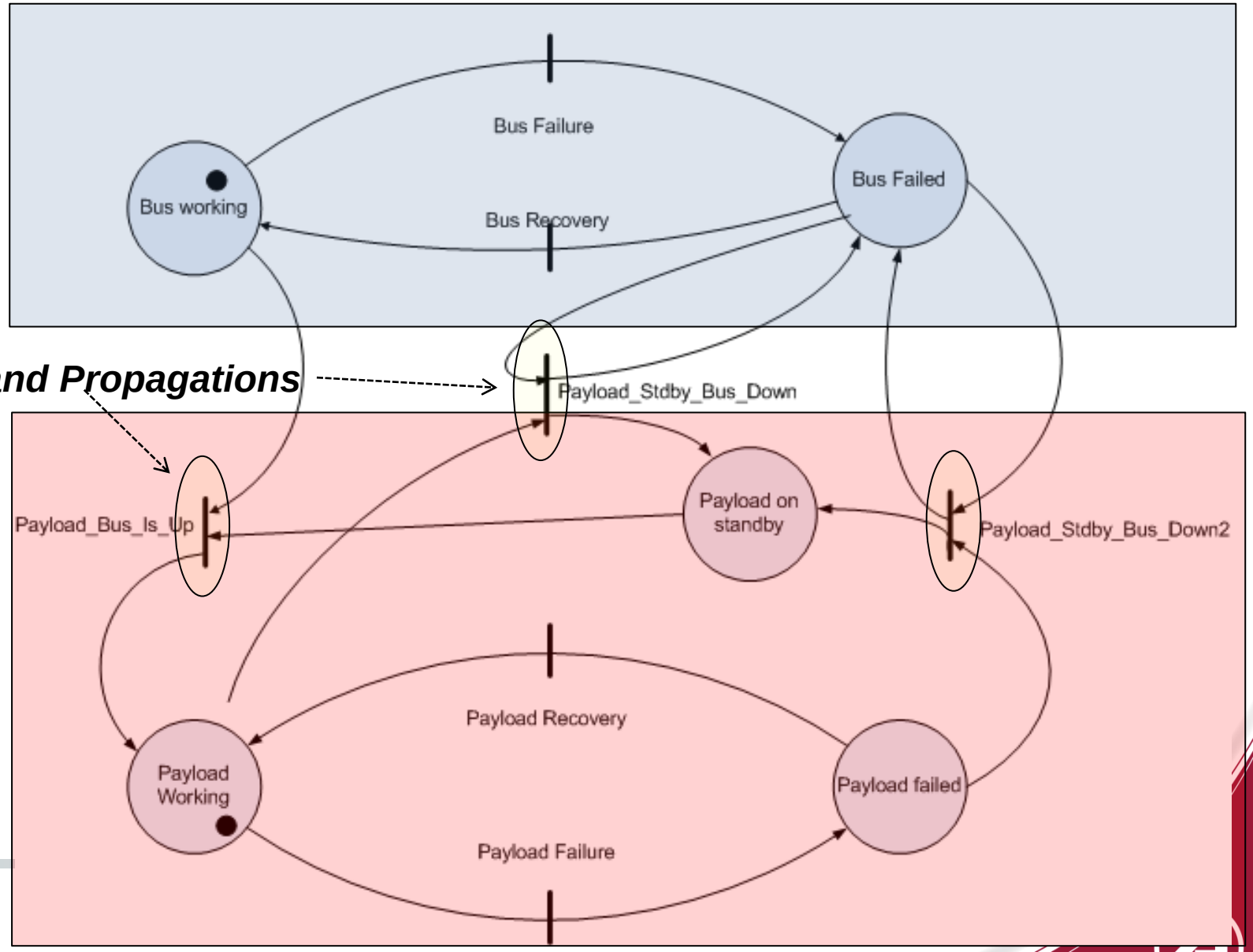


Petri Net derived from AADL Model

Bus

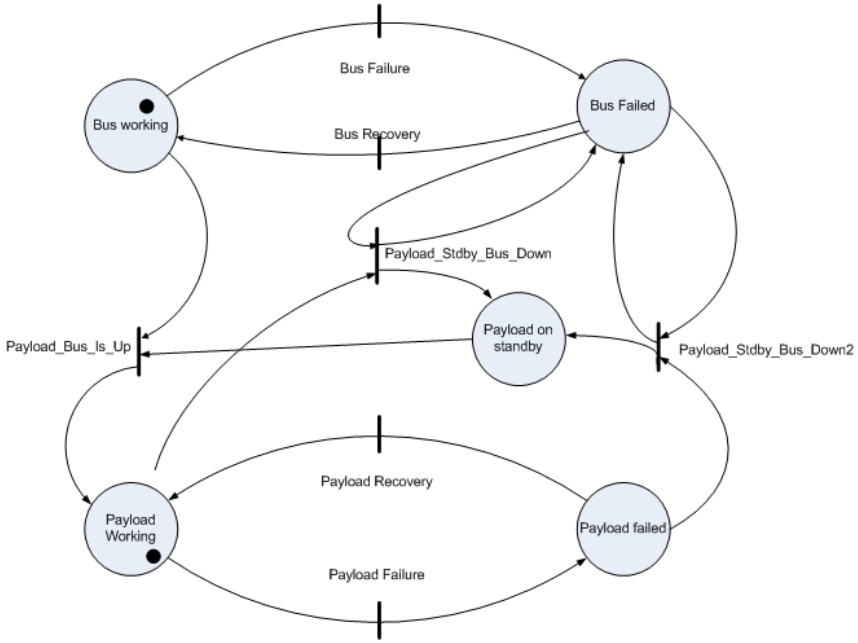
Events and Propagations

Payload

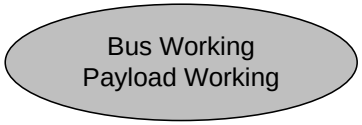


