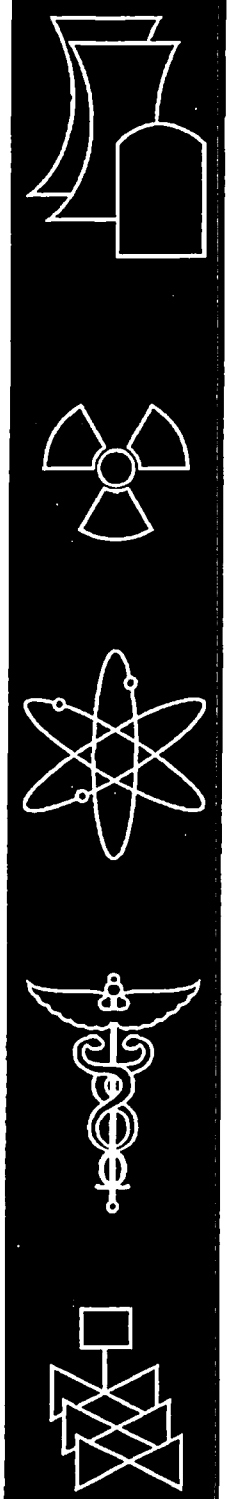
NUREG/CR-6901



Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments

The Ohio State University

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

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: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@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, and 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).

NUREG/CR-6901

Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments

Manuscript Completed: October 2005
Date Published: February 2006

Prepared by
T. Aldemir[1], D.W. Miller[1], M.P. Stovsky[1], J. Kirschenbaum[2], P. Bucci[2],
A.W. Fentiman[1], L.T. Mangan[1]

[1]The Ohio State University
Department of Mechanical Engineering
Nuclear Engineering Program
Columbus, OH 43210

[2]The Ohio State University
Department of Computer and Information Science
Columbus, OH 43210

S.A. Arndt, NRC Project Manager

Prepared for
Division of Fuel, Engineering and Radiological Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code K6472

ABSTRACT

Digital systems offer the potential to improve plant safety and reliability through features such as increased hardware reliability and stability and improved failure detection capability. Because of these advantages and obsolescence issues with current analog systems there is a desire to use more digital systems in both safety and non-safety systems in nuclear power plants. However there are currently limited guidance and consensus on the reliability modeling of digital systems, which prohibits the use of risk informed regulatory reviews of digital systems. While the static event-tree/fault-tree (ET/FT) approach has been used in the reliability modeling of digital I&C systems in nuclear power plants, numerous concerns have been raised in the reliability literature in the past about the capability of the ET/FT approach to properly account for dynamic interaction between the digital systems and the rest of the plant processes and within the hardware and software of the digital system itself. Any modeling method that is used should be capable of modeling the digital system to a level sufficient to ensure that all risk important interaction are included, as well as, all of the systems features that are required by current regulatory guidance.

This report describes the issues that need to be addressed both in the reliability modeling of digital instrumentation and control (I&C) systems and in the incorporation of the digital I&C system reliability models into existing PRA models for improved risk-informed decision making with regard to a digital system's contribution to plant risk. The report also outlines the acceptance criteria to be used for the digital I&C system models prior to the implementation in regulatory applications.

All the methodologies reviewed in the report have features that can make them preferable over the others depending on the system under consideration, including the conventional ET/FT approach. The methodologies that rank as the top two with most positive features and least negative or uncertain features (using subjective criteria based on reported experience) are the DFM and dynamic event tree approach/Markov approach, each with different advantages and limitations. Regarding the applicability of the conventional ET/FT approach to digital I&C systems, no actual comparisons to dynamic methodologies have been encountered in the literature. The extrapolation of existing computational evidence based on a few comparative studies on dynamic systems seems to indicate that the ET/FT approach may yield satisfactory results for certain class of systems. It is concluded that no single available methodology satisfies all the requirements. Some promising methodologies are identified and the need for a benchmark exercise for a comparative evaluation of the promising methodologies is indicated.

FOREWORD

In 1995, the U.S. Nuclear Regulatory Commission (NRC) issued the Probabilistic Risk Assessment (PRA) Policy Statement, which encourages the increased use of PRA and associated analyses in all regulatory matters to the extent supported by the state-of-the-art in PRA and the data. This policy applies, in part, to the review of digital systems, which offer the potential to improve plant safety and reliability through such features as increased hardware reliability and stability and improved failure detection capability. However, there are presently no universally accepted methods for modeling digital systems in current-generation PRAs. Further, there are ongoing debates among the PRA technical community regarding the level of detail that any digital system reliability model must have to adequately model the complex system interactions that can contribute to digital systems failure modes. Moreover, for PRA modeling of digital reactor protection and control systems, direct interactions between system components and indirect interactions through controlled/supervised plant processes may necessitate the use of dynamic PRA methodologies.Dynamic methodologies are defined as those that can account for the coupling between systems through explicit consideration of the time element in system evolution. These methodologies include Dynamic Fault Trees, Markov models and Dynamic Flowgraph methodology.

While the static event-tree/fault-tree (ET/FT) approach has been used in modeling the reliability of digital I&C systems in nuclear power plants, the reliability literature has raised numerous concerns regarding the capability of the ET/FT approach to properly account for interactions. Studies reported in the literature indicate that such interactions may lead to coupling between the triggered or stochastic logical events (e.g., valve openings, pump startups) during an accident with significant impacts on the predicted system failure probabilities The lack of treatment of such dynamic interactions means that the ET/FT approach may not identify or properly quantify potentially significant dependencies between the failure events.

This report investigates a number of dynamic PRA methodologies, with regard to their applicability for modeling digital systems in nuclear power plant PRAs. Specifically, these methodologies include Markov modeling, dynamic flowgraph modeling, and Petri net approaches. This report also describes the issues that need to be addressed, in both modeling the reliability of digital I&C systems and incorporating digital I&C system reliability models into existing PRA models to determine the overall plant response. In addition, this report outlines proposed preliminary acceptance criteria that could be used for digital system models prior to their implementation in regulatory applications.

This report is intended to provide technical support for the development of regulatory guidance for risk-informing digital systems and guidance on the best approaches for the development of a tool to support independent evaluation of the risk associated with the use of digital systems in commercial nuclear power plants.

Carl J. Paperiello, Director
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

CONTENTS

Figures

Tables

EXECUTIVE SUMMARY

Digital systems offer the potential to improve plant safety and reliability through features such as increased hardware reliability and stability and improved failure detection capability. There are currently limited guidance and consensus on the reliability modeling of digital systems. This report describes the issues that need to be addressed both in the reliability modeling of digital instrumentation and control (I&C) systems and in the incorporation of the digital I&C system reliability models into existing PRA models for improved risk-informed decision making with regard to digital system contribution to plant risk. The report also outlines the acceptance criteria to be used for the digital I&C system models prior to the implementation in regulatory applications.

A conclusion of the National Academy of Sciences Committee on the Safety and Reliability Issues of Digital Instrumentation and Control Systems in Nuclear Power Plants is that digital I&C systems (and digital systems in general) should not be addressed only in terms of hardware or software. From a reliability modeling perspective, this conclusion implies that the dynamic interactions between: a) the reactor protection and control systems and controlled plant physical processes (e.g., heatup, pressurization), and, b) the components of the reactor protection and control systems itself (e.g., communication between different components, multi-tasking, muliplexing) need to be accounted for. These interactions will be referred to as Type I and Type II interactions, respectively.

While the static event-tree/fault-tree (ET/FT) approach has been used in the reliability modeling of digital I&C systems in nuclear power plants, numerous concerns have been raised in the reliability literature in the past about the capability of the ET/FT approach to properly account for Type I interactions. Studies reported in the literature indicate that such interactions may lead to coupling between the triggered or stochastic logical events (e.g., valve openings, pump startups) during an accident with significant impacts on the predicted system failure probabilities. Similar arguments can be made for Type II interactions as well, based on the computational evidence for very simple situations. The lack of treatment of such dynamic interactions means that potentially significant dependencies between the failure events may not be identified or properly quantified.

Dynamic methodologies are defined as those that can account for the coupling between the triggered or stochastic logical events in system reliability modeling through explicit consideration of the time element in system evolution. Historically, the development of dynamic methodologies that have been proposed to account for Type I and Type II interactions have evolved separately with a few exceptions. Although dynamic methodologies provide a much more accurate representation of probabilistic system evolution in time than the ET/FT approach, generally it is difficult to integrate a dynamic model into existing plant PRAs almost all of which are based on the static ET/FT approach.

The dynamic methodologies proposed for the representation of Type II interactions can be grouped as follows:

- Markov models
- Dynamic Flowgraph methodology (DFM)
- Bayesian methodologies
- Petri net methodologies
- Test based methodologies
- Software metric-based methodologies
- Black-box methodologies (Schneidewind Model)

These methodologies use diverse approaches to the reliability modeling of digital I&C systems including:

- a discrete-state representation of the system with transition rates between states estimated by fault injection (Markov),
- a discrete-state representation of the system with the physical and software component functional behavior modeled through decision tables (DFM),
- using a software tool that can represent the structure of the program, including requirements, functions, and data structures and Bayesian updating,
- a graph theoretic approach with simulation (Petri nets),
- running a number of tests and measuring the number of failures,
- using software metrics gathered in the software development process to approximate the reliability of software,
- using a non-homogeneous Poisson process as the basis to predict reliability of software components (Schneidewind Model).

The Markov model approach is able to integrate software's ability to mask hardware faults, but does not provide enough information to justify its usage of failure rates, repair rates and fault injection. Dynamic flowgraphs are able to model both Type I and Type II interactions and produce output that can be readily incorporated into existing PRAs. However, physical process representation in the description of Type I interactions may need to be validated. The Bayesian updating approach is able to integrate changes in failure data to produce new values for the reliability measures, but is only used for software and is only useful when applied to software that was developed using a specific method. While the Petri net approaches are able to model Type II interactions well, the size of the resulting model may affect its solvability in a reasonable amount of time. The results of testing and metrics approaches are able to integrate easily with a PRA, but are based on only testing the software component of the digital system or using metrics to evaluate the software component. The Schneidewind model was useful for its applicability to the space shuttle but would require software failure data for nuclear power plants that are currently unavailable. Finally, even if the data were available, such data may not apply accurately to this particular model due to the model's assumptions about the development process of software.

The dynamic methodologies that have been proposed for the modeling of Type I interactions can be divided into three main categories:

- Continuous-time methods
- Discrete-time methods
- Methods with visual interfaces.

While the methods with visual interfaces are also either continuous or discrete time methods, the reason they are listed separately is because the availability of a visual interface is usually regarded as rendering them more user-friendly.

Continuous-time methods consist of

- the continuous event tree (CET) method,and,
- the continuous cell-to-cell-mapping (CCCM) method.

These methods can use accurate descriptions of system dynamics to model Type I and Type II interactions and yield the probability of finding the system at a specified location in the system state-space at a specified time in a specified configuration.

The discrete-time methods include the following:

- DYLAM (Dynamical Logical Methodology)
- DETAM (Dynamic Event Tree Analysis Method)
- DDET (Dynamic Discrete Event Tree)
- ADS (Accident Dynamic Simulator)
- ISA (Integrated Safety Assessment)
- DDET/Monte Carlo hybrid simulation
- CCMT (Cell-to-Cell Mapping Technique)

DYLAM, DETAM, DDET, ADS and ISA are dynamic event tree generation techniques. They use a simulator to model the deterministic dynamic system behavior with a set of branching rules and associated probabilities to generate and quantify the likelihood of possible scenarios of system evolution following an initiating event. DDET/MC generates the branchings with a DDET engine and follows them using Monte Carlo sampling for uncertainty quantification of the likelihood of possible scenarios. CCMT is based on a discrete time version of CCCM and follows the probabilistic evolution of the system using a Markov chain.

Methods with visual interfaces include

- Petri nets,
- DFM,
- dynamic fault-trees,
- the event-sequence diagram (ESD) approach, and,

- the GO-FLOW methodology.

The first two methods are similar to those described earlier within the context of Type II interactions, except that states include sets of intervals of the controlled/monitored process variables. Dynamic fault-trees use timed house events or functional dependency gates to represent the time varying dependencies between basic events. Quantification of dynamic fault-trees is performed using time dependent Boolean logic or Markov models. The ESD approach uses 6-tuple of events, conditions, gates, process parameter set, constraint and dependency rules to represent the probabilistic system evolution. The events represent transitions between system states. The probabilistic approach is an extension of the CET approach. The GO-FLOW methodology uses signal lines and operators. The operators model function or failure of the physical equipment, a logical gate, and a signal generator. Signals represent some physical quantity or information.

Subject to given failure data and deterministic system model accuracy, the techniques that allow the most accurate and comprehensive modeling of the probabilistic system dynamics are the ones based on the Chapman-Kolmogorov equation including CET, CCCM, CCMT, and ESD approaches. The main challenge with these techniques is their computational complexity, both in model construction and implementation. Another challenge is compatibility with existing PRA structures. The advantage of the dynamic event-tree generation techniques is that they are compatible with the existing PRA structure and are able to generate possible scenarios of the system evolution exhaustively. The main disadvantage is that the number of branches increases according to the power law with the number of branch points. Most of the methods with visual interfaces can be regarded as semi-dynamic, because they represent system dynamics qualitatively (e.g., dynamic fault trees, GO-FLOW) or in a coarse partitioning of the system state space (i.e., in terms of large, small, medium changes in controlled process variables such as the case with DFM). The others have similar capabilities regarding process dynamics, representing it in a semi-quantitative fashion. All the methods with visual interfaces are capable of scenario and cut set outputs. However, cut sets may change with system evolution in time. Petri nets can be converted to fault trees. Again, fault-tree structure may change in time.

Table I below gives an overview of the requirements for the methodologies to be used for the reliability modeling of digital I&C systems and how the methodologies reviewed in this report meet these requirements. Due to the lack of a benchmark against which to compare the methodologies, the evaluation is subjective. The classification of compliance with the requirements is based on the examples provided in the cited literature. From Table I it is clear that there is no single methodology available which satisfies all the requirements. Also, it is not clear that the data used in the quantification process would be credible to a significant portion of the technical community for any methodology.

While the DFM ranks as the most preferable methodology, it is not clear that it can satisfy Requirement 4 for all digital I&C systems (i.e. the model must quantitatively be able to represent dependencies between failure events accurately). The exact magnitude and direction of change of the physical process variables at the time of hardware failure can affect the mode

of system failure in systems relevant to nuclear engineering. Based on the digraph approach, the DFM works with only qualitative changes in physical variables. Similarly, if the branching probabilities are provided by fault–trees in dynamic event-tree construction, it is not clear that dependencies between basic events can be completely accounted for. Such problems can be avoided by using Markov models, but digital processor failure data generation can be problematic for Markov models. Also, Markov models require highly time-dependent or continuous plant state information (Requirement 11 in Table I) and it is not clear that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed with output from Markov models. Finally, ESD, in principle, avoids some of these problems by combining CET with a graphical interface, but an application to digital I&C systems has not been encountered in the literature.

The modeling method that is used needs to be able to model the digital system to a level sufficient to ensure that all risk important interaction are included, as well as, all of the systems features that are required by current regulatory guidance. Almost all the methods reviewed in this report are capable of modeling a digital system to this level of detail, in the sense that they are probabilistic methods capable of describing common cause failures, and that can model software integrated with hardware.

Almost all the methods listed in Table I may help to evaluate a digital system's compliance with these regulatory requirement (at least superficially) in the sense that they are probabilistic methods capable of describing common cause failures, and can model software integrated with hardware. However, these documents also emphasize the need to identify the possible new failure modes. Since new failure modes can arise from both Type I and Type II interactions, it is particularly important that the methodologies satisfy Requirement 4 in Table I.

Table I: Methodologies and Requirements

Requirement/ Methodology	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees [89]	X	X	X	X	O	?	?	X	?	?	O
Dynamic Event Trees [91-95, 98]	X	X	X	?	X	?	?	?	X	X	O
Markov Models [13, 90, 99]	X	X	X	X	O	?	X	X	?	?	O
Monte Carlo Simulation [96]	X	X	X	X	?	?	?	?	?	?	O
Petri Nets [69, 70, 71, 100, 84]	X	X	X	X	O	?	?	?	?	?	O
DFM [22, 83]	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees [101, 102]	X	?	?	?	X	?	X	?	X	?	X
ESD [103]	X	X	X	X	O	?	?	?	X	X	O
GO-FLOW [104,105]	X	?	X	?	O	?	?	?	X	X	X
Bayesian Methodologies [67, 68]	X	?	?	?	O	O	?	?	?	?	X
Test Based Approaches [75]	?	?	X	O	X	?	X	X	?	O	X
Software Metric Based Approaches[76]	O	?	O	O	?	?	X	X	O	O	X
Schneidewind Model [53, 77]	X	?	?	?	?	?	?	?	O	O	X

X: Fulfills requirement
O: Does not fulfill requirement
? Needs further study to determine whether or not the methodology fulfills the requirement

Requirements

1. The model must be able to predict encountered and future failures well.
2. The model must account for the relevant features of the system under consideration.
3. The model must make valid and plausible assumptions.
4. The model must quantitatively be able to represent dependencies between failure events accurately.
5. The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement.
6. The data used in the quantification process must be credible to a significant portion of the technical community.
7. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
8. The model must be able to differentiate between faults that cause function failures and intermittent failures.
9. The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
10. The methodology must be able to model the interaction of the digital I&C system portions of accident scenarios with non-digital I&C system portions of the scenarios.
11. The model should not require highly time-dependent or continuous plant state information.

In conclusion, the methodologies to be used for digital systems assessments in nuclear power plants need to demonstrate that they meet the following requirements satisfactorily as minimum criteria for acceptance:

1. The methodology should account for both Type I and Type II interactions.
2. The model must be able to predict encountered and future failures well and cannot be purely based on previous experience.
3. The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified.
4. The data used in the quantification process must be credible to a significant portion of the technical community.
5. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
6. The model must be able to differentiate between faults that cause function failures and intermittent failures.
7. The model must have the ability to provide uncertainties associated with the results.

