Final Report | 2011

FA 9550-08-1-0139 & FA9550-08-1-0158

A Framework for Designing Reliable Software-Intensive Systems

Table of Contents

Final Report | 2011

FA 9550-08-1-0139 & FA9550-08-1-0158

COVER

PI Names:

I.Y. Tumer

School of Mechanical, Industrial and Manufacturing Engineering
Oregon State University
Corvallis, Oregon, USA

C. Smidts

Mechanical and Aerospace Engineering
Ohio State University
Columbus, Ohio, USA

Grant/ Contract Title: A Framework for Designing Reliable Software-Intensive Systems

Grant/ Contract Number:

Oregon State University, PI: Irem Tumer: FA9550-08-1-0158

Ohio State University, PI: Carol Smidts: FA 9550-08-1-0139

Reporting Period (Start): 10/31/2008

Reporting Period (End): 11/30/2010

Program Manager: David Luginbuhl

Changes in Research Objectives: None

Changes in Program Manager: None

Extensions Granted and Milestones if Any: None

Attach report if Any: MS thesis for David Jensen (2009) and Chetan Mutha (2011)

Executive Summary

This project involved a joint research performed primarily at Oregon State University and "The Ohio State University. Software-driven hardware configurations account for the majority of modern safety-critical complex systems. The often costly failures of such systems can be attributed to software specific, hardware specific, or software/hardware interaction failures. The understanding of how failures propagate in such complex systems might provide critical information to designers, because, while a software component may not fail in terms of loss of function, a software operational state can cause an associated hardware failure. The least expensive phase of the product life cycle to address failures is during the design stage. This research presents a means to evaluate how a combined software/hardware system behaves and how such failures propagate to result in potential failures downstream, during the conceptual design stage. In particular, this research proposes the use of high-level system modeling and model-based reasoning approaches to model failure propagation in combined software-hardware systems, based on the Function-Failure Identification and Propagation (FFIP) analysis framework to help formalize the design of safety-critical systems.

The main contribution of the research is the "Integrated Failure Analysis Methodology", developed to analyze complex hardware-software systems in a coherent manner. This integrated approach is a unification of two different approaches namely, Fault Failure Identification and Propagation (FFIP) and Fault Propagation and Simulation Approach (FPSA), used to analyze hardware and software design respectively. The following provides the details of joint research activities between the two institutions:

- Completed mapping between elements of different Unified Modeling Language (UML) diagrams.
- Formulated a software fault propagation and effect analysis approach called Fault Propagation and Simulation Approach (FPSA) which allows us to propagate faults throughout a software design expressed using UML diagrams. Two variations of FPSA have been introduced, i.e. a high level and executable.
- Applied the software fault propagation and simulation approach to the case study of the Space Shuttle's Reaction Control System's (RCS) Helium tank sub-system.
- Established collaboration with the Institute for Energy Technology/OECD Halden Reactor Project in Norway which focuses on the study of Common Cause Failure propagation in digital nuclear reactor upgrades (which are planned for all reactors in the United States) and which will use the methodology in development for AFOSR (See: The OECD Halden Reactor Project).
- Performed a survey, analysis, and classification of software testing techniques relying on an operational profile (OP) and characterized the type and frequency of the software inputs during testing.
- Established an ontology-based approach used to verify UML model properties. The approach uses ontology related techniques and tools to represent UML knowledge and properties, specify models as instances of the ontology, and verify design correctness and completeness aspects.
- Formalized a hardware failure propagation methodology called Function-Failure Identification and Propagation (FFIP) analysis framework for extension to the software-hardware system design.

- Developed full set of models for an electrical power system test-bed, liquid rocket engine, and boiling water reactor and implemented failure scenarios using FFIP in Simulink and ModelCenter.
- Developed new logic rules based on flow state to handle failures (vs. nominal modes) using functional modeling and implemented rules on the 3 applications above.
- Started the design of an electro-mechanical actuator testbed using FFIP fundamentals to serve as a testbed for our methodology and tools, to be flown at NASA Ames on Airforce and Army platforms to test models and assumptions about actuator failure indicators derived using FFIP.
- Applied FFIP to the design-stage analysis of failures in a Boiling Water Reactor in collaboration with the Helsinki University of Technology; presented to STUK, Safety Authority for nuclear power in Finland (the equivalent of NRC in the United States.)
- Formulated an integrated approach for hardware-software fault propagation and failure identification at the early design stage. The integrated approach is based on the metamodel (Figure 1) which describes the relationships between the different hardware-software design elements.
- Transferred knowledge gained from the AFOSR project into a funded effort through DARPA's Meta-II program.