Bus, Payload Working

Petri Net

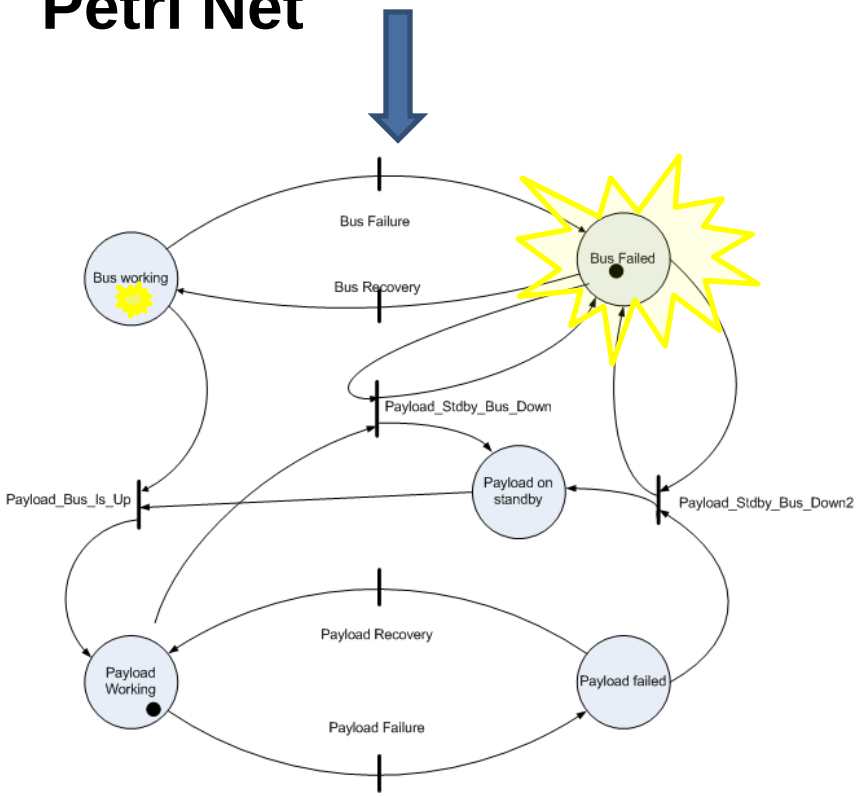


Petri Tree

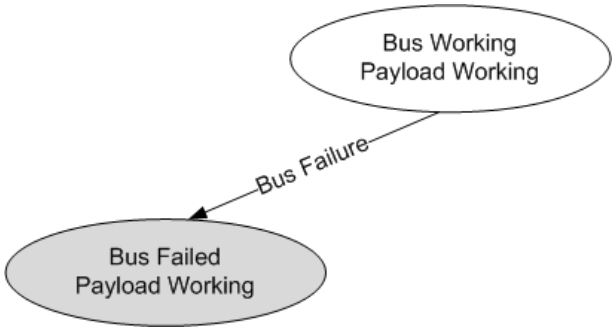


Bus Failed, Payload Working

Petri Net

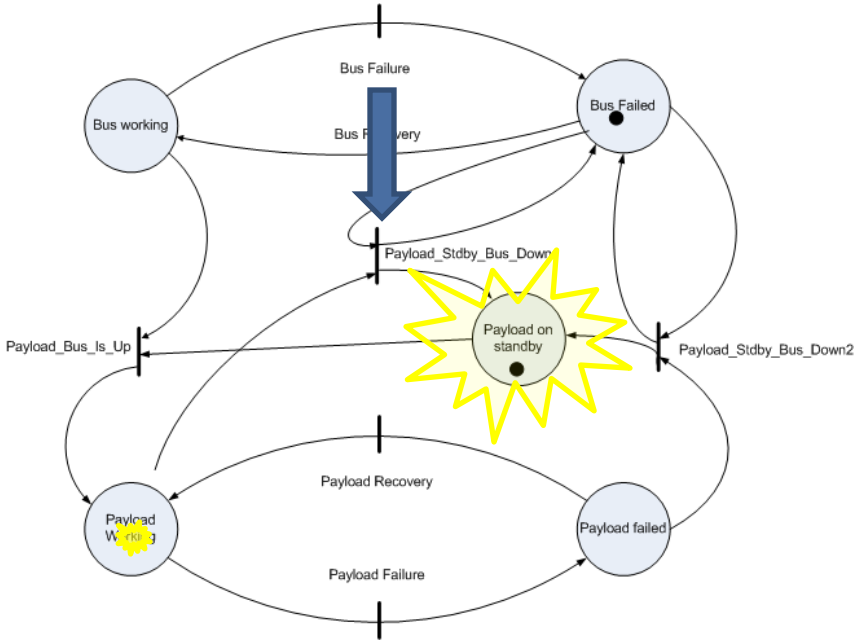