No single methodology has been identified that satisfies all the requirements. Also, none of the methodologies reviewed has been shown to satisfy Item 4 (or Requirement 6 of Table I). Since it is highly unlikely that issues related to data credibility will be resolved in the near future, investigation of the impact of digital systems on PRAs should include the sensitivity of the results to the data used and proposed resolutions.

The methodologies that rank as the top two with most positive features and least negative or uncertain features (using subjective criteria based on reported experience) are the DFM and dynamic event tree approach/Markov approach, each with different advantages and limitations. As indicated above, an application of ESD to digital I&C systems has not been encountered in the literature. While the DFM ranks as the most preferable methodology, it is not clear that it can account for Type I and Type II interactions adequately due to its semi-quantitative representation of these interactions. In that respect, the next phase of this research will undertake the following work:

- Two benchmark problems will be defined that respectively capture important features of the existing analog I&C systems and their digital counterparts expected to be encountered in applications.
- The benchmark problems will be used to compare the DFM and the Markov methodologies with regard to the modeling of Type I and Type II interactions using a common set of hardware/software/firmware states and state transition data.
- If the DFM and Markov methodologies produce similar results, then the impact of analog to digital I&C conversion will be investigated on a full PRA using prime implicants from DFM results and the state transition data used for the benchmark problem.
- If the DFM and Markov methodologies do not produce similar results, possible origins of the differences will be investigated.
- The feasibility of developing a dynamic methodology on a platform compatible with the current ET/FT approach (e.g. SAPHIRE) will be also investigated.

It should also be mentioned that there is no regulatory requirement for a single methodology to be applicable to all digital I&C systems relevant to the reactor protection and control systems. All the methodologies reviewed in the report have features that can make them preferable over the others depending on the system under consideration, including the conventional ET/FT approach. The availability of a single methodology that is applicable to all digital I&C systems of interest provides convenience from a regulatory viewpoint in the sense that it can be used as a common platform to evaluate the validity of the analyses performed by different methodologies.

Regarding the applicability of the conventional ET/FT approach to digital I&C systems, no actual comparisons to dynamic methodologies have been encountered in the literature. The extrapolation of existing computational evidence based on a few comparative studies on dynamic systems seems to indicate that the ET/FT approach may yield satisfactory results when a digital I&C system does not:

- interact with a process that has multiple Top Events, logic loops and or substantial time,
- have delay between the initiation of the fault and Top Event occurrence,
- rely on sequential circuits which have memory,
- have tasks which compete for the I&C system resources, and,

- need to anticipate the future states of controlled/monitored process.

In all these comparisons, the ET/FT approach has been found to overestimate the predicted Top Event frequencies. However, the overestimation can be very large (by a factor of 2 or 3 or even by an order of magnitude). The ET/FT approach may also not be able to identify possible dependencies between failure events due to the omission of some failure mechanisms.

ABBREVIATIONS

ADS	accident dynamic simulator
ARW	advanced research workshop
BTP	branch technical position
BWR	boiling water reactor
CCCM	continuous cell-to-cell-mapping
CCF	common cause failure
Cdf	cumulative distribution function
CCMT	cell-to-cell mapping technique
CET	continuous event tree
CMM	capability maturity model
CMMI	capability maturity model integration
COTS	commercial off-the-shelf
D3	defense-in-depth and diversity
DDET	dynamic discrete event tree
DETAM	dynamic event tree analysis method
DFM	dynamic flowgraph methodology
DOD	Department of Defense
DYLAM	dynamical logical methodology
EPRI	Electric Power Research Institute
ESD	event-sequence diagram
ET/FT	event-tree/fault-tree
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FMEA	failure modes and effects analysis
FTR	failure to run
GSPN	generalized stochastic Petri nets
IEEE	Institute for Electrical and Electronics Engineers
HPCS	high pressure core spray
I&C	instrumentation and control
ISA	integrated safety assessment The Instrumentation, Systems, and Automation Society
LOCA	loss of coolant accident
MC	Monte Carlo
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
PLC	programmable logic controller
pdf	probability distribution function
PRA	probabilistic risk assessment
PWR	pressurized water reactor
RG	regulatory guide
SBLOCA	small-break loss of coolant accident
SEI	Software Engineering Institute
SRPN	stochastic reward Petri net
SRV	safety relief valve
SU	structural unit

1. INTRODUCTION

1.1 Purpose of the Report

Nuclear power plants are now replacing and upgrading aging and obsolete instrumentation and control (I&C) systems. Most of these replacements involve transitions from analog to digital technology. An important difference between analog and digital I&C systems is the use of software/firmware in digital I&C system information processing (see Section 2.1.1.2). Digital systems offer the potential to improve plant safety and reliability through features such as increased hardware reliability and stability, and improved failure detection capability [1].

Even though many activities such as configuration management, testing, and verification and validation are carried out in the life cycle of software to ensure a high quality product, processes for quantitatively assessing the risk implications of digital upgrades have not yet been developed. Such processes are expected to involve the development of reliability models for digital systems and the subsequent integration of these models for determining reliability into the existing probabilistic risk assessment (PRA) models for overall plant response. For near term PRA applications, a digital I&C system reliability model needs to be compatible with the structure of current nuclear power plant PRAs which use the static event-tree/fault-tree (ET/FT) approach. This report describes the issues that need to be addressed both in the reliability modeling of digital I&C systems and in the incorporation of the digital I&C system reliability models into existing PRA models for overall plant response. The report also outlines the acceptance criteria to be used for the digital I&C system models prior to their implementation in regulatory applications.

1.2 Background and Motivation

In 1995 the U.S. Nuclear Regulatory Commission (NRC) issued a policy statement "Use of Probabilistic Risk Assessment Methods in Nuclear Activities", which encouraged greater use of this analysis technique to improve safety decision making and improve regulatory efficiency [2].

In 1994, the NRC's Advisory Committee on Reactor Safeguards (ACRS) recommended and subsequently NRC commissioned a study by the National Academy of Science (NAS) to study the use of digital systems in nuclear power plants. Simultaneous with this study the NRC Regulatory staff initiated a revision of Chapter 7 (I&C) of the Standard Review Plan (SRP) (NUREG 0800) [127]. During the course of this revision several meetings were held by the ACRS to review progress on the revision of Chapter 7 and to review progress on the NAS study.

The findings of the NAS study were published as a National Research Council report in 1997 [3]. When the ACRS issued a Letter Report in 1997 that recommended acceptance of the revision of Chapter 7 (I&C) of the SRP[4], the letter included the following recommendation "For some time we have raised questions about the treatment of software and digital systems in

PRAs. The National Research Council report addresses this issue and recommends that the staff develop methods for estimating failure probabilities in software-based digital systems including commercial off-the-shelf (COTS) software and hardware. We support the research on these topics initiated by the staff"

The National Research Council-NAS Report [3], among its many recommendations includes the following two which are relevant to reliability of digital systems:

1. The U.S. NRC should require that the relative influence of software failure on system reliability be included in PRAs for systems that include digital components.
2. The U.S. NRC should strive to develop methods for estimating failure probabilities of digital systems, including COTS software and hardware for use in probabilistic risk assessment. These methods should include acceptance criteria, guidelines, and limitations for use and any needed rational and justification.

In 2002 the Department of Energy sponsored a workshop on Instrumentation, Control and Human Machine Interface Technology. There were 70 participants in this workshop from six countries who represented industry, national laboratories and universities. Among the recommendations made by the participants in this workshop, the following one is relevant to the topic of this report: "Research should be initiated into digital failure modes and probabilities as input to overall plant PRAs" [4].

1.3 Overview of Approaches to the Reliability Modeling of Reactor Protection and Control Systems

A conclusion of the National Research Council report is that digital I&C systems (and digital systems in general) should not be addressed only in terms of hardware or software [3]. From a reliability modeling perspective, this conclusion implies that there is a need to account for the dynamic interactions between the reactor protection and control systems and controlled plant physical processes (e.g., heatup, pressurization) and also between the components of the reactor protection and control systems itself (e.g., communication between different components, multi-tasking, muliplexing). These interactions will be referred to as Type I and Type II interactions, respectively, in the rest of the report.

While the static ET/FT approach has been used in the reliability modeling of digital I&C systems in nuclear power plants [5, 6, 7], numerous concerns have been raised about the capability of the ET/FT approach to treat the coupling between the plant physical processes and triggered or stochastic logical events (e.g., valve openings, pump startups) that may arise due to Type I and Type II interactions. If the coupling is not accounted for, potentially significant dependencies among the failure events may not be identified or properly quantified [8]. Even if these dynamic interactions are semi-quantitatively modeled through a classification of changes in process variables (e.g., "small," "moderate," "large"), as is common practice with semi-dynamic techniques (see Section 2.2), some potential difficulties are the following:

- Failure mechanisms may be omitted due to inconsistencies in the definition of the allowed ranges for the process variables [8,9] or due to possible significant changes in the system behavior arising from very small changes in system parameters [10].
- The competition between system failure modes (or Top Events) may not be properly represented due to the possible dependence of the system failure modes on the exact timing of the component failures with respect to the changing magnitudes of the plant process variables and not just the sequencing of the component failures (see Section 1.3.2).
- Predicted Top Event frequencies may be in error due to the possible sensitivity of these frequencies to the magnitude of a stochastic change in the digital I&C system settings (e.g., as illustrated in Section 1.3.3 for setpoint drift).

A more detailed treatment of process modeling issues is discussed in [11] and [12] and also in Section 2.2.

Dynamic methodologies are defined as those that can account for the coupling between triggered or stochastic logical events in system reliability modeling through explicit consideration of the time element in system evolution. In 1992, a North Atlantic Treaty Organization Advanced Research Workshop (ARW) on the Reliability and Safety Analysis of Dynamic Process Systems was held in Turkey to discuss the advantages and limitations of the dynamic methodologies proposed to date, as well as to identify practical situations where the dynamic methodologies could lead to significantly improved results. The participants represented 26 different institutions including universities, national laboratories, private consulting companies, and regulatory bodies. Their combined expertise covered the areas of nuclear, chemical, mechanical, aerospace and defense systems. From the presentations and the discussions that followed in the ARW, dynamic methodologies seem to be needed whenever there is complex hardware/software/ process variable or hardware/human/process variable interaction in time [8], such as for a digital feedwater control system or the control room crew of a nuclear power plant responding to an accident.

Similar arguments can be made for the dynamic interaction between the components of the digital I&C system (i.e. Type II interactions). Key characteristics of the digital systems include real-time processing, data communications, sequential operation, multiplexing, multitasking, memory sharing, diverse data transmission and storage media [3]. The following statements are taken verbatim from Appendix F of [3] regarding real time processing:

A typical real-time system includes a controlling system and a controlled system. The controlling system periodically receives and processes information about the controlled system and the environment and generates control commands in response to this information, which are applied to the controlled system. For this operation to be stable and meet performance requirements, the timing relationship between the controlling system and the controlled system must be such that the complete control sequence (parameter sampling, transmission process, control command generation, and control command transmission back to the process) must be faster than the response time of the controlled process.

The only coupling through time-dependencies that can be modeled using static fault trees is the one that can be represented by a Priority AND gate [13] (e.g., for sequence dependent events). Subsequently, static ET/FT approach may not be able to fully describe the stochastic behavior of digital I&C systems with significant hardware/software/firmware/process interaction. The traditional approach to represent time-dependence with the ET/FT approach has been to discretize the static models into phased missions [14]. A phased mission is defined as a task performed by a system during the execution of which the system is altered such that the the logic model changes at specified times. The basic events which comprise the system logic model may be statistically independent or they may have statistically dependent occurrence properties. In analyzing failure to run (FTR) rates for emergency diesel generators, [15] identified three different FTR rates (including recovery) applicable to different portions of a mission time. Using nuclear component cooling water system failure initiating event frequency as a metric, [16] illustrates that time-averaged and simplified fault tree models support a good approximation to the more rigorous time-dependent Markov models if common cause failure is negligible and for short mission times. However, [16] also indicates that Markov approach may be more appropriate for systems with components that have different failure/repair characteristics[1] and/or mission times. Section 1.3.1 gives an overview of the approach used in [16]. For I&C systems that interact with a physical process (such as reactor cooling after shutdown), the times at which the system logic model changes may be statistically dependent upon the stochastic performance of the system constituents and reliability modeling of the system may require a more complicated approach. Section 1.3.2 illustrates how the competition between Top Events may be sensitive to the exact timing of the component failures with respect to the changing magnitudes of the plant process variables. Section 1.3.3 illustrates the sensitivity of the Top Event frequencies to the magnitude of a stochastic change in the I&C system settings, as well as the relationship of the settings to process dynamics.

1.3.1 Frequency Determination for the Loss of a Pump Train of a Nuclear Component Cooling Water (NCCW) System [16]

Figure 1.1 shows the example system under consideration. The NCCW train consists of two pump trains TF11 and TF12, one heat exchanger train, heat exchanger bypass line with 2 motor operated valves 2TF10S002 and 1TF10S001 (normally closed). Pump train TF11 has 5 components: pump suction manual valve (0TF11S008), pump suction filter (0TF11N001), pump (1TF11D001), pump discharge check valve (0TF11S001) and pump discharge manual valve (0TF11S002). Pump train TF12 has similar components. The heat exchanger train consists of the heat exchanger (0TF10B001), heat exchanger inlet check valve (0TF10S004), heat exchanger cooling water inlet valve (0VE11S003), heat exchanger cooling water filter (0VE11N001) and heat exchanger cooling water outlet valve (0VE11S004).

[1] or recovery characteristics in the case of digital I&C systems

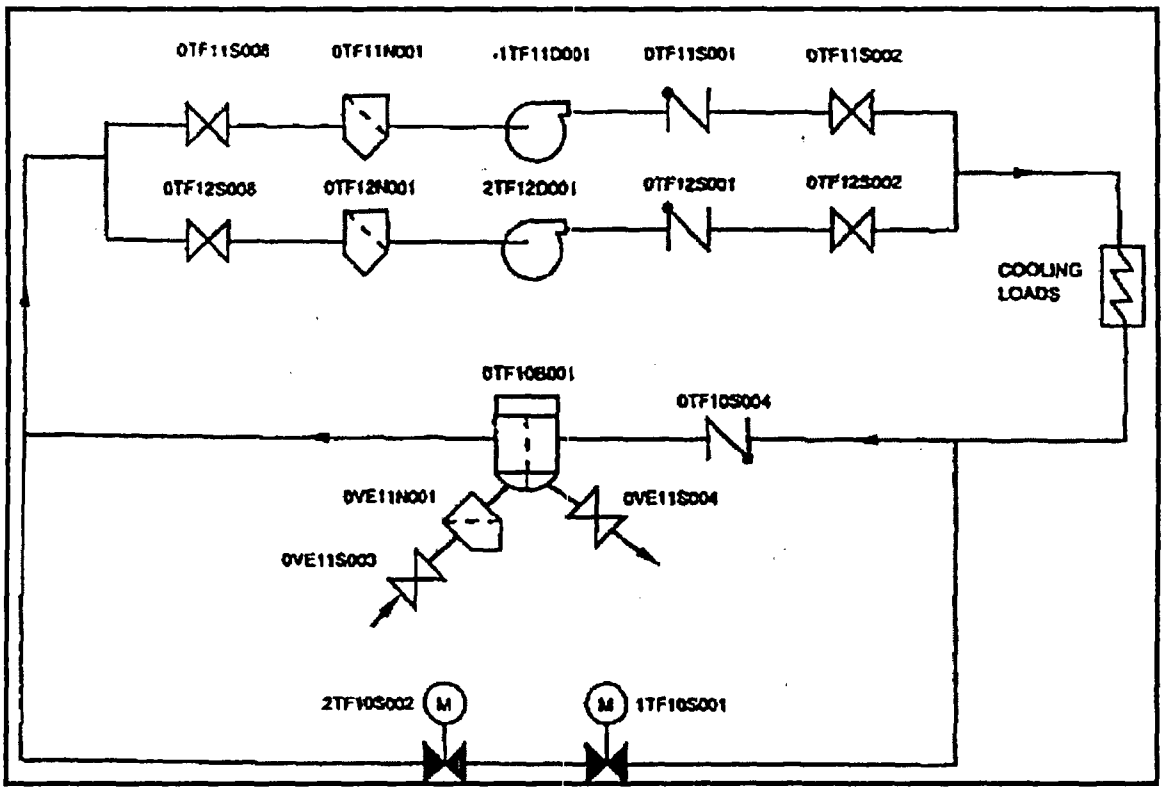


Figure 1.1 The Example NCCW Train [16]

The system is functional if either TF11 or TF12 is operational and the heat exchanger train is operating. The pumps 1TF11D001and 2TF12D001are normally running and the heat exchanger is in service. Each pump train TF11 or TF12 can fail independently with failure rate λ_I or due to common cause with failure rate λ_C. If one pump train fails, repair starts immediately and takes place with constant repair rate μ. The failure of the heat exchanger train is represented by a single failure rate λ_H and is not repaired. The task is to find the frequency of the loss of the NCCW train during the plant outage (80 hours).

Figures 1.2 and 1.3 respectively show the Markov transition diagram and the fault-tree for the example system. All the states with failed heat exchanger loop ($\overline{H}$ in Fig.1.2) and both pumps failed ($\overline{P}$ in Fig.1.2) represent a failed system configuration and can be merged into a single absorbing state. In Fig.1.3, τ_r is repair time of a pump train and τ_m is the mission time (8,760 hours).