Cumulative list of people involved:

1. Prof. Carol Smidts, The Ohio State University, US
2. Chetan Mutha, The Ohio State University, US
3. Dr. Manuel Rodriguez, The Ohio State University, US
4. Prof. Irem Tumer, Oregon State University, US
5. David Jensen, Oregon State University, US
6. Josh Wilcox, Oregon State University, US
7. Sizarta Sarshar, EHPG, Halden, Norway
8. Prof. Eric Coatanea, Helsinki University of Technology, Finland
9. Dr. Seppo Sierla, Helsinki University of Technology, Finland
10. Dr. Tolga Kurtoglu, Mission Critical Technologies at NASA Ames Research Center, US

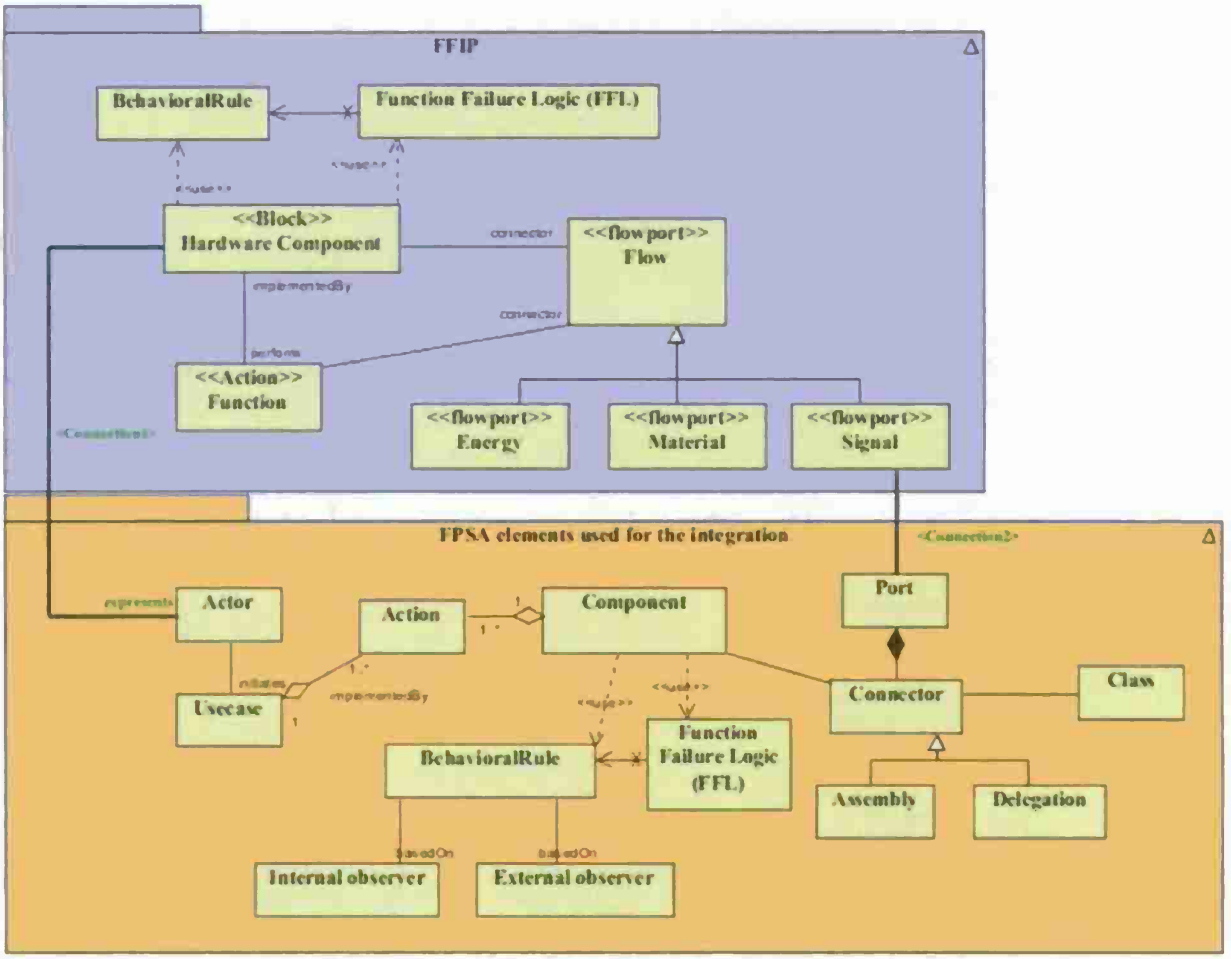

Figure 1: Metamodel of the Integrated System Failure Analysis Method

Publications (*electronic copies can be provided upon request*)

2008

Conference papers:

D. Jensen, I.Y. Tumer, and T. Kurtoglu, "Modeling the Propagation of Failures in Software-Driven Hardware Systems to Enable Risk-Informed Design." ASME 2008 International Mechanical Engineering Congress and Exposition, Safety Engineering, Risk Analysis, and Reliability Methods Track, Boston, MA. 2008.

Journal papers:

N/A.

Thesis & Reports:

N/A.

2009

Conference papers:

D. Jensen, I.Y. Tumer, and T. Kurtoglu, "Design of an electrical power system using a functional failure and flow state reasoning methodology". The 2009 Prognostics and Health Management Conference, PHM'09. October 2009, San Diego, CA.

D. Jensen, I.Y. Tumer, and T. Kurtoglu, "Flow State Logic (FSL) for analysis of failure propagation in early design". The 2009 ASME International Design Theory and Methodology Conference, IDETC/CIE2009. September 2009, San Diego, CA.

Journal papers:

N/A.

Thesis & Reports:

D. Jensen, "Design Analysis Using Function-Based Failure Propagation in Failed System States", MS Thesis, School of Mechanical, Industrial, and Manufacturing Engineering, Oregon State University. 2009.

2010

Conference papers:

C. Mutha, M. Rodriguez, C. Smidts, "*Design and Analysis of Safety Critical Software Using UML*". Proceedings of the Man-Technology-Organization Sessions, HPR-372 Vol. 2, C5.8, 2010.

S. Sarshar, C. Mutha, and C. Smidts, "Common Cause Failures: Status of the Collaborative Research on Assessment of a Power Range Monitoring System", Proceedings of the Enlarged Halden Programme Group Meeting (EHPG), March 2010.

C. Mutha, M. Rodriguez, and C. Smidts, "Software Failure and Error Propagation Analysis Using the Unified Modeling Language," International Probabilistic Safety Assessment Management Conference (PSAM). 2010.

E. Coatanea, T. Ritola, I.Y. Tumer, D. Jensen, "A framework for building behavioral models for design stage failure identification using dimensional analysis." *The 2010 ASME International Design Theory and Methodology Conference*, IDETC/CIE2010. Montreal, Canada. August 2010.

Journal papers:

T. Kurtoglu, D. Jensen, I.Y. Tumer, "A functional failure reasoning methodology for evaluation of conceptual system architectures". *Research in Engineering Design*. Vol. 21:209-234. 2010.

Thesis & Reports:

C. Smidts, J. McGill, P. Lakey, M. Rodriguez, "Operational Profile Testing", to appear in Encyclopedia of Software Engineering, Taylor & Francis Group, 29 pages, 2010.

2011

Conference papers:

D. Jensen, I.Y. Tumer, C. Mutha, and C. Smidts, "Functional Failure Analysis Of Complex Software-Hardware Systems: An Integrated Approach", ***submitted*** *to* ASME 2011 International Design Engineering Technical Conferences (IDETC) and Computers and Information in Engineering Conference (CIE). 2011.

