U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7151, Vol. 4

Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems

Volume 4

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: DISTRIBUTION.RESOURCE@NRC.GOV
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7151, Vol. 4

Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems

Volume 4

Manuscript Completed: November 2011
Date Published: December 2012

Prepared by:
C. R. Elks, N. J. George, M. A. Reynolds, M. Miklo,
C. Berger, S. Bingham, M. Sekhar, B. W. Johnson

The Charles L. Brown Department of Electrical
and Computer Engineering
The University of Virginia
Charlottesville, Virginia

NRC Project Managers:
S. A. Arndt, J. A. Dion, R. A. Shaffer, M. E. Waterman

NRC Job Code N6214

Prepared for:
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Office of Nuclear Regulatory Research

NUREG/CR-7151, Vols. 1 to 4 have been reproduced from the best available copy.

ABSTRACT

Today's emergent computer technology has introduced the capability of integrating information from numerous plant systems and supplying needed information to operations personnel in a timely manner that could not be envisioned when previous generation plants were designed and built. For example, Small Modular Reactor (SMR) plant designs will make extensive use of computer based I&C systems for all manner of plant functions, including safety and non-safety functions. On the other hand, digital upgrades in existing light water reactor plants are becoming necessary in order to sustain and extend plant life while improving plant performance, reducing maintenance costs of aging and obsolete equipment, and promoting prognostic system monitoring and human machine interface (HMI) decision making.

The extensive use of digital instrumentation and control systems in new and existing plants raises issues that were not relevant to the previous generation of analog and rudimentary digital I&C systems used in the 1970's style plants. These issues include the occurrence of unknown failure modes in digital I&C systems and HMI issues. Therefore, digital system reliability/safety, classification of digital I&C system failures and failure modes, and software validation remain significant issues for the Light Water Sustainability and SMR initiatives and the digital I&C system community at large.

The purpose of the research described in volume 1 thru volume 4 is to help inform the development of regulatory guidance for digital I&C systems and potential improvement of the licensing of digital I&C systems in NPP operations. The work described herein presents; (1) the effectiveness of fault injection (as applied to a digital I&C system) for providing critical safety model parameters (e.g., coverage factor) and system response information required by the PRA and reliability assessment processes, (2) the development and refinement of the methodology to improve applicability to digital I&C systems, and (3) findings for establishing a basis for using fault injection as applied to a diverse set of digital I&C platforms. Some of the specific issues addressed in Volume 1 are:

- Fault Injection as a support activity for PRA activities.
- Development of the UVA fault injection based methodology.
- Fault models for contemporary and emerging IC technology in Digital I&C Systems.
- Requirements and challenges for realizing Fault Injection in Digital I&C systems.
- Solutions to challenges for realizing fault injection in digital I&C systems.

Volume 1 presents the findings of developing a fault injection based quantitative assessment methodology with respect to processor based digital I&C systems for the purpose of evaluating the capabilities of the method to support NRC probabilistic risk assessment (PRA) and review of digital I&C systems. Fault injection is defined as a dependability validation technique that is based on the realization of controlled validation experiments in which system behavior is observed when faults are explicitly induced by the deliberate introduction (injection) of faults into the system [Arlat 1990]. Fault injection is therefore a form of *accelerated testing* of fault tolerance attributes of the digital I&C system under test.

Volumes 2 and 3 of this research present the application of this methodology to two commercial-grade digital I&C system executing a reactor protection shutdown application.

In Volumes 2 and 3, the research identified significant results related to the operational behavior of the benchmark systems, and the value of the methodology with respect to providing data for the quantification of dependability attributes such as safety, reliability, and integrity. By applying a fault injection-based dependability assessment methodology to a commercial grade digital I&C, the research provided useful evidence toward the capabilities and limitations of fault

injection-based dependability assessment methods with respect to modern digital I&C systems. The results of this effort are intended to assist NRC staff determine where and how fault injection-based methodologies can best fit into the overall license review process.

The cumulative findings and recommendations of both applications of the methodology and application of the generalized results to broader classes of digital I&C systems are discussed in volume 4.

The digital I&C systems under test for this effort, herein defined as Benchmark System I and Benchmark System II, are fault tolerant multi-processor safety-critical digital I&C systems typical of what would be used in a nuclear power plant 1-e systems. The benchmark systems contain multiple processing modules to accurately represent 4 channel or division 2 out of 4 reactor protection systems. In addition, the systems contain a redundant discrete digital input and output modules, analog input and output modules, inter-channel communication network modules, other interface modules to fully represent and implement a Reactor Protection System. The application Reactor Protection System software was developed using the benchmark systems software development and programming environments.

To establish a proper operational context for the fault injection environment a prototype operational profile generator tool based on the US NRC systems analysis code TRACE [NRC 2011] was developed. This tool allowed generation of realistic system sensor inputs to the Reactor Protection System (RPS) application based on reactor and plant dynamics of the simulated model. In addition, the tool allowed creation of accident events such as large break LOCAs, turbine trips, etc., to stress the RPS application under the various design basis events.

Bibliography

[NRC 2001] Commission, U.S. Nuclear Regulatory. *Computer Codes.* April 2011. http://www.nrc.gov/about-nrc/regulatory/research/comp-codes.html (accessed 2011).

[Arlat 1990] J. Arlat, M. Aguera, et. al. "Fault Injection for Dependability Evaluation: A Methodology and Some Applications." *IEEE Transactions on Software Engineering*, February 2 , 1990.

FOREWORD

As discussed in the NRC Policy Statement on Probabilistic Risk Assessment (PRA), the NRC intends to increase its use of PRA methods in all regulatory matters to the extent supported by state-of-the-art PRA methods and data. Currently, I&C systems are not modeled in PRAs. As the NRC moves toward a more risk-informed regulatory environment, the staff will need data, methods, and tools related to the risk assessment of digital systems. Fault injection methods can provide a means to estimate quantitatively the behavior model parameters of the system. The quantification of these parameters (in a probabilistic sense) can be used to produce more accurate parameter estimates for PRA models, which in turn produces more a accurate risk assessment to inform the risk oversight process.

A challenge for evaluating system reliability relates to relatively undeveloped state of the art methods for assessing digital system reliability. Quantitative measures of digital system reliability are available for digital system hardware, but procedures for evaluating system level reliability (both hardware and software) are not well defined in current industry literature. However, comprehensive use of fault injection techniques for providing critical data toward evaluating digital system dependability may reduce software reliability uncertainties.

The conduct of fault injection campaigns often yields more information than just quantifying the fault tolerance aspects of a system; it also is a means to circumspect and comprehend the behaviors of complex fault tolerant I&C systems to support overall assessment activities for both the developer and the regulator. Fault injection experiments cannot be performed without gaining a deeper understanding of a system. The process itself is a learning experience, providing richer insights into how a system behaves in response to errors arising from system faults. The inclusion of fault injection information into review processes and PRA activities can enlighten the review processes of digital I&C systems. Finally, the process of conducting fault injection testing allows two very important pieces of information to come into direct connection with each other: what the system is supposed to do, and what it actually does. This information is essential for anticipating system behaviors, performing verification and validation (V&V) activities, and conducting methodical system evaluations.

This report describes an important step toward developing a systematic method of evaluating digital system dependability. Volume 1 presents a broad and in-depth development of a digital system dependability methodology, and the requirements and challenges of performing fault injections on digital I&C systems. The process developed in this research project was applied to two digital systems that modeled nuclear power plant safety functions. The results of this phase of the research are described in volume 2 and volume 3. The cumulative findings and recommendations of both applications of the methodology and application of the generalized results to broader classes of digital I&C systems are discussed in volume 4.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

ABVFI	Assertion Based Verification Fault Injection
BDM	Background Debug Mode
CFR	Code of Federal Regulations
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DFWCS	Digital Feedwater Control System
EMI	Electromagnetic Interference
ESFAS	Engineered Safety Features Actuation System
FARM	Faults, Activations, Readouts, and Measures
FDIM	Fault Detection, Isolation, and Mitigation
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
GOOFI	Generic Object Oriented Fault Injection
HiPeFI	High Performance Fault Injection
HMI	Human Machine Interface
I&C	Instrumentation and Control
IC	Integrated Circuit
ICE	In Circuit Emulator
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
JTAG	Joint Test Action Group
LOCA	Loss of Coolant Accident
MTTF	Mean Time to Failure
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OCD	On-Chip Debugger
OP	Operational Profile
OS	Operating System
PRA	Probabilistic Risk Assessment
RPS	Reactor Protection System
SCIFI	Scan Chain Implemented Fault Injection
SMR	Small Modular Reactor
SWIFI	Software Implemented Fault Injection
TOP	TRACE-based Operational Profile
TRACE	TRAC/RELAP Advanced Computational Engine
UNIFI	Universal Platform-Independent Fault Injection
UVA	University of Virginia
V&V	Verification and Validation
VLSI	Very Large Scale Integration

1. INTRODUCTION

1.1. Background

This report is Volume 4 of a multi-volume set of reports that present the cumulative efforts, findings, and results of U.S. Nuclear Regulatory Commission (NRC) contract JCN N6124 – "Digital System Dependability Performance." The reports are organized as follows:

Volume 1 – Presents a broad and in-depth development of the methodology, the requirements, and challenges of realizing fault injection on digital instrumentation and control (I&C) systems.

Volume 2 – Presents the application of the methodology to Benchmark System I.

Volume 3 – Presents the application of the methodology to Benchmark System II- employing the lessons learned from Benchmark System I.

Volume 4 – Presents the cumulative findings and recommendations of both applications of the methodology and generalizes the results to broader classes of digital I&C systems.

1.2. Purpose

This report (Volume 4) presents the cumulative findings and lessons learned for applying a fault injection-based quantitative assessment methodology (presented in Volume 1) to processor-based digital I&C systems for the purpose of evaluating the capabilities of the method to support NRC probabilistic risk assessment (PRA) and standard review processes of digital I&C systems. The purpose of Volume 4 is to summarize the overall findings to present a complete picture of the application of the methodology to digital I&C systems. This summary identifies the strengths, the weaknesses, and the applicability of the methodology to enhance and streamline the standard review processes. The further purpose of this research is to inform the development of regulatory guidance processes for digital I&C systems and provide potential improvements to the digital I&C system licensing process for nuclear power plant (NPP) systems.

1.3. Background and Motivation

NRC regulations require licensees to develop an overall safety strategy for I&C systems to ensure that potential abnormal operating conditions and design basis accidents do not adversely impact public health and safety. In particular, the design criteria for NPP safety systems embody principles such as high quality, integrity, reliability, independence, and process qualification. To achieve these attributes the rigorous application of fault tolerance, separation, redundancy, and fault containment barriers (e.g. independent power, electrical isolation, independent clocking) are generally applied as design measures to address potential vulnerabilities related to a single point failure and the propagation of failure effects. These measures are intended to minimize the propagation effects of faults and their impact. However, the acceptability of an overall safety strategy is strongly dependent on the design, development process and the implementation of safety and fault tolerance functions in these systems.

Accordingly, in recent years, significant effort has gone into improving safety critical system design methodologies, assessment methods, and the updating of industry standards and NRC regulatory guidelines to ensure that digital I&C systems can be designed and assessed to the high safety levels required for highly critical applications. Of particular interest recently are

quantitative dependability assessment methodologies that employ fault injection methods to ensure proper compliance of digital I&C system fault handling mechanisms [Arlat 1993; Yu 2004; Smith 2000; Elks 2009(a); Aldemir 2007; Smidts 2004]. The goal of a dependability assessment methodology is to provide a systematic process for characterizing the safety and performance behavior of embedded systems (e.g., digital I&C systems) in the presence of faults.

Dependability evaluation involves the study of failures and errors and their potential impact on system attributes such as reliability, safety, and security. Very often the nature of failures or crashes and long error latency can make it difficult to identify the causes of failures in the operational environment. Thus, it is particularly difficult to recreate a failure scenario for large, complex systems from failure logs alone. To identify and understand potential failures, the use of an experiment-based or measurement-based approach for studying the dependability of a system is gaining acceptance in the nuclear industry for better understanding the effects of errors and failures to promote an informed understanding of risk. Such an approach is useful not only during the concept and design phases, but also during licensing review activities. Fault injection is *a formal-based process* to collect evidence to gauge the dependability of safety functions associated with I&C systems. Fault Injection has an underlying mathematical theory (with explicitly stated assumptions) allowing one to place stronger justification or refutation to the claims of the overall design and safety of an I&C system.

From a practical point of view, most digital I&C systems are designed to be safety critical systems employing extensive fault detection/tolerance and design diversity features to ensure proper fail operational and fail safe behavior. For example, Fault Detection, Isolation, and Mitigation (FDIM) software or online diagnostic functions of the benchmark systems in this research effort account for as much as 40 percent to 50 percent of the executable system software code. This code is rarely exercised in the real world because faults and failures occur infrequently. This FDIM code is vital toward system dependability and safety compliance, and can only be effectively tested and validated by realistic fault injection campaigns.

1.4. Relevance of Research with Respect to Regulatory Guidance

The NRC has a comprehensive set of regulatory guidelines for reviewing and assessing the safety and functionality of digital I&C systems. The NRC PRA technical community has not yet agreed on how to model the reliability of digital systems in the context of PRA and the level of detail that digital systems require in reliability modeling. Nonetheless, it is clear that PRA models must adequately represent the complex system interactions that can contribute to digital system failure modes. The essential research aim of the PRA technical community is to accurately model digital I&C system behaviors to take into account interactions of the system fault handling behaviors, coverage of fault tolerance features, and the view of the system as an integrated software and hardware system.