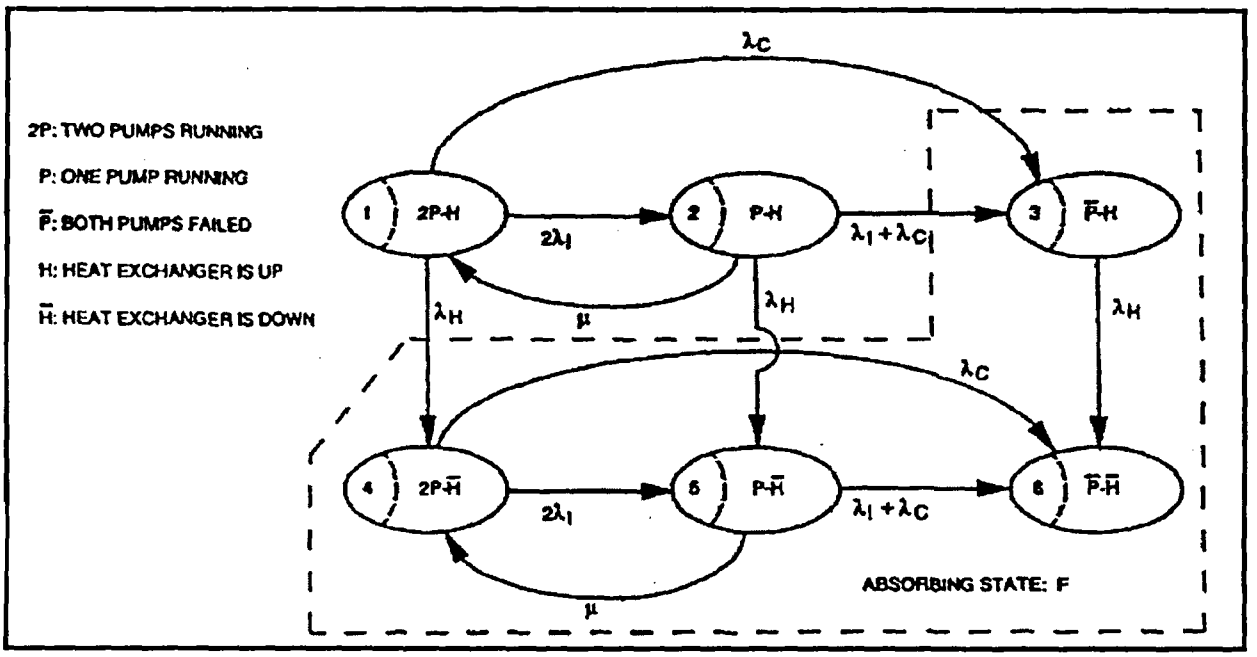


Figure 1.2 Markov Transition Diagram for the Example NCCW Train [16]

Figure 1.3 illustrates one way how time dependence of events can be accounted for by the fault-tree approach through the definition of states. For example, two of the events leading to the Top Event are:

1. Pump Train 11 fails and Pump Train 12 fails *before* Pump Train 11 is repaired
2. Pump Train 12 fails and Pump Train 11 fails *before* Pump Train 12 is repaired

Similarly, a condition leading to Event 1 above is "Pump Train 12 fails *when* (or during) Pump Train 11 is under repair". Also note that in the quantification of the event "Pump Train 11 fails to run" the mission time T_m is used whereas in the quantification of event "Pump Train 12 independent failure" the repair time T_r is used, because this is the time interval during which the failure of TF12 is relevant to the event "Pump Train 12 fails when 11 is under repair".

As summarized earlier, the results of [16] show that:

- the longer the mission time, the less necessary it is to use the Markov model to accurately model the dynamic system behavior,
- when the common cause failure rate is large, the fault-tree results are very close to that of the Markov model,
- when the independent failure rate is high and the mission time is short, the effect of repair is important and the system dynamics can no longer be neglected,

- the use of a Markov model may be more appropriate if components have different failure/repair characteristics, and
- the use of a Markov model may also be more appropriate if there are many components each with different failure/repair characteristics.

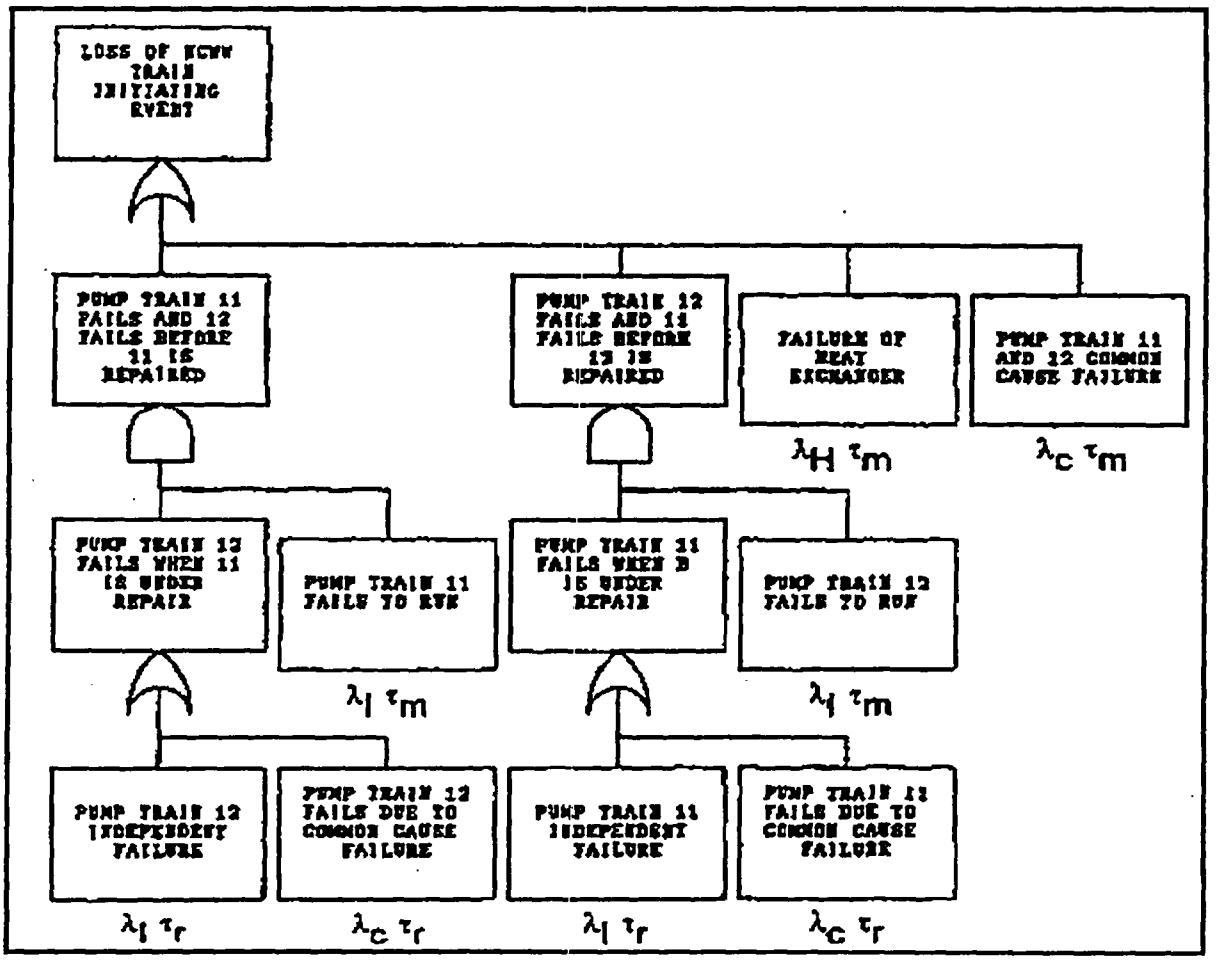


Figure 1.3 Fault-tree for the example NCCW train [16]

1.3.2 Feed-bleed Cooling of a BWR/6 Following a Small Break Incapacitating the Reactor Core Isolation Cooling (RCIC) System [17]

One limitation of the example system of [16] with regard to the digital I&C systems under consideration in this study is that the example system of [16] does not consider Type I or Type II interactions that may lead to coupling between these events through the I&C system. This section illustrates possible impacts of Type I interactions on the predicted I&C system failure frequencies.

Figure 1.4 shows the example system layout. Following a loss of coolant accident (LOCA) resulting from a 1% a double-ended guillotine break in the recirculation line, the rate of enthalpy addition to the reactor vessel due to decay heat is larger than rate of enthalpy removal from the core through the break. Subsequently, the level (L) decreases and pressure increases. When

L<-36 in (measured with respect to some reference point in the reactor vessel), the high pressure core spray (HPCS) system pump turns on and the valve F001 opens. The HPCS pump is normally on after the first demand. The valve F004 opens if *L*<-36 in and closes if *L*>+55 in. There are 19 safety relief valves (SRVs). SRV1 is set to lift at *P*=1103 psi, SRV2-SRV10 at *P* = 1113 psi and SRV11 through SRV19 at *P* = 1123 psi. The SRVs close once the pressure falls below these setpoints. The SRVs can also be opened by operator action using compressed air. The Top Events under consideration are:

1. *P*> 1110 psi (high pressure)
2. *P* < 300 psi (low pressure)
3. *L*> +60 in (high level)
4. *L*< -148 in (low level)

The selection of the Top Events does not reflect safety concerns but rather the desired system operation. However, Top Event 4 frequency affects the demand frequency for the low pressure core spray system whose malfunction does have safety implications.

From Fig.1.4, it is seen that the components that make up the HPCS communicate:

- internally only through a level change in the reactor vessel which is effectively controlled by the action of the injection valve F004, and,
- externally with SRV1 through spray-pressure interaction.

Subsequently, the whole HPCS can be modeled as a single on-off structural unit (SU1) or a macro-component without compromising the accuracy in the representation of the dynamic interaction (and subsequently the dependency) between the HPCS and SRV1 operation. Similarly SRV1 can be modeled as a single on-off SU. The example system in its modularized form is shown in Fig.1.5. The following results are reported in [17] for pre-break conditions that lead to pressure reaching 1039.4 psi and level reaching 36.0 in within 2 minutes following the LOCA, using the cell-to-cell-mapping technique (see Section 2.2) as the dynamic methodology:

1. *Low level* (<-148 in) occurs if only SU1 fails-off or only SU2 fails-open.
2. *High level* (>+60 in) occurs if SU2 fails-closed after SU1 fails-off.
3. *High pressure* (>1110 psi) occurs if the level at the time SU2 fails-closed is such that it takes longer for the level to reach -148 in than the time it takes pressure to reach 1110 psi.
4. *Low level* occurs if the level at the time SU2 fail-closed is such that it reaches -148 in before pressure reach 1110 psi.
5. *High level* occurs if the level at the time SU2 fails-closed is such that the level reaches +60 in before pressure reaches 1110 psi.

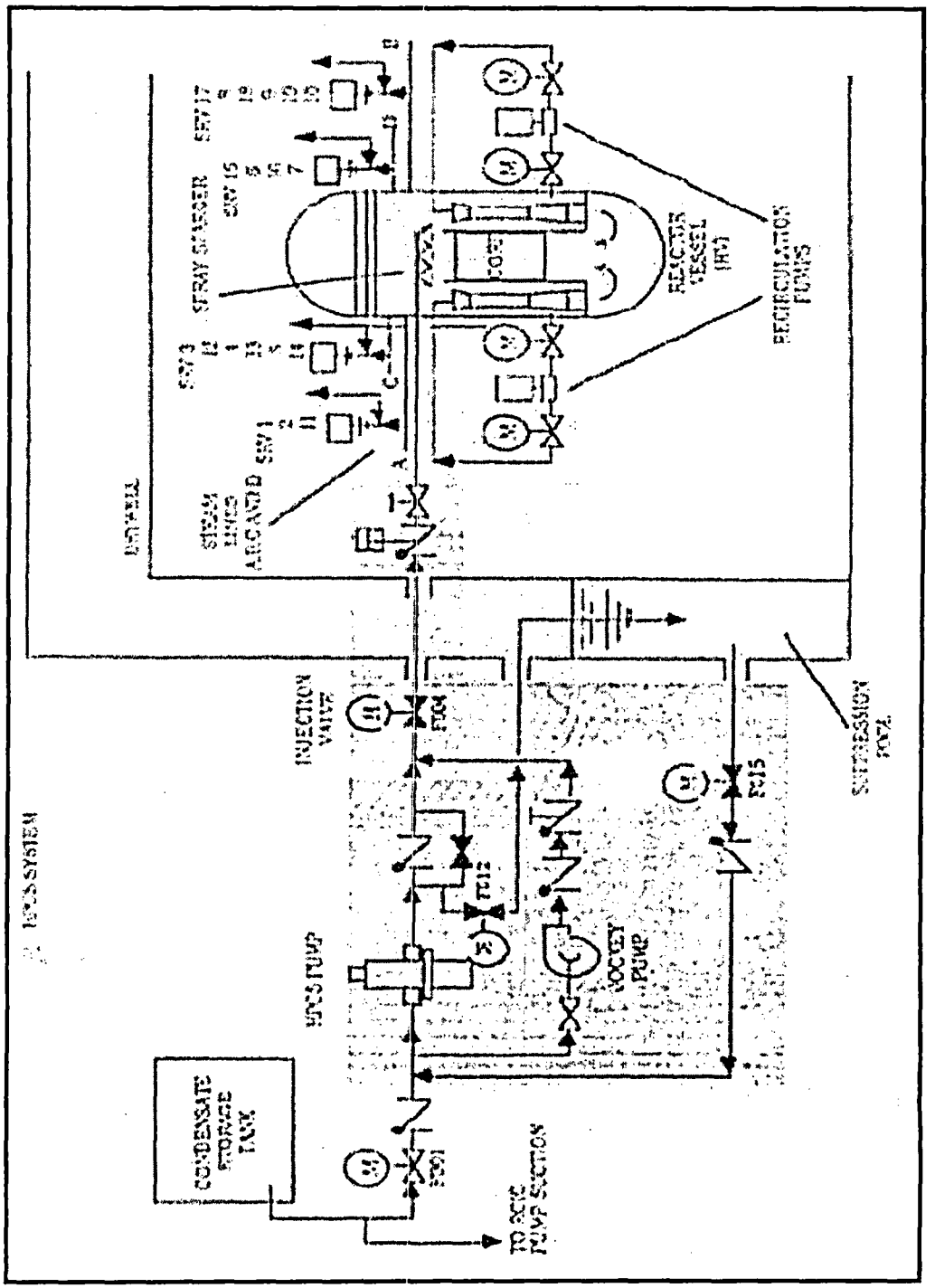


Figure 1.4 The Example BWR/6 Layout [17]

Results 1 and 2 illustrate the failure sequence dependence of competing Top Events. Results 3, 4 and 5 show how the competition between the Top Events can be sensitive to the magnitudes of the process variables at the time of component failure. A conventional ET/FT analysis of the same initiating event [17] overestimates low pressure probability by a factor of 3

and low level probability by a factor of 2. The ET/FT results for high level and high pressure were found to be close to the dynamic methodology results.

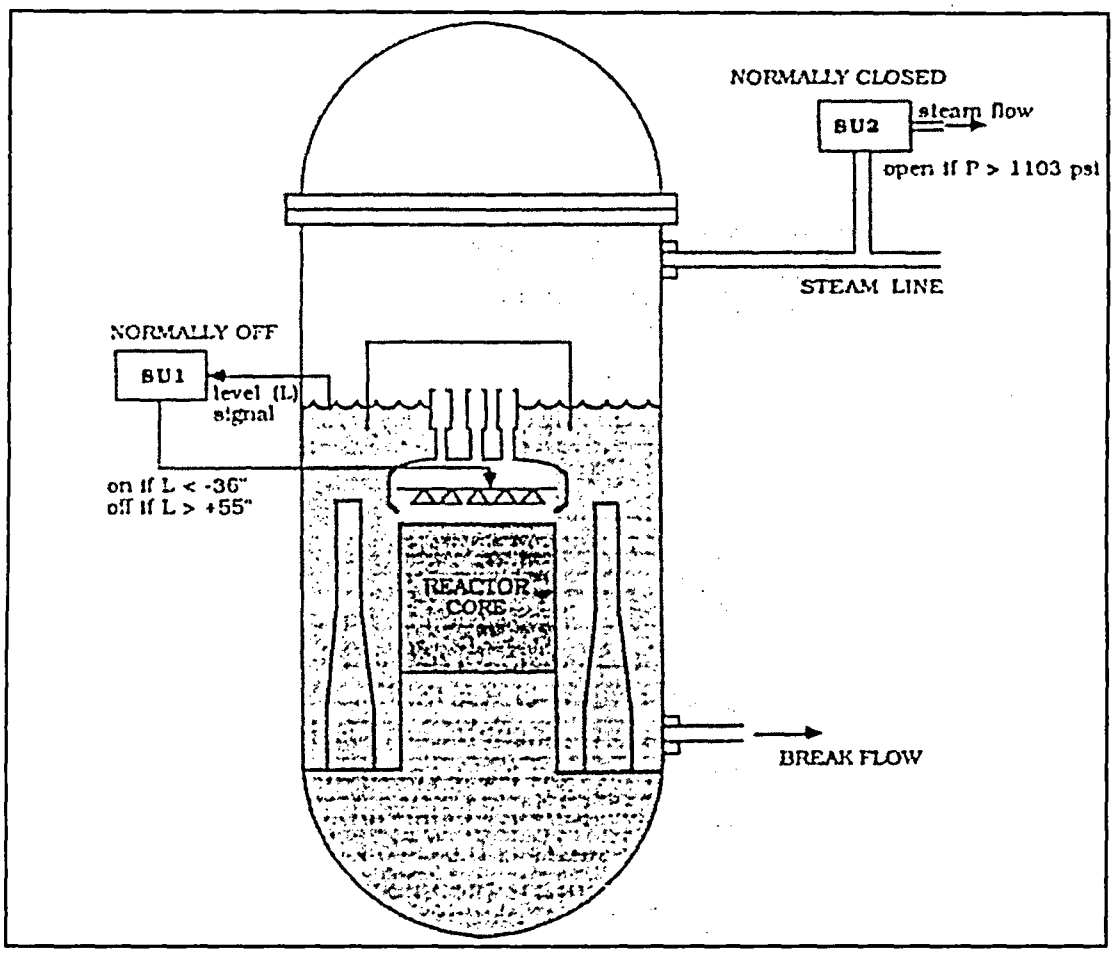


Figure 1.5 The Modularized Example BWR [17]

1.3.3 Setpoint Drift in a Level Controller [18]

Section 1.3.2 illustrated how the representation Type I interactions may be sensitive not just to the sequencing of the component failures, but also to the magnitudes of the process variables at the time of component failure using part of the reactor protection and control systems in a BWR/6. This section illustrates the effects of the changes in the properties of the I&C system itself by focusing on the level control.