Petri Tree

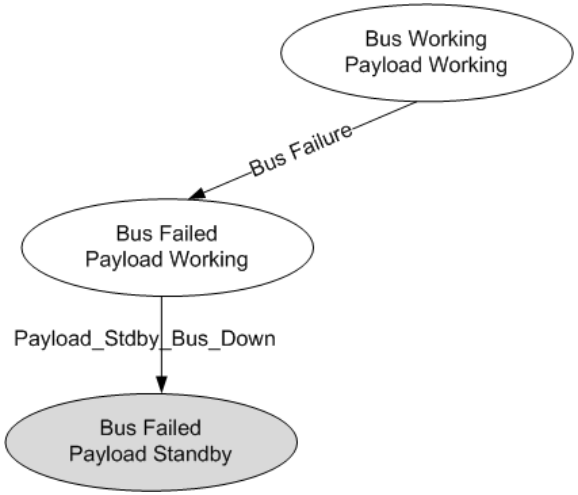


Bus Failed, Payload on Standby

Petri Net

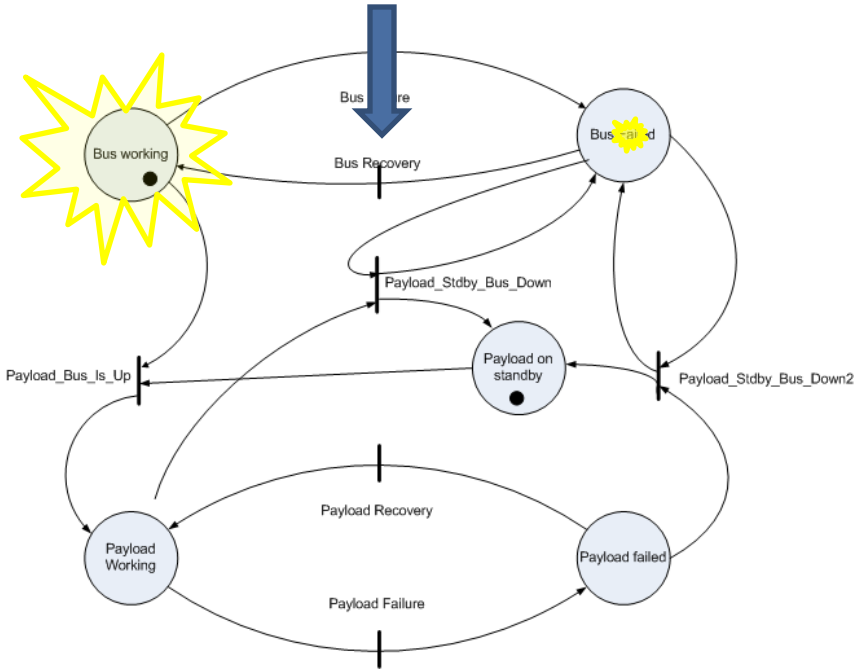


Petri Tree

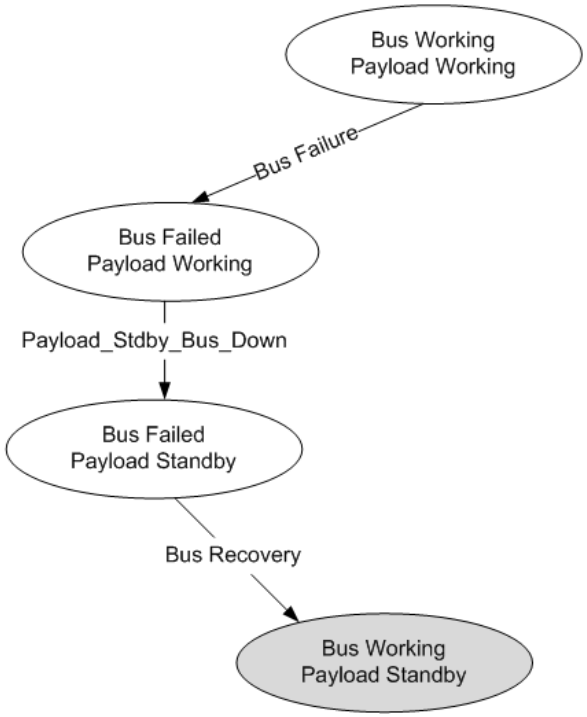


