Phase Two Feasibility Study for Software Safety Requirements Analysis Using Model Checking

NASA Formal Methods Symposium

April 13, 2010

Greg Turgeon
PPT Solutions, Inc.
Huntsville, Alabama

Agenda

- Introduction
- Overview of System
- Methodology
  - Stages of Analysis
  - Toolset
- Results
  - Defects
  - Assumptions
  - Safety Properties
- Return on Investment
- Ending Thoughts

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Introduction

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Introduction

- Overall goal is to utilize more objective techniques for analyzing software system safety
- Approach uses formal methods techniques and tools that are gaining acceptance in industry
- Study used model checking to analyze a sample system
- Phase 1 used a tool from Rockwell Collins
- Phase 2 used a COTS tool, SCADE

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Phase 1 Conclusions

- Tool set was useful in detecting potential safety issues.
- Could not model entire system at once. Had to partition it.
- Training in MATLAB/Simulink and the Rockwell tools plus college level math necessary.
- 15% of SRS modeled in 1200 labor hours. Training and learning the tools was a significant portion of the hours.

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Goals of Phase 2

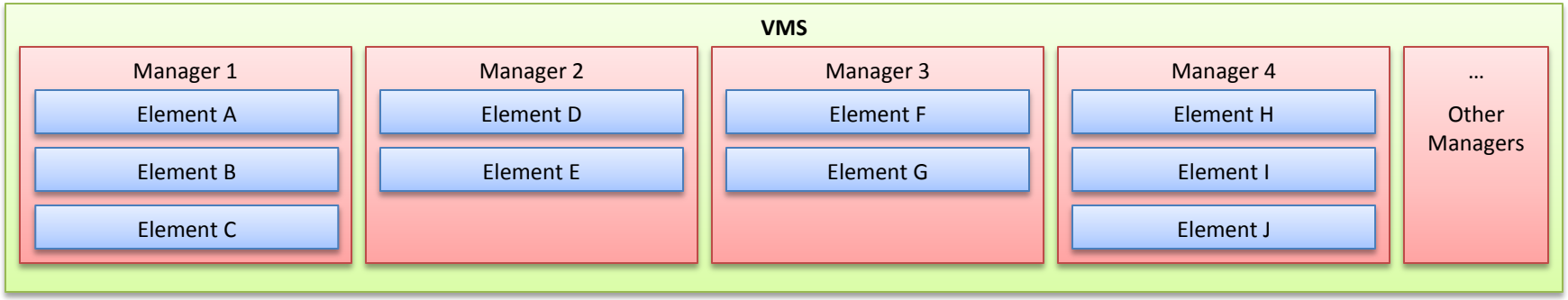
- Examine other tool sets for scalability and ease of use
- Determine metrics for rate of development, assumptions per requirement, and defects per requirement
- Create training package to complement existing Simulink and Gryphon training

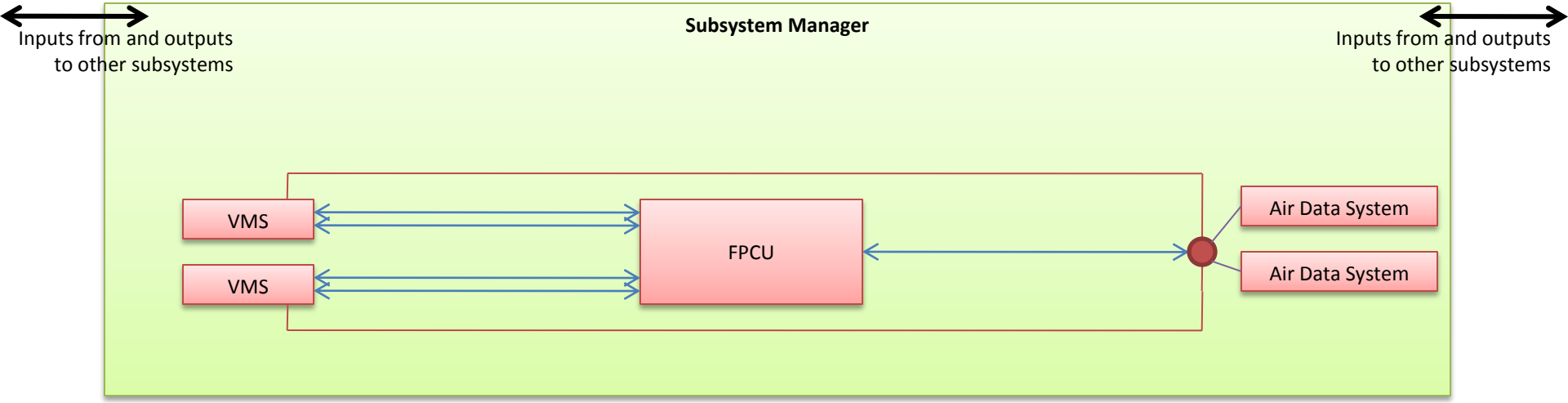
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Overview of System

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Description of Sample System