The level control system shown in Fig.1.6 is taken from [18] and uses on-off controllers. Under normal operation, both Units 1 and 2 are off. If level x is between the bottom the tank, a and the low level set point, r_l $(a<x<r_l)$, then Unit 2 turns on to supply makeup water. Unit 2 turns off if the level is between the top the tank, b and the high level set point r_h $(b>x>r_h)$ and Unit 1 turns on. Unit 1 turns off if $x<r_l$. Under the assumption that Unit 1 is failed off, the system operation

is similar to the level control mechanism in the feed-bleed cooling of the BWR/6 described in Section 1.3.1. The level control system shown in Fig.1.7 is also taken from [18] and uses a controller that provides makeup water in a manner proportional to $x_0 - r$ where r is the setpoint nominally set at $r = x_0$. While there are analog proportional controllers, this type of controller can also be regarded as an example of a "smart" type of controller that anticipates the future state of the controlled variable and which could be a feature of the digital I&C system (see Section 2.1.1.2).

Figures 1.8 and 1.9, respectively, illustrate the impact of setpoint drift on the cumulative distribution function (Cdf) for high level ($x>b$), for the on/off and proportional controllers as a function of changes in controller parameters. The differences between Curves 1-4 in Fig.1.8 and Curves 1-8 in Fig.1.9 can be regarded as the consequence of a very simple Type II interaction between the setpoint drift and the other controller parameters. The dynamic methodology results in both Figs.1.8 and 1.9 have been obtained using a dynamic methodology similar to the continuous event tree methodology (see Section 2.2). The conventional results have been obtained from fault-trees based on digraphs.

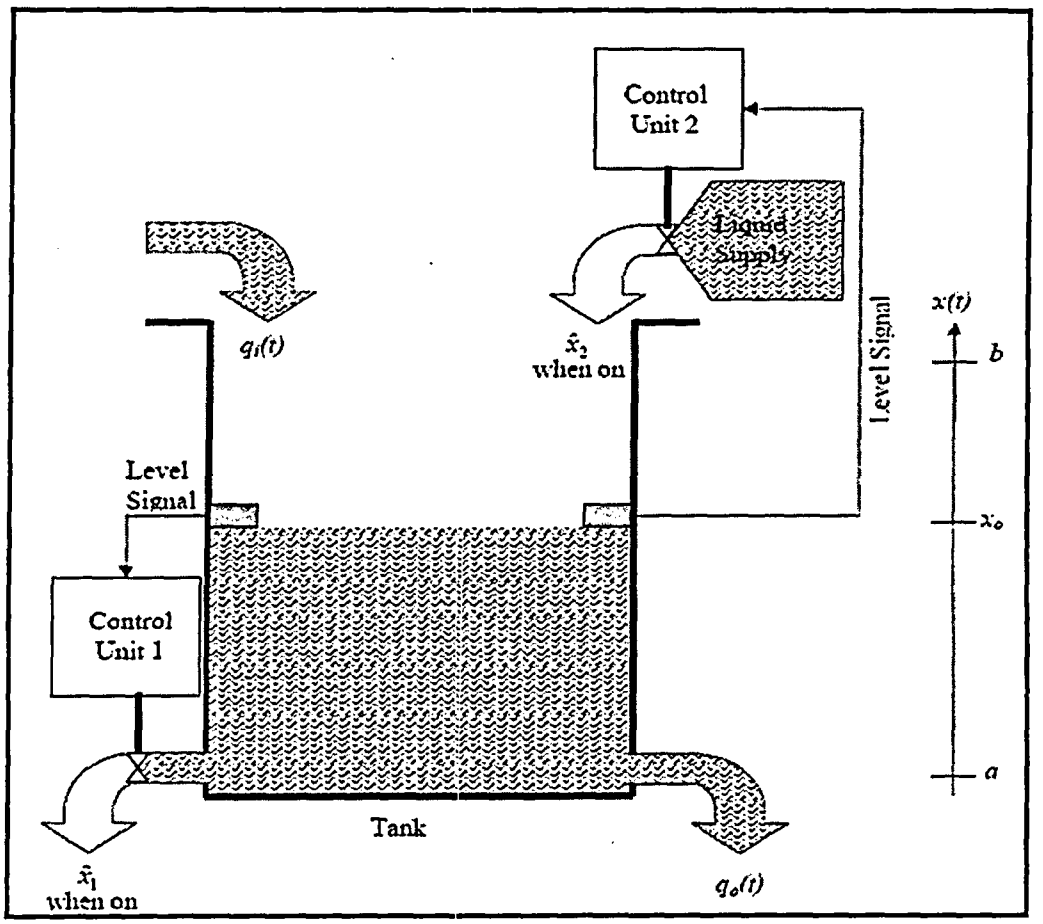


Figure 1.6 A Level Controller with 2 On/Off Controllers

Some observations that can be made from Figs.1.8 and 1.9 are the following:

- The differences between dynamic methodology and conventional results can be very large depending on the magnitude of setpoint drift and controller parameters. For example, Curve 4 in Fig.1.8 shows that, for overflow rate/controller bias equal to 1, the conventional methodology result for the asymptotic value of the Cdf for overflow is 20 times larger than that predicted by the dynamic methodology. Curve 8 in Fig.1.9 shows a similar overestimation for a normalized magnitude of setpoint drift of 1. It should be indicated that while digital I&C systems can monitor setpoint drift and take mitigating measures in case of setpoint drift (e.g. compensation or fallback to a preset value), the likelihood of success of the detection process and/or mitigating measures cannot be assured to be unity.
- In general conventional results are larger than the dynamic methodology results.
- The conventional and dynamic methodology results are similar in some cases (Fig.1.9 Curve 1 and all the curves in Fig.1.8).

It is also shown in [18] that Fig.1.8 and 1.9 results are not sensitive to the probability distribution function (pdf) for the magnitude of the drift.

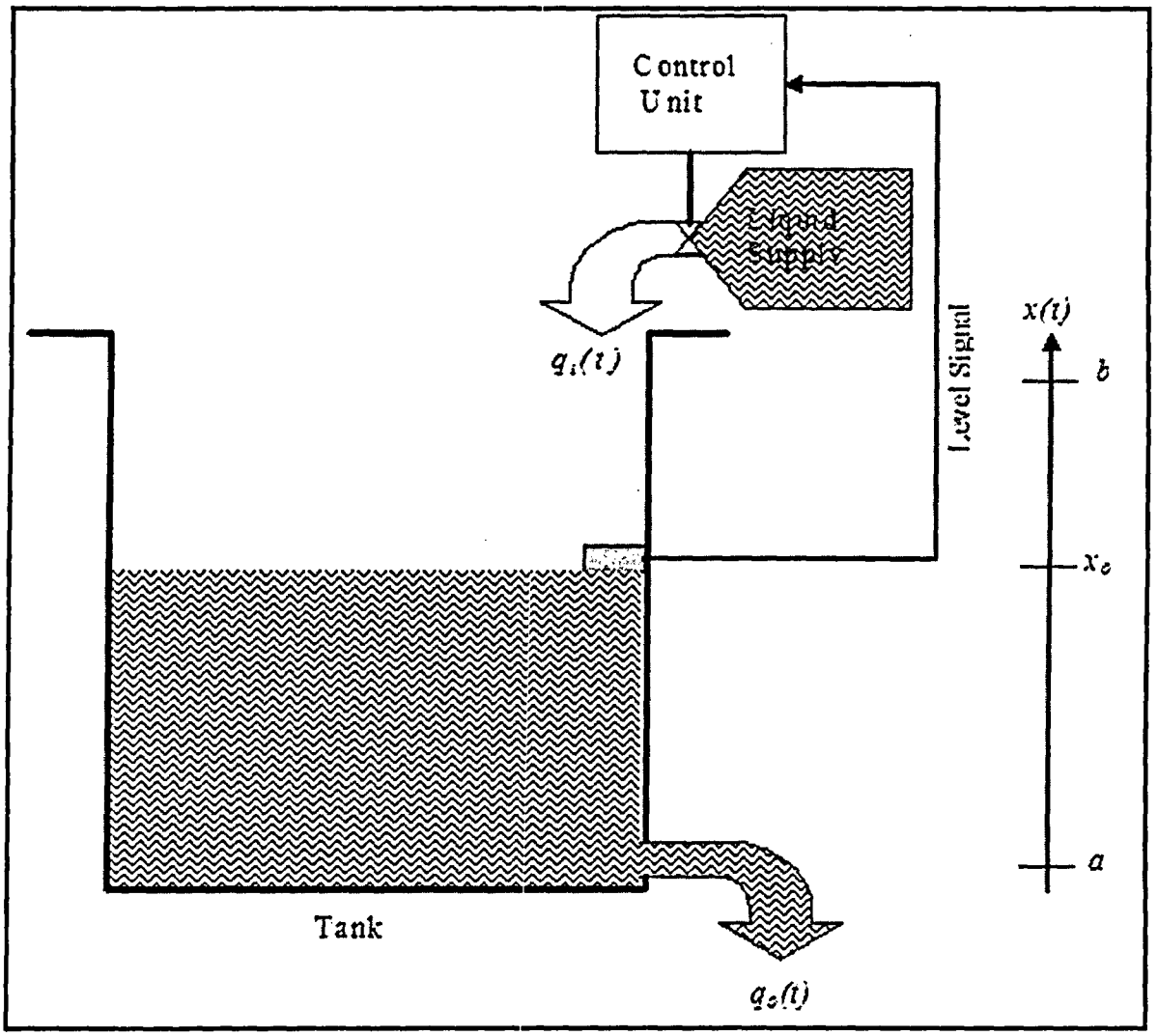


Figure 1.7 A Level Controller with 1 Proportional Controller

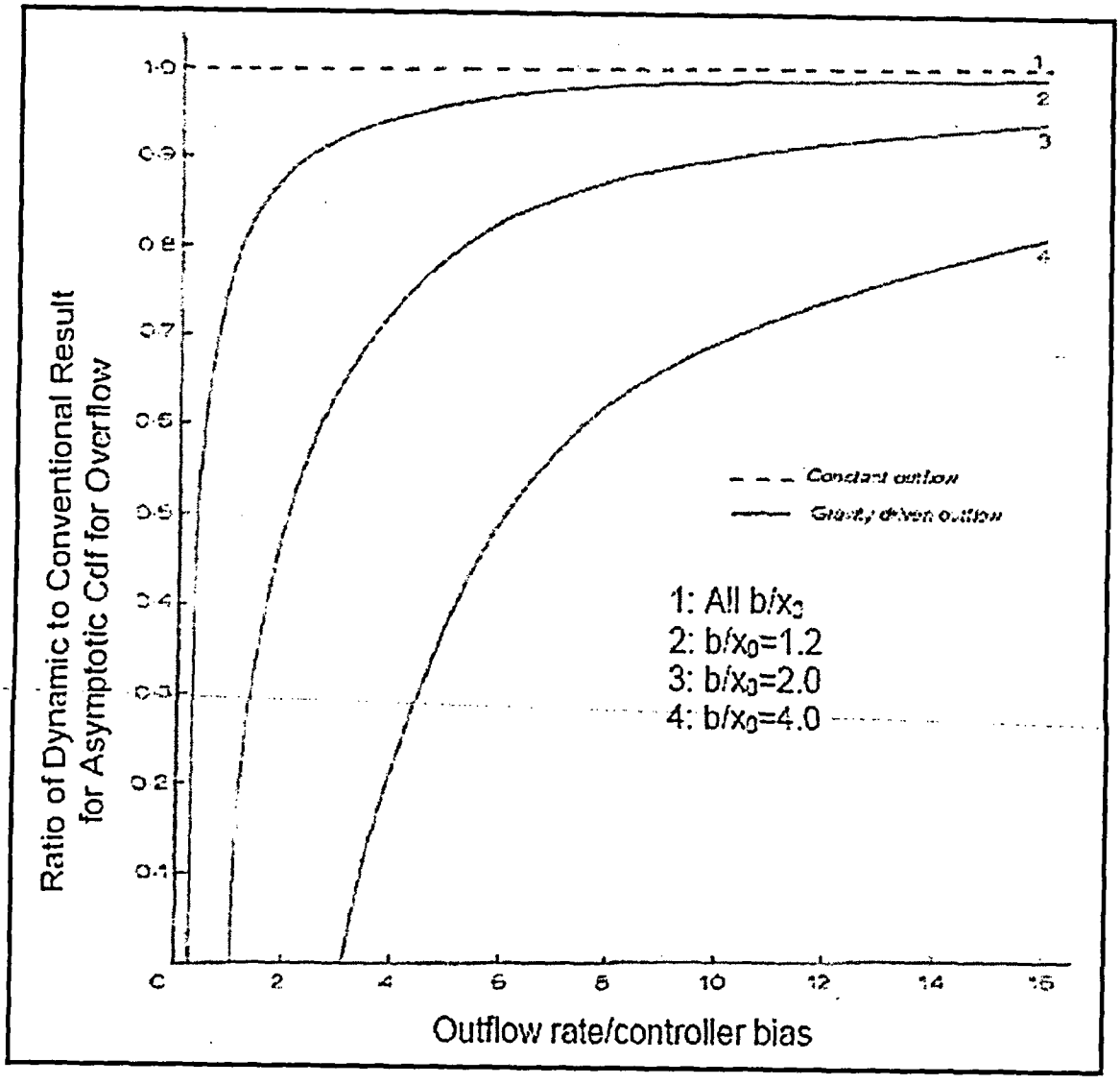


Figure 1.8 Setpoint Drift Effect on the Cdf for Overflow: On/Off Level Controller [18]

1.3.4 Initial Conclusions

An overview of approaches to the reliability modeling of reactor protection and control systems indicates that while the conventional ET/FT approach has been used to model digital I&C systems, concerns have been also expressed about the ability of the ET/FT approach to represent the dynamic interactions between the I&C system and controlled plant physical processes and also between the components of the I&C system itself (i.e. Type I and Type II interactions). Relatively little work is encountered in the literature about the potential consequences of such interactions. The available work suggests that unless dynamic methodologies are used to represent these interactions:

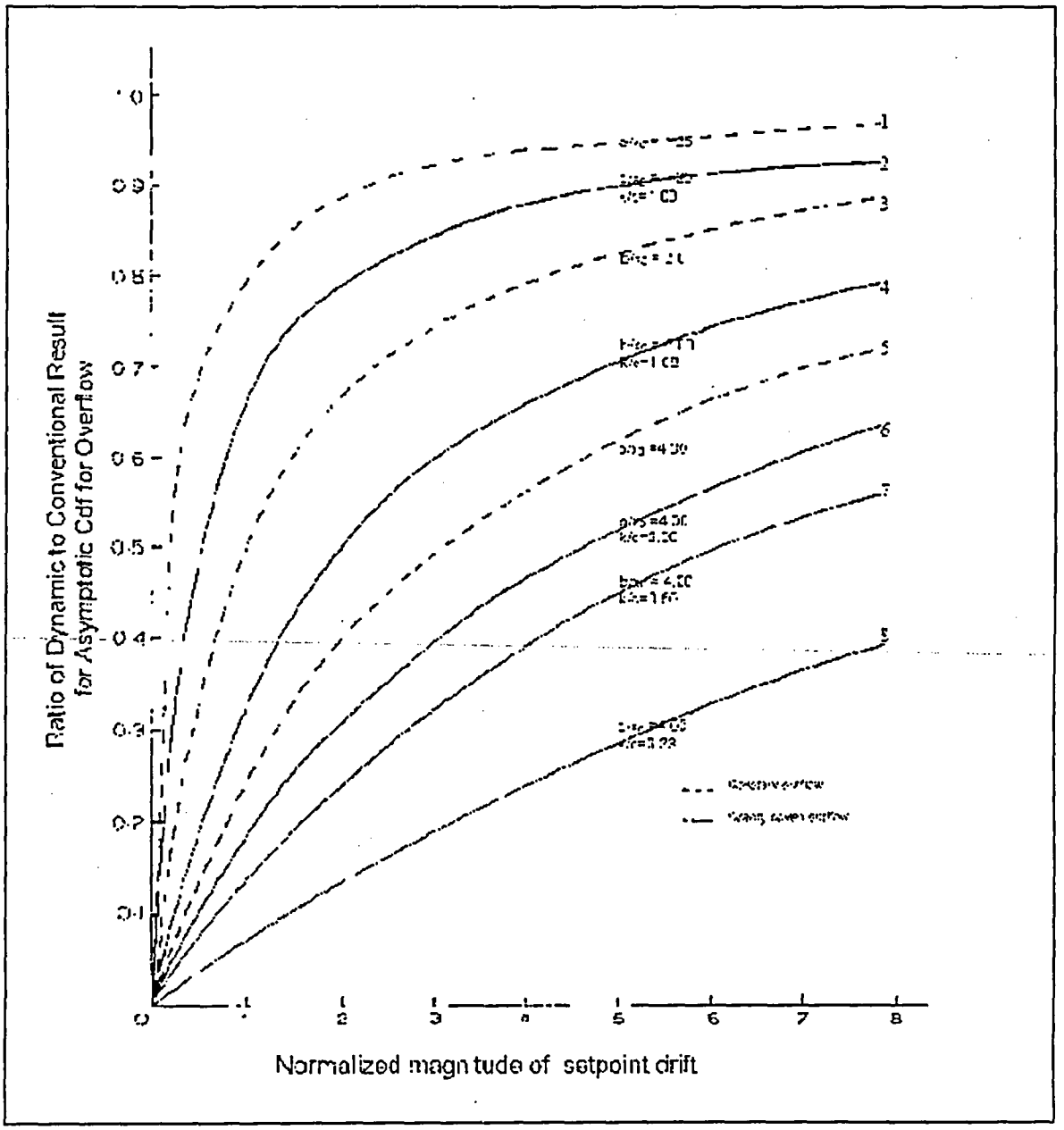


Figure 1.9 Setpoint Drift Effect on the Cdf for Overflow: Proportional Level Controller [18] (k: Controller gain, c: Level rate of change/height unit)

- some failure mechanisms may be omitted,
- the competition between Top Events may not be properly represented,
- predicted Top Event frequencies may be in error.

The existing work also indicates that the conventional ET/FT approach may be appropriate for I&C systems that do not have:

- more than one failure mode,
- substantial time delay (with respect to the time constants of the controlled process) between the failure events and the occurrence of the Top Events, or,
- interaction between hardware/firmware/software constituents of the I&C system and/or the controlled/monitored process.