Fault injection is a formal-based process to collect evidence to gauge the dependability of safety functions associated with I&C systems that has an underlying mathematical theory (with explicitly stated assumptions) that allows one to place stronger justification or refutation on claims of the overall safety of an I&C system. Fault injection as part of a quantitative assessment process is a robust testing process that can support verification and validation (V&V) and quality assurance activities to gather evidence that the digital I&C system can perform its safety functions in the presence of faulted and failure conditions in compliance with NRC regulations. In addition, those aspects of Appendix B of Title 10 of the Code of Federal Regulations (CFR), Part 50 (10 CFR 50), the NRC Standard Review Plan (NUREG-0800), and other relevant guidelines that address requirements for testing processes, methods and

evidence to support safety function operational effectiveness are clear candidates for the application of fault injection methods.

1.5. Overview of the Project

The overall objective of this research was to develop a body of evidence to inform the development of regulatory guidance processes for digital I&C systems and potentially improve the licensing process of digital I&C systems in NPP operations. In support of this objective the research investigated the effectiveness of fault injection (as applied to digital I&C systems) for providing critical parameters and information required by PRA and reliability assessment processes. The results and findings of this effort are aimed at assisting NRC staff determine when, where and how fault injection-based methodologies can best fit in the overall license review process.

Three phases of work were conducted in the research. The first phase developed the methodology so that it could be applied to the benchmark systems. The second phase of the research applied the methodology to the Benchmark System I based on the recommendations and plan of action from the first phase of the work. The third phase of the work applied the methodology to Benchmark System II incorporating on the lessons learned from the first and second phase of the research. Phases II and III of this research employed two different representative digital I&C systems as test platforms for the methodology. Both of these systems are described in detail in Volumes II and III.

Both Benchmark System I and Benchmark System II were prototypes of safety grade Class 1E qualified digital I&C systems specifically developed for high safety and high reliability functions in nuclear NPPs. The benchmark systems development platforms provided to the University of Virginia (UVA) for this research were used to develop scaled versions of a typical 4-division digital I&C system used for Reactor Protection System (RPS) functions. The make and model of the benchmark systems cannot be disclosed due to non-disclosure and proprietary agreements. The salient features of the systems were their ability to be adaptable to plant-specific requirements, with varying degrees of redundancy. This scalability permits development of solutions for a spectrum of safety-related tasks within the NPP system. Typical applications include the RPS and the Engineered Safety Features Actuation System (ESFAS.

It should be noted that the benchmark systems used in this research were testing platforms to exercise the fault injection methodology. In that regard, the benchmark systems represent the complexity of RPS processing and fault tolerance from both a hardware and software perspective. However, typical in-plant RPS digital I&C systems are considerably more complex in their fault tolerance and diversity attributes than the representative benchmark systems used in this research. Therefore, the results of this study are intended to be a reflection of the ability of the methodology to accommodate fault injection experiments on digital I&C systems, and should not be construed as representative of the performance and suitability of the benchmark systems for RPS applications.

1.5.1. Research Objectives

The overall objective of this research was to develop a body of evidence to inform the development of regulatory guidance processes for digital I&C systems and potentially improve the licensing process of digital I&C systems in NPP operations. In support of this objective the research investigated the effectiveness of fault injection (as applied to digital I&C systems) for providing critical parameters and information required by PRA and reliability assessment processes. The results and findings of this effort are aimed at assisting NRC staff determine

when, where and how fault injection-based methodologies can best fit in the overall license review process.

The major goals of the research effort are listed below:

Objective 1
Demonstrate the effectiveness of the University of Virginia (UVA) quantitative safety assessment process on commercial safety grade I&C systems executing reactor protection applications with respect to a simulated NPP safety system design.

Objective 2
Identify, document, and develop improvements to the fault injection-based process that make it easier and more effective to apply to a wider spectrum of digital I&C systems.

Objective 3
Document the limitations, sensitive assumptions, and implementation challenges that would encumber the application of fault injection processes for digital I&C systems. Also document the quantitative and qualitative results that can be obtained through application of the assessment process, and provide the technical basis upon which NRC can establish the regulatory requirements for safety-related digital systems, including the acceptance criteria and regulatory guidance documents.

Secondary Objective 1
Assess the level of effort and cost for implementing fault injection capability in a vendor or licensee environment.

Secondary Objective 2
Identify and develop innovative fault injection methods that would make fault injection more efficient and easier to adopt by NRC and the nuclear industry.

The scope of this work is targeted at safety critical digital I&C systems, but applies to non-safety related systems as well. The target benchmark systems were configured to be representative of a four-channel RPS, but were limited in scale due to budget constraints on equipment availability. Therefore, the benchmark systems lacked some redundant hardware modules that would normally be found in an actual RPS. The overall complexity and configuration of the system was sufficient to stress the methodology, which was the objective of the research effort. The specific benchmark system data results obtained from the study should be interpreted with respect to the benchmark system configuration described in this report unless otherwise stated.

The methodology that was developed and applied in this research effort is part of a larger comprehensive assessment and review process, and is not intended to be interpreted as a “replacement” for existing processes. Rather, the methodology should be viewed as a complementary method to support existing and emerging design assurance and license review processes in an effort to establish more efficient, repeatable, and objective design assessment and review processes.

Fault injection-based methods are but one part of a comprehensive process of estimating the reliability of digital systems (hardware and software) for the purpose of PRA applications. From the highest level perspective, reliability estimation requires (1) the knowledge of the likelihood of faults (software or hardware) and (2) the consequence of activating these faults in the system context. Fault injection methods are most useful in characterizing system responses to activated faults - the second requirement. That is, providing empirical knowledge on the triggering, detection, tolerance, and propagation of errors due to software or hardware faults in the system. As such, the methodology developed and presented in this set of reports is aimed

at providing empirical data in support of estimating system fault response data, such as fault detection, error propagation, fault latency, and timing delays.

1.6. Organization of this Report

This report is organized around several main themes:

(1) Overview of the methodology

(2) Summary of the application of the methodology to Benchmarks Systems
(3) Success of meeting objectives

(4) Results, outcomes and challenges associated with the application of fault injection to the benchmark systems

(5) Lessons learned

(6) Recommendations based on the research

1.7. Overview of Fault Injection

Section 3 of Volume 1 presents a detailed discussion of fault injection concepts and theories needed for the development of a fault injection methodology for digital I&C systems. This section presents a brief overview of fault injection to reacquaint the reader with the associated principles.

Consider the target digital I&C system shown in Figure 1–1. When fault injection is applied to the target system, the input domain corresponds to the following sets:

(1) A set of faults ***F*** taken from a class of faults "$\boldsymbol{F_{class}}$"
(2) A set of activations, ***A***, that specifies the domain used to functionally exercise the system
(3) An output domain corresponding to a set of readouts, ***R***
(4) A set of derived measures ***M***.

Together, the Faults, Activations, Readouts, and Measures (FARM) set constitute the major attributes that can be used to fully characterize fault injection.

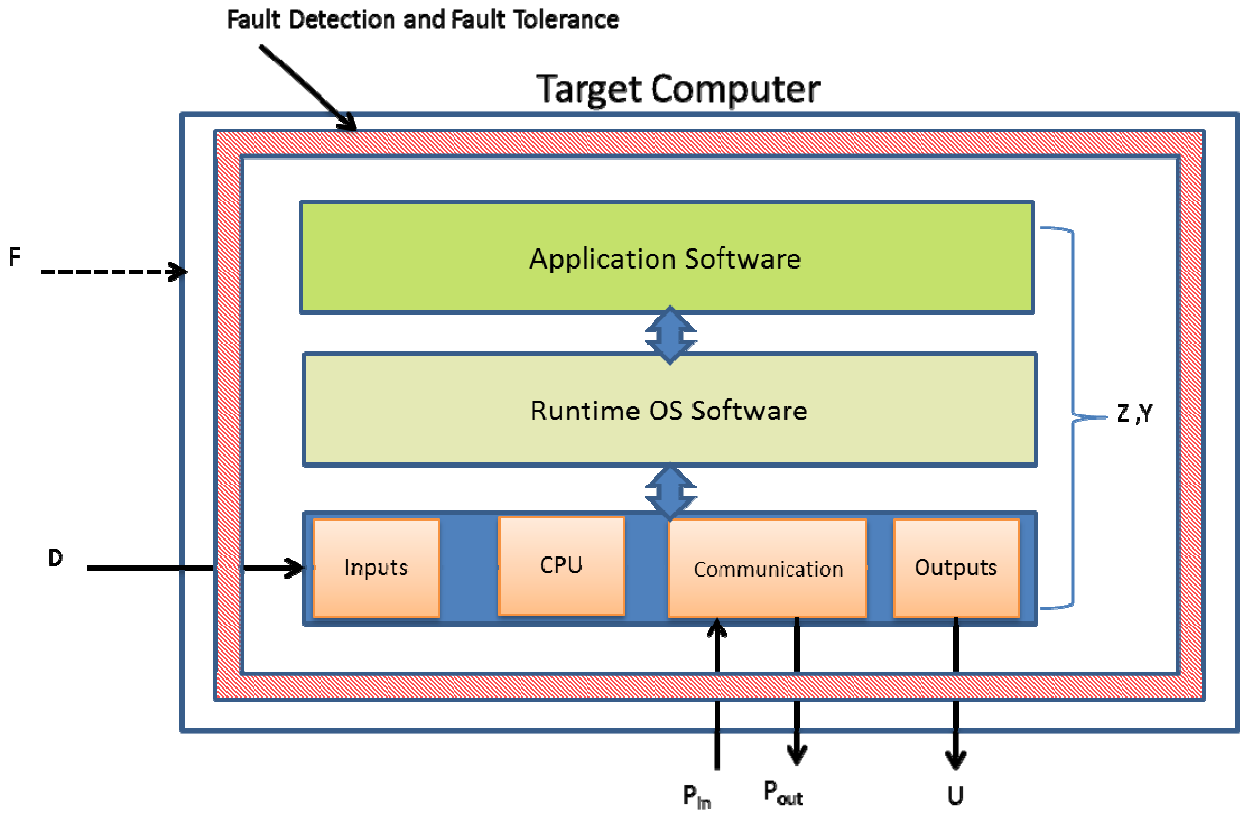

Figure 1-1 Fault injection model for digital I&C

Fault injection is a formal experiment-based approach. For each experiment, a fault ***f*** is selected in ***F*** and an activation trajectory ***a*** is described in ***A***. The reactions of the system are observed and form a readout ***r*** that fully characterizes the outcome of the experiment. An experiment is thus characterized by the triple ordinate ***< f, a, r >***, where the readouts, ***r,*** for each experiment form a global set of readouts ***R*** for the test sequence and can be used to elaborate a measure in ***M.*** A *campaign* is a collection of experiments to achieve the quantification of a measure ***M***.

Consider a test sequence of ***n*** independent fault injection experiments. In each experiment, a point in the ***{F x A}*** space is randomly selected according to the distribution of occurrences in ***{F x A}*** and the corresponding readouts. Expanding the ***F*** to include the fault space dimensionality of time, location, value, and fault type, yields six parameters that define a fault injection experiment:

a = the set of external inputs

Δ = is the duration of the injected fault

t = fault occurrence time, or when the fault is injected into the system

l = fault location

v = value of the fault mask

f_m = a specific fault type as sampled from fault classes

The basic concept of a fault injection experiment is shown in Figure 1-2, which shows that faults from ***F*** are sampled from the fault space (discussed in Section 3.7 of Volume 1). These faults are elaborated by the fault type f_m, the fault duration Δ, the fault location ***l***, the value of the fault mask, time of occurrence ***t***, and the set of inputs ***a*** to characterize the set of experiments. The fault experiments are applied to the target computer, and a set of readouts (the ***R*** set) is used to derive the ***M*** set (coverage estimation) by statistical estimation.

More importantly, from a practical perspective, the parameters of the coverage equation serve as the essential requirements in the development of a fault injection methodology or tools to support fault injection. Fault injection frameworks of any type must address the control of these parameters and the observable responses of a system to these parameters as they are sampled. The following sections discuss the statistical theory behind the coverage estimation and the dependent parameters of coverage.