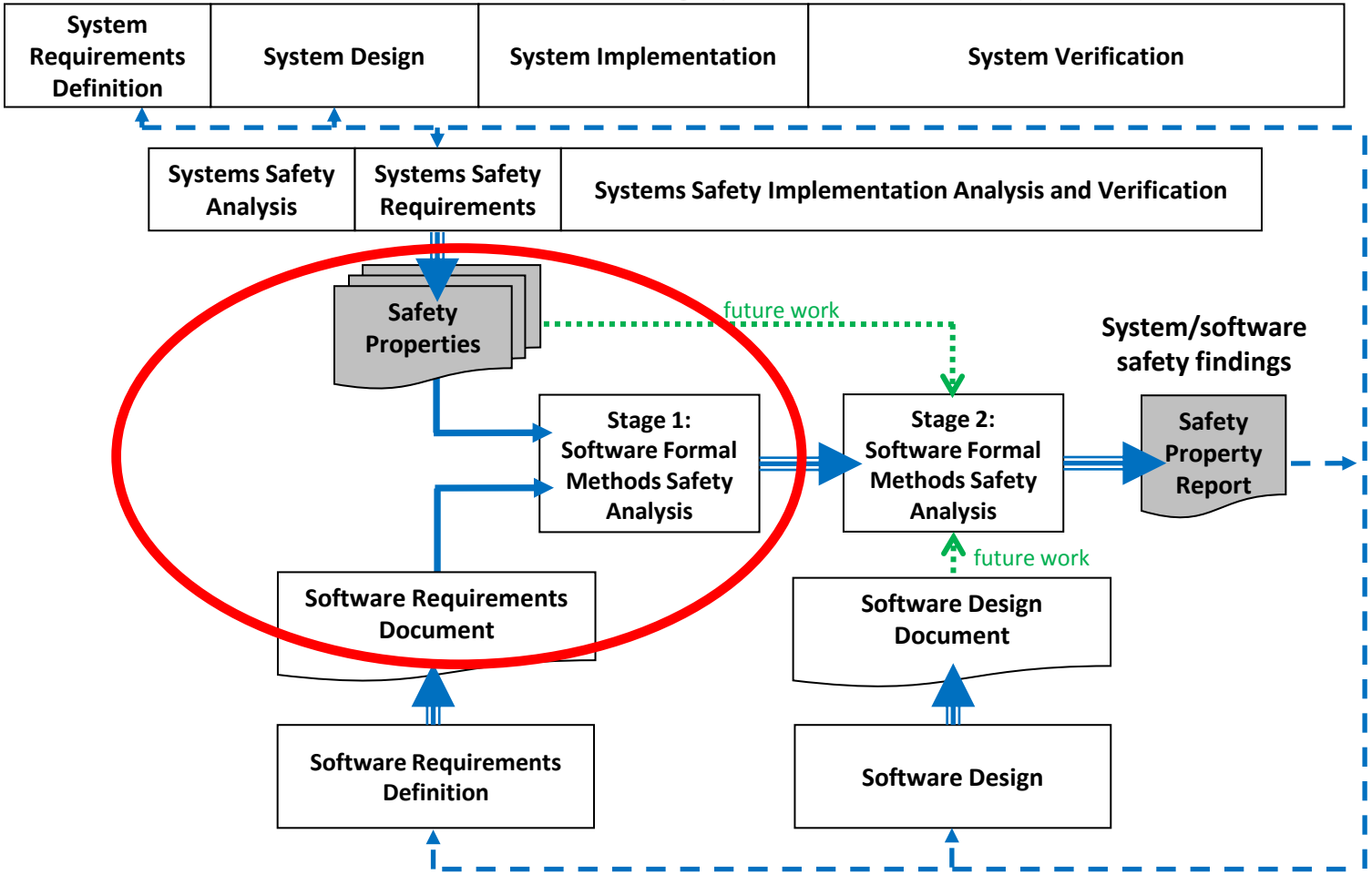




Methodology

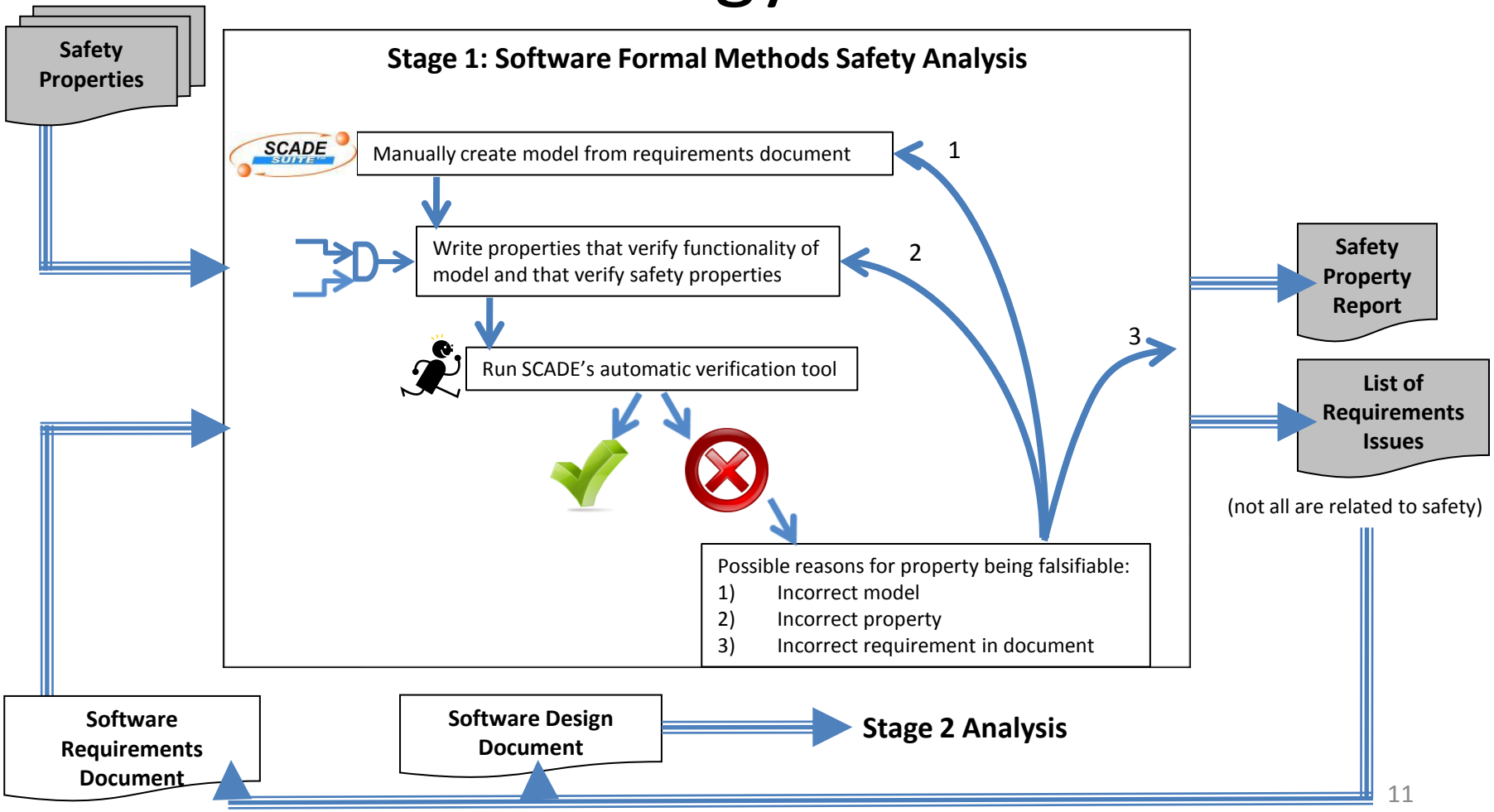
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Methodology - Lifecycle