In all the comparisons of ET/FT versus dynamic methodologies encountered in the literature, the conventional ET/FT have been found to overestimate the predicted Top Event frequencies. On the other hand, the ET/FT approach may not be able to identify possible dependencies between failure events due to omission of some failure mechanisms [19].

1.4 Overview of Requirements for Integrating a Digital I&C System Model into an Existing PRA

Arndt et al. [20] discussed some methodology requirements to allow the integration of digital I&C system reliability models and analysis into existing PRAs. In general, the methodology needs to qualitatively model the digital I&C system portions of accident scenarios to such a level of detail and completeness that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed.

In addition, the model needs to have the capability to quantify the likelihood of system failure in a credible manner and the methodology must be compatible with current PRA techniques. This implies that it cannot require highly time-dependent or continuous plant state information and must provide discrete system states which can be directly related to the performance of components or operator actions dependent on the digital I&C system. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones. Also, it must be able to differentiate between faults that cause function failures and intermittent failures. The model must quantitatively be able to accurately represent dependencies between failure events including common cause failures. The data used in the quantification process must be credible to a significant portion of the technical community, and key modeling assumptions that can lead to significantly different results need to be identified and their reasonableness discussed.

1.5 Organization of the Report

Sections 2.1 and 2.2 of this report review the dynamic methodologies proposed to date to address the issues outlined in Section 1.3 as they relate to the digital system and process, respectively. Sections 2.1 and 2.2 also indicate how digital I&C systems differ from their analog counterparts. Section 2.3 discusses the regulatory issues that need to be addressed for the reliability modeling of digital I&C systems. Section 3 expands upon the requirements outlined in Section 1.4 to describe:

- the requirements for the correct representation of stochastic digital I&C system behavior (Section 3.1.1),
- integration of the stochastic digital I&C system model into existing PRA studies (Section 3.1.2), and,

- current availability of tools that fulfill these requirements (Section 3.1.3).

Section 4 presents the conclusions of the study.

2. REVIEW OF THE CURRENT METHODS

2.1 Methodologies for the Reliability Modeling of Digital Systems

Digital systems distinguish themselves from other control and instrumentation systems due to the presence of active hardware and software components. While this report will generally not address software in isolation from the complete digital system, it is useful to state the properties that a model of software should have to identify the properties of each model discussed. Iannino et al. [21] discuss some criteria to evaluate proposed models of software reliability which include predictive value, capability, quality of assumptions, applicability, and simplicity. The model needs to be able to predict future failures well and not just rely on past experience. It must have the ability to provide relevant information to users. In the digital I&C universe, this ability includes failure scenario identification, generation of cut sets and prediction of system failure frequency. The model must make valid and plausible assumptions. It also must be applicable to many types of digital systems, not just domain-specific or general purpose systems. It should be mentioned at this point that there is no regulatory requirement for a single methodology to be applicable to all digital I&C systems relevant to the reactor protection and control systems. However, since there has not been sufficient experience with digital I&C systems to decide a priori if a methodology is applicable to a given digital I&C system, the availability of a single methodology that is applicable to all digital I&C systems of interest provides convenience from a regulatory viewpoint in the sense that it can be used as a common platform to evaluate the validity of the analyses performed by different methodologies. Finally, it must be designed so that it is not hard to collect data from it, it is not hard for an analyst to learn the concepts, and not hard to implement.

Garrett and Apostolakis [22] suggest, "...to reason effectively about the completeness of the safety requirements of a digital system, it is necessary to model the software in combination with the rest of the system". In addition, NASA guidelines conclude that "...most PRA or system reliability assessments consider software contribution to risk negligible in comparison to, or included in, hardware component contributions to system failure probability" [33]. The authors agree with these assertions which imply that software should not be regarded as a separate entity in the reliability modeling of digital I&C systems and provide more information in subsequent sections.

2.1.1 Analog vs. Digital Instrumentation and Control Systems

The literature focused on nuclear power plant safety assessment generally describes a watershed associated with the migration from 'analog' to 'digital' instrumentation and control systems. However, definitions of these terms and characterizations of the systems themselves are largely absent from available papers. The lack of definition and characterization of these critical concepts results in confusion as to what the terms actually mean and what the systems actually look like. Consequently, it is difficult, if not impossible, to analyze in a meaningful way the impact of the changes made to instrumentation and control systems—particularly their impact on nuclear power plant safety.

In this section, the authors attempt to characterize analog and digital systems for a meaningful comparative analysis of their control characteristics and reliability. While the following examples may not capture fully all salient characteristics of such systems, it is believed the following sections provide common definitions and assumptions upon which to base analysis and conclusions throughout the remainder of this report.

2.1.1.1. Analog Instrumentation and Control Systems

Perhaps the simplest familiar analog control system that relates to a system in a nuclear power plant is a very simple water level control system. Level control can be an important protection function in a nuclear power plant as illustrated in Section 1.3. The analog system that will be considered here, however, will have much simpler features than the one considered in Section 1.3.2 in order to facilitate the illustration of the similarities and differences between analog and digital I&C systems from a reliability modeling viewpoint. The simple water level control system's essential characteristics and control points include the following:

- a water reservoir
- a single water drain control valve
- a direct mechanical linkage, i.e. rods and levers, etc., to open the drain control valve (closure of the valve is gravity-based)
- a float to detect low and high water levels based on the setpoints for the inlet control valve
- a single inlet water control valve connected to the float.

A correctly functioning simple water level control system maintains the water level between the low and high setpoints, opening and closing the inlet control valve as appropriate in an analogous manner to the injection valve (F004) of the HPCS system in Fig.1.4 (or SU1 in Fig.1.5 or Control Unit 2 in Fig.1.6). The drain control valve (counterpart of Control Unit 1 in Fig.1.6) is calibrated to close when a minimum water level is reached in the reservoir. The minimum water level is independent of the setpoints for the inlet control valve (such as Top Event 4 in Section 1.3.1). A properly functioning system works as follows:

- A human operator opens the drain control valve through its direct mechanical linkage.
- Water drains from the reservoir.
- The drain control valve closes when the minimum water level is reached.
- When the water level reaches the low setpoint the water inlet valve is opened.
- When the water level in the reservoir reaches the high setpoint the inlet control valve is closed.

The inlet control system is completely independent of the drain control system in this example. That is, there is no control-coupling present. The water inlet control system has no information about the position of the drain control valve or its history. This lack of information has no bearing on the system's ability to control the water level in the reservoir between the setpoints as long as the rate of inflow into the reservoir can match or exceed the rate of outflow.

Ideally, of course, the system would close the drain control valve prior to or simultaneously with the opening of the inlet control valve. However, the lack of control-coupling between the inlet and drain systems cannot assure such behavior. The ability to behave in accordance with the preferred ideal is a matter of calibration of the various setpoints and tuning of the mechanical and hydraulic components. Drift from the ideal behavior may be experienced as parts wear and go out of tolerance.

It is observed that both the inlet and drain control systems are direct control systems. That is, the operator controls, through mechanical means, the ability to open the drain valve. The drain valve is tuned to close via gravitational force when the minimum water level is reached. Similarly, the float controls directly the opening and closing of the inlet control valve. Such systems may be characterized as 'hard-coded' or 'hard-wired' systems, that is "having a direct physical connection, such as by wire or cable" or "controlled by wiring of the hardware, rather than by software" [24]. Alternatively, hard-coded may be defined as "an aspect of an electronic circuit which is determined by the wiring of the hardware, as opposed to being programmable in software or controlled by a switch" [25]. Of course, in the above example, the system lacks any electrical components. Nevertheless it is the system's "wiring" that determines its control characteristics.

There are several other germane characteristics available from this simple water level control system that characterize analog control systems in general. The simple water level control system contains only combinatorial logic. Combinatorial logic contains no logic loops. In addition, the output from combinatorial logic depends only on the current value of the inputs. Analog controllers generally contain "random logic", that is, there is no regularity to the control logic. Therefore, algorithmic logic, as exemplified by finite state machines[2], does not apply to random logic controllers [26]. In this manner, analog controllers are reactive in that the controller acts on input it measures through its sensors. Finally, pure analog instrumentation and control systems perform their functions continuously and the data values and their internal representations are continuous waveforms.

It is noted that 'analog' controllers may contain elements that exhibit 'digital' characteristics. In the above example, the inlet control valve may have only two positions—open and closed. In analyzing systems like the simple water level control system, the analysts are not concerned, in general, whether the valve may be opened partially or not. In fact, such systems are designed to include components that have *only* two positions. The same binary nature may apply to the drain control valve.

In addition, 'analog' control systems that include electrical components historically have contained vacuum tubes, relays, transistors, etc. These components are types of electrical switches whose only states are 'on' and 'off.' These components have been used to build combinatorial circuits for many years.

[2] A Finite State Machine is "a computational model consisting of a finite number of states and transitions between those states, possibly with accompanying actions" [19].

Finally, 'ladder logic' control systems have been used for many years for controlling machinery, pumps, fluid levels, etc. Ladder logic systems are a type of combinatorial circuit built originally from discrete components such as relays, resistors, transformers, etc. [27]. Ladder logic systems are still used extensively. However, the mechanisms for realizing ladder logic have changed dramatically over the years. Currently, ladder logic control systems, traditionally considered to be analog controllers, are realized in programmable logic controllers (PLCs). Such devices are actually digital processors masquerading as analog devices.

2.1.1.2 Digital Instrumentation and Control Systems

Perhaps the greatest advantages for migration from analog to digital controllers are cost and flexibility. From their inception, microprocessors demonstrated significant design and fabrication cost advantages over custom-design random logic systems [28]. In addition, the programmability of these systems permits the use of standard hardware components while allowing customization of functionality through programming. Unlike the analog devices examined in the previous section, digital devices are not limited to single functions that are determined by the hard-wired connections to the outside world. Digital stored-program control devices may be specialized to the tasks at hand by loading different programs depending on the responsibilities required of them. Such programs are actually "codification" of processes that previously may have been performed through random logic, human intervention, or a combination thereof.

Microprocessors and the resulting digital I&C systems constructed from them are not combinatorial logic machines. Rather, they rely on sequential circuits—they have memory. Consequently, their outputs may be a function of system history as well as the measured current state of the world, based on sensor inputs. In addition, sequential circuits have a timing mechanism (clock) associated with them. The clock helps determine the rate of progress for a given task as well as coordinating tasks that may compete for a digital controller's resources.

The same external sensors and actuators may be connected to a digital controller and an analog controller through the same sets of wires. However, in the digital universe one must be careful to insure the sampling rate used for analog to digital conversion is sufficient to overcome the creation of artifacts that may result from too low a sampling rate [29,30]. Also, the sampling rate, algorithm, and processor speed must be selected and matched carefully to ensure that the response time performance requirements are met. There exist alternate mechanisms for connecting digital controllers to the outside world, such as buses and networks, which are not available to analog controllers. The selection of connection mechanism and the communication protocol chosen affect the rate of data communications as well as the reliability and robustness (see Section 2.1.1.4 below for more information on this topic). The ability for digital I&C systems to have exclusive access to resources, suspend processing (waiting) while holding exclusive access resources, inability to preempt another digital I&C system from holding a resource, and a possibility of circular waiting for resources also implies the need to analyze the system for potential problems such as deadlock[3] or starvation that may result.

[3]Deadlock is a situation in which computer processing is suspended because two or more devices or processes are each awaiting resources assigned to the others [19]

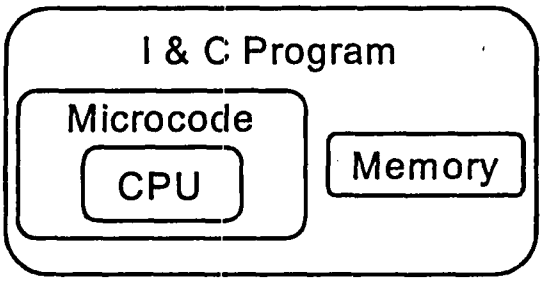


Figure 2.1 Architectural Diagramof a Digital I&C Controller

Figure 2.1 illustrates the primary elements of a digital I&C controller. These elements include a central processing unit (CPU) along with its associated microcode[4], memory, and I&C program. Such a controller may be connected to sensors and actuators. In addition, it is possible to connect several digital I&C controllers via shared memory, networks, or buses so they may cooperate and optimize the control they exert over the process physics. Figure 2.2 illustrates such connections between digital I&C controllers. The benefits and mechanisms used for these connections are described in sections 2.1.1.3.3 and 2.1.1.4 below.

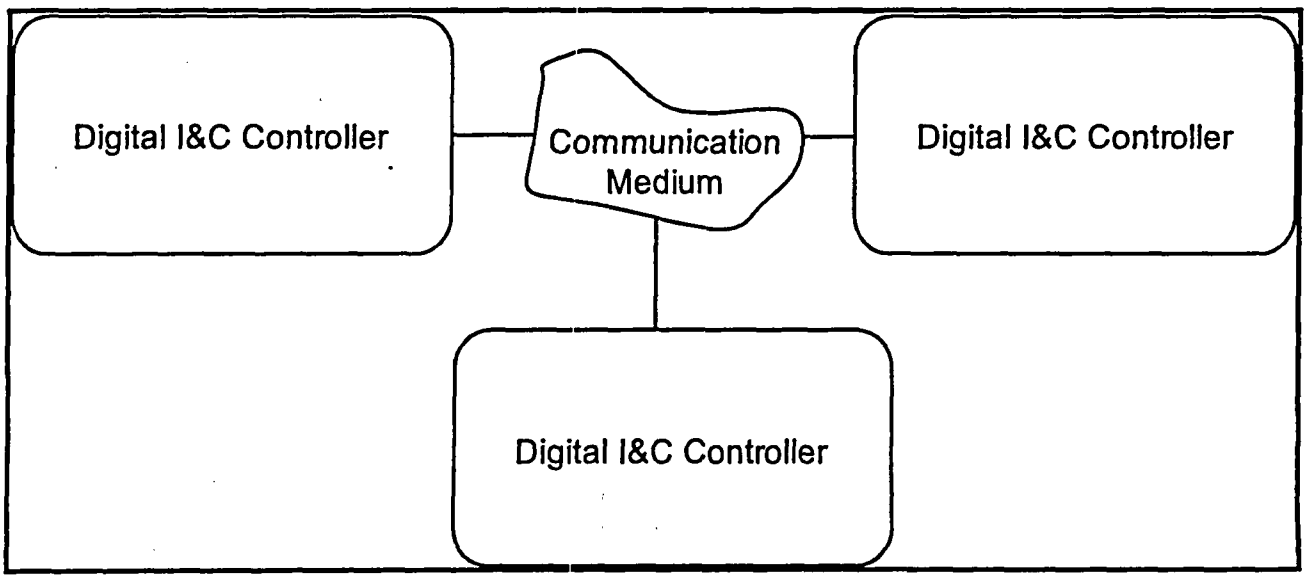


Figure 2.2 Multiple Digital I&C Controllers Connected via a Communication Medium

In the analog simple water level control system examined in the previous section it was noted that the inlet control system and the drain control system were completely independent of one another. Certainly one may design and construct digital systems that 'communicate' with one another only indirectly (e.g., through the process) as well. However, the ability to directly and

[4]Microcode consists of the lowest-level instructions that control a processor. A single machine-language instruction typically is translated into several micro-instructions.

explicitly coordinate multiple digital controllers may lead to a finer degree of control and control opportunities not available in the absence of such communication and coordination. When communicating digital controllers are employed, it is possible to more easily optimize results. A digital controller can remain active and not only react to data, but can anticipate the state of the system. A digital controller which communicates in this manner would have both information on the state of the world through its sensors and what is most likely to occur through knowledge of the actions of other digital controllers.

For example, a digital controller may close the drain control valve and open the inlet control valve simultaneously in order to fill a vessel more quickly. Such control mechanisms may be considered to be "tightly-coupled". It is observed that ideally such a system may require additional sensors and actuators to insure the various external components behave as instructed by the controller. In the previous example, additional sensors may be needed to determine the actual position of the valves. Of course, adding more sensors and actuators may affect the overall reliability of the system in a negative way, so careful analysis is required.

Digital instrumentation and control systems represent data internally as discrete values; they are approximations of the analog values that exist outside of the digital elements. As described further in Section 2.1.2.1, discrete representations of analog values may introduce errors, aliasing, or artifacts. In addition, digital I&C systems perform their computations based on an internal clock—the computation process itself is discrete, unlike the continuous computation performed in analog systems. Table 1 below summarizes the differences between analog and digital I&C systems.

Table 1: Summary of Differences between Analog and Digital I&C Systems

Analog I&C Systems	Digital I&C Systems
Hard-wired control	Software-based control
Random logic	Regular logic blocks
Combinatorial logic	Sequential logic
Continuous values and computation	Discrete values and clocked computation

2.1.1.3 Evolution of an Analog Control Based System into a Digital Control Based System

In this section one possible scenario for migrating the analog control based simple water level control system described previously into one that includes digital control is presented. Of course, many such evolutionary pathways are possible in addition to the one explored below. Nevertheless, it is believed the evolutionary path presented is plausible and realistic—not only for the simplified example presented but for the introduction of the digital I&C system in a nuclear power plant in general.

2.1.1.3.1 Adding the Digital I&C System for the Water Inlet System

A first step in adding digital I&C system to the simple water level control system described previously consists of replacing the hardwired analog control valve with an inlet control valve that is opened and closed through an actuator. The actuator is capable of opening fully or closing fully the inlet valve to the reservoir through the use of a relay and a solenoid. A microprocessor controls the position of the actuator by sending appropriate commands ('open' and 'close') to the actuator.

Of course, the microprocessor must be able to determine when a change in valve position is needed. For the sake of economy, a waterproof microswitch is attached to the float already present in the reservoir. The microprocessor is capable of sensing the position of the microswitch. When the microswitch is in the closed position (current flows through the microswitch) the water level in the reservoir is at the upper setpoint. When the water level in the reservoir falls below the lower setpoint, the microswitch opens, preventing current from flowing through the micoswitch. Once the water level reaches the upper setpoint, the float closes the microswitch again.