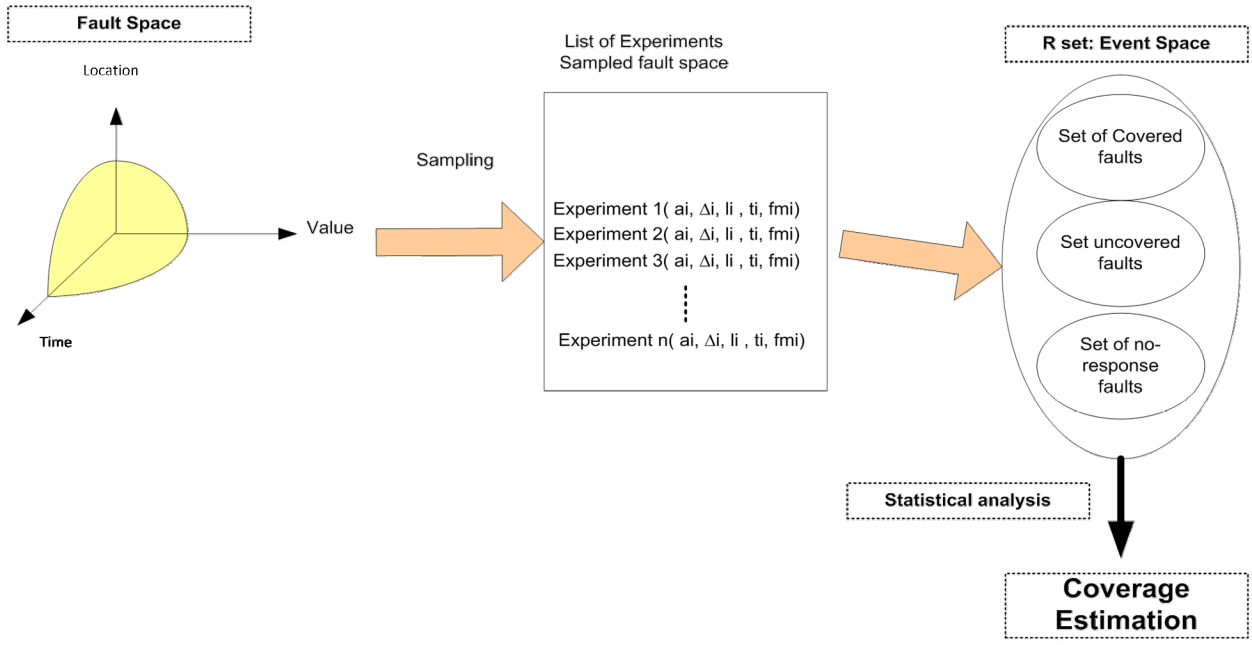

Figure 1-2 Fault injection experiment

1.8. Applicability of Fault Injection

As discussed in Section 5 of Volume 1, the domain and use of fault injection spans important domains of typical embedded system development processes. In the embedded software development community, it is used as a stress testing technique and is widely considered to be an important part of developing robust software for both application software and operating system software. Techniques such as syntax testing (Fuzzing) and mutation testing are but a few fault injection methods widely used in the embedded software testing community. In the hardware world fault injection is used to emulate physical faults that can occur in the environment in which embedded systems operate. These include faults both internal and external to semiconductor integrated circuits (ICs). In the communications domain, fault injection is used to test the vulnerabilities of communication protocols, interfaces, and application programmer interfaces (APIs) where significant security breaches or safety integrity problems can occur.

It is important to note that the methodology developed in Phase I of this research is not tied to any one specific fault injection technique; however, it is principally aimed at real physical systems as opposed to simulations of systems. The fault models and fault injection techniques that were developed as part of this research are adaptable to application software and operating system (OS) software, hardware, and communication aspects of digital systems. The methodology is easily accommodated in a simulation environment [Bastien 2004]. This research was aimed at fully developing the methodology to apply to digital I&C systems.

1.9. Overview of the Fault Injection-based Dependability Assessment Methodology

The UVA fault injection-based dependability assessment methodology was developed realizing that a fault injection approach may serve different goals and purposes. Thus, the methodology was designed to be as flexible as possible to the needs of the assessor and designer.

The goal of the dependability assessment methodology described in this report was to provide a generic, formal, systematic means of characterizing the dependability behavior of digital I&C systems and their full plant interactions in the presence of anomalous behaviors, faults, and failures. This is termed the *full system approach* to fault injection. The goal methodology provides practical means for characterizing digital I&C system/plant dependability attributes that will assist developers in improving V&V processes, while helping regulatory entities make informed confirmatory decisions about licensing I&C systems for critical plant operations.

Figure 1-3 shows the basic conceptual framework of the fault injection-based dependability assessment process. In this depiction, the process is driven by the needs of PRA modeling efforts to estimate more accurately parameters for PRA modeling activities. Statistical sampling principles are used to guide the parameter estimation process. Then, representative fault models are selected with respect to the target I&C system. After the faults are injected into the system, the data is post-processed to produce new estimates of model parameters, and these are instantiated back into the PRA models to enhance better predictions of the PRA models. The methodology is described in more detail in Section 4 of Volume 1. The characteristics of each step in the process are described in this section.

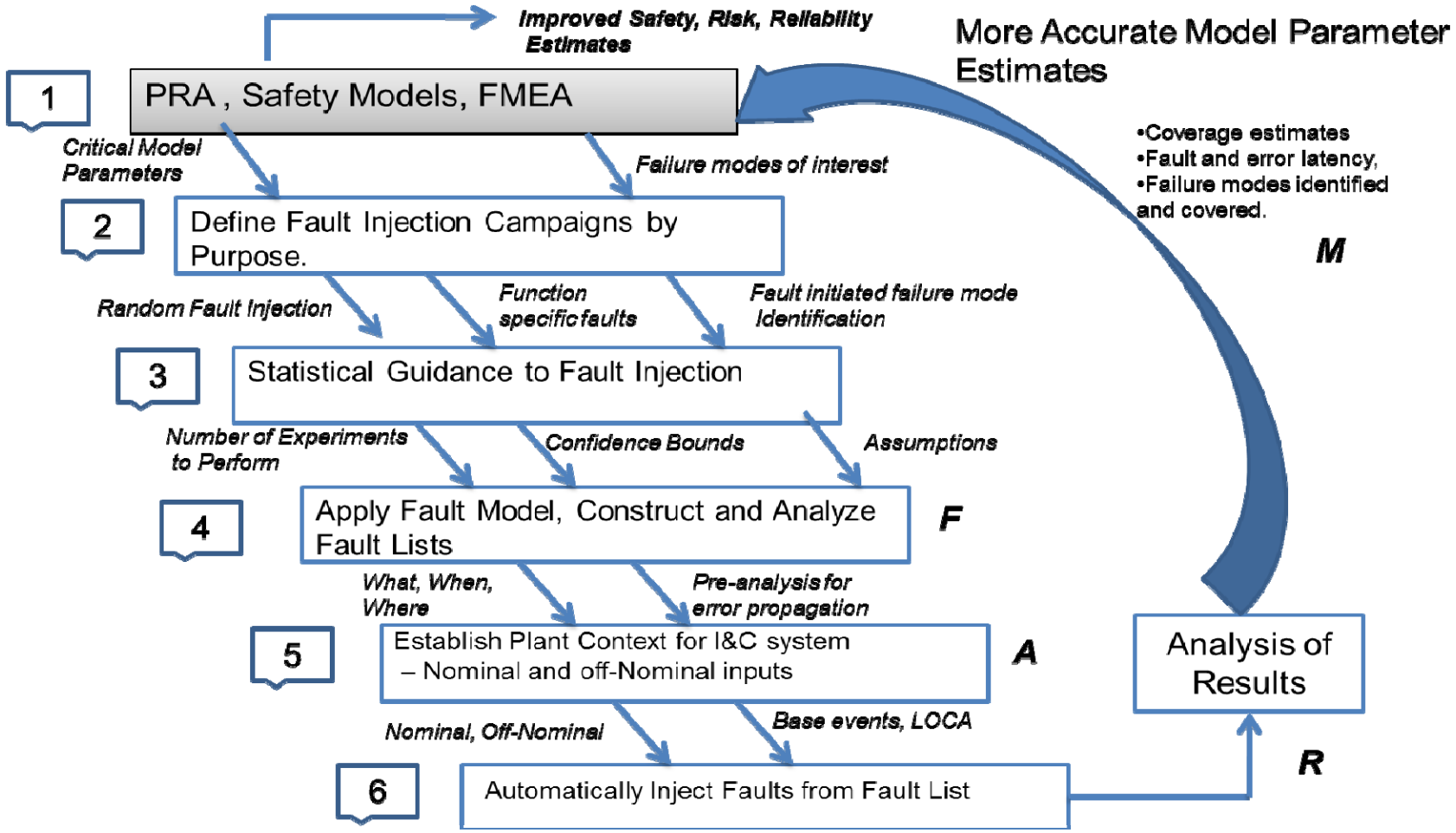

Figure 1-3 Operational view of the fault injection-based dependability assessment methodology

1.9.1. Step 0: Defining the Dependability Metrics

The assessment process begins with defining or selecting the dependability metric of interest. The metrics that can be used in I&C systems include but are not limited to

- system reliability
- probability of coincident failure
- system safety
- probability of failure on demand
- mean time to system failure
- mean time to unsafe system failure
- steady state unsafe system failure

For instance, an actuation system such as a RPS would be more accurately characterized by probability of failure on demand, and an instantaneous availability metric rather than a mean time to failure (MTTF) or a system reliability metric. So, how the system is employed in the context of the plant is very important to the selection of an appropriate metric. In the case of the RPS, it is a reactive system.

A reactive system is characterized by its ongoing interaction with its environment, continuously accepting requests from the environment and continuously producing results [Wieringa 2003]. In reactive systems, correctness or safeness of the reactive system is related to its behavior over time as it interacts with its environment. Unlike functional computations, which compute a value upon termination, reactive system computations usually do not terminate. If the computations do terminate, it is most often due to the fact that an exception event has occurred. Example applications of reactive systems include process control systems, actuation systems, operating systems, and telecommunications.

1.9.2. Step 1: Support for PRA Activities and Design Review Processes

The purpose of a reliability and safety assessment process is to ensure a system will meet its reliability and safety requirements, show that risk mitigation measures produce reliability and safety improvements, and the unreliability risk is controlled to an acceptable level. A *probabilistic* safety and reliability safety assessment process usually begins with asking three basic questions: (1) what can go wrong, (2) what is the likelihood, (3) what are the consequences? Referring to Figure 1-3, the starting point in the methodology is to understand what is needed from the PRA process.

The PRA modeling process usually begins with defining or selecting a set of measurement-based attributes that are appropriate for informing the risk assessment process. These attributes typically include reliability, unreliability, safety, etc. In a typical risk-informed PRA process there may be several dependability attributes that are used to characterize the system risk. In digital I&C system reliability assessments, measures such as probability of system failure, probability of coincident failure, probability of failure on demand, mean time to system failure, mean time to unsafe system failure, and steady state unsafe system failure are often seen.

The important point is that PRA activities employ modeling methods such as fault trees, event trees, and Markov models to assist in the determination of risk. These models have parameters that represent attributes of the system, such as physical failure rates, detection capability, capability to tolerate faults, fail-safe capability, repair capability, etc. Fault injection methods provide a means to estimate quantitatively the behavior model parameters of the system.

A behavioral model parameter is a measure of how a system behaved or responded with respect to a stimulus (e.g., a fault or a set of inputs). The important coverage factor parameter presented in Section 3.6 of Volume 1 is a behavioral parameter in the PRA model. Equally important is stating the underlying assumptions the models or model parameters produce in light of incomplete knowledge of the systems. Since fault injection provides response information that can be used to statistically estimate these parameters, the quantification of these parameters (in a probabilistic sense) can be used to produce more accurate parameter estimates for the PRA models, which in turn produces more a accurate risk assessment to inform the risk oversight process.

1.9.3. STEP 2: Fault Injection by Purpose and Type

The fault injection process is used for different purposes in order to get a complete picture of a system's behavior response. As indicated in Section 3.4 of Volume 1, fault injection is used in validation processes and design processes of digital I&C systems.

From a broader stance, fault injection is viewed as a measurement-based process that provides important experimental techniques for assessing and verifying fault-handling mechanisms. It allows researchers and system designers to study how digital systems react in the presence of faults. Fault injection processes are used in many contexts and can serve different purposes, such as

- Supporting on-line monitoring so that system performance can be effectively monitored.
- Assessing the effectiveness of fault-handling mechanisms in software and hardware.
- Studying error propagation and error latency in order to guide the design of fault-handling mechanisms.
- Providing evidence to support conclusions regarding the resiliency of a system to unexpected faults and failures.

All fault injection techniques have specific drawbacks and advantages as indicated in Section 5 of Volume 1. Since fault injection can be used for many purposes, it is necessary to identify as early as possible the fault injection method and measurements that will be used, and whether fault injections will be applied to a physical system or a model of the physical system. The comprehensive survey and characterization of fault injection methods and techniques presented in Section 5 of Volume 1 serve as a guide toward selecting the fault injection process for a target digital I&C system.

1.9.4. Step 3: Statistical Guidance to Fault Injection

The purpose of the statistical model is to provide a formal basis for (1) conducting fault injection experiments and (2) providing a statistical model for a estimating the measures of a fault injection experiment, such as coverage. As developed in Section 3 and Appendix A of Volume 1, the statistical model supports four specific needs of the fault injection based dependability assessment methodology:

- Characterize the fault injection experiment in formal statistical framework.
- Quantify and characterize the uncertainty of model parameters.

- Characterize and define the assumptions of the estimation process.

- Statistically estimate, based on the assumptions of the model and model parameters, the numbers of observations required to estimate a parameter to a known confidence level.

1.9.5. Step 4: Fault Model Selection

Digital I&C systems are subject to faults and failures from a variety of sources that can be manifested in many ways, as was discussed in the fault taxonomy discussion in Section 1.7.3 of Volume 1 [Avizienis 2004]. Fault models are abstract representations of real faults. For example, a single event upset caused by a power surge or a cosmic particle strike can be modeled by the bit-flip fault model.

Fault models allow assessors to evaluate the effectiveness of fault detection, diagnostic tests, and fault tolerance mechanisms with respect to the faults that are anticipated to arise in the operation of a digital I&C system. Applying these fault models to I&C systems and observing the responses are key components of fault injection-based assessment processes.

Selecting the appropriate fault model for a fault injection campaign is a crucial decision. In Figure 14 are the fault classes that were selected to apply to the benchmark systems based on the research on fault and failure behavior of digital I&C systems. These fault models and their justifications were discussed in detail in Section 4.5 of Volume 1.

The output of a fault model selection process should produce a set of faults that is relevant to a particular digital I&C system. More importantly, the process of fault model selection should produce an audit trail or evidence trail so the assumptions and factors for determining the fault models can be verified during licensing and review activities.