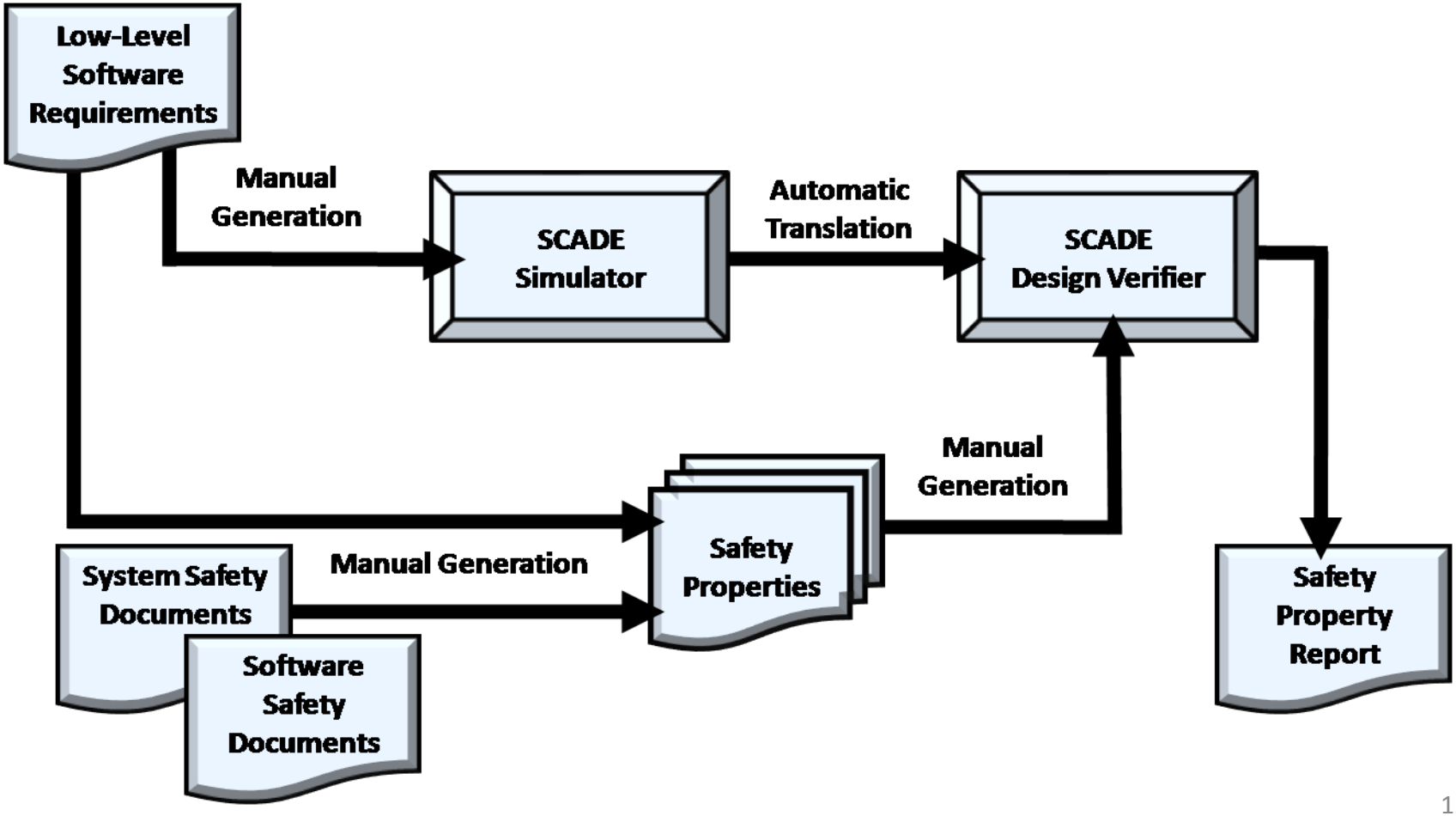
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Methodology – SCADE