Intuitively, the inlet valve will be in the closed position whenever the microswitch is in the closed position and the inlet valve will be open when the microswitch is in the open position. (The logic could be reversed without adversely affecting system operation, but for clarity a design decision was made so the microswitch and inlet control valve will be in the same state—open or closed.) It is observed that the microswitch's position may need to be latched (stored in memory) and de-bounced[5] to prevent oscillations—rapid opening and closing of the valve—from occurring in the system.

Obviously, the new digital I&C system will need to be programmed in firmware or software to realize the intended behavior. The program may require the processor to read the microswitch's state frequently so it may determine if the inlet valve's position should change state. For this simple example, such a polling mechanism will prove sufficient because the processor is dedicated full-time to insuring the correct state of the inlet control valve based on the microswitch's position. Finally, it is noted that there is no feedback mechanism in place for this system—the processor assumes the valve actually opens and closes as instructed by the processor.

2.1.1.3.2 Adding Digital I&C System for the Water Drain System

Because of the successful digitalization of the simple water level control system's water inlet system as described above, a new project is initiated to upgrade the water drain system. In order to characterize the introduction of digital I&C systems in nuclear power plants more realistically, it is assumed this project is completely independent from the inlet system upgrade—perhaps to be implemented by a different subcontractor with no knowledge of our previous upgrade. Because the water inlet and drain systems are loosely-coupled, the digital upgrade projects need not be coordinated in any way and may occur in either order.

For this project, the direct mechanical linkage used currently to open the drain valve in the reservoir is replaced. Again, there are many reasonable solutions to this challenge. It is decided to replace the drain control lever for the reservoir with a control lever that includes a microswitch and a spring to return the drain control lever to its neutral position once it has been released by the human operator. The microswitch will be 'open' when the human operator depresses the drain control lever. Otherwise, the spring insures the microswitch will be in the 'closed' position. When this microswitch's position changes from 'closed' to 'open', the drain

[5] Many mechanical switches do not open or close cleanly. When a switch is pressed, it makes and breaks contacts several times before settling into its final position. The oscillation of the switch contacts causes several transitions or "bounces" to occur. The process of filtering switch input to eliminate the oscillations is called de-bouncing.

valve should be opened. *However, closure of this switch, caused by control lever release and the return spring, does not indicate a need to close the drain control valve.* The mechanism for closing the drain control valve is described below.

The reservoir's drain control valve will be replaced with a relay and solenoid-controlled valve. In addition, a small float valve and microswitch are added to the bottom of the reservoir so that the low water setpoint for the drain control valve may be determined. The switch attached to this float valve will be in the 'closed' position whenever the water level is at or below the minimum level setpoint for the reservoir. When this switch closes, the drain control valve will be closed. This switch will be in the 'open' position whenever the water level is above the minimum level setpoint. *Note that we do not want to change the drain control valve's position when this switch opens.*

The logic for programming the drain control valve is a bit more complex than the logic for the inlet control system. This additional complexity is due to the system's need to react to external commands from a human operator, communicated to the system by depressing the drain control lever ("open the drain valve") in addition to maintaining the water level at the minimum setpoint for the reservoir. Consequently, this system has two sensors—one to open the drain valve and another to close the valve. The digital I&C system must position the drain valve based on its current state as well as the state of its sensors. Consequently, the digital I&C system's knowledge of its current state is crucial to ensure the proper operation of the drain control system.

2.1.1.3.3 Adding Coordination to the Two Digital Systems

Based on the two digital I&C system upgrades described above, the resulting system behavior mimics closely the analog control system that was replaced. However, the overall simple water level control system has gained no functional advantage at this point. In addition, it is possible that, due to the need for microswitches, springs, additional floats, and solenoids, the overall simple water level control system may have additional potential failure points, be more costly to implement, and may exhibit less overall reliability than the analog control system. Finally, it is observed that the system requires electrical power to function—a requirement that was absent from the analog control system introduced previously.

In this section, it is proposed to take advantage of the additional control capabilities of the overall digital systems by augmenting them to optimize water use. Note that the overall simple water level control system with the two digital I&C systems described previously may be in a state where the drain valve is in the open position while the inlet valve is also in the open position. Clearly such a situation wastes water. This situation is a direct consequence of the loose-coupling of the two control systems. It is possible to accomplish the goal of reduced water usage by adding another digital system to oversee and coordinate the two upgraded systems described previously.

The digital I&C system-based inlet control and drain control systems are augmented by adding a third digital controller containing another microprocessor. This additional processor will receive all sensor inputs directly and then forward appropriate sensor readings to the inlet control and drain control processors, respectively. In fact, the new 'supervisory' controller may synthesize sensor signals to the other controllers so that they will perform the appropriate tasks. The advantage of this architecture is that neither of the existing control systems requires modification—sensor wiring will be re-routed as necessary to existing digital controllers connected as appropriate. This architecture also changes the coupling of the inlet and drain systems so they will be "tightly-coupled." That is, they will no longer operate independently of each other.

The new processor optimizes water usage by closing the drain valve and opening the inlet valve simultaneously. Because of the coupling of valve open/close commands through the new controller, the system will not waste water by having the inlet and drain valves open at the same time. The cost of our optimization includes additional complexity, the extra digital I&C system unit, programming the additional digital I&C system, rewiring the sensors, and the additional electricity needed to supply the third processor. Of course, on a large enough scale, these costs may be more than offset by the savings from using less water.

It is observed that in making the changes described above, a network of sorts among the control units has been created. While this network may not have all of the characteristics of the networks described in Section 2.1.1.4, it still must deal with issues of data communications. It is also noted that from a reliability analysis standpoint, the challenge has grown significantly from the original design. Many of the challenges associated with this resulting three controller system are an artifact of its evolution. An existing system was modified one subsystem at a time. Then the resulting subsystems were combined in a manner they had not been previously and in a manner they were not originally designed to be used. The end result, of course, is increased functionality and utility. However, as has been noted, the resulting complexity is one of the costs of the more tightly integrated system.

Of course, one could decide to design a digital I&C system-based simple water level control system from the ground up. In doing so, it is very possible that the resulting architecture would have been more elegant and straightforward. A system designed to be digitally controlled from its inception might be able to use fewer sensors and a single processor. However, the evolutionary approach of the upgrades precluded this option. Additionally, it may be possible to include additional functionality such as usage statistics (water usage, frequency of drain refill cycles and time of day correlations with those cycles, etc.) that were cost prohibitive when basing the design solution on an existing system. Still, the evolutionary approach of replacing analog systems one at a time using multiple subcontractors seems to be based on real-life experience.

2.1.1.4 Network Example

As illustrated in Section 2.1.1.3.3, one example of a component that may be present in a digital I&C system that is absent from an analog system is a network. In the description of a nuclear power plant's upgrade from an analog system to a digital one [32], a "data highway" is

presented in the schematics. It is not clear from the documentation, however, just what constitutes a data highway. Depending on how such a communication mechanism is implemented (both its physical architecture and the communication protocol selected), there are profound effects on its data communication ability, throughput, and reliability. Without the additional information suggested above one cannot analyze the upgrade fully and it is possible to omit failure modes indigenous to the system.

For an example, assume there is a desire to upgrade a computer network. Also, assume the current system uses an implementation of Ethernet, standardized in 1986, —a network protocol and corresponding network architecture. The network will be upgraded to a version of Ethernet, standardized in 1991, to reduce the cost of maintaining the current system.

The version of Ethernet, standardized in 1986, called 10Base2, uses a bus topology as shown in Fig.2.3 [33]. All the devices in the network are connected through one pipeline (the bus) that is connected in turn to every device on the network. This link may be partitioned by using bridges and other devices, but in this example it is assumed that the network is small enough to be entirely on one link. This setup physically requires terminators at each end of the network and requires each device to be hooked to the bus through a "T" connector. From the network's perspective the digital controller is just another device on the network.

From a physical connection standpoint there are several possible failure modes. If the network cabling is damaged at any point, the entire network will fail. If a device fails or is removed, only the respective node is affected. However, if the device fails in a way such that it sends data continuously, the whole network will fail due to the inability of other devices to transmit data. Finally, if a terminator, which is at the end of each side of the link, is disconnected from either side of the link, the entire network will fail as the terminator removes old data from the link. Without the terminator, the signals will never be removed from the link and will make it impossible for new data to be sent.

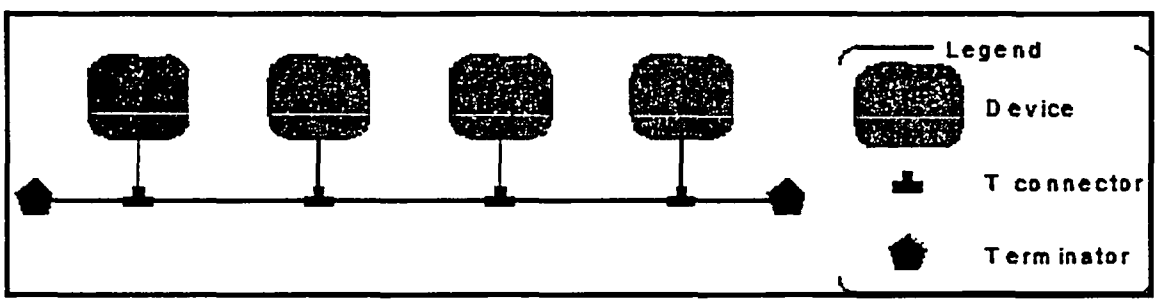


Figure 2.3 Bus Architecture Ethernet

The version of Ethernet, standardized in 1991, called 10BaseT, uses a star topology [33] as shown in Fig.2.4. A star topology has all devices connected directly to an intermediary device. One may think of the spokes on a bicycle wheel all connecting to a hub in the center. In order to communicate, a device on the star sends a message through the hub to the receiving node. These intermediate central devices in the star may be 'hubs' or 'switches.' Hubs are repeating devices that do not understand network protocols. They simply retransmit all data received on

one link to all other links. Switches understand the network protocol and thus can select which links should receive the retransmitted data to minimize network traffic.

Using 10BaseT Ethernet in a star topology, if a device other than the hub/switch fails or a device is removed from the network, only that device is affected. If the network cabling is damaged, then the link will be partitioned into two or more sections that will be unable to communicate. If a hub or switch fails, then all nodes that use that hub or switch to communicate will be unable to communicate. A feature not found in 10Base2 Ethernet is that the hubs and switches have a fail-switch that can deactivate the nodes that are sending bad data. Thus the failure case in 10Base2 Ethernet described above can be eliminated or reduced significantly. In spite of this added safety measure, this safety feature may fail in a way that causes the hub or switch to deactivate devices that are sending valid data.

As seen in the above example, it is necessary to enumerate and model all failure modes that may occur in all types of network components to understand fully the impact to all devices attached to the network. Also, it is necessary to model the safety devices and auxiliary devices that may affect the network, such as hubs and switches. Finally, our modeling should include appropriate analysis to understand the reduced capacity of a damaged, but still functioning, network. As the example shows, new issues may need to be addressed in the reliability modeling of digital systems. Subsequently, the modeling should account for this complexity for credible predictions of the digital I&C system stochastic performance.

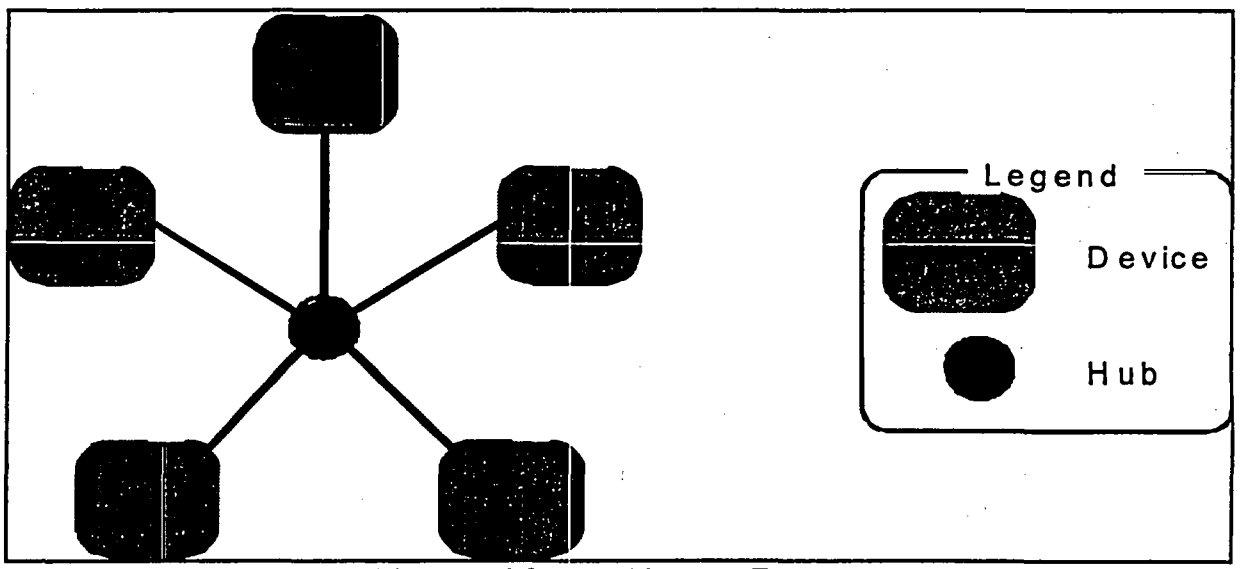


Figure 2.4 Star Architecture Ethernet

2.1.1.5 Other Issues

This section discusses other issues involved in digital systems not explored previously, namely coupling, self-diagnosis, and security.

Coupling of events in the system can be characterized in two ways, either tightly or loosely

coupled, as defined previously. "In tightly coupled systems the buffers and redundancies and substitutions must be designed in; they must be thought of in advance" [34]. Tightly coupled systems have little 'slack' to play with; there must be little variation from the design specifications in order for operation to continue in accordance with the design. "In loosely coupled systems there is a better chance that expedient, spur-of-the-moment buffers and redundancies and substitutions can be found, even though they were not planned ahead of time" [34]. Loosely coupled systems have a larger degree of 'slack' and can accommodate more operational variation before the system does not behave as desired.

In order to refine and characterize the differences in coupling between the fully analog and integrated digital control systems, refer again to the simplified water level control example. The analog simplified water level control system exhibits loose coupling between the different components, the inlet controller, and the drain controller. This loose coupling can be seen from the example stated previously in that the inlet and drain controllers do not communicate directly—the water in the reservoir acts as the communication mechanism. The low setpoint may drift, however, as long as the drift is away from the minimum water level and below the high setpoint and the inlet flow rate is strictly less than the drain flow rate, the system may continue to function, though the system will operate at a reduced degree of efficiency. In this case, the inlet control valve is open while the drain valve is open. This is a primitive form of fault tolerance that can occur due to the loose coupling of/between the inlet and drain control systems.

Consider the supervised digital control system mentioned previously for the simplified water level control system. There are several features that may cause the simplified water level control system to fail that are not present in the analog system. The drain valve in the analog version is constructed such that gravity will cause it to close. In the digital control system, the digital system is designed with explicit control over when the drain valve will close; it will be opened and closed by a solenoid under the auspices of the digital controller. In such a design, however, an issue exists as to whether the drain valve is really closed. Just because the controller signaled for a valve to close does not mean that it closed. For issues such as this, more sensors are needed to increase the controller's knowledge of its environment. However, additional sensors, the associated wiring, and additional logic codified in the controller increase the complexity of the system. Also, these additional sensors may fail just like any other sensor. At some point, the utility of the new data gained will be offset by the increased probability of sensor failure, additional complexity and possibility for inconsistent readings [34]. When such capabilities are introduced into a digital system, they must be introduced explicitly as is shown in the example above. In other words, the system must be designed a priori to have this type of functionality. Otherwise, a design change may lead to several possible impacts on system reliability. For the scenarios that are covered correctly by the self-diagnosis and repair, it may mitigate failures in operation. However, the ability to react to and "repair" a faulty component/sub-system may cause abnormal operation in some other component that depends on the affected component/sub-system. Finally, the increased diagnostic and repair capabilities may make it more difficult to implement the digital system's design functions correctly, thus these additional features may affect reliability.

Security is an issue that must be addressed in the recent climate of large scale, possibly unintended, interconnections to the world outside of a nuclear power plant through the Internet.

The use of security is directed both to mitigate unintended usage of the digital system and to ensure that operators who need access to the system may access it at an appropriate level. While there are physical security concerns about objects colliding with nuclear power plants and the impact of these collisions on the reliability and safety of the plant, the digital system security concerns are also critical. For instance, a computer worm, a program designed to self-replicate and remain self-contained [35], was able to disable a safety monitoring system in a nuclear power plant for 5 hours[6] [36]. Although this incident did not appear to cause anything more serious than forcing operators to use analog backup systems, the coupling among systems due to an unprotected pathway within the plant resulted in a 'backdoor' through which the worm could enter the nuclear power plant through a route unintended by the system designers. This incident shows that these concerns must be addressed to fully characterize the impact of digital systems on a nuclear power plant's safety and reliability. This task is beyond the scope of this report.

2.1.1.6 Summary

The purpose in reviewing what constitutes analog controllers and digital controllers is to provide a common framework for moving forward. Without such a framework, the characteristics of the controllers may be interpreted too broadly to permit appropriate analysis. It is noted that while the above discussion may not be fully comprehensive, it is believed to include many, if not all, of the essential characteristics.

Finally, it is noted that few, if any, systems are likely to be characterized easily as an analog instrumentation and control system or a digital I&C system. Rather, there is a continuum between a 'pure' analog system and a 'pure' digital one. Most systems are comprised of a combination of analog and digital devices and must be analyzed based on their design characteristics.

2.1.2 Survey of Techniques from Other Industries

In this section we review the approaches used by other industries to deal with digital system reliability issues. All of the industries selected, covering aerospace, medical device, defense system, and telecommunications, include "mission critical" digital systems. As such, and as is the case with nuclear power plants, these digital systems have the potential to enhance or negatively impact the safety of the general population. An examination of the approaches used by these representative industries to digital system reliability analysis may prove instructive.