Bus Working, Payload on Standby

Petri Net

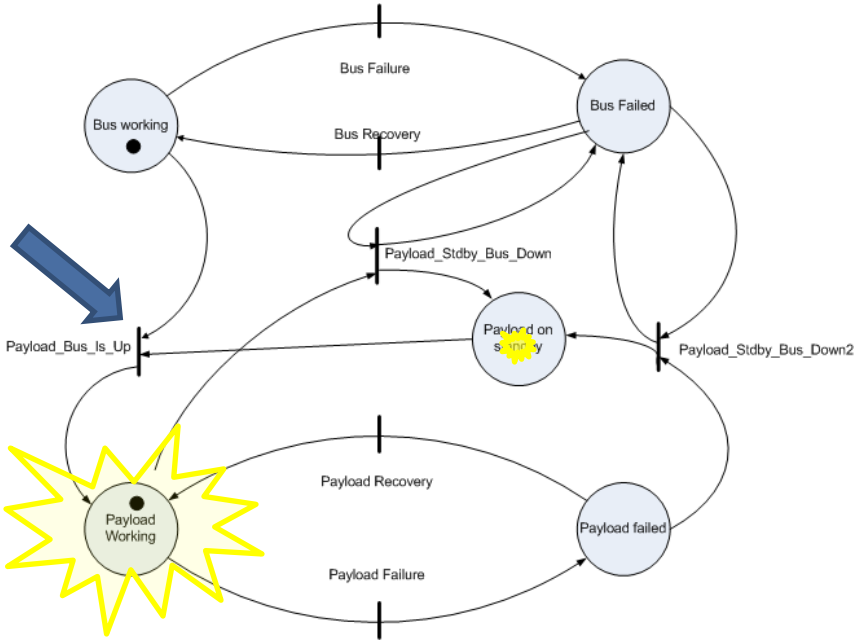


Petri Tree

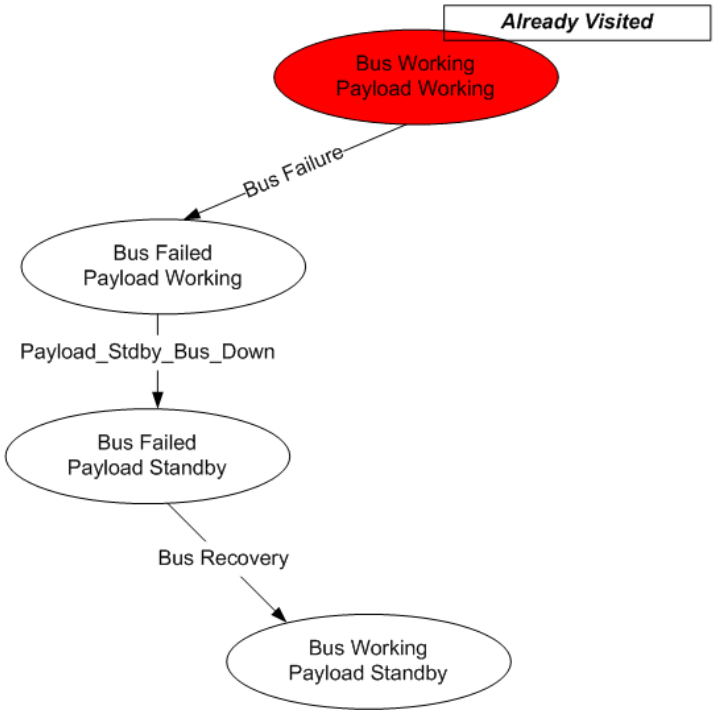


Bus Working, Payload Working (already visited)