N. Papakonstantinou, D. Jensen, S. Sierla, I. Tumer, "Capturing interactions and emergent failure behavior in complex engineered systems at multiple scales", ***submitted*** *to* ASME 2011 International Design Engineering Technical Conferences (IDETC) and Computers and Information in Engineering Conference (CIE). 2011.

Journal papers:

I.Y. Tumer and C.S. Smidts, "Integrated design and analysis of software-driven hardware systems." ***In print.*** IEEE Transactions on Computers. 2011.

C. Mutha, D. Jensen, I.Y. Tumer, and C. Smidts, "A Multi-Domain, Integrated Approach to Functional Failure Analysis of Complex System Design", ***submitted*** *to* ASME Journal of Mechanical Design Special Issue on Designing Complex Engineered Systems. 2011.

M. Rodriguez, and C. Smidts, "Software Testing with an Operational Profile: Survey, Analysis & Classification", ***submitted*** *to* ACM Computing Surveys. 2011

S. Sierla, I.Y. Tumer, N. Papakonstantinou, K. Koskinen, D. Jensen, "Early Integration of Safety to the Mechatronic System Design Process by the Functional Failure Identification and Propagation Framework", ***submitted*** to Mechatronics. 2011

D. Jensen, I.Y. Tumer, T. Kurtoglu, "Flow State Reasoning as a Framework for Failure Analysis During System Design", ***submitted*** to the ASME Journal of Mechanical Design. 2011.

E. Coatanea, S. Nonsiri, T. Ritola, I.Y. Tumer, D. Jensen, "Dimensional analysis based behavioral modeling for design-stage failure analysis", ***submitted*** to the ASME Journal of Mechanical Design. 2011.

Thesis & Reports:

C. Mutha, "Software fault failure and error propagation at early design stage using Unified Modeling Language", MS Thesis, Department of Mechanical and Aerospace Engineering, The Ohio State University. 2011.

Appendix A: Master Thesis by Mutha Chetan

Software fault failure and error analysis at the early design phase with UML

THESIS

Presented in Partial Fulfillment of the Requirements for the Degree Master of Science in the Graduate School of The Ohio State University

By

Chetan Mutha

Graduate Program in Mechanical Engineering

The Ohio State University

2011

Master's Examination Committee:

Prof. Carol Smidts, Advisor

Prof. Tunc Aldemir

Appendix B: Master Thesis by David Jensen

The thesis document can be found at the link below:

http://ir.library.oregonstate.edu/xmlui/bitstream/handle/1957/11874/2009%20Jensen%20Thesis%20Final.pdf?sequence=6

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03/35/2011	Final Report	10/31/2008-11/30/2010

4. TITLE AND SUBTITLE
A Framework for Designing Reliable Software-Intensive Systems

5a. CONTRACT NUMBER
FA9550-08-1-0158

5b. GRANT NUMBER
FA9550-08-1-0158

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Irem Y. Tumer
Carol Smidts

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Oregon State University
Ohio State University

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Airforce Office of Scientific Research

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-OSR-VA-TR-2012-0502

12. DISTRIBUTION/AVAILABILITY STATEMENT
Publically available. - A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Software-driven hardware configurations account for the majority of modern safety-critical complex systems. The often costly failures of such systems can be attributed to software specific, hardware specific, or software/hardware interaction failures. The understanding of how failures propagate in such complex systems might provide critical information to designers, because, while a software component may not fail in terms of loss of function, a software operational state can cause an associated hardware failure. The least expensive phase of the product life cycle to address failures is during the design stage. This research presents a means to evaluate how a combined software/hardware system behaves and how such failures propagate to result in potential failures downstream, during the conceptual design stage. In particular, this research proposes the use of high-level system modeling and model-based reasoning approaches to model failure propagation in combined software-hardware systems, introducing the Function-Failure Identification and Propagation (FFIP) analysis framework to help formalize the design of safety-critical systems.

15. SUBJECT TERMS
Integrated Design-Stage Analysis, Software-Hardware Reliability, Formalisms, Failure Propagation Analysis, Safety-Critical Systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*