2.1.2.1 Fundamental Issues

As noted previously, digital systems may consist of hardware components such as processors, memory, peripheral devices, sensors, actuators, and networks. All of the devices may include software and/or firmware. Reliability data for the hardware components may be obtained in a number of ways including accelerated life testing, stress testing, and sampling techniques. These components tend to follow the bathtub curve of product reliability [37]. However, the

[6] In August of 2003, the Slammer worm was able to enter a network that was believed to have been protected by a firewall at the Davis-Besse power plant, disabling a safety monitoring system for almost 5 hours. This required analog backups to be used until the problem was corrected. The worm entered through an unsecured private contractor network that was attached to the plant's network, bypassing the firewall.

firmware and software elements of these systems do not demonstrate any wear characteristics whatsoever. Consequently, these elements of digital systems do not respond to accelerated life testing, stress testing, etc. Nor is firmware/software reliability modeled accurately using a bathtub curve approach [38]. Flaws in software/firmware elements of systems are present when they are released, even if they are not discovered until long after they have been installed [39]. The lag time for discovering such flaws cannot be predicted or modeled, as they are not a consequence of usage or aging. As a result, reliability treatment of digital systems tends to include firmware and software as a largely invisible element of the hardware that encapsulates it.

In the introduction of their paper, Kang and Sung [40] present many issues that can arise with digital systems as opposed to analog ones. One of the large issues with modeling digital systems is that the function/behavior of such systems may change over their operational lifetime due to hardware changes, software changes or both. Another issue is that digital systems of any type operate in discrete time steps. Consequently, artifacts and aliasing may be introduced if the sampling rate is too low for the application [41]. Kang and Sung also state "...the failure modes[7] of digital systems are not well defined". For example, errors in design and software implementation can cause the digital system, which appeared to be functioning correctly, to suddenly fail due to some specific input being received. In addition, the system may fail not only on that specific input but also on other inputs that are semantically similar or even equivalent/correlated. Also, digital systems may have a much smaller operating environment temperature range than analog counterparts. Although temperature is an environmental stressor not specific to digital systems and the digital system would be qualified for the environment it is to operate in, a smaller operating environment temperature range would make the digital system more vulnerable to temperature fluctuations compared to analog systems. Another feature of digital systems is that software may be able to mask intermittent failures due to hardware failures, environmental effects, and undesirable conditions. For example, communication protocols [33], error detection and correction codes and methods, fault tolerance, and self-stabilization algorithms all provide the ability for software to mask intermittent hardware failures. In addition, distinct digital systems may demonstrate common cause failures due to their construction from standardized hardware/software components. Finally, it is possible for digital systems to introduce new failure modes. Protocols, while providing cost savings and fault tolerance, may introduce dependencies between different systems such that if a system fails in a way that introduces 'garbage' data as input to the other devices (see Section 2.1.1.4), the 'bad' data subsequently may cause all other systems using that input resource to fail. Similarly, when digital systems are used to 'multi-task' and save expenses, such multi tasking may introduce new failure dependencies.

In summary, the issues that must be addressed when examining the digital I&C-based systems that are not present in their analog counterparts are the following:

- The function/behavior of digital systems may change over their operational lifetime due to hardware changes, software changes or both.

[7]Failure modes refer to a complete description of the conditions for the failure to occur, the usage of the device, causes of the failures and the results of the failure. [45]

- There may be internal communication between different components of the digital I&C system (Section 2.1.1.4) that can introduce new failure modes.
- Since digital systems operate in discrete time steps, artifacts and aliasing may be introduced if the sampling rate is too low for the application [41].
- The failure mechanisms of digital systems are not well defined [40].
- Digital systems may have a much smaller operating environment temperature range than analog counterparts.
- Digital systems may be affected differently than analog systems by external stressors such as electromagnetic interference (EMI)/radio frequency interference (RFI), temperature, pressure, vibration and radiation. Consequently, they must be qualified to operate in all expected conditions as specified by IEEE Std 323 [42], IEEE Std 344 [43] and NRC Regulatory Guide 1.180 [44].
- In uni-processor and distributed environments, software may be able to mask intermittent failures in hardware as measured by Fault Coverage in [13] and has the ability to introduce corrective actions or mitigate failed hardware through fault tolerance or fault recovery [46].
- Different hardware systems may demonstrate common cause failures due to the use of standardized components for building the systems [40].
- Software-based digital may also exhibit common cause failures due to software design errors in redundant systems [30, 47-50].
- It is possible for digital systems to introduce new failure modes.

2.1.2.2. Aerospace

The aerospace industry includes aircraft and spacecraft. In the U. S. aircraft are evaluated by and certified for flight through the Federal Aviation Administration (FAA). NASA oversees spacecraft development and maintenance. Each agency follows its own procedures and certification system. Issues involving aerospace digital systems have become more important as flight control systems have evolved to 'fly-by-wire' systems as replacements for 'stick and rudder' approaches.

2.1.2.2.1 The FAA

The FAA has developed guidelines for all software to be installed on aircraft as stated in DO - 178B [51] (and its companion for errata, DO-248B [52]). These guidelines partition software according to its 'flight criticality.' Specifically, the impact of anomalous behavior by the software and its contribution of system functionality that may lead to a failure condition for the aircraft form the basis of the FAA's approach. The partitions are categorized by the FAA as follows:

Level A	catastrophic
Level B	hazardous/severe-major
Level C	major
Level D	minor
Level E	no effect

DO-178B mandates 6 software development processes to be performed, 20 life-cycle data artifacts to be developed, and up to 66 objectives to be met, depending on the flight criticality

level as identified above. A primary concern in DO-178B is traceability among development artifacts such as requirements, design, code, testing, etc. The authors note the FAA's approach focuses on development processes and artifacts created during software development as opposed to evaluating risk based on the delivered software itself.

2.1.2.2.2 NASA

The NASA has recently developed guidelines for conducting PRAs for spacecraft systems [23]. These guidelines acknowledge the challenges for conducting PRAs for software outlined above and observe that "no risk modeling framework and technique development has been generally accepted as a widely acceptable solution to the assessment problem" [23]. The guidelines conclude "...most PRA or system reliability assessments consider software contribution to risk negligible in comparison to, or included in, hardware component contributions to system failure probability" [23].

NASA notes the inability of testing to provide appropriate coverage to assess software risk for anything but the simplest (smallest) programs. The NASA guidelines identify black box reliability models and conditional software failure models exemplified by Schneidewind [53], ET/FT and DFM approaches respectively. These approaches are discussed in detail in Section 2.1.3 and 2.2.

2.1.2.3 Medical Devices

In the U.S., the Food and Drug Administration (FDA) regulates the ability of manufacturers to market medical devices. The FDA recognizes that a variety of medical devices include digital systems and has tracked a number of product recalls and failures due to problems with such systems. Consequently, the FDA has published guidelines covering principles of software validation [39]. These guidelines apply to all medical devices developed after June 1, 1997. The intent of the guidelines is to minimize the risk to the population-at-large from defects in medical devices containing digital systems.

The guidelines note that unlike hardware, software is not a physical entity and as such does not wear out. In addition, the guidelines note testing alone is not sufficient to verify that software is complete and correct. Finally, the guidelines note that software failures may occur without any advance warning as latent defects may be discovered only when a particular execution path is exercised. Such defects may remain hidden for long periods after a product has been in general use [39].

As a consequence of these observations, the FDA guidelines suggest that a risk management, quality assurance, and quality control approach be used to minimize risk associated with medical devices containing digital systems. The guidelines note that both quality assurance and quality control processes should produce 'objective evidence' of the correct application of development processes and system behavior.

In essence, the guidelines promote a 'process validation' approach to software validation. The authors note that the guidelines do not endorse any specific engineering, quality assurance, or quality control techniques. Furthermore, no specific development methodology is sanctioned.

In fact, the guidelines suggest that the 'least burdensome approach' is the best approach. Finally, no formal risk assessment is conducted for affected medical devices.

2.1.2.4 Defense Systems

The U.S Department of Defense (DOD) is, perhaps, the world's largest customer of digital systems. DOD systems are used for logistics, strategic planning, tactical planning, communication and control, and, of course defensive and offensive weapons and support systems. Such systems are fundamental to the DOD's ability to succeed in its endeavors. Over the years, the DOD has experienced both spectacular successes and tragic failures in its digital systems [54]. In order to improve its ability to obtain systems biased heavily towards success, the DOD initiated the Software Engineering Institute (SEI) at Carnegie Mellon University in 1984.

In 1987 the SEI published the Capability Maturity Model (CMM) [55]. The CMM is a combination of an evaluation of software development practices, a vision of idealized processes and practices, and a road map to achieving the vision. The CMM evolved into the Capability Maturity Model Integration (CMMI) [56, 57] but retains many of its original principles. The overall focus of the SEI is on-time delivery of systems within budget and with full functionality.

In essence, the CMMI is a set of planning and management practices, development approaches and techniques, and quality assurance and quality control techniques to be applied to software development and system (hardware/software) development. Companion reports address risk management [58], commercial off-the-shelf (COTS) software and a variety of related topics.

Despite the wealth of materials developed by the SEI, the overall approaches taken by the organization include management techniques, specific technologies to be used [59], evaluation techniques for products and processes, and improvement based on best practices. While all of these approaches are valuable in their own right, none addresses PRA for digital systems or software components of such systems.

Finally, the DOD uses a variety of proving grounds to determine if the systems developed are truly battlefield-ready. The tests conducted at these proving grounds are essentially system-level tests under harsh conditions. While such tests often reveal deficiencies, all too often they fail to find problems that are exposed only under real battlefield conditions.

2.1.2.5 Telecommunications

The telecommunications industry has evolved over the years from a pure hardware-based switching system using tip/ring boards and human operators to connect calls to a fully automated, fully digital system. In 1994, the European Union began requiring all suppliers of telecommunications equipment within its member countries to be registered to one of the ISO 9000 quality system standards.

The ISO 9000 family of quality system standards was published initially in 1987 [60]. Like the SEI's CMM, ISO 9000 has evolved since that initial publication and the current version of the standard is ISO 9001:2000 [61].

The ISO standard is a set of requirements essential for quality assurance and quality control. The standard is generic in nature and is thought to capture quality management approaches applicable to engineering, production, installation, and servicing for any product or service offered by an organization. To that end, the aforementioned activities as they relate to digital system development and software development are covered by the standard.

While the philosophy and approach of ISO 9001 is different than the SEI's CMMI, the essence of the two systems is more alike than dissimilar. However, like the CMMI, ISO 9001 does not address risk management in terms of PRA analysis or something equivalent. ISO 9001 is truly a quality assurance and quality control approach at an enterprise level. The system may imply that risk management is included in the resulting management system, but there are no specific requirements or processes identified at a product level.

The ISO 9000 standard was compared to 10 CFR 50 Appendix B by the NRC in 2003. The report [62] advocated that ISO 9000 was not as appropriate in meeting nuclear power plant quality needs as Appendix B.

2.1.2.6 Process-oriented Industries

Process-oriented industries include manufacturers whose challenge is to produce products consistently over large production runs and for significant time periods. An example of a process-oriented industry is the chemical industry. Chemical producers transform their feedstock ingredients through a series of processes into end products for their customers. Challenges to these producers include creating products with consistent yield and purity regardless of the variations in ambient temperature and humidity, feedstock purity and structure, equipment wear, and changes in personnel.

ISO 9001:2004 [63], discussed briefly above, provides requirements for process-oriented industries. For chemical manufacturers that supply laboratory-grade products for the pharmaceutical industry, the FDA's Good Manufacturing Practices [64] provide requirements for quality system regulation. Both ISO and the FDA rely on management responsibility, quality assurance, and quality control discussed previously. In addition, both sets of requirements include proper training for associates, documentation and use of standard operating procedures (SOPs), identification of appropriate workmanship standards, capture of inspection and test results, and periodic inspections and audits of the overall quality system. Neither approach appears to require risk assessment as part of the system, however.

2.1.2.7 Initial Conclusions

In this section, the risk management and assessment approaches taken by industries that rely heavily on digital systems for mission critical functions were reviewed. The goal was to

determine whether there was a body of work on which the nuclear power industry may build to develop appropriate techniques for digital system PRAs in nuclear power plants.

It appears that most, if not all, approaches taken by other industries include software development process, management and testing as their primary activities. Certainly these approaches are central to the medical device, defense system, telecommunication and process oriented industries. In addition, the aircraft industry under the FAA also follows these approaches. As described in Section 2.3, these approaches for digital systems are consistent with those used in the nuclear power industry. However, the nuclear industry, with the leadership of the NRC [2], is in the forefront of introducing risk informed methods into system modeling and design using PRAs. The spacecraft industry, under NASA's guidance, also appears to be moving to a true risk evaluation system using PRAs. The NRC and NASA both recognize the challenges associated with conducting PRAs for software-only systems. Consequently, they suggested that digital systems be evaluated holistically rather than attempting a separation into hardware and software components.

Therefore, this project will treat digital systems as units rather than composites of separately analyzed hardware and software systems. A number of methodologies that have been proposed for conducting PRAs on digital systems are examined below.

2.1.3 Reliability Modeling Approaches for Digital Systems

As indicated in Section 1.2, while the static ET/FT approach has been used in the reliability modeling of digital I&C systems in nuclear power plants, the presence of the complex hardware-software-physical process interaction may necessitate the use of dynamic methodologies for dependable results. Some specific issues relevant to such an interaction are the following (see Section 2.1.1.2):

- Digital I&C systems rely on sequential circuits which have memory. Consequently, digital I&C system outputs may be a function of system history, as well as the rate of progress of the tasks.
- Tasks may compete for a digital controller's resources. This competition requires coordination between the tasks and may lead to problems such as deadlock and starvation [31].
- The choice of internal/external communication mechanisms for the digital I&C system (such as buses and networks) and the communication protocol affect the rate of data transfer and subsequently the digital I&C system reliability and robustness.
- The ability to coordinate multiple digital controllers directly and explicitly may necessitate a finer degree of communication and coordination between the controllers.
- A digital controller can remain active and not only react to data, but can anticipate the state of the system.
- Tight coupling and less tolerance to variations in operation increases the digital I&C system sensitivity to the dynamics of the controlled physical process and hence its representation in the digital I&C system reliability model.

There is a large body of work in the area of software reliability modeling, measurement, and prediction. A variety of models and techniques have been suggested. Existing approaches to model reliability of software consider one or more of the following factors [65]:

- testing metrics
- process quality data
- static analysis of software
- analysis of software structure
- simple software metrics or combinations of them.

However, in spite of the progress of the past 30 years, the field is not yet at a mature stage. The existing approaches exhibit substantial limitations [65,66]. Some of these limitations include:

- applicability of some models or assumptions that are unlikely to be satisfied by the actual system
- need for data that is difficult or impossible to collect
- prohibitively large complexity of the model when used in realistic applications
- limited level of reliability the model can assure
- lack of evidence and/or empirical data to support the validity of the model.

There is no consensus in the community about how the reliability of software systems should be modeled, measured, and predicted, and even whether such a concept makes sense for software. Therefore, in this report we are considering only those approaches that have been applied to mission critical applications or are being researched in the context of mission critical applications.

The methodologies proposed for the reliability modeling of digital I&C systems can be grouped as follows:

- Markov models [13]
- Dynamic Flowgraph methodology (DFM) [22]
- Bayesian methodologies [67, 68]
- Petri net methodologies [69-74]
- Test based methodologies [75]
- Software metric-based methodologies [52]
- Black - box methodologies (Schneidewind Model) [53, 77]

The references cited above are not exhaustive but are representative of the methodologies proposed for the reliability modeling of digital I&C systems. It should be noted that this comparison is done only through the examples cited in literature that may pertain to nuclear power plants. There is no current benchmark system for a common comparison (see Section 4). As a consequence, the discussion may seem to focus more on certain methodologies; that is a side effect of the availability of the literature examples on the topic. These section labels

are designed to group the methodologies reviewed, not to exclude other methodologies that were not reviewed. Additional references may be found in [78].

2.1.3.1 Markov Models

Based on the survey of current literature, Smith et al. [13] propose the only Markov approach that is relevant to digital systems in nuclear power plants. They describe how to apply this Markov procedure that uses five key steps to determine the reliability modeling of a digital I&C system. These steps are the following:

- Identify the system's metrics
- Generate an analytical model for the system
- Validate the model
- Identify the critical model parameters
- Estimate the critical model parameters

An example of this approach with repair rates, failure rates, and fault coverage as parameters, and fault injection[8] of the digital I&C system to estimate those critical parameters is given in [13]. The model can describe the complex Type II interactions due to its explicit modeling of software and hardware through fault injection. It is also widely applicable to many types of digital systems, from high availability e-commerce sites to high reliability systems that are analogous to digital I&C systems. For instance, a high-availability website is roughly analogous to an instrumentation panel in a nuclear power plant. Finally, this approach may be more easily integrated into a PRA than some other approaches.

However, there are some limitations to this approach. Repair rates, used in the Markov model for digital systems, are not necessarily appropriate to express the ongoing dynamics of such systems. For example, identifying the cause of a problem and repairing hardware-only systems may be accomplished through a defined fault removal process to locate the defective component(s). Ultimately, the defective part(s) may be swapped out and replaced with fully functional components. However, software contributions to digital system failures may be much more difficult to locate and repair. A debugging process is needed to fully characterize and locate all causes of the defect. The impact of changes made to repair the defect must be analyzed and tested as well. Depending on the nature of the system and the flaw, it is possible the error may not be uncovered using the same input stream that has caused the error to be exposed previously. For example, software that uses time in its calculations may perform unpredictably due to variation in time values reported by the system clock. Clearly, such behavior can complicate the localization, identification, repair, and validation processes significantly. In addition, the required corrections may not be confined to a single location or module in the code and may also introduce new errors. For instance, fixing the bug may entail significant changes to the semantics of how the software is constructed. These semantic changes may cause other sections of the program that use this section to fail in subtle ways. In fact, it is possible that significant re-design of the system may be required to repair a particular flaw. Thus, it is not clear how a mean-time-to-repair rate can be predicted.

[8] Fault Injection is a process in which deliberate faults are introduced into a system and the system response is observed [79].