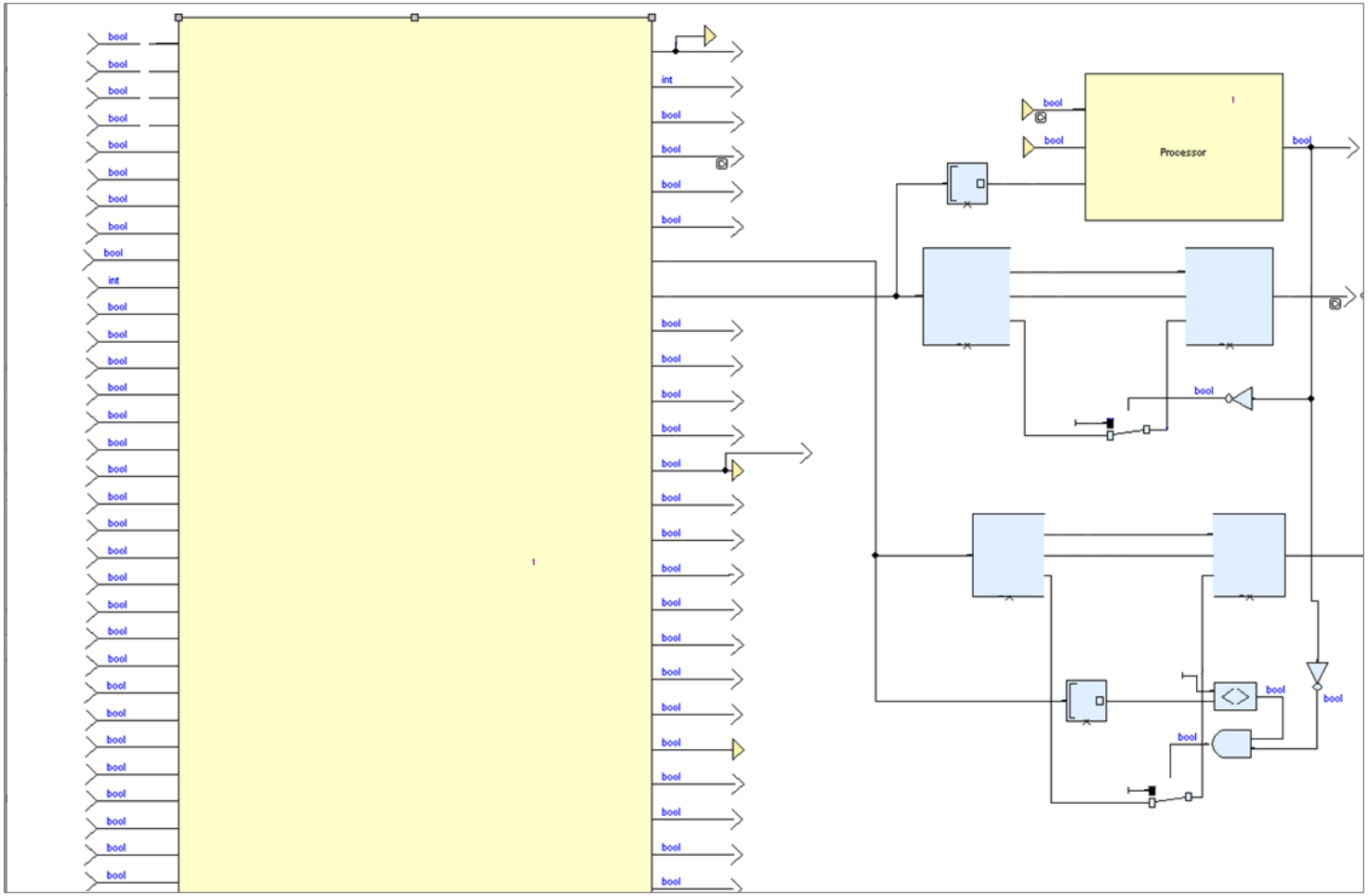
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Safety Analysis Tool Set



www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

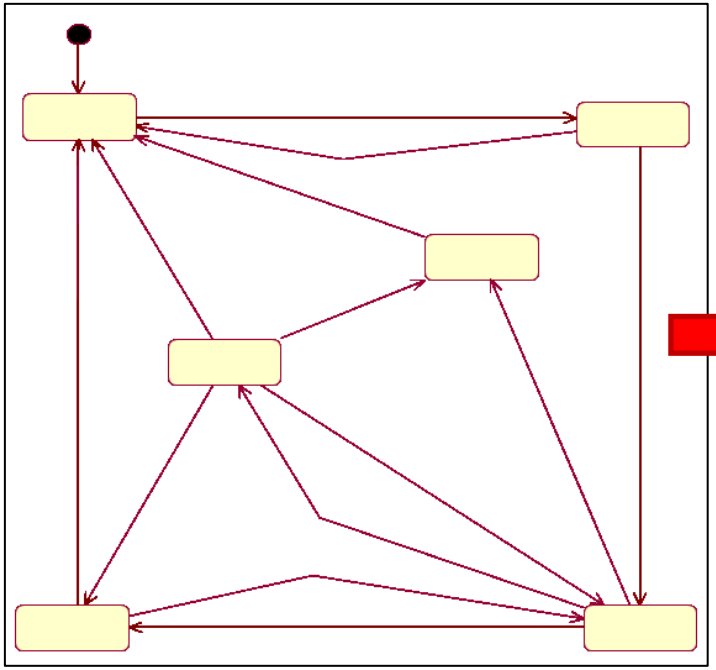
Portion of SCADE Model



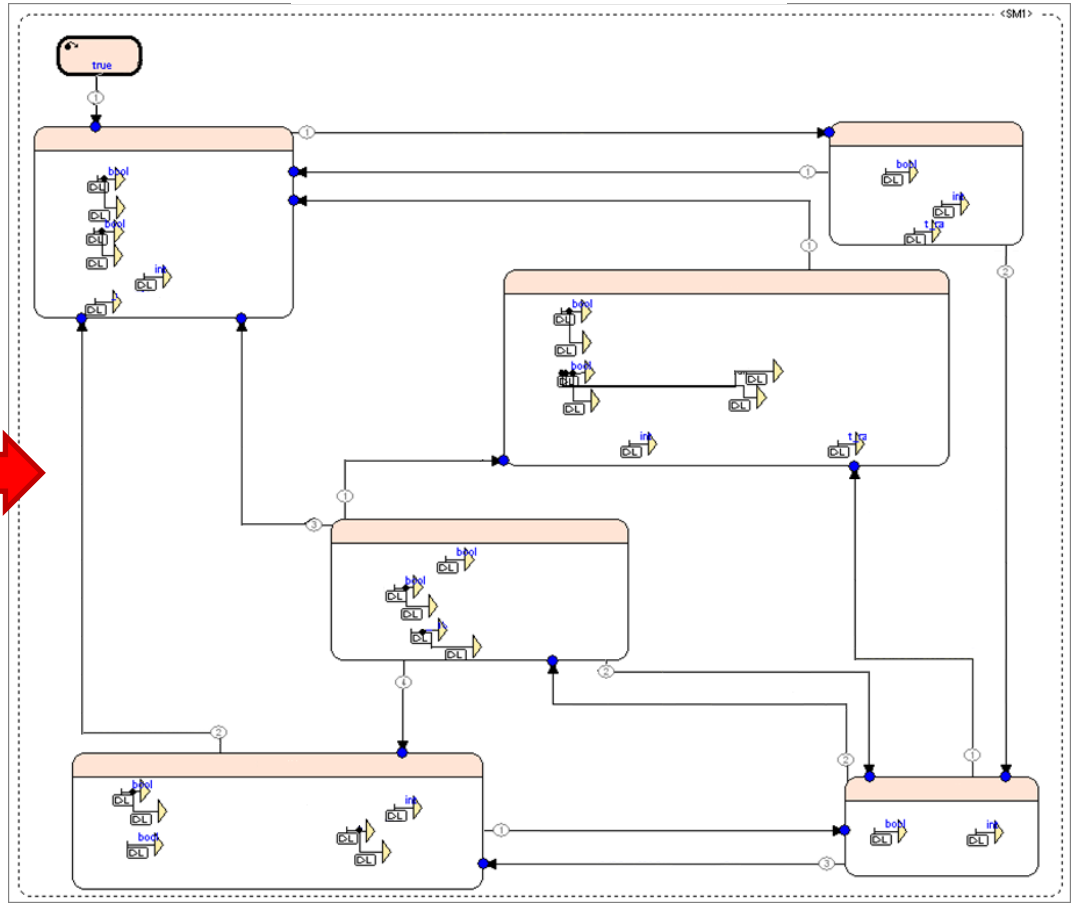
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Portion of SCADE Model – State Transitions