Petri Net

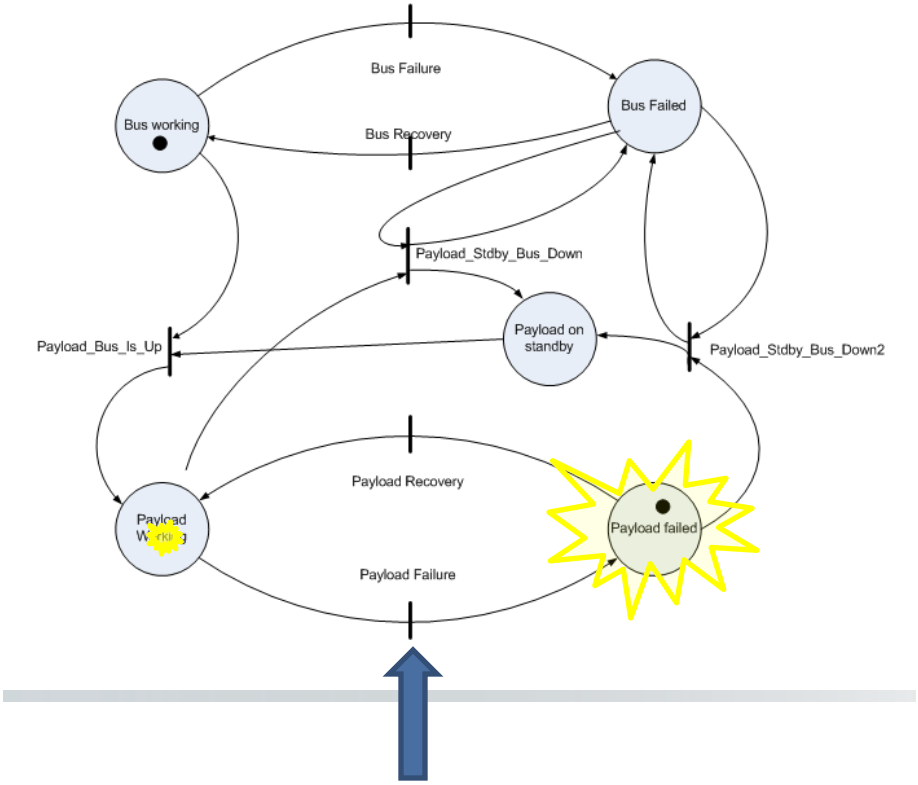


Petri Tree

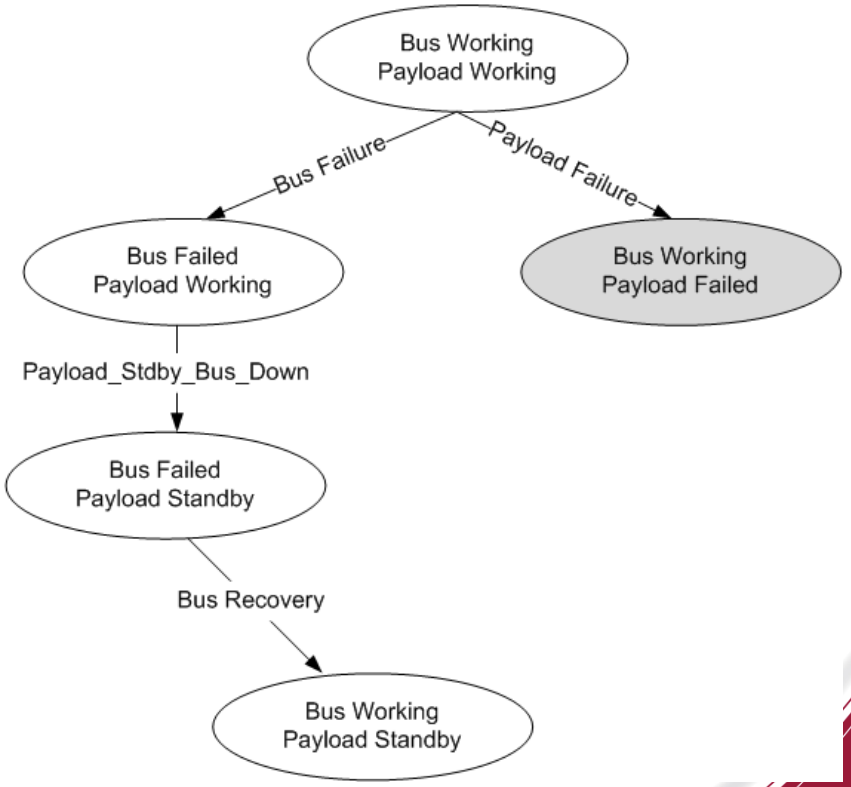


Bus Working, Payload Failed

Petri Net

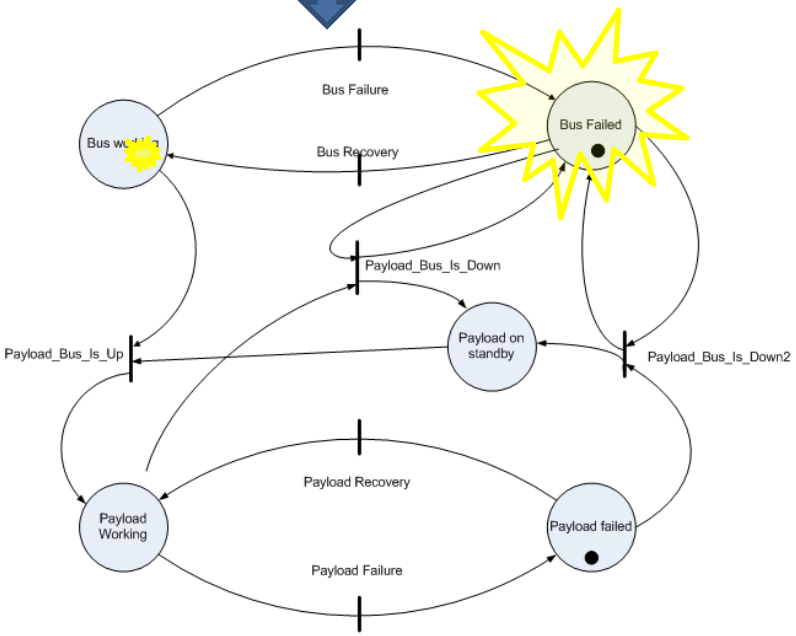


Petri Tree

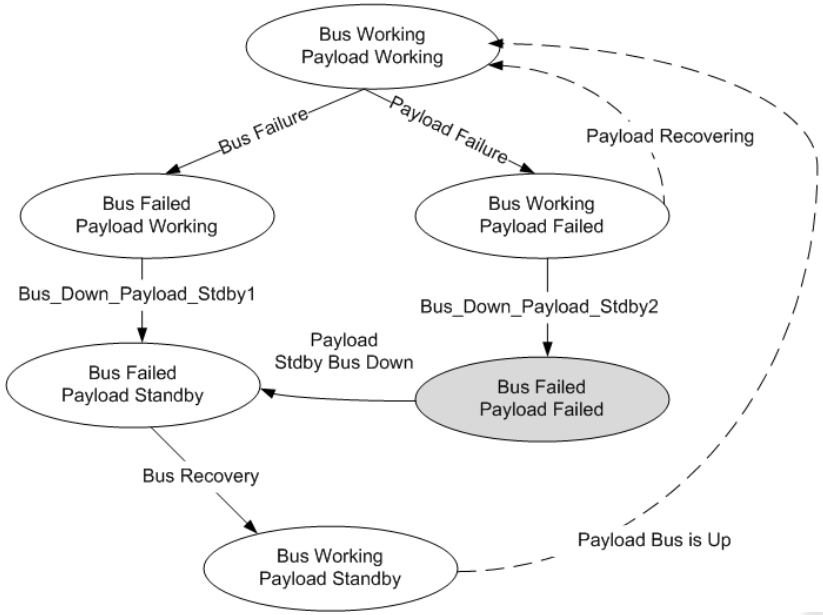


Bus Failed, Payload Failed

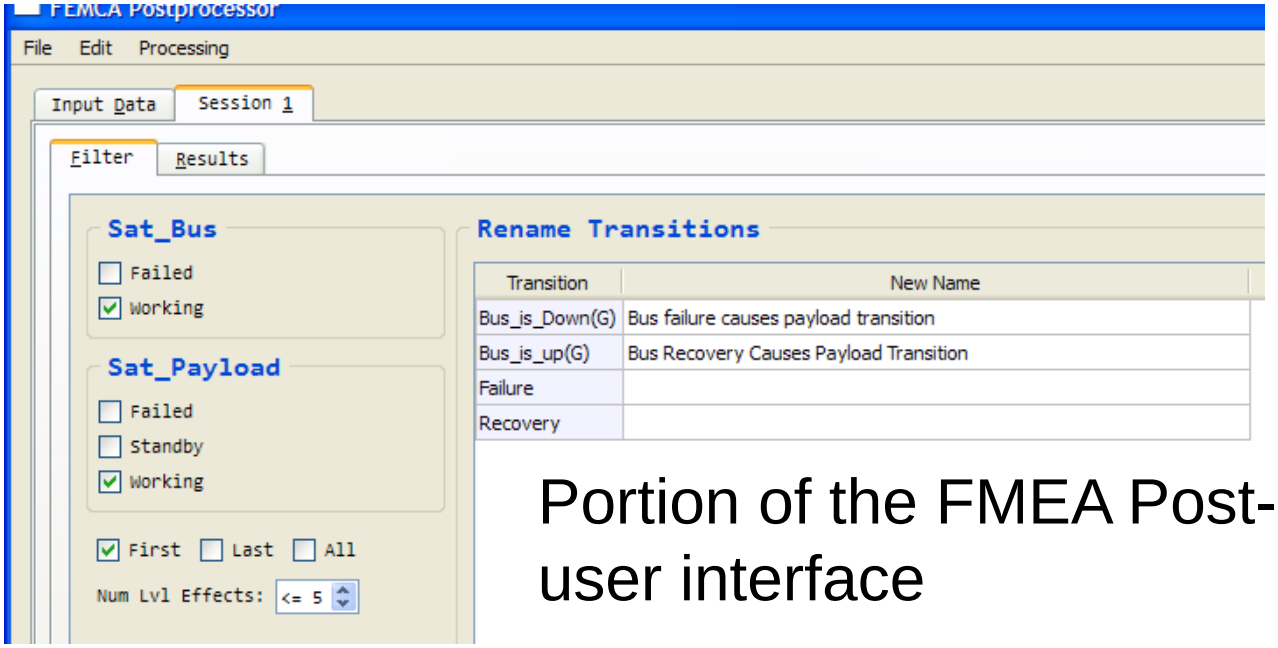
Petri Net



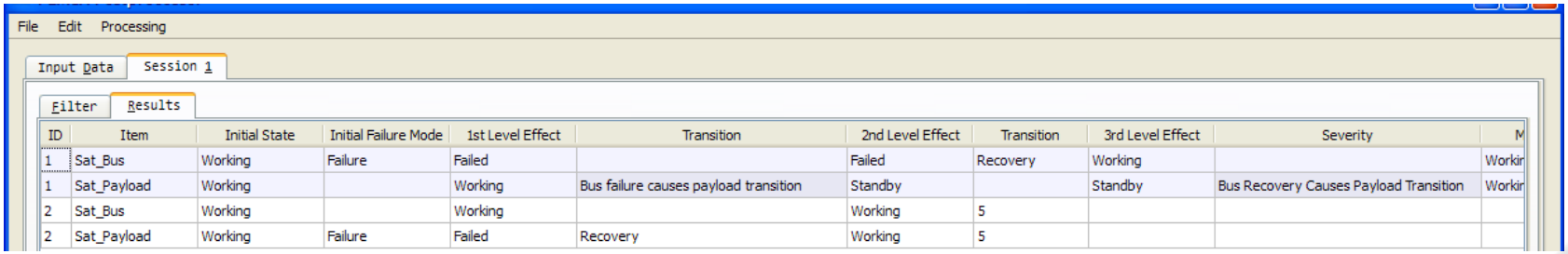
Petri Tree



Filtering the Results



Portion of the FMEA Post-processing tool user interface



ID	Item	Initial State	Initial Failure Mode	1st Level Effect	Transition	2nd Level Effect	Transition	3rd Level Effect	Severity	M
1	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Workir
1	Sat_Payload	Working		Working	Bus failure causes payload transition	Standby		Standby	Bus Recovery Causes Payload Transition	Workir
2	Sat_Bus	Working		Working		Working	5			
2	Sat_Payload	Working	Failure	Failed	Recovery	Working	5			