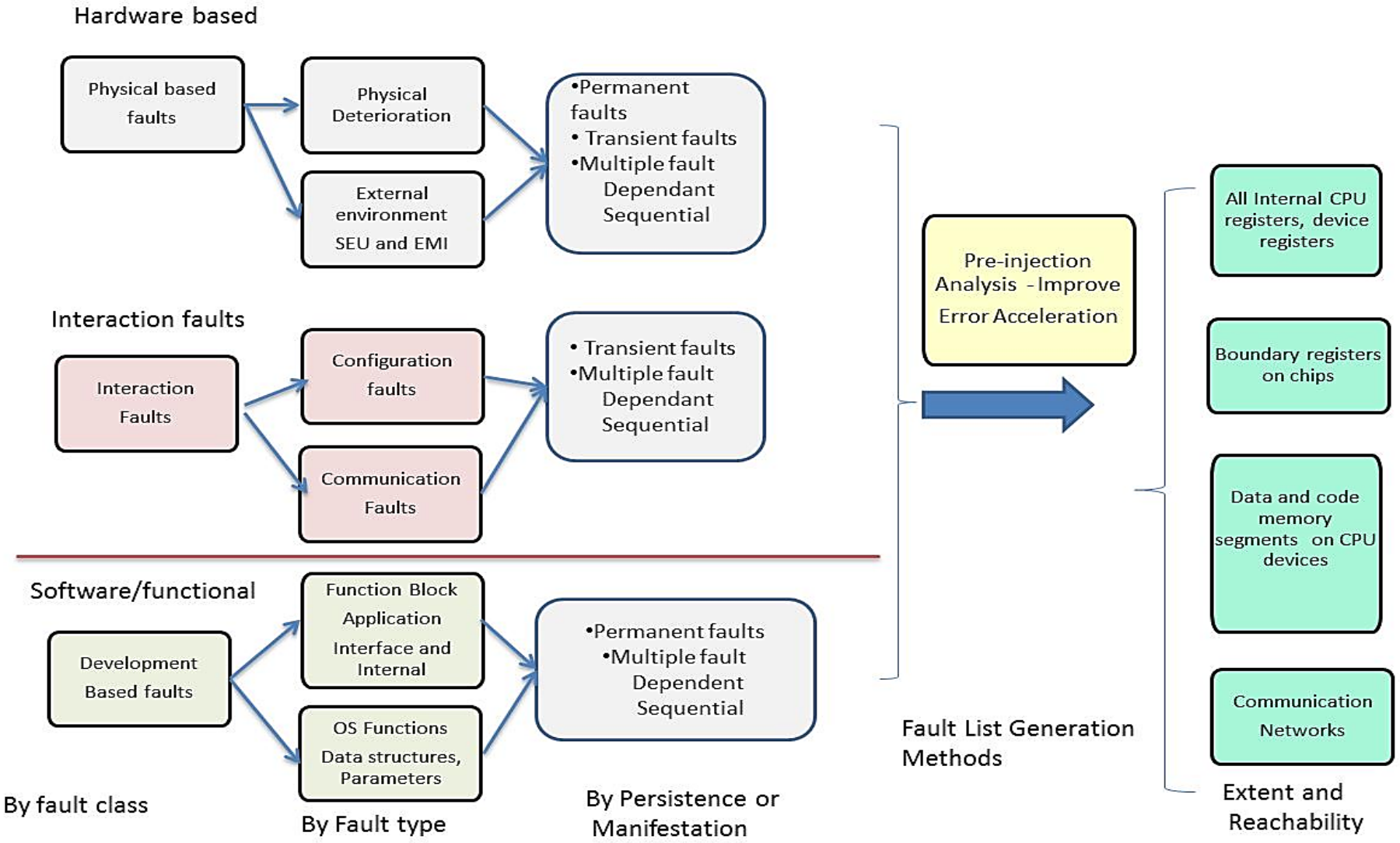

Figure 1-4 Fault model classes for benchmark digital I&C systems

After a representative set of fault models has been selected, the next step is to determine a means for organizing and applying the faults to a digital I&C system. This activity is called *fault list generation*. Generating fault lists for a fault injection experiment or campaign is a critical activity for fault injection.

A *fault list* is a sample set of faults taken from the fault space of the target I&C system. Specifically, for a single fault notation in a fault list, each entry identifies:

- The type of fault to be injected (governed by the fault model selection)
- Where the fault is to be injected (where the corruption is to take place with respect to program execution behavior or component use)
- When the fault is injected (at what time the injection takes place, either relative to an event, or when a resource is in use, or randomly selected).
- How long the fault is injected (the persistence of the fault with respect to the time domain)
- The error mask of the fault (the values that represent the fault injection process with respect to a resource or a component)

The fault list can be thought of as a set of directives to the fault injector apparatus. Each of the directives is under the control of the experimenter. The fault list is used to instruct the fault injection process according to a particular campaign purpose. The fault list is strongly tied to the fault injection environment and its capabilities to emulate the faults of concern.

An important aspect of fault list generation is improving the efficiency and effectiveness of the fault injection process, which is often referred to as *error acceleration* [Chillarege 2002] or pre-injection analysis [Sekhar 2008; Barbosa 2005]. Pre-injection analysis is defined by a set of rules that enables fault injection experiments to increase the probability of a system failure by identifying the most likely fault injection experiments. Section 8 of this report presenat new fault list generation methods that produce efficient and effective fault injection results for digital I&C systems.

1.9.6. STEP 5: Establishing Operational Profile and Workload

An *operational profile* (OP) is a quantitative representation of how a system will be used within its use environment [Musa 1998]. An OP models how users interact and use the system, specifically the occurrence probabilities of system and user modes over a range of operations. Traditionally, an OP is used to generate test cases and to direct testing to the most used system functions, thus the potential for improved reliability with respect to the use environment is achieved. The OP associates a set of probabilities or weighting factors to the program input space and therefore assists in the characterization of possible behaviors of the program or collection of programs that comprise a system.

As discussed in Section 4 of Volume 1, digital I&C systems that are real-time and reactive operate on a deterministic, time-triggered basis. The difference between an OP for general purpose computing and a real-time OP is that general purpose OPs typically represent many customer or user domains, while real-time OPs are specific to a particular application (user) and its environment. In this research, an operational profile is defined in the context of its application-specific nature (i.e., RPS).

Real time operational profiles to be used in the fault injection experiments must be selected to be representative of the system under various modes of operation and configuration. Digital I&C system configurations may invoke different hardware and software modules in response to real time demands, and it is important that the fault injection assessment include sufficient combinations of these configurations to ensure a thorough evaluation of their behavior in the presence of faults.

1.9.7. STEP 6: Injecting Faults into the Target System

Most fault injection tools have been developed with a specific fault injection technique in mind, targeting a specific system, and using a custom-designed user interface. Extending such tools with new fault injection techniques, or porting the tools to new target systems is usually a cumbersome and time-consuming process. Since one of the objectives in this research was to apply fault injections to digital I&C systems of the type found in NPP systems, the need for a flexible and portable fault injection environment was a requirement for efficient application of the UVA fault injection-based dependability assessment methodology. To this end, the research effort developed the Universal Platform-Independent Fault Injection (UNIFI) fault injection environment to manage and coordinate the tasks associated with automated fault injection in physical I&C systems. UNIFI is described in detail in Section 5 of Volume 2. A summary of the UNIFI system is described in the following paragraphs.

Figure 1-5 shows the UNIFI tool with different plug-ins and how the tool interfaces with a target system and target system software development environment. In the UNIFI framework, the various fault injection plug-ins, the database that stores information, and results from experiments are located within the host computer.

The *operational profile generator* module receives as input a special pre-processed input file from the TRAC/RELAP Advanced Computational Engine (TRACE) thermal hydraulic simulation tool that provides all of the sensor data that the target system will acquire in its operational setting. The *experiment set up and control* plug-in function selects fault injector(s), configures the fault injectors, and initializes the UNIFI tool for a fault injection campaign. The *fault list generation plug-in module* generates a fault list that is parameterized with fault models of interest, locations of fault injections on the target system, types of fault injection, and when the s are to be injected. The *real time data monitoring and collection module* interfaces to the target system diagnostics and error monitoring server to collect error messages and error logs after each fault is injected into the target system. The *fault injection engine plug-in module* allows different types of fault injection techniques to be used by the UNIFI tool.

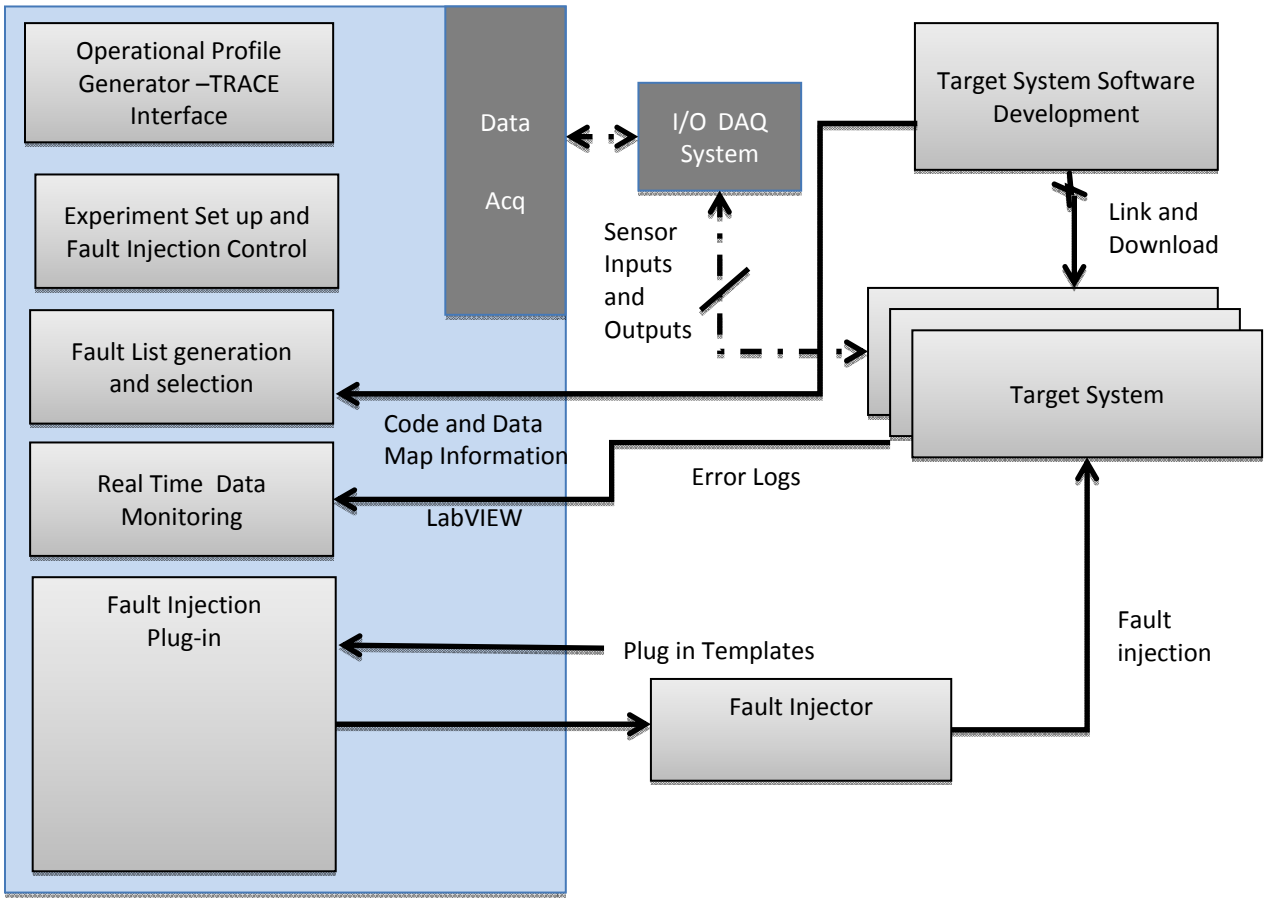

Figure 1-5 UNIFI fault injection environment

1.10. Quantitative Assessment and Qualitative System Attributes

The UVA fault injection based methodology presented in the previous section is primarily a quantitative assessment process. As such, a few words describing the nature of quantitative assessment processes are in order.

In engineering, quantitative assessment refers to the systematic empirical investigation of system behaviors via statistical, mathematical, or computational techniques [Williams 2000]. The objective of quantitative assessment is to develop or employ mathematical models, theories and/or hypotheses pertaining to a system behavior or assertion (e.g. a claim). The process of measurement is central to quantitative research because it provides the fundamental connection between empirical observation and mathematical expression of quantitative relationships.

Quantitative data is any data that is in numerical form such as statistics, percentages, enumerations, etc. [Williams 2000] In layman terms, this means that the researcher poses a specific question about a claim or assertion of the system behavior and collects evidential data from the system under test to answer the question. The important point is that quantitative assessment/analysis is not about the measurements, but the *reasoning* with the results of the measurements. It is about trends, patterns, and indications that the data suggest with respect to a system attribute or assertion.

The NRC advocates the use of *deterministic safety assessment* in its review processes for digital I&C systems. Here deterministic means that "causality completely defines the effects". As applied in nuclear technology, it generally deals with evaluating the safety of a nuclear power plant in terms of the consequences of a predetermined accident sequence. Deterministic risk assessment is strongly supported by *qualitative arguments or evidence;* that is, the assessor evaluates information/data related to a claim or assertion with respect to compliance of regulations. Regulations typically are non-prescriptive and qualitative. For, the single failure criterion states;

> *"The protection system shall be designed for **high** functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be **sufficient** to assure that (1) no single failure results in loss of the protection function….."*

The bolded terms high and sufficient are subjective textual non-numerical attributes that the system must possess in order to comply with the regulations. Quantitative analysis or assessment is complementary to qualitative attributes or assertions like those highlighted above; specifically as it supplies by way of measured data and inference on that data a *different* means to reason about the system with respect to its design purposes. It provides an additional way to verify the claims or assertions and under what conditions they hold.