Additionally, the reliance of Smith et al [13] on fault injection techniques may make the resulting Markov model unreasonably large or it may take an unreasonable amount of time to create, run, and justify the correctness of the model. "From a fault injection standpoint, simulating distributed faults is nearly an impossible task." [80] Fault injection must be applied with care and must not be used to craft the reliability of the system. "Fault injection is generally incapable of determining correctness... because anomalies are injected into the code and... the program is run in an altered state." [81] Based on a conversation with the authors [82], it appears that the fault injection exploration conducted was based solely on 'random flipping' of bits in the address space of the memory and the units in the processor. It is not clear if the bits perturbed were single bits, clustered in some way—either based upon memory location or temporal characteristics—or if they were located solely in hardware or part of a communication protocol such as Ethernet that can detect and correct such anomalies. While this approach does seem to have merit in describing the ability of software to mask intermittent hardware failures and/or stuck at one or stuck at zero failures, it is not clear that such a fault injection procedure can be used as primary evidence of the reliability of a digital system. Also, although software inputs may be classified statistically into equivalence classes, values that are statistically or semantically "close" may not be "close" with respect to what the software computes on those inputs (see section 2.1.3.5). In these respects, conclusions based upon these explorations can be of concern. Finally, the high level treatment of the approach in [13] may have overlooked some essential properties of the system.

2.1.3.2 Dynamic Flowgraph Methodology

Garrett and Apostolakis describe how to apply DFM to validate the safety requirements of digital I&C systems [22]. The approach integrates the digital I&C system and the other physical components with the process aspects of the system. Garrett and Apostolakis model the physical and software variables by mapping them into a finite number of states. The effects of physical and software component functional behavior (including failures) on the system performance are represented by decision tables.

Fundamental issues that may have an impact on the effectiveness of this approach include the difficulty of choosing a proper set of states for each variable and the accuracy of the constructed decision tables. The trade-off, of course, is between the accuracy of the model and the size and complexity of the model. In addition, the model is qualitative in nature. As stated earlier, some applications of DFM have indicated that, with failure data, quantification is possible [83]. Its integrablity into an existing PRA will require further testing (see Section 4).

2.1.3.3 Bayesian Methodologies

Zhang and Golay [67] describe a software engineering framework for using Bayesian updating to determine a reliability measure for software produced. This method uses a CASE (Computer Aided Software Engineering) tool that can represent the structure of the program, including requirements, functions, and data structures. This tool is integrated into a development methodology, Development Before The Fact (DBTF), which allows for feedback very early in the development process. The software is designed in a hierarchical, object-oriented network of components. Essentially, all of the decisions are checked by an automatic checker to insure

consistency and adherence to the set standards. From this check, a program code is automatically generated using the tool.

Reliability is determined algorithmically using the equation:

$$R = 1 - \frac{Number\ of\ Untested\ Paths}{Total\ Number\ of\ Paths}\Theta \quad (1)$$

Each path is defined as a path through the program that limits all loops to at most *k* iterations and Θ is the probability that the path contains at least one error. Bayesian updating is used for estimation in Eq.(1). The updating relation is defined as

$$f^*(\Theta) = C\Theta^m(1-\Theta)^{n-m} f(\Theta) \quad (2)$$

where $f(\Theta)$ is the prior probability distribution function (pdf) for Θ, $f^*(\Theta)$ is the posterior pdf, *m* is the number of software errors found, *n* is the number of paths tested and C is a constant.

The main advantage of this method is that $f(\Theta)$ can estimate Θ incrementally while testing the system, increasing the reliability accuracy when new testing is available. In addition, the application of the methodology at the development stage of the software may be able to increase the confidence in the product. The limitations of the approach are as follows:

- The total number of paths, *m,* must be estimated, which can be hard (or impossible) to accomplish depending on the software examined.
- The assumptions that produce Eq.(2) may not be applicable to digital systems in general.
- The execution paths that are not used for the reliability assessment must be analyzed to ensure it is reasonable to not use them for the analysis. If this is not the case, it is possible to skew the results such that the reliability estimate is too pessimistic or too optimistic.
- The approach cannot be used for software already developed.
- This approach works only on source code validation of software and it does not analyze auxiliary systems that create the artifacts such as compilers and hardware that may have flaws. These flaws may impact the reliability of the system and may not be accounted for in this approach.
- It does not take into account Type I or Type II interactions.

Finally, it is unknown if this approach may integrate into a PRA.

2.1.3.4 Petri Net Methodologies

Peterson [72] describes Petri nets as a graphical modeling language. It is similar to a finite state machine, with transitions, arcs and nodes. Arcs connect either transitions to nodes or nodes to transitions. It also uses tokens that can move when the Petri net is executed. A token moves from a node or place and is consumed by a transition. When a transition fires, it produces tokens in places that it connects to and consumes one token in each of the places

that connect to it. In order for a transition to fire it must have at least one token on each of its input places.

The study of Petri nets typically uses the structure of the Petri net to discover properties about the system being modeled. For instance, a Petri net that has at most 1 token on each place is called safe. If it allows at most *k* tokens in each place, it is called *k*-bounded. Another property that is very important in deadlock detection is conservation of tokens; a Petri net that conserves all tokens is called conservative. Most evaluations of Petri nets are used to discover if the models hold these properties.

Marsan and G. Conte [73] describe Generalized Stochastic Petri Nets (GSPN) as Petri nets with the addition of a set of transitions that fire at random times. In this approach, the normal transitions are chosen to fire through user provided pdfs when multiple immediate transitions are eligible. One may also include an inhibitor transition type that is used as an inverse of a normal transition - i.e., it can only fire if there are no tokens in its input arcs. The inhibitor transitions do not affect the power of the GSPN, but can reduce the model size. It is shown in [73] that the GSPN are equivalent to Markov chains if bounded. Reference [73] also discusses how Markov chains can be generated automatically from the GSPNs.

Liu and Chiou [74] describe how Petri nets may be used to directly simulate a fault tree, with combinations of nodes and transitions representing different types of logic gates, including inhibit gates, delay gates and M-out-of-N gates. An algorithm for generating minimal cut sets and path sets from these translated fault trees is presented. Finally, a new representation of Petri nets called dual Petri nets is introduced. A dual Petri net is a Petri net with multiple input transitions reduced to only include one transition, with multiple arcs. Dual Petri nets are useful for constructing the fault trees directly. Using these methods, one may use a Petri net to detect faults in a manner similar to that of employing fault trees.

Balakrishnan and Trivedi [71] describe a case study for applying stochastic reward Petri nets (SRPN) to network routing. The SRPN are GSPN with rewards marked for each of the characteristics desired. This type of Petri net is used like GSPN to determine Markov chains from the model. Such Petri nets may be used as a high-level description of a system.

Rauzy [70] describes a generalization of Petri nets: mode automata. A mode automaton is an input/output automaton with a finite number of states called modes. With some restrictions on the mode automata and some loss of information, these automata can be compiled into fault trees. The mode automaton is always at one mode and may transit to other modes based on the transition function that each mode carries. One may check reachability, deadlocks, liveness, etc., on these automata as is done on Petri nets with explicit support for synchronization and compositions of different automata. When the automaton is compiled according to Boolean formulas, the sequence or ordering of events is removed as it is simply all of the events conjoined together. For instance, a series of valves failing, one after another is simply the logical AND of the state of each valve. The modeling power of a general mode

automaton is greater than a Turing machine[6], as "mode automata are a super set of Petri nets with inhibitor arcs. Since the latter have the power of Turing machines" [72], mode automata can model everything a computer can compute.

Goddard [69] describes how Petri nets and failure modes and effects analysis (FMEA) may be applied to requirements to determine missing safety requirements, uncertainties in safety requirements, and inconsistencies in safety requirements. This method uses standard Petri nets with the addition of inhibitor arcs and condition places. Condition places are the same as normal places but they cannot receive a token through execution of the Petri net or lose a token through execution of the Petri net. These condition places are useful for modeling switches or conditions that are not controlled by the system being modeled. The safety requirements are then translated into a Petri net and the Petri net is executed.

Petri nets may also be used during design to verify that safety requirements are met. If the Petri net indicates that a hazard can occur with fewer than a pre-specified number of independent failures (e.g. based on safety requirements), then the system design can be revised to increase the number of independent failures necessary for that hazard to occur. This way, one can remove potential common cause failures. Also, in some cases, a hazard occurs if a state cannot be reached. For example, a system may eventually need to reach a quiescent state and will never do so. In this case, the reachability graph is used to determine if there is a path to the quiescent state desired by modifying the design or the operational procedures for the system. Once the revision takes place, the Petri net is changed to account for transition failures and a FMEA is conducted by changing the input possibilities or its ability to fire. Essentially, the Petri net is first used to validate the design of the system, and then it is used to ensure that extraordinary conditions that are possible in the system because of errors are accounted for in the reliability analysis.

The advantages with the above-described types of Petri nets are many. The main advantage of GSPN/SRPN is that Markov chains may be used to evaluate performance of a system. Consequently, this technique may be used to increase modeling realism with respect to a normal Petri net. Due to the ability to generate fault trees from the models through dual Petri nets [74], Petri nets seem to be compatible with the current ET/FT approach to PRA. Mode automata may be used to simulate anything a computer can compute and such automata may be used to generate Markov chains automatically. Dutuit et al [84] also provide a concrete example of how GSPN can model both the process and component actions of digital I&C systems using a level control system similar to the one shown in Fig.1.6.

The limitations of these approaches include the following:

- The stochastic Petri nets assume an exponential distribution of timed firings, which may not be reasonable for certain type of systems.
- Petri nets are limited to systems that can be represented as states and transitions, which implies that the system has to have a finite number of states. Thus, a Petri net could not represent a continuous variable directly.

[6]A Turing Machine is a model of computation that consists of a finite state machine controller, infinite tape memory and a read/write head [31]

- Simple systems may result in many parameters and many states which may lead to computational difficulties in processing the Petri net.
- Solutions may be hard for a computer to find (this is especially an issue as the different Petri net types get more complex, in particular mode automata—computers might not be able to solve all of the models that a mode automata may generate [70]).
- Reachability graphs may become extremely large even for relatively small Petri nets which can again lead to computational difficulties in processing the Petri net.
- It may be time consuming to create models that can be integrated into a PRA.

2.1.3.5 Test-Based Methodologies

Li, Li, and Smidts [75] describe a conventional test-based approach that may be used to approximate the reliability of a digital system. By running a number of tests and measuring the number of failures, a measure of reliability can be generated. One advantage of this approach is that conceptually it is relatively easy to implement. The only support that is needed is a test driver for the system. Another advantage is that it can accommodate both analog and digital systems in the same model. Also, by using this model, it may be possible to fix faults in the system while testing its reliability. The technique produces quantitative output that can be used in a PRA since it was designed with such an application in mind. Finally, the input to the model may be probabilistic to simulate a 'typical' application and to better estimate the reliability of the system.

One of the limitations of test based methodologies is that testing is a value added activity with respect to errors in software, i.e., it can only inform the tester of the presence of an error under the tested conditions. Testing provides no information regarding the absence of software errors under different conditions. A simple example of this, as stated previously, is when time is used in calculations. Some inputs may produce correct results because they were run at the "right" time. Another example is if there is non-determinism in the digital I&C system, such as a race condition, there may be test cases that complete correctly even though another test using the same inputs may fail to run correctly. This approach does not produce much confidence in the tested system, as it is hard to quantify how successful the testing process was for software. For instance, code coverage, path coverage, equivalence partitioning, and boundary value analysis [38] are used to determine the test cases for software, but they may miss significant test cases that could cause errors due to the partitioning of the test inputs. The test cases might not be representative of real world workloads; they may not be rigorous enough to exercise the system to predict accurately its reliability. In 1985, Parnas [85] described the infeasibility of testing software: "The number of states in software systems is orders of magnitude larger than the number of states in the non-repetitive parts of computers. The mathematical functions that describe the behavior of these systems are not continuous functions, and traditional engineering mathematics does not help in their verification." Also, the quality of the reliability analysis is highly dependent on the tester's abilities. If the tester is not able to find faults that are present, faults may be still uncovered when the system is run under a 'typical' workload. Subsequently, the reliability predicted through this method may be too optimistic. Finally, the system must be completed or nearly so for this method to be used.

2.1.3.6 Software Metric-Based Methodologies

A software metric-based approach [76] uses software metrics gathered in the software development process to approximate the reliability of software. This approach is discussed in more detail in NUREG/CR-6848 [120] and NUREG/GR-0019 [86]. In these documents, it is concluded that this method was shown to be sufficiently accurate for applications of failure rates of 10^{-4}. One advantage of this method is that the metrics that are required for the method are the easiest to gather. These metrics should have been already gathered as part of a mature software development process. Also, the method is fast and the calculations are simpler than most of the other approaches surveyed. Finally, the method will produce reliability measures that integrate easily as basic events in a fault tree.

The main limitation of the approach is that it only measures the software development process—not the end result of the process. It assumes there is a high correlation between the process and the products resulting from applying the process. However, this may not be the case. For example, defect density is a function of the defect control processes in the software development process, not the true number of defects in the software. Also, when this method was evaluated using 'real' software, the software had a much lower reliability than is required in a nuclear power plant. Thus it has yet to be shown that this method can scale to high-reliability requirements with a large system as stated in NUREG/CR-6848 [87]. The metrics chosen are based on the expert opinion that may change as new metrics are discovered. Finally, this method is applicable only to software systems, not digital I&C systems. Software reliability metrics provide no insight into hardware component reliability.

2.1.3.7 Black-Box Methodologies (Schneidewind Model)

Black-box models consider the software associated with a system or subsystem as one "black box," which is characterized by one overall failure rate (referred to a unit of execution time or execution cycle), regardless of which subfunction(s) the software may be executing. Schneidewind and Keller [53] discuss an application of such a reliability model for the space shuttle. The reliability model uses a non-homogeneous Poisson process [88] as the basis to predict the reliability of software components [77]. The Schneidewind model was chosen to be the reliability model for software components in the space shuttle based upon how well the software's failure data matched the generated data from the model. The application was fit to the model through a clever representation of the software changes to fulfill the requirements of the model.

Schneidewind and Keller [53] mention that a reliability methodology must have three elements to be successful: prediction, control, and assessment. Prediction is the ability of the methodology to predict future failures in some manner, as in failure rate, number of failures, time to next failure, etc. Control is the ability to use the model as a quality control measure, with the ability to determine if software meets the reliability goals required by the project. "Assessment is the activity of determining what action to take when software fails to meet goals" [53].

In the implementation of the Schneidewind model, one must represent the software that is being developed in such a way as to satisfy the assumptions of the model. For instance, the Schneidewind model assumes that the software system is changed only when there is an observable failure. This assumption may be accommodated by considering each revision of the software as a set of pieces of software, each of which is changed only when there is an error or if it is removed by another, more recent version. Advantages to this approach include a model that fits the software failure history of a particular application and a model/methodology that can provide prediction, control, and assessment for a successful reliability program.

An important limitation, however, is that software failure data are needed for quantification, and such data may not be available. Selecting a model appears to be an iterative process with the goal of identifying an appropriate software representation that meets the prediction, control, and assessment requirements of the approach. Any model that is fitted to a system using this method must also provide mechanisms to evaluate the results that the chosen model arrives at, including test case selection, test time and rework criteria [53, 77]. This model was not designed to be integrated into a PRA. Finally, this approach is only presented for software; it is unclear if the complete digital system could be fitted to the model as the space shuttle was.

2.1.3.8 Initial Conclusions

In this section we reviewed a variety of techniques that have been suggested to assess the 'reliability' of digital I&C systems. We also have identified potential advantages and limitations to each technique with respect to treating a digital system as a single system as well as integrating the resulting reliability model into a PRA. The goal was to evaluate possible methods to determine what properties an ideal model should have and to enumerate the possible limitations that could arise by using the possible techniques proposed. Due to the lack of a benchmark against which to compare these techniques, the review is based on case studies that have been presented in the literature and that have relevance to reactor protection and control systems. Since some techniques have more relevant applications than the others, the discussion of different methods may be uneven in breadth and depth.

It appears that all of these approaches have limitations that may preclude them from being used as the technique of choice without modification. The Markov model approach is able to integrate software's ability to mask hardware faults, but does not provide enough information to justify its usage of failure rates, repair rates and fault injection. Dynamic flowgraphs are able to predict future failures and are able to integrate hardware and software components easily. It is not clear in [22] that quantitative measures can be applied to this framework which may hinder its integration into a PRA. However, other applications of DFM indicate that quantification is possible if failure data are available [83].

The Bayesian updating approach is able to integrate changes in failure data to produce new values of the reliability measures, but is only used for software and is only useful as applied to software that was developed using a specific method. Petri net approaches are able to model digital systems well, but the size of the resulting model may affect its solvability in a reasonable amount of time. The testing and metrics approaches are able to integrate easily with a PRA, but are based on only testing the software component of the digital system or using metrics to evaluate the software component. While NUREG/CR-6848 [87] advocates using the metrics, it

has yet to be shown that the methodology could scale up to the large and distributed systems found in nuclear power plants. The Schneidewind model was useful for its applicability to the space shuttle but would require software failure data for nuclear power plants that is currently unavailable. Finally, even if the data were available, such data may not apply accurately to this particular model due to the model's assumptions about the development process of software.

Based on this analysis, it seems that there is no 'silver bullet' for assessing quantitatively the reliability of digital systems. It also noted that there was no common system that these methodologies were evaluated upon. Consequently, the information that can be gained from a survey such as this is limited to the applications reported in the literature. Each of the methods surveyed, however, did have unique points that may be suitable for specific applications.

2.2 Methodologies for the Reliability Modeling of Dynamic Processes

As indicated in Section 1.3, the static ET/FT methodology does not treat the time-dependent interactions between plant physical processes (e.g., heatup, pressurization) and triggered or stochastic logical events (e.g., valve openings, pump startups) during an accident that may lead to coupling between these events through the control system (i.e. Type I interaction). The lack of treatment of these dynamic interactions means that potentially significant dependencies between failures events may not be identified or properly quantified. The dynamic methodologies that can be used for the modeling of Type I interactions can be divided into three main categories: (i) continuous-time methods, (ii) discrete-time methods, and (iii) methods with visual interfaces. While the methods with visual interfaces are also either continuous or discrete time methods, the reason they are listed separately is because the availability of a visual interface is usually regarded as rendering them more user-friendly.

Continuous-time methods such as the continuous event tree (CET) approach [89] yield the probability of finding