Fragment of the resultant FMEA

Postprocessing Tool Output Examples

FMEA Generator Original Output

Failure	Component	State	Transition	Effect	Transition2	Effect2	Transition3	Effect3	Transition4	Effect4	Severity
1	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Working	5
1	Sat_Payload	Working		Working	Bus_is_Down(G)	Standby		Standby	Bus_is_up(G)	Working	5
2	Sat_Bus	Working		Working		Working					5
2	Sat_Payload	Working	Failure	Failed	Recovery	Working					5
3	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Working	5
3	Sat_Payload	Failed		Failed	Bus_is_Down(G)	Standby		Standby	Bus_is_up(G)	Working	5

Renaming Rule

Failure	Component	State	Transition	Effect	Transition2	Effect2	Transition3	Effect3	Transition4	Effect4	Severity
1	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Working	5
1	Sat_Payload	Working		Working	Bus Failure Prop.	Standby		Standby	Bus Recover Prop	Working	5
2	Sat_Bus	Working		Working		Working					5
2	Sat_Payload	Working	Failure	Failed	Recovery	Working					5
3	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Working	5
3	Sat_Payload	Failed		Failed	Bus Failure Prop.	Standby		Standby	Bus Recover Prop	Working	5

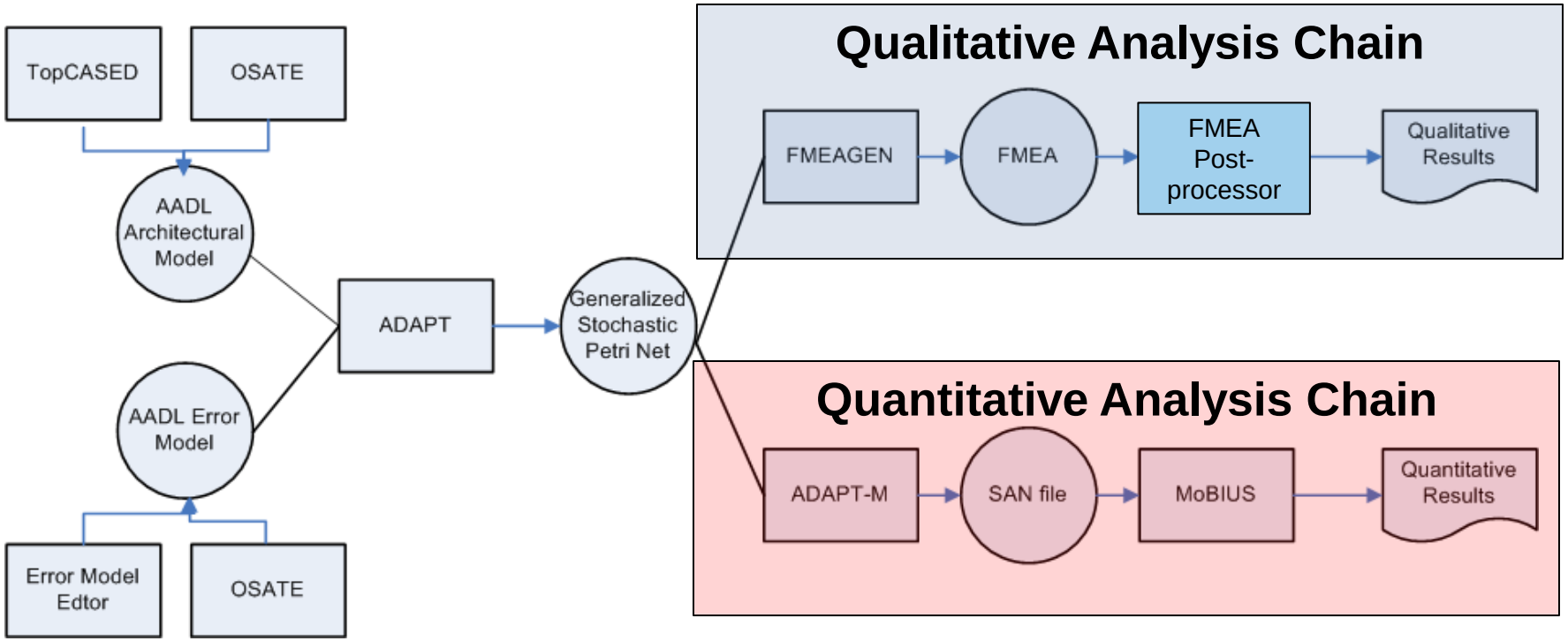
Filtered Output

Failure	Component	State	Transition	Effect	Transition2	Effect2	Transition3	Effect3	Transition4	Effect4	Severity
1	Sat_Bus	Working	Failure	Failed		Failed	Recovery	Working		Working	5
1	Sat_Payload	Working		Working	Bus Failure Prop.	Standby		Standby	Bus Recover Prop	Working	5
2	Sat_Bus	Working		Working		Working					5
2	Sat_Payload	Working	Failure	Failed	Recovery	Working					5