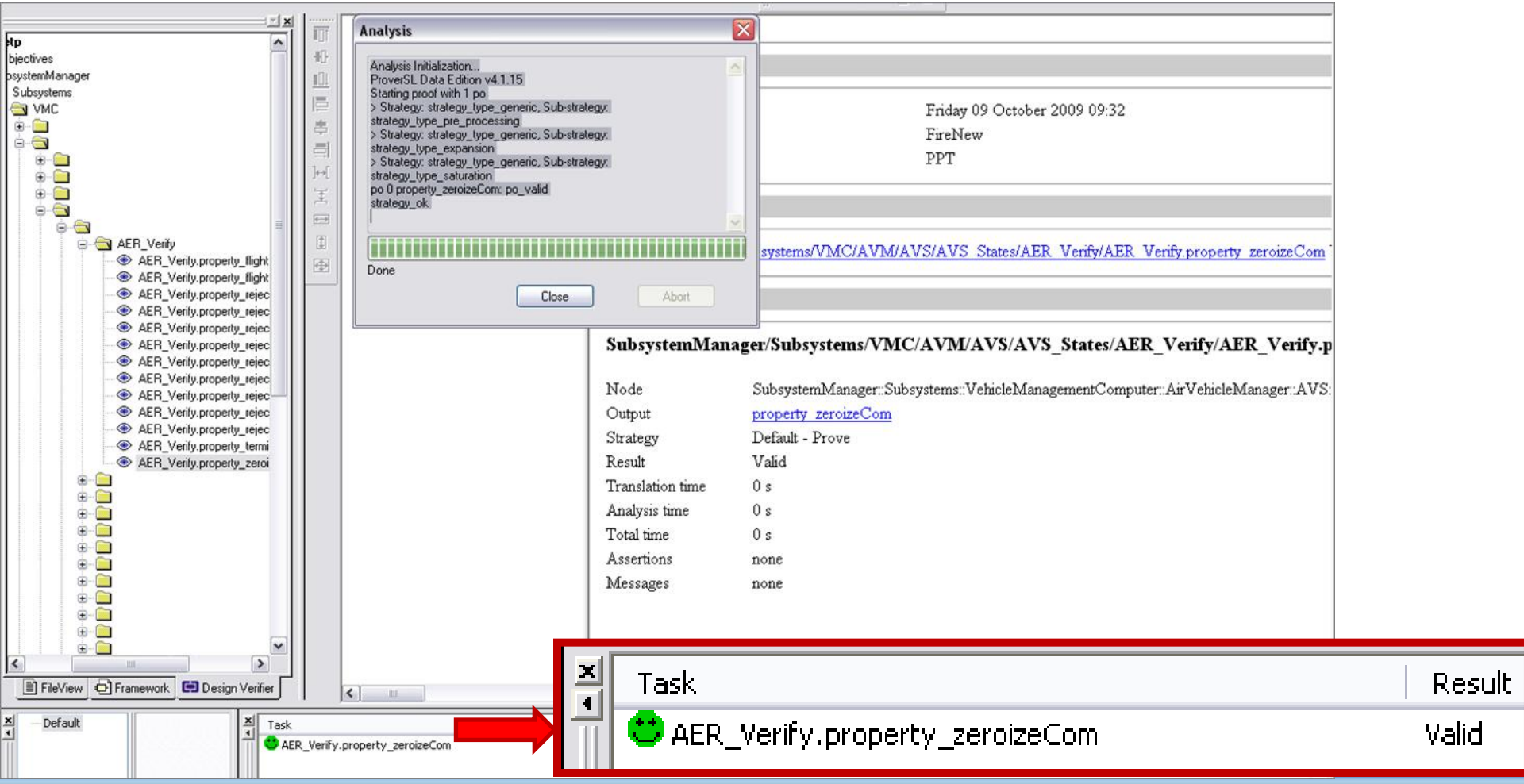
Diagram from the SRS



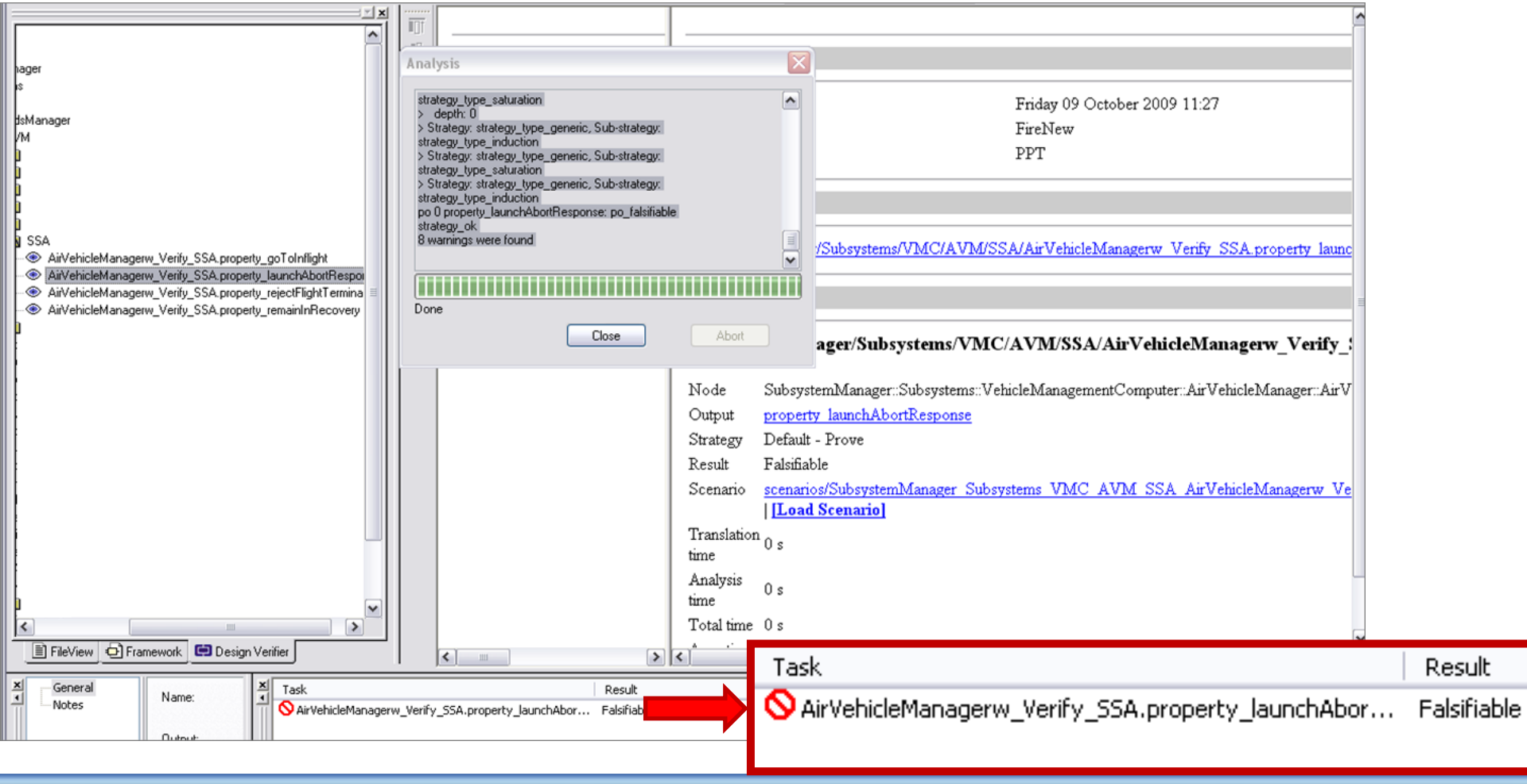
SCADE implementation



Obtain Result (automatic)



Obtain Result (automatic)



Results

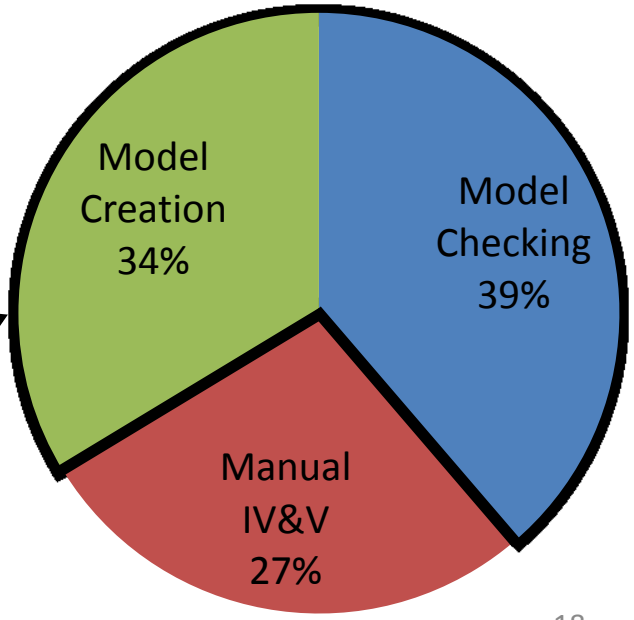
www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Defects Detected

- Total Number of Requirements Modeled: 925 (82% of SRS)
  - Other 18% either didn't add value to the model or were unrelated to software.

- Total Number of Requirements Defects Found: 198
  - Found through manual IV & V: 54 (27%)
  - Found through creation of model: 67 (34%)
  - Found as a result of model checking: 77 (39%)
- Formal methods approach using SCADE method found 144 defects (73% of all defects found) traditional IV&V would miss.

Possible Defects



www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Example Defects

Method of Detection	Requirement and Defect
Manual IV&V	*If in State A and Input I is true, go to State S.* *If in State A and Input I is true, go to State T.* Requirements conflict because states S and T are mutually exclusive.
Model Creation	*If the VMS is Master and the other VMS fails, then it shall remain Master.* What if the VMS is Slave and the other VMS fails? No requirement for this situation.
Model Checking	*If the Launch Abort Command input is true, then the launch abort sequence should begin.* Modeled property shows a counterexample where receiving a “Launch Abort Command” does not result in the software signaling to abort the launch sequence.