The model parameters and information that is produced by the UVA fault injection methodology are an approach to fully understand the context and the importance of qualitative attributes such as high reliability, sufficient fault tolerance, etc. It is important to note, that no one assessment method (quantitative or qualitative) is adequate for all cases, more often than not it is a combination of both methods that enable a richer understanding of a system.

1.11. References

[Avizienis 2004] A. Avizienis, J.C. Laprie. "Basic Concepts and Taxonomy of Dependable and Secure Computing." *IEEE Transactions on Dependable and Secure Computing Archive*, 2004: vol. 1.

[Arlat 1993] Arlat, J, A Costes, Y Crouzet, J-C Laprie, and D Powell. "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems." *IEEE Trans. on Computers*, no. 42 (1993).

[Bastien 2004] B. Bastien, B.W. Johnson. *A Technique for Performing Fault Injection Using Simics.* UVA-CSCS-SFI-001, Charlottesville: University of Virginia, 2004.

[Barbosa 2005] Barbosa, R., Vintern, J., Fokesson, P., Karlsson, J. "Assembly-Level Pre-Injection Analysis for Improving Fault Injection Efficiency." *Lecture Notes in Computer Science, vol. 3463*, 2005: 246-262.

[Elks 2009(a)] C. Elks, B.W. Johnson, M. Reynolds. "A Perspective on Fault Injection Methods for Nuclear Safety Related Digital I&C Systems." *6th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology.* Knoxville, TN: NPIC&HMIT, 2009(a).

[Smidts 2004] C. Smidts, M. Li. *Validation of a Methodology for Assessing Software Quality.* NUREG/CR-6848, Washington, D.C.: NRC, Office of Nuclear Regulatory Research, 2004.

[Chillarege 2002] Chillarege, R., Goswami, K., Devarakonda, M. "Experiement Illustrating Failure Acceleration and Error Propagation in Fault-Injection." *IEEE International Symposium on Software Reliability Engineering*, 2002.

[Smith 2000] D. Smith, T. DeLong, B.W. Johnson. "A Safety Assessment Methodology for Comples Safety Critical Hardware/Software Systems." *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technology.* Washington, D.C., 2000.

[Musa 1998] Musa, J. *Software Reliability Engineering.* McGraw Hill, 1998.

[Sekhar 2008] Sekhar, M. *Generating Fault Lists for Efficient Fault Injection into Processor Based I&C Systems.* Charlottesville, VA: University of Virginia, 2008.

[Aldemir 2007] T. Aldemir, M.P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L.A. Mangan, D.W. Miller, A. W. Fentiman, E. Ekici, S. Guarro, B.W. Johnson, C.R. Elks, S.A. Arndt. *Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessment.* Regulatory Guide NUREG/CR-6942, NRC, 2007.

[Wieringa 2003] Wieringa, R.J. *Design Methods for Reactive Systems, 1st ed.* Morgan Kaufman, 2003.

[Williams 2000] Williams, F. *Reasoning with Statistics: How to do Quantitative Research.* Wadworth Publishing, 2000.

[Yu 2004] Y. Yu, B.W. Johnson. "Coverage Oriented Dependability Analysis for Safety-Critical Computer Systems." *The International System Safety Conference (ISSC).* System Safety Society, 2004.

2. OVERVIEW OF TECHNICAL ACCOMPLISHMENTS AND FINDINGS FOR THE RESEARCH PROJECT

2.1. Introduction

The overall goal of this research was to develop a body of evidence to inform the development of regulatory guidance processes for digital I&C systems and potentially improve the licensing process of digital I&C systems in NPP systems. The basic research objectives in Section 1.6 of this volume were formulated to address significant perceived issues and challenges at the outset of this research. As often happens, the "process of discovery" uncovered new challenges and issues that should be addressed. In each of these cases, these new challenges were addressed with solutions or proposed solutions.

The success of this project is gauged by the success of applying the methodology to the benchmark systems to conduct comprehensive fault injection campaigns to collect critical data and information for PRA and design review processes. On both accounts the research fully succeeded by developing advanced fault injection techniques for both digital I&C systems, and by applying these fault injection techniques under the guidance of the methodology.

Over 20,000 automated fault injections were cumulatively applied to the benchmark systems, resulting in a comprehensive database of system response data to the injected faults. This accomplishment was the culmination of many incremental achievements attained from the beginning of the research project to its conclusion. The following sections summarize the significant technical accomplishments and findings with respect to each phase of the research project.

2.2. Phase I - Technical Accomplishments and Findings

The Phase I research was aimed at further developing the methodology toward the application to physical digital I&C systems. The Phase I effort (as described in Volume 1) presents a broad and in-depth development of the theory, methodology, the requirements, and the challenges of realizing fault injection on digital I&C systems. A significant outcome of the Phase I research was identifying the challenges of applying the fault injection methodology to physical digital I&C systems based on previous experience and from research. The principle findings of this Phase I effort are summarized below.

2.2.1. Development of a Formal Model of Fault Injection for Digital I&C Systems (Section 3.3 Volume 1)

It is important to have a formal model to characterize the applicability and understanding of the fault injection process to ultimately guide its use and facilitate understanding of the results with respect to assumptions. The importance of the formal model is to provide a *reference* for all fault injection-based methodologies with respect to the necessary requirements for fault injection. The reference model analogy is significant if the methodology is to be raised to the level of a Branch Technical Position or regulatory guidance.

2.2.2. Development and Analysis of Statistical Models for Fault Coverage Estimation (Section 3.6 and Appendix A of Volume 1)

The purpose of a statistical model is to provide a formal basis for (1) conducting fault injection experiments and (2) providing a statistical model for a estimating the measures of a fault injection experiment, such as coverage. Section 3.6 and Appendix A of Volume 1 present a

formal and mathematical description of statistical estimation concepts that are fundamental in the assessment of fault coverage. The presentation and analysis provides a sufficient and adequate approach that applies to a wide variety of statistical models for fault coverage estimation. In Appendix A of Volume 1, two widely referenced and used models for statistical estimation of fault coverage are analyzed, and summary findings on both models are presented. These models are important so that fault injection experiments can be designed and implemented from a statistical perspective, allowing sound inferences to be drawn from the data to support greater conclusions about the system under test, and to support estimation of PRA model parameters and system response data.

2.2.3. Survey and Characterization of Fault Injection Techniques for Digital I&C Systems (Section 5 of Volume 1)

Section 5 in Volume 1 described a proposed and developed characterization schema for fault injection techniques based on eight properties. These eight properties represent attributes that are desired for a fault injection technique to support the requirements of the FARM model and the fault injection based dependability assessment methodology presented in Section 4. The purpose of the characterization was to describe fault injection techniques in a manner that better informs the NRC on the applicability of specific fault injection techniques for digital I&C systems.

In addition to fault representativeness (i.e., the plausibility of the supported fault model with respect to actual faults) that is one concern often raised in conjunction with fault injection experiments, Section 5 describes a wide range of criteria that can be considered for assessing the merits of the fault injection techniques. This is particularly important with respect to physical fault injection where complete controllability and reachability are difficult to achieve with just one fault injection technique. This Section is significant because all advantages and disadvantages that must be weighed during the selection process of fault injection methods and techniques with respect to digital I&C systems.

2.2.4. Lessons Learned from Previous Experience (Section 7 of Volume 1)

By examining the application of fault injection on a Digital Feedwater Control System (DFWCS), the research effort gained insights into specific issues and challenges of applying fault injections to digital I&C systems of the type found in NPP systems. The challenges and the resolution of those challenges showed that the application of fault injection to digital I&C systems is a complex process involving the integration of several systems to achieve a fault injection capability. The integration process involved such diverse systems as the fault injector, the target computer, the fault injection controller to initiate the fault injection process, the OP system to supply inputs to the target system, and the data acquisition system to collect data. To improve the methodology to better support physical-based fault injection, the research identified key tasks to investigate and realize fully support fault injection for digital I&C systems. These tasks were acknowledged as challenges to be addressed in the later phases of the research effort, and include:

- Better measurement practices and tools
- Guidance for fault selection and realization
- Guidance for automation of fault injection processes -
- Tools for operational profile generation.

- Methods to improve the efficiency and effectiveness of fault injection (pre-fault injection analysis)

- High performance fault injection

2.2.5. Significant Findings of Phase I

Despite the preliminary nature of Phase I, several key findings in Phase I could form the foundation of a technical basis for the application of fault injection to digital I&C systems. Key findings that stand out as noteworthy for the inclusion of technical basis or branch technical position are:

2.2.5.1. Support Guidance for Fault Injection-Based Dependability Assessment Methodology

As indicated in Section 7 and Section 8 of Volume 1, the application of physical-based fault injection to digital I&C systems requires significant coordination of processes and systems to faithfully represent the modified FARM model (Section 3.3 of Volume 1) and the methodology presented in Section 4 of Volume 1. These levels of coordination and integration are unique to physical-based fault injection, and are not a significant issue in simulation-based fault injection. The challenges of applying physical based fault injection to the DFWCS revealed this oversight in the methodology. While the steps in the methodology as presented in Section 4 are necessary to perform fault injection, guidance on how to effectively implement and apply physical based fault injection will be needed to establish a technical basis. The later stages of the research effort (Phases 2 and 3) addressed this challenge with the development of UNIFI.

2.2.5.2. Characterization of Fault injection Methods and Techniques

Section 5 of Volume 1 presents a comprehensive description of contemporary and emerging techniques for fault injection. There are a variety of fault injection techniques and tools for the practitioner or user of fault injection. The claimed capabilities (often stated without assumptions), and tradeoff space make decisions about fault injection difficult. This report provides a structured survey in order to organize fault injection according to classes.

To further aid the reviewer, the benefits, assumptions, and disadvantages of various techniques are summarized so that decision-making regarding the selection or analysis of a fault injection method can be done in a systematic manner. This type of information was compiled and guided by the researchers' extensive experience with fault injection over many years of research and practice in the field. The inclusion of this information as guidance can form a common baseline of understanding of fault injection between the NRC staff and the licensee.

2.3. Phase II Technical Accomplishments

Phase II research efforts were principally devoted to applying fault injection to Benchmark System I. The key activities were:

(1) Developing the fault injection methods and techniques that were applied to Benchmark System I

(2) Developing a fault injection environment for digital I&C systems

(3) Developing pre-injection analysis methods for automatically generating fault lists for digital I&C systems

(4) Evaluating the results of the application of fault injection to Benchmark System I.

The technical accomplishments and findings from realizing fault injection on Benchmark System I digital I&C system are summarized in the following sections.

2.3.1. Identification and Selection of Appropriate Fault Injection Techniques

Benchmark System I was analyzed in Phase II to identify appropriate physical fault injection techniques for the benchmark system based on:

- The types of faults that could affect end-to-end system processing and thus impact I&C system functionality,

- The sub-systems or modules where fault injection should be applied to represent realistic faults.

Based on these criteria, a fault injection technique matrix was developed that indicated appropriate fault injections for each sub-system in Benchmark System I.

Due to the proprietary nature of the Joint Test Action Group (JTAG) test ports on Benchmark System I and the inability to acquire system level source code, the research was limited to implementing two fault injection techniques. These were the in circuit emulator (ICE)-based fault injection technique and the X-bus fault injection technique. Both of these techniques were developed to provide a capability to inject processor level faults into the system processor and protocol level faults into X-Bus.

Several fault injection techniques that were surveyed and reviewed were not feasible or applicable to Benchmark System I. For example, Software Implemented Fault Injection (SWIFI) assumes that the source code of the system software is available. While this may be the case for open OSs such as POSIX or Linux, most digital I&C systems of the type this research tested have proprietary OSs making it difficult to implement this popular type of fault injection on digital I&C systems by an independent assessor.

2.3.2. Development of a Platform Independent Fault Injection Environment

Most fault injection tools have been developed with a specific fault injection technique in mind, targeting a specific system, and using a custom designed user interface. Extending such tools with new fault injection techniques, or porting the tool to new target systems is usually a cumbersome and time-consuming process. Since one of the objectives in this rersearch was to apply fault injection to digital I&C systems typical of the type found in NPPs, a flexible and portable fault injection environment is required for efficient application of the UVA fault injection based dependability assessment methodology.

The research results presented in Section 5 of Volume 2 toward developing appropriate fault injection techniques and environments for digital I&C systems produced a body of work the

NRC and the nuclear industry could use to establish a basis for the development and standardization of fault injection processes.

The work toward developing the UNIFI serves a larger purpose in that it provides a detailed understanding of the complexities and processes involved in implementing physical fault injection effectively and efficiently in contemporary digital I&C systems. The successful application of the fault injection methodology using UNIFI shows that it has the capability to allow fault injections on complex digital I&C systems. The benchmark systems used in this research were not designed or developed with fault injection in mind; therefore, the benchmark systems present the same challenge an independent assessor would encounter if employing a fault injection methodology on a comparable digital I&C system.

2.3.3. Tools for Automated Operational Profile Generation

Context is important in fault injection. Operational profiles must be representative of different system configurations and workloads that would be experienced in actual field operations. For a fault injection-based assessment methodology, the operational profiles must represent the input conditions and system interactions that can occur not only during nominal operations, but also in off-nominal operations and more importantly during “accident” event scenarios.

Gathering profile real plant data across all of these domains of operations is a challenging task. As part of this research effort, an innovative approach to providing high fidelity operational profiles of NPP digital I&C systems was developed. Before this phase of the research project, the methodology provided guidance on how to use an operational profile for fault injection, but provided little guidance on the various means to realize an operational profile. To address this need for the digital I&C systems, a TRACE-based Operational Profile (TOP) model generation tool was developed.