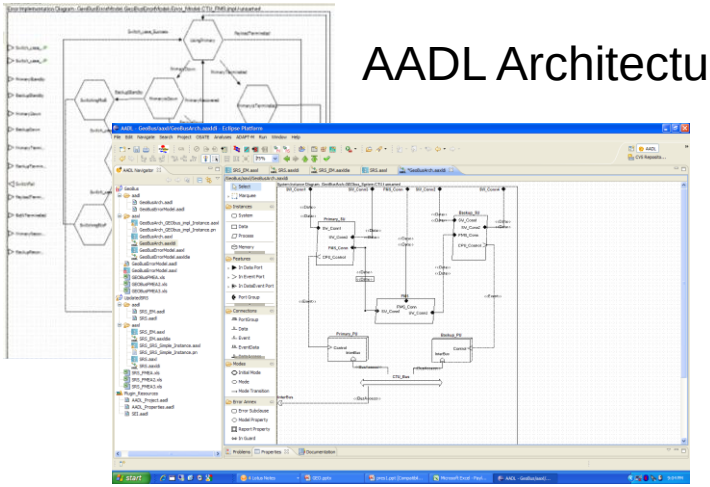
Model Driven Design and Analysis Workbench Tool Set

- 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)*
  - ***FMEA Post-Processor*** *(The Aerospace Corporation newly developed)*

Model Driven Design and Analysis Data Flow

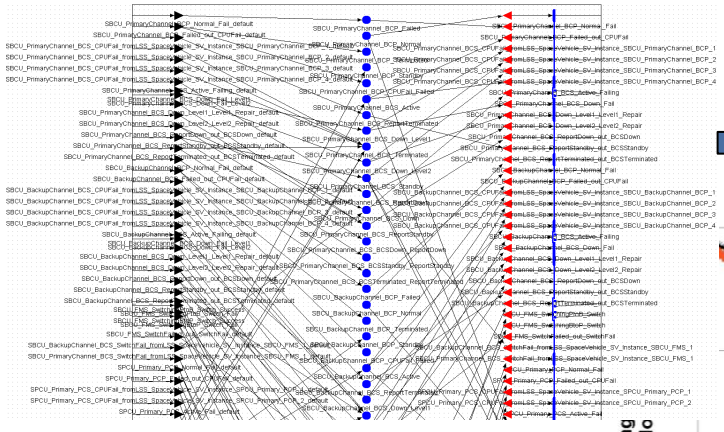


Tool Set Capabilities for Quantitative Evaluation

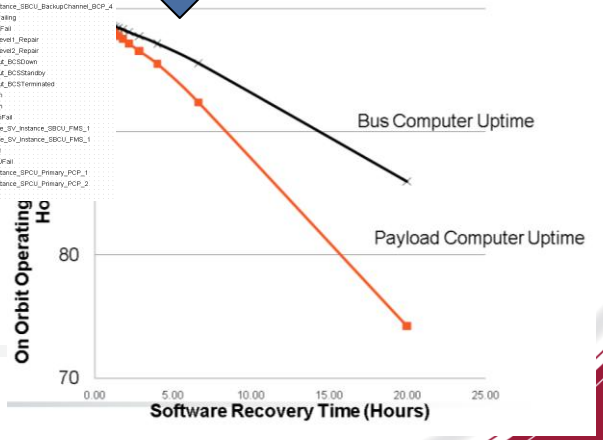


AADL Architecture and Error Models

Mobius Stochastic Analysis Network Model



Results



Discussion: Recent Experience

- Largest analysis to date consists of 26,000 failure modes,
  - *More detailed model of satellite bus*
  - *500 Mbyte output file*
  - *20 states perform failure mode*
  - *Longest failure mode sequences have 25 transitions (i.e., 25 effects)*
- Care must be used in creation of models
  - *Some legal constructs have unpredictable side effects*
    - Multiple simultaneous instantaneous transitions
    - Propagations on transitions as opposed to states
    - Event propagation using name matching rather than explicit guard interfaces
  - *Automated approach means that many technically insignificant failure mode sequences are produced*
    - Example: failure/recovery sequences on some components in combination with termination sequences on others; termination sequence dominates irrespective of what other failure/recovery occurs

Conclusions

- A new generation tool set for 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
- Additional work is needed to create an “industrial strength” capability
  - *Proper representation of event and error propagations*
  - *Use of instantaneous transitions*
  - *Syntax checker to avoid errors*
  - *Model design rules to create more reasonably sized FMEA tables*

References

- Society of Automotive Engineers (SAE) AS-2c Committee, SAE Architecture Analysis and Design Language (AADL) Annex Volume 1: Annex A: Graphical AADL Notation, Annex C: AADL Meta-Model and Interchange Formats, Annex D: Language Compliance and Application Program Interface Annex E: Error Model Annnex, June 2006, available online http://standards.sae.org/as5506/1/ (charges apply).
- Behavior, Data Modeling, and ARINC653 Annex Compendium, (in progress), http://standards.sae.org/wip/as5506/2.
- TOPCASED consortium home page, http://www.topcased.org, last visited June 27, 2010.
- Software Engineering Institute, AADL OSATE home page, http://www.aadl.info/aadl/currentsite/tool/toolsets.html, last visited June 27, 2010.
- Eclipse Foundation Open Source Community Website, http://www.eclipse.org/, last visited December 15, 2010
- Eclipse Foundation Modeling Documentation – Eclipspedia, http://wiki.eclipse.org/Modeling, last visited December 15, 2010
- 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).
- M. Hecht, A. Lam, C. Vogl “A Tool Set for Integrated Software and Hardware Dependability Analysis Using the Architecture Analysis and Design Language (AADL) and Error Model Annex”,Proc ICECCS 2011, Las Vegas, NV, May 2011