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Assumptions

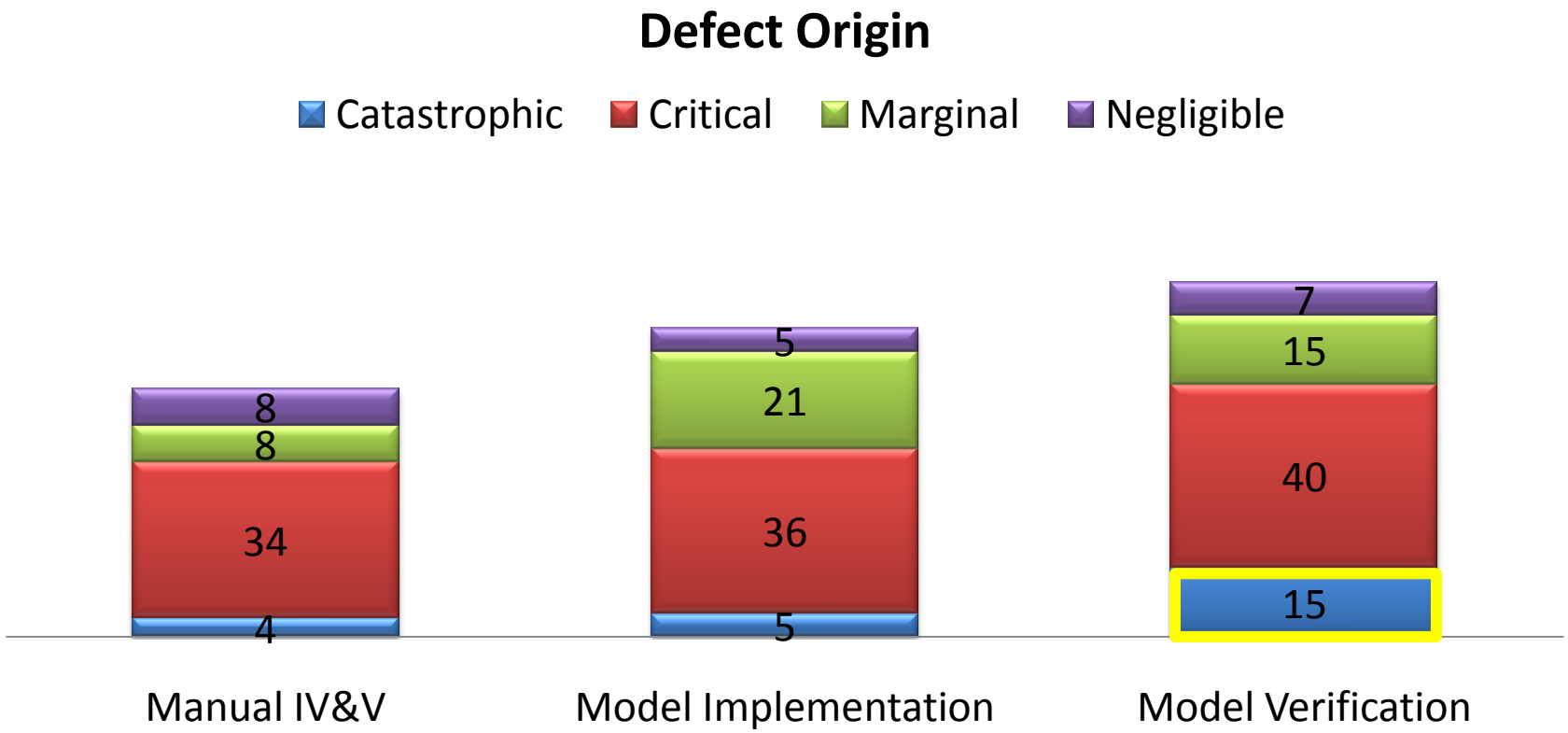
- Made 121 assumptions, or about 1 assumption for every 7.6 requirements.

Requirement	Assumption
If the VMS is in State S and is the master, it shall send a synchronization message to the other VMS.	The VMSs are communicating.
Thirty-five seconds after power up, the VMS shall begin periodic communications with the other VMS on the datalink.	“Periodic” communications occur on every cycle.
When counting the number of times Event E occurs, the software shall not log more than the limit specified in the spreadsheet.	The name of the spreadsheet and where to find it are not indicated. Assumed that the limit was a constant.
The software shall read the RT address of its terminal to determine its own identity.	The RT address signal is latched.

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Defect Criticality Breakdown

62.5% of all “Catastrophic” defects were found through Model Verification.



www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Example Safety Properties

- Modeled 215 safety properties.
- 68 (32%) evaluated to false and returned a counterexample.

Safety Property	Verification Operator Implemented As	Returned
If the datalink is broken, can both VMSs be master?	After the first cycle, if VMS_A is not communicating and VMS_B is not communicating, then VMS_A is not master or VMS_B is not master.	false
An invalid VMS is declared halted.	If a VMS is not valid, then it is in the halted state.	false
If the engine oil temperature is out of range a fault will be set.	If the oil temp is less than -50 or greater than 110, then oilTempFault will be true.	false
Before the engine started message is sent, the engine start request message must be received.	Is it true that the signal engineStartComAccepted has never been true and the signal engineRunning is true?	false

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

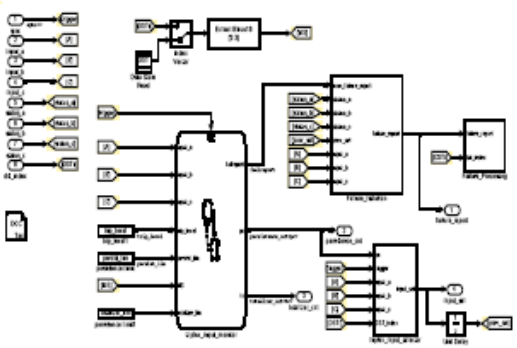
Similar Results by Other Companies

Rockwell Collins

Subtle Errors – LM Aero UAV Sensor Voting

OFP Triplex Voter

- 96 Simulink Subsystems
- 3 Stateflow Diagrams
- 6×10^{13} Reachable States



Formal Verification

- 25 Informal Requirements
- 57 Formal Properties
- 40 Minutes to Analyze

10^{100+} reachable states in Rockwell examples

Resulting In

- 24 Counterexamples
- 10 Design Modifications
- Several Requirements Clarifications

Formal verification has found subtle errors that would likely be missed by traditional testing.