The TOP modeling tool is co-resident with the UNIFI fault injection environment. TOP normally operates as a separate set of programs from LabView and passes its operational profile data sets to the UNIFI/LabView environment. Operational profile data files are generated for the target system for each type of operational profile or test case of interest. The operational profile data for a specific test case or design basis event is then repeatedly used for a set of fault injection campaigns. Changing the operational profile or test case or obtaining a new set of process variables only entails rerunning the TRACE simulation to collect a new set of data.

The important contribution of this work is that a set of tools that were developed that allow profile data to be seamlessly integrated into digital I&C fault injection processes for digital I&C testing in general.

2.3.4. Methods to Improve the Efficiency and Effectiveness of Fault Injection (Pre-fault Injection Analysis)

Pre-injection analysis is a means to reduce or eliminate the “no-response” and the long fault latency problem associated with typical fault injection campaigns. Being a statistical experiment, fault injection testing may require a large number of experiments to be conducted in order to guarantee statistically significant results. Thus, efficiency of the fault injection testing is important.

A typical digital I&C system will have a significant memory space (hundreds of megabytes is not uncommon), a large number of processor register files, special purpose configuration registers, and (relatively) long control cycle times (50 ms to 200 ms). With random fault injection experiments (i.e., with no regard to when and where a fault is injected), a large fraction (up to

90%) of fault injection experiments may have no-response outcomes [Sekhar 2008; Barbosa 2005].

A large percentage of these "no-response" outcomes resulting from fault injections are due to non-use of the corrupted data by the executing program. For example, a randomly generated fault could be injected into a memory location or a processor register that is not used by an application. These instances in which the tested system would not respond to an injected fault do not convey meaningful information about the fault tolerance capabilities of the system. Since time has an associated cost value, if the efficiency of the fault injection campaign is low, then the cost of the fault injection campaign is increased.

The pre-fault injection analysis techniques developed in this research and demonstrated by way of simulation have the potential to significantly improve the effectiveness and efficiency of physical-based fault injection. Preliminary results show at least a 50% improvement over random-based fault injection. Another important benefit of pre-fault injection analysis is being able to deduce the fault equivalence from a space-time perspective once the window of opportunity is known. Knowing the fault equivalence sets of a window of opportunity allows for fault expansion in the window. Fault expansion provides a means to increase the number of equivalent fault injections without having to actually perform each fault injection.

2.3.5. Application of the Fault Injection Methodology to Benchmark System I

The culmination of this research effort was the application of the fault injection-based dependability assessment methodology to the benchmark system. These experiments represent the types of fault injection tests that would be typically conducted by an assessment organization or the digital I&C equipment vendor during the course of a V&V activity. The experiments were chosen to stress the methodology and the supporting tools (UNIFI) in order to provide a basis for determining the effectiveness of the methodology to support system safety assessment activities (e.g., license reviews and failure modes and effects analysis (FMEA)) and PRA activities. All of the experiments were conducted successfully, providing a rich set of information on the fault handling behavior of the benchmark system that would be very supportive of PRA assessment activities.

2.4. Significant Findings for Phase II

This research effort lays a foundation for vendors and regulators to consider fault injection as a method to help inform the assessment of digital I&C systems in nuclear energy applications. Several findings were significant with respect to applying fault injection to the benchmark system digital I&C system, namely:

- Establishing the baseline elements and functionality of a fault injection environment for digital I&C systems;
- Developing new methods and tools for generating high-fidelity operational profiles from NPP simulation tools and establishing a basis for integrated digital I&C and plant analysis and testing.
- Developing new methods to improve the efficiency and effectiveness and to guide fault list generation for digital I&C systems;
- Creating new methods for applying fault injection testing to digital I&C systems.

The fault injection methodology applied to the benchmark system successfully obtained independent information about the benchmark system that corroborated vender and regulator information, and in some cases produced information that would have been very difficult to deduce from vendor information alone. The experience of conducting fault injection often yields more information than just quantifying fault tolerance aspects of the system; it also is a means to comprehend the behavior of complex fault tolerant I&C systems to support overall assessment activities for both the regulator and the developer.

2.5. Phase III Technical Accomplishments

Phase III of the project was dedicated to applying the fault injection methodology developed in Phase I and Phase II to Benchmark System II. The key activities for this phase of work were;

(1) Developing the fault injection methods and techniques that are appropriate and suitable to the benchmark system

(2) Developing an innovative filed programmable gate array (FPGA)-based high performance fault injector for digital I&C systems

(3) Performing a preliminary investigation into the uncertainty factors and sources of uncertainty that could affect fault injection

(4) Presenting the results of the application of the fault injection method to Benchmark System II

(5) Describing the findings from addressing challenges and establishing a basis for implementing fault injection to digital I&C platforms.

The following sections summarize the technical accomplishments and conclusions from of this phase of the research.

2.5.1. Development of a High Performance Fault Injection Environment

As discussed in this set of reports, the need for fault injection techniques to support various fault models for fault injection in manner that are minimally intrusive, controllable, repeatable and reproducible is critical to the application of fault injection methods for digital I&C systems.

On the basis of experiences and lessons learned from previous fault injection efforts, it became apparent that a new approach for injecting faults in digital I&C systems was needed if fault injection was to become practical for digital &C systems. Accordingly, innovative and practical methods that address many of the problems encountered trying to perform fault injection on real-time digital I&C systems were developed. The realization of this research is a FPGA-based high performance fault injection (HiPeFI) fault injector.

The HiPeFI fault injector was used exclusively on Benchmark System II with outstanding success achieved in performing over 10,000 fault injections without any significant issue. By moving to a single, multi-purpose fault injector designed specifically to support diverse fault injection on digital I&C systems, fault injection has been optimized around performance (e.g., minimal intrusiveness) and controllability simultaneously. Furthermore, by uniting a variety of fault injection techniques with a common interface onto a single platform, the integration of the fault injector into digital I&C system fault injection experiments is more or less consistent from one digital I&C platform to the next. This aspect becomes important when fault injection is used as a benchmarking activity. That is, the same set of faults and operational conditions can be

applied to each digital I&C system by the same fault injection technique to form an objective basis for comparison or compliance.

2.5.2. Investigation of Measurement Practices and Uncertainty Factors for Fault Injection

An objective of this research effort was to assess a dependability assessment methodology with respect to oversights or deficiencies that must be addressed in the context of physical fault injection processes for digital I&C systems. First, fault injection is a measurement-based assessment process that depends on sound measurement practices. In spite of steady advances in fault injection research over the past 20 years, quantitative evaluations of dependability attributes remains a complex task lacking standard processes and techniques. Until recently, measurement practices and uncertainty analysis for fault injection testing has been largely overlooked. As fault injection has moved from the laboratory to the working environment of various industries, a greater awareness of the need to incorporate metrology concepts into dependability studies has arisen.

Measurement-based assessment processes must characterize the various types of uncertainty that can occur during the assessment process to better inform the set of conclusions that can be made about measured results, and how those results can be interpreted in a broader, more general context. This becomes especially important when trying to relate or compare fault injection-based findings from one type of system to another. The methodology presented in Volume 1 and Section 1 of this report has not developed this important topic to the degree required for the evaluation of safety critical systems. This initial work is a first step toward developing a better awareness of (1) better measurement practices for dependability studies and (2) identifying to the best extent possible the types of uncertainty that are germane to fault injection processes. In Section 6, a number of potential sources for uncertainty with respect to fault injection processes were identified and characterized.

Further, guidance of toward better measurement practices is one area of the methodology that requires more consideration and improvement. The UVA intends to continue work on this important area to improve the applicability of the methodology for testing digital I&C systems.

2.5.3. Pre-Fault Injection Analysis Revisited

Section 7 of Volume 2 introduced and developed the concept of *Pre-injection analysis* as a means to reduce or eliminate the “no-response” fault injection testing result and to improve the overall effectiveness and efficiency of the fault injection process. However, the application of pre-injection analysis methods to the benchmark systems has not been entirely successful.

The principle reason for this ineffectiveness is mainly due to an assumption that real-time execution trace data was required to realize an acceptable pre-injection analysis. However, acquiring such data was shown to be problematic with both benchmark systems. Given that, it has been shown through simulation studies that the using a pre-injection analysis process can have a significant impact on fault injection studies by only improving efficiency and effectiveness, and allowing the use of fault list reduction methods. As such, efforts were refocused to make pre-injection analysis viable for digital I&C systems. The current idea is to use a powerful interactive disassembler and debugger tool such as IDA Pro to extract control flow and data flow program information that could be used by the pre-injection analysis algorithms to generate highly effective fault lists. This approach is in the initial stages of development, but preliminary results suggest that using tools such as IDA Pro will provide the necessary information needed for pre-injection analysis for large variety of digital I&C systems.

2.5.4. Application of the Fault Injection Methodology to Benchmark System

The culmination of the research described in this report was the application of the fault injection-based dependability assessment methodology to Benchmark System II. The fault injection experiments represent the types of fault injection tests that typically would be conducted by an assessment organization or the digital I&C equipment vendor during the course of a system V&V. The experiments were chosen to stress the methodology and the supporting tools (UNIFI) and HiPeFI to provide a basis for determining the effectiveness of the methodology for supporting system safety assessment activities (e.g., license reviews and FMEA) and PRA activities.

All of the fault injection experiments were conducted successfully, providing a rich set of information on the fault handling behavior of Benchmark System II that would be supportive of PRA assessment activities. Over 10,000 faults were injected into the benchmark system during the course of this research. Approximately 8 gigabytes of system response data were collected for these fault injection campaigns.

The key findings for this effort were used to develop a novel method of fault list generation to support function block level fault injection experiments on RPS and OS code. Critical PRA modeling parameters such as fault coverage, fault latency, and system trip responses were directly measured from the system under test, thereby successfully validating that the UVA assessment methodology is applicable, feasible, and appropriate for digital I&C systems of the type tested to date.

2.6. Significant Conclusions for Phase III

Phase III research efforts were in many ways the most successful in the research project. The technical accomplishments and findings are summarized in the following discussion points:

2.6.1. Optimizing Fault Injection Processes

Fault injection methods for digital I&C systems require flexibility to adapt to different target processors while maintaining low intrusiveness. Digital I&C systems often contain multiple types of processors and FPGAs from different manufacturers in their design. These configurations can exacerbate physical fault injection implementation processes because multiple processor types usually require developing fault injection campaigns specific to the processor type. This is particularly true of ICE-based fault injection methods where a new ICE pod for each different central processing unit (CPU) must be purchased and fault injection instrumentation software must be written for each processor. As observed in the Benchmark System I fault injection research, commercial off-the-shelf (COTS) debugging tools and environments for embedded systems (e.g., ICE machines and interactive debuggers) are not designed with fault injection in mind; thus, their performance in this capacity is limited.

As the diversity of different digital I&C technologies increases, physical fault injection methods must keep pace with these changes in a way that allows developers and regulators to establish a stable base which remains consistent with changing technology. One approach to addressing this dilemma is to adopt fault injection methods built from existing organization standards for IC testing and embedded software debugging. These include Institute of Electrical and Electronics Engineers (IEEE) JTAG/ Scan Chain Implemented Fault Injection (SCIFI) standards, the IEEE 5001 Nexus Standards, the Intel XDP standard and the Motorola Background Debug Mode (BDM) standards. These standard interfaces are available for nearly all semiconductor reference designs – CPUs, FPGAs, embedded cores, etc. The key point is that realizing a fault injection capability around these standardized test interfaces specifically for digital I&C systems

can obviate many of the implementation challenges physical-based fault injection processes face.

The approach developed by this research project was to unite on a single high performance FPGA-based fault injection module a variety of test port-based fault injection methods in a modular fashion. By moving to a single multi-purpose fault injector designed specifically to support diverse fault injection campaigns on digital I&C systems, the fault injection process was optimized around performance (e.g. minimal intrusiveness) and controllability simultaneously. Furthermore, by uniting a variety of fault injection techniques with a common interface onto a single platform, the integration of the fault injector into a digital I&C system is more or less consistent from one digital I&C platform to the next. The performance of the HIPEFI fault injection module was several orders of magnitude faster than ICE-based fault injection and commercial-based on-chip debuggers. This type of performance allows for fault injection to be effectively invisible (in time) to the target system.

2.6.2. Measurement of Critical Parameters

Previous fault injection applications (Benchmark System I and DWFCS) were challenged by imprecise measurements of critical parameters such as fault/error detection latency. The imprecisions of the measurements were mainly due to the use of timestamps in error logs. The error messages of Benchmark System I and the DFWCS are time stamped when they enter the error log, not at the time the error detection predicate is asserted. Therefore, the measurement of fault/error latency from the error logs was overly conservative.

Measurement theory for a fault injection methodology must be developed and incorporated as a specific step just like all of the other steps in the process. Since error detection response is a critical measurement, the process by which error measurements in fault injection experiments should be carried out had to be developed. Specifically, a single time reference was required (e.g., a precise global clock), from which all time references would be made. Moreover, this time reference should be independent of the target system, and preferably part of the fault injection environment.

The Labview precision sampling clocks were used in the UNIFI fault injection to provide an independent time stamp for all of the output response data from the target system.

2.7. References

[Barbosa 2005] Barbosa, R., Vintern, J., Fokesson, P., Karlsson, J. "Assembly-Level Pre-Injection Analysis for Improving Fault Injection Efficiency." *Lecture Notes in Computer Science, vol. 3463*, 2005: 246-262.

[Smith 1997] D.T. Smith, B.W. Johnson, N. Andrianos, J.A. Profeta III. "A Variance Reduction Technique Using Fault Expansion for Fault Coverage Estimation." *IEEE Transactions on Reliability*, September 1997: 366-374.

[Sekhar 2008] Sekhar, M. *Generating Fault Lists for Efficient Fault Injection into Processor Based I&C Systems.* Charlottesville, VA: University of Virginia, 2008.

[Pierce 2008] W. Pierce, J. Larson, L. Miras. *Reverse Engineering Code with IDA Pro.* Elsevier Science, 2008.

3. CHALLENGES AND LESSONS LEARNED

3.1. Introduction

Over the course of this research project many challenges were encountered and as a consequence many important lessons were learned along the path of discovery. These challenges, how they were addressed, and the lessons learned are described in this section for the broader purpose of informing the digital I&C systems community.

3.2. Challenges

3.2.1. Third Party Assessments

Fault injection performed by the vendor has the distinct advantage that all of the technical knowledge of the system (both hardware and software) is already in place and for the most part in-house. This is not the case for third party assessors such as universities, national laboratories, and independent certification organizations (e.g., TÜV). Third party assessors not only require traditional training on a system, but also continued and involved technical support from the vendor of the system to effectively implement and conduct fault injection campaigns. It cannot be overstated that the level of technical support and interaction is significant for third party assessors. Success is directly proportional to the level of technical support and should be planned for the entire duration of the effort. Expert personnel in the vendor organization should be identified as early as possible. These key personnel should be briefed in entirety on the goals of the project, the needs of the project, and the expected outcomes of the project. Based on experiences with both benchmark systems, it is prudent to plan for 25 percent of the project effort to be dedicated to vendor technical interactions.

3.2.2. Choosing and Implementing Fault Injection Techniques

As presented in Section 5 of Volume 1, the choices of fault injection techniques for any given digital I&C system are diverse and varied. From the high vantage point, it would appear the users of fault injection techniques have many choices. In reality, this is usually not the case. There are several factors that tend to constrain, limit, or focus the types of fault injection techniques that can be deployed on a particular digital I&C system platform. This was a problem that was encountered on Benchmark System I.

For example, the researchers wanted to move away from ICE-based fault injections (for all of the reasons stated previously in Section 7 of Volume I), however alternative options such as JTAG/SCIFI and SWIFI-based fault injection were not viable due to the inability to obtain proprietary information about the benchmark systems to implement these fault injection techniques. It is important to note that this type of impediment would only occur with a third party assessor.

Other factors that tend to down-select or focus choices are related to the technology used in a digital I&C system. Benchmark System I tended to use older, more mature technology that was lacking in newer test port capabilities (e.g., on-chip debugger (OCD) test ports). As such, OCD-based fault injection was not an option for this target system. In some cases, the exclusive use of FPGA technology can constrain the choices to more advanced fault injection techniques such Assertion Based Verification Fault Injection (ABVFI) [Bingham 2009], and JTAG/SCIFI.

The key point is that the user or assessor must make determinations of the fault injection methods to use that are not entirely based on the desired attributes of the fault injection

technique, but also are dependent on what is realizable on the target system. Choosing an appropriate fault injection technique to deploy on a target system should be begun as early as possible, and will require close coordination with the vendor (if a third party is doing the assessment) in that determination.

3.2.3. Developing a Robust Fault Injection Environment

Early experience with developing a fault injection environment showed that moving from the requirements of the FARM model and the methodology to a fully supported and automated fault injection environment was not a trivial task. The issues faced here were that the FARM model and the methodology are largely abstract models that provide little guidance on how to implement a fault injection environment. Related research on fault injection environments such as Generic Object Oriented Fault Injection (GOOFI) and Xception offered some help in better defining the requirements of the fault injection environment. However, the open literature reports tended to describe the features of the fault injection environments rather than their implementation details.

In addition to the basic requirements imposed on the fault injection environment by the methodology and the FARM model, the fault injection environment needed to be extensible and modular to support various types of digital I&C system interfaces. The amount of time and effort to design the fault injection environment (UNIFI) was seriously under-estimated by project planning. In fact, refinements to UNIFI continued to be implemented until the very end of the research project.

Having an effective fault injection environment in place before a fault injection project begins is a considerable advantage. Having a developed and tested fault injection environment in place allows the focus of the project to be directed at critical activities; such as the development of fault injection experiments, implementing fault injection techniques, conducting the experiments, and methods for data reductions.

3.2.4. Operational Profile Generation

The decision was made from the outset of the research project to use the TRACE NPP simulator tool to generate operational profiles. The main challenges encountered with this effort were; (1) translating the process data from the TRACE models into data that is representative of real time sensor data that would be normally acquired by the target system during its operation, and (2) structuring the data files into formats that the could be read by the target system. These activities required some time to convert the simulator data into sample representative data into data that could be input into the target systems RPS.

3.2.5. Integration of Fault Injection into Target Systems

An important observation is that each system on which fault injection were performed involved a different set of integration interfaces and practices. Both benchmark systems had different input/output (I/O), fault injection control interfaces, error logs, and monitoring interfaces. As such, interfaces had to be modified or developed for each of these functions. Once the interfaces were implemented, testing had to be performed to ensure that the interfaces operated as intended, which took additional time that had not been included in the research schedule. The modular nature of UNIFI made these integration tasks easier; however, these experiences point to the fact that digital I&C system interfaces are likely to be very different from system to system, and the time to develop interfaces should be included in the project planning.

3.2.6. Measurement

As discussed in these volumes, precise measurement of system responses is critical to a measurement-based assessment process. It is easy to lose track of this simple concept by getting "tunnel vision". Specifically, there is a tendency to be preoccupied with the many design and implementation details to the point where a vital part of the process may be overlooked or taken for granted.

Incorporation of good metrology concepts is the next step for the maturity of fault injection methods. To do so, it is necessary to regard tools such as those used for fault injection and data collection as measuring instruments, and to scientifically obtain measurement results that can be compared and reproduced by others. Challenging this approach is the fact that digital I&C systems are not typically designed to be monitored to the level and extent required for dependability evaluation by fault injection. Nonetheless, this challenge is not seen as being so great that it requires significant basic research. It is more likely that fault injection users must begin to understand good metrological practices and incorporate them into their processes.

3.2.7. Data Analysis and Reduction

Automated fault injection processes produces vast amounts of diverse data. Approximately 10 gigabytes of fault injection data were collected over the course of this research project. This amount of data requires at the very least user-assisted data reduction methods and tools. This aspect of the project was found to be the most vexing in terms of trying to find a general solution for data reduction and analysis. The approach to this problem was to write specialized parsing scripts to iteratively parse the data files to extract important data. This worked reasonably well, but it was still a very time-intensive process. In addition, each benchmark system needed its own set of data reduction parsers because each system produced data in a format unique to that system. Much work needed for this aspect of the methodology and in general for fault injection processes as a whole. The use of relational data bases, data mining techniques, and data visualization methods are some approaches that might solve this problem. Only a few research efforts within the fault injection community have seriously addressed this issue [Munkby 2008].

3.2.8. Fault List Generation and Pre-injection Analysis

Generating fault lists for a fault injection experiment or campaign is a critical activity for fault injection. The fault list can be thought of as a set of directives to the fault injector apparatus. Each of the directives is under experimental control of the experimenter. The fault list is used to instruct the fault injection process according to a particular campaign purpose. As part of this effort, the researchers realized that much work was needed to develop fault lists that conveyed information about the software/hardware structure on the digital I&C system so the system could be observed from this perspective. Several techniques of extracting information from the system to generate fault lists were successfully developed and implemented. These were map file-based fault lists and function block fault lists. Map file-based fault list generation exploits the map file from complier/linker of the target system to identify program variables, data segments, code segments, global variables, etc. These structures have meaning to the programmer of the system and thus the fault injection use can target specific instances of these structures.

Another approach the research developed is *function block oriented fault injection*. Most digital I&C systems of the type found in NPP safety systems are programmed by function block programming (e.g., International Electrotechnical Commission IEC 61131). Function block oriented fault injection is aimed at characterizing the function block at its lowest level – data structures, assembly code, parameters, and internal and interface variables – so that both hardware and proposed software fault models can be applied to a function block. The main

goal of function block oriented fault injection is to promote traceability from the function block representation (high level) to the low level implementation (assembly code, data structures, and variables that are realized on the target I&C machine). The applications development engineer understands the operation of the I&C system through the function block representation.

Both of these efforts were a significant challenge to address. Each benchmark system required a new fault list extraction module to be written because the compilers were radically different on each machine. However, the high level algorithm to generate each type of fault list is fairly general.

Another important research effort was to develop a process for performing pre-injection analyses. Despite the promising results in simulation, the application of pre-injection analysis methods to the benchmark systems was not entirely successful. The principle reason for this ineffectiveness was due to the initial assumption that real-time execution trace data would be required to realize pre-injection analysis. However, acquiring such data was shown to be problematic on both benchmark systems. Initial attempts at implementing pre-injection analysis on the benchmark systems were incorrect. A completely different approach using advanced interactive dissembler tools and debuggers like IDA Pro to pre-analyze fault lists has been developed.

3.3. Lessons Learned

Based on the many challenges and experiences encountered during this project, an awareness has been developed of the requirements for implementing physical fault injection on digital I&C systems. As such, this awareness can be conveyed as lessons learned or knowledge that furthers the state of the practice for both NRC and the I&C community. The most important lessons learned are summarized in the following sections.

3.3.1. Use a Model of Fault Injection

The FARM model developed and employed in Volume 1 serves a significant purpose in the overall methodology and to the fault injection user. The importance of the model is to provide the fundamental connection between empirical observations and a mathematical expression of quantitative relationships. There is a direct connection from theory to practice. The FARM model is the basis for the methodology and the methodology is realized by the UNIFI fault injection environment, and experiments are conducted under the guidance of statistical models. The FARM model presented in Section 3 of Volume 1 is a model that can be used for fault injection. It is not imperative to use the FARM model, but any model used should provide the same level of detail as that provided by the FARM model.

3.3.2. Understand the Statistical Model

The statistical model is often overlooked in the process of fault injection. So much work is done getting to the point where fault injection can be accomplished on a digital I&C system that the urge to just start injecting faults into the system is tempting. Understanding the implications and assumptions of statistical modeling before starting fault injections allows the user to construct experiments with a clear purpose in mind. This lesson was learned after several thousand experiment) had been performed. The choices of statistical models are many, but for most cases the three presented in Volume 1 will cover most cases for the estimation of coverage.

3.3.3. Match the Fault Injection Technique to the Target System

Benchmark System I and Benchmark System II were completely different types of computer architectures. Fault injection techniques that were employed on Benchmark System I would not have worked on Benchmark System II. The lesson to be learned is that fault injection technique selection must take into account the amount of intrusiveness that can be tolerated by the target system. Benchmark System I could tolerate more intrusiveness because of its asynchronous message passing operation. Benchmark System II was a clock synchronized architecture, and as such the amount of intrusiveness it could tolerate was considerably less than Benchmark System I.

3.3.4. Fault Model Selection

Fault model selection almost always begins with first selecting fault models that represent faults that the system was designed to detect/tolerate by the designer, that is, the *fault hypothesis* of the system [Elks 2005]. These models may include a number of fault classes as indicated in Column 1 of Figure 1-4 in Volume 1, such as hardware faults (permanent and transient), commission faults, omission faults, interaction faults, etc.

However, just because a system is designed to tolerate certain classes of faults, it does not mean that it is not susceptible to other types of faults. Thus, the fault hypothesis of the system does not guarantee all representative faults for the system or for that matter any representative faults for the system have been selected.

The evidence of fault representativeness comes from *empirical or experiential* sources that indicate that certain components have certain failure mechanisms under certain conditions. These failure mechanisms are then paired with the most appropriate fault model to represent the failure mechanism.

Empirical evidence of faults/failures in digital I&C systems is often guided by the use of failure databases based upon observed failures of systems in the field. Databases of this type are most useful for characterizing failures when the failure data is homogenous to a specific type or make of system. However, these databases are very rare, and most often proprietary to specific manufacturers. Beyond this use, there are a number of concerns with relying solely on failure database for determining fault representativeness.

First, faults and failures that occur in systems are often *technology dependent*. A digital I&C system built from 1990s electronic technology will not have the same fault susceptibility profile as a contemporary digital I&C system. As example, very large scale integration (VLSI) semiconductor manufacturing processes in the 1990s were still at that time building semiconductors with relatively large transistor feature sizes, and as such, the susceptibility to transient faults due to cosmic particle strikes and electromagnetic interference (EMI) were almost non-existent. This is not the case in contemporary ICs.

Secondly, the operational or environmental context of digital I&C system is important to its fault and failure susceptibility profile, and this fact is poorly represented in most databases. Lastly, failure databases often report how the system failed, but rarely report the underlying cause or failure mechanism of the system.

Experiential data is usually collected from accelerated testing methods and/or high fidelity simulation of semiconductor physical processes to determine failure mechanisms. These methods usually determine the upper bound or worst case scenario for failures-in-time (FIT) for a component.

Taken altogether, there are no short cuts toward determining a representative fault model or fault-load for a digital I&C system. The most prudent approach is to employ an “all-sources” approach where all available information is used to select appropriate fault models.

The selection of fault models for digital I&C systems should be more structured and this process should be included in the fault injection methodology as a support step. The steps of the fault model selection process should include the following activities:

- Examination of the fault hypothesis of the system.
- The use of a structured fault taxonomy (e.g., like the one presented in Section 1.7) as a starting point to help guide the fault model selection process.
- Examination of failure data from empirical and experiential data sources that is relevant to the system.
- The operational context of the system.
- The interaction context of the system.

The output of a fault model selection process should produce a set of faults that is relevant to a particular digital I&C system, but more importantly the process of fault model selection produces an audit or evidence trail so the assumptions, factors for determining the fault models can be assessed during the licensing and review activities.

3.3.5. Vendor Participation is Essential

As stated above, the implementation of a fault injection process on a digital I&C system requires knowledge that is over and beyond what is typically found in training classes or workforce development classes. The type of knowledge that is required is at the system designer level, often contained in system level design and development documents. This type of information is often proprietary in nature and thus may or may not be disseminated to the third party assessor. In these cases, it may be necessary to have second option solutions to keep moving forward.

3.3.6. Employ Good Measurement Practices

One of the first steps or tasks that should be undertaken in a fault injection process is to develop an awareness of good measurement practices and how they can be used in the fault injection process. Without sound measurement principles in place, keeping track of measurement precision and uncertainty is difficult and could taint the results of the experiments. The methodology may need to be modified to account for this important step, and as such, sound metrological practices are required with respect to fault injection.

3.3.7. Uncertainty Identification and Analysis

The difficulties in comparing and reproducing results of dependability measurements arise from a wide range of uncertainties associated with measurement procedures, non-representativeness, instruments, and monitoring processes of the target system. Examples of non-representativeness are non-realistic workloads and fault-loads. Errors can occur when the wrong time instants are chosen for collecting measurements. Also, approximate implementation of a measurand definition can result in errors as well as instrument uncertainty due to misconfiguration of the measurement tools used in the process. Such factors cause variations

in measurement results. It is therefore necessary to the best extent possible to characterize and estimate the magnitude of such variations and to assess the *metrological compatibility* of measurement results, that is, whether different measurements, possibly obtained in different studies, relate to the same measurand.

In combination with good measurement practices, the user/assessor should examine the potential sources of uncertainty and what types of uncertainty may arise with their fault injection procedures. An additional step in the methodology should be added to account for uncertainty identification and analysis.

3.3.8. Data Reduction and Analysis

Data reduction and analysis for fault injection must be addressed as early as possible in the course of a fault injection project. For the reasons described above, vast amounts of diverse data can be acquired over a relative short period of time. Extracting information from this data to derive/estimate model parameters can be a daunting and labor intensive process. Data extraction techniques and data mining techniques must be used to effectively reduce the data to the important data sets.

3.4. References

[Elks 2005] Elks, C. *A Theory of Run-Time Verification.* Charlottesville, VA: University of Virginia, Ph.D. Thesis, 2005.

[Munkby 2008] G. Munkby, S. Schupp. "Improving Fault Injection of Soft Errors Using Program Dependencies." *IEEE Testing Academic and Industrial Conference.* IEEE, 2008. 77-81.

[Bingham 2009] S. Bingham, J. Lach. "Enhanced Fault Coverage Analysis Using ABVFI." *Workshop on Dependable and Secure Nanocomputing.* 2009.

4. RECOMMENDATIONS AND CONCLUSIONS

4.1. Introduction

This Section presents final recommendations and conclusions for the project. The recommendations are classified into three types: technology related, methodology related, and program related. Technology related recommendations enable or enhance fault injection on digital I&C systems. Methodology related recommendations are steps that the must be added to the methodology to address a limitation or deficiency. Program related recommendations address the programmatic level to facilitate the use of fault injection-based methodologies.

4.2. Methodology Related Recommendations

In the course of the research project and after applying the methodology to two benchmark systems at least three changes or additions to the methodology were identified:

(1) Develop and Implement Sound Metrological Practices –The UVA fault injection-based methodology should include as a basic step a process for characterizing the measures of interest, how the measurands are to be quantified in the context of the fault injection experiment, and the metrological principles used to quantify the measurands in the presence of known uncertainties. This step of the methodology should occur after the measures of interest (model parameters) are identified.

(2) Identify the Sources of Uncertainty and Minimize –The methodology should include a step subsequent to the measurement practices step that identifies to the best extent possible the potential sources of uncertainty in the quantification of the measurands. The steps should address the sources enumerated in Section 6 of Volume 3 and any others that are pertinent to address uncertainty in the fault injection process.

(3) Define Fault Injection Selection Criteria – A step should be added that indicates how a particular fault injection technique is selected for a particular digital I&C system. This step is needed to justify why a particular technique was chosen over another technique on the basis of the criteria established or stated. This step will promote end to end connection between the fault injection theory model the fault injection technique ultimately employed.

As a global recommendation, the methodology steps should be updated with new information and findings from this effort where needed. Figure 4-1 presents the new process flow of the methodology with steps 1 and 2 added. These steps are; (1) definition of measurement methods and (2) identify uncertainty shown as steps (1a) and (3a) in the figure. The measurement characterization step (1a) takes as inputs the parameters of interest to be measured by the fault injection process. The assessor determines the appropriate means to measure the data guided by metrological practices. The output of this step is a method for measuring the degree of resolution needed for the measurement. Step (3a) is associated with identifying sources of uncertainty that can impact the experiment results. Potential sources are identified, their impact assessed, and if the impact is believed (or estimated) to be significant then additional steps should be taken to minimize the uncertainty if possible.

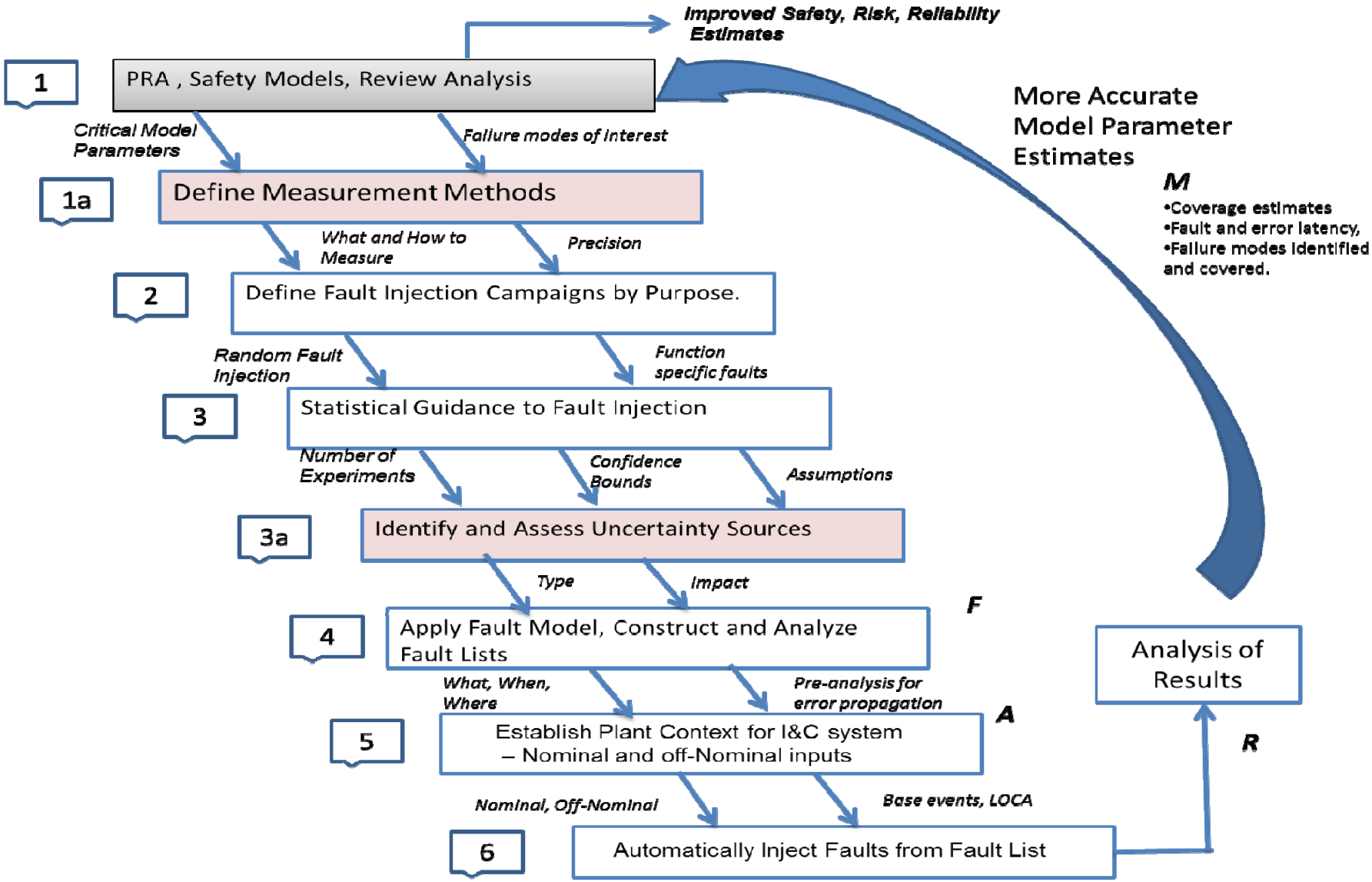

Figure 4-1 Modified methodology process view (1a and 3a are new steps)

4.3. Technology Related Recommendations

In the course of the research project and after applying the methodology to two benchmark systems, a number of technology related issues were identified that can be resolved with modest changes. These changes are:

(1) **Adaptation of Standard Test Interfaces to Digital I&C Systems** – Fault injection and fault injection based methodologies can be more consistent from one system to the next if all digital I&C systems eventually adopt industry standard test and debug interfaces. The interfaces are typically governed by IEEE standards, but on occasion they are IC manufacturer-specific, such as the BDM interface. These types of interfaces allow fault injection to be employed in a more flexible and less obtrusive manner than most fault injection techniques. In addition to the benefits for fault injection, these standard test and debug interfaces enhance the testability of digital systems. This recommendation will have no bearing on current digital I&C systems, however future I&C systems and upgrades to digital I&C systems can benefit from this recommendation.

(2) **Tools for Analyzing Data** - Given the vast amounts of data produced by fault injection campaigns, data reduction and analysis tools are required to efficiently parse and mine the data for important events and conditions. The techniques to accomplish these tasks are within the realm of conventional data mining and visualization methods, however, these techniques have yet to be applied to fault injection data in any substantial way.

(3) **Tools for Organizing Data in a Standard Review Plan Context** - Ultimately, the information garnered from fault injection methods will be used to validate digital I&C systems. The organization of the data can be used to assess claims of sufficiency of various fault and error detection capabilities of the system. The type of tool for organizing this data is something similar to the diversity evaluation spreadsheet tool described in [NRC 2010].

4.4. Programmatic Related Recommendations

Addressing the technology and methodology issues are not sufficient in themselves to fully enable fault injection-based dependability assessment to be used in digital I&C systems. Specifically, programmatic level actions are needed to help both the NRC and the vendors fully understand the concepts of fault injection and to implement consistent guidance for using fault injection in V&V or the acceptance testing of digital I&C systems. The following steps are proposed to facilitate a broader understanding:

- **Establishment of Staff review Guidance** – If the NRC decides that fault injection-based methodologies are applicable to digital I&C systems and add value to the review process, the material contained in these volumes would be a starting point for synthesizing staff guidance on the applicability of fault injection for digital I&C systems. The staff guidance would provide the first step toward a consistent view of fault injection between the NRC and licensees/vendors.

- **Regulatory Guide** – Over and beyond the staff guidance, a regulatory guide, which could provide more succinct definitions, positions and requirements as official NRC guidance to the nuclear industry.

- **NRC Workforce Development** – Fault injection, while not overly complex, is not well known to the nuclear engineering community nor to the I&C community. Technical

classes, seminars, and hands-on seminars would greatly facilitate the understanding at the level that would be required for the NRC and the nuclear industry.

4.5. Final Comments

The experience of conducting fault injection campaigns often yields more information than just quantifying the fault tolerance aspects of a system; it also is a means to circumspect and comprehend the behaviors of complex fault tolerant I&C systems to support overall assessment activities for both the regulator and the developer. Fault injection experiments cannot be performed without gaining a deeper understanding of the system. The process itself is a learning experience, providing a richer insight into how a system behaves in response to fault introduction. The inclusion of fault injection information into review processes and PRA activities can only enlighten the review processes of digital I&C systems. Finally, the process of conducting fault injection allows two very important pieces of information to come into direct connection with each other: What the system is supposed to do, and what it actually does. This information is essential for V&V activities and license reviews.

5. REFERENCES

[NRC 2010] **NUREG/CR-7007**, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Washington DC, February 2010.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-7151
Volume 4

2. TITLE AND SUBTITLE
Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems: Volume 4

3. DATE REPORT PUBLISHED
MONTH: December
YEAR: 2012

4. FIN OR GRANT NUMBER
N6124

5. AUTHOR(S)
C.R. Elks, N.J. George, M.A. Reynolds, M. Miklo, C. Berger, S. Bingham, M. Sekhar, B.W. Johnson

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)
The Charles L. Brown Department of Electrical and Computer Engineering
The University of Virginia
Charlottesville, Virginia

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES
S.A. Arndt, J.A. Dion, R.A. Shaffer, M.E. Waterman, Project Managers

11. ABSTRACT (200 words or less)
This report is volume 4 of a multi-volume set of reports that present the cumulative efforts, findings, and results of NRC contract JCN N6124 – "Digital System Dependability Performance"

This report (Volume 4) presents the findings, lessons learned, and recommendations of applying a fault injection-based quantitative assessment methodology to two processor-based digital I&C systems for the purpose of evaluating the capabilities of the method to support NRC probabilistic risk assessment (PRA) and standard review processes for digital I&C systems. The purpose of this work is to help inform the development of regulatory guidance processes for digital I&C systems and potential improvements to the licensing process of digital I&C systems in nuclear power plant (NPP) systems. The work described herein presents: (1) reflective overview of the project and accomplishments, (2) the lessons learned from Phase I, Phase II and Phase III of the project, (3) significant findings, (4) recommendations for establishing a basis for using fault injection in digital I&C systems, and (5) future work.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Fault injection, dependability, PRA, digital instrumentation and control systems, I&C

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG/CR-7151
Volume 4

Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems

December 2012