- Lockheed Martin

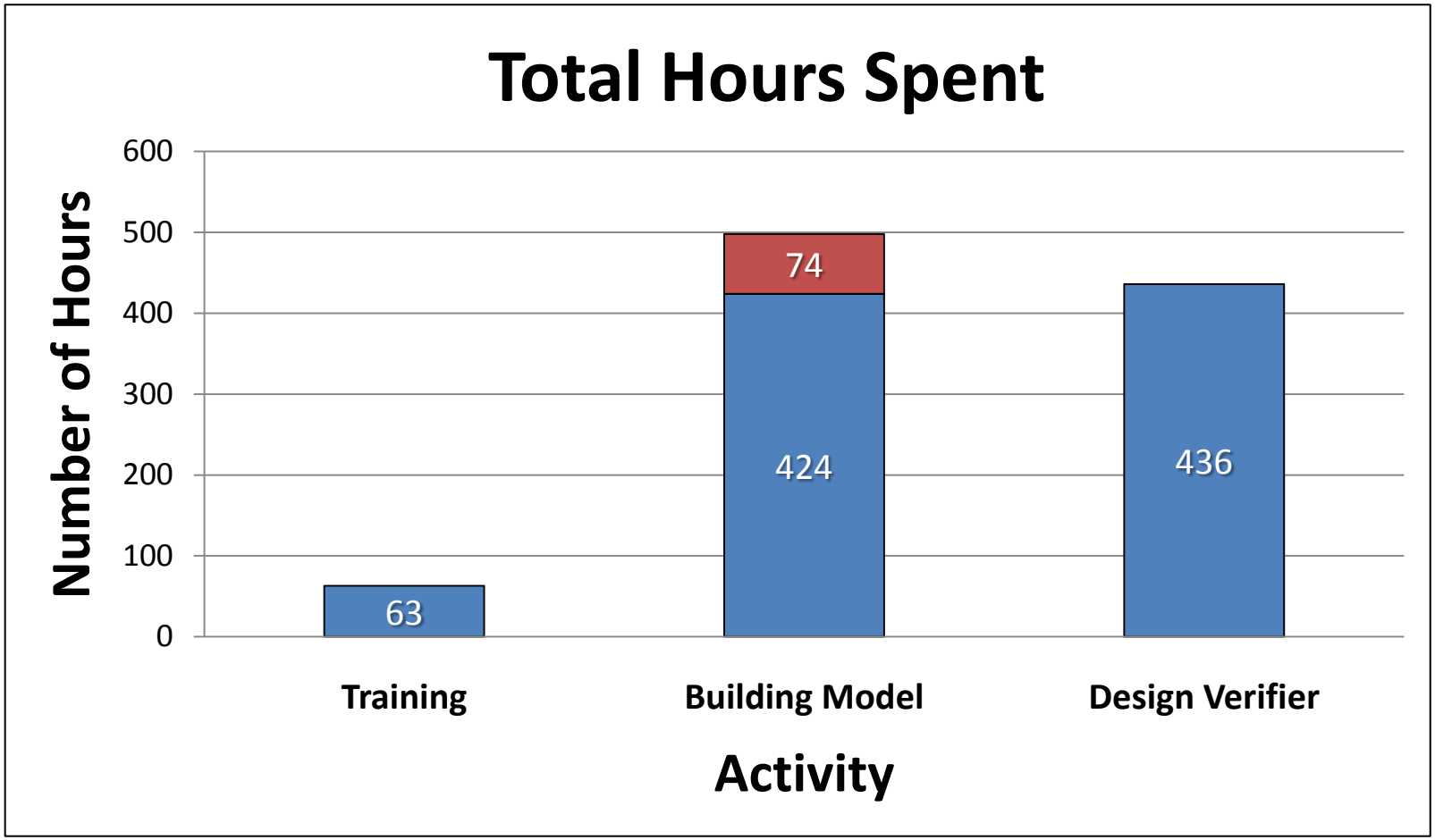
© 2006 Rockwell Collins, Inc. All rights reserved.

56

Slide from the course *Model-Based Engineering with the SAE AADL* by the Software Engineering Institute, October 2009.

Return on Investment

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815



925 requirements modeled / 934 hours ≈ 1 requirement per hour

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Example of the Frequency (%) of Where Errors Are Found, in Relationship to Where They Were Introduced

Where Errors are Introduced (%)	Where Errors Are Found					
	Requirements Gathering and Analysis/Architectural Design	Coding/Unit Test	Integration and Component Test	Early Customer Feedback/Beta Test Programs	Post-product Release	Total
Requirements Gathering and Analysis/Architectural Design	3.5 ($1x)	10.5 ($5x)	35 ($10x)	6 ($15x)	15 ($30x)	70
Coding/Unit Test		6 ($1x)	9 ($10x)	2 ($20x)	3 ($30x)	20
Integration and Component Test			6.5 ($1x)	1 ($10x)	2.5 ($20x)	10
Total	3.5	16.5	50.5	9	20.5	100 %

Taken directly from NIST Table 5-2 and 5-3

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Return on Investment
Requirements Review Savings

- Assumptions
  - Entire Project: 45,550 man hours (based on known LOC)
  - Entire Project : 20% of lifecycle in requirements phase
  - Entire Project : 25% of requirements phase spent in review
  - Entire Project : Therefore, **2278** man hours in requirements review
- PPT spent **1376** total man hours on this effort
  - Or, 40% less time spent in requirements review

Assumptions based on metrics from *Introduction to the Team Software Process* by Watts S. Humphrey.

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Return on Investment
Early Requirements Defect Removal

- We found 144 defects in the requirements phase that otherwise would not be found until later phases
- Effort to fix those 144 defects later in the lifecycle is approximately 3500 man hours
- Assuming a savings of 3500 man hours and $100 per man hour, early defect removal savings is **$350K**
- PPT cost to perform formal methods analysis: **-$137K**
- Net savings of **$213K** or 5% of the total project

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Ending Thoughts

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Conclusions

- Usability
  - SCADE is easy to learn and similar to Simulink
- Scalability
  - 80% + of requirements modeled
  - No problems with state space or execution time
  - No partitioning required
- Personnel requirements
  - Degree in a technical field
  - Training in SCADE
- Metrics
  - About 1 requirement modeled and verified per hour
  - Found about 1 defect per every 4.7 requirements
  - Made 1 assumption per every 7.6 requirements

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Future Activities

- Use this technique more widely for IV&V
- Investigate SCADE for other uses throughout the software lifecycle
  - Automatic code generation
- Investigate other requirements specification methods (DOORS, UML)
- Apply technique to PLDs to realize cost savings and reduce rework

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815

Sources

- NIST Planning Report 02-3. "The Economic Impacts of Inadequate Infrastructure for Software Testing," May 2002. http://www.nist.gov/director/prog-ofc/report02-3.pdf, last viewed December 2009.
- *Hands-on Modeling with the SAE AADL*, Software Engineering Institute, course given October 5-6, 2009.
- Esterel Technologies. http://www.esterel-technologies.com/, last viewed December 2009.
- Watts S. Humphrey. *Introduction to the Team Software Process*. Addison Welsey, 2000.
- Greg Turgeon and Petra Price. "Feasibility Study for Software Safety Requirements Analysis Using Formal Methods." Presented at the 27th International System Safety Conference, Huntsville, Alabama, August 2009. Available for purchase at http://www.system-safety.org/products/.

www.pptsinc.com P 256.319.1550 F 256.319.1553 4825 University Square, Suite 6 Huntsville, AL 35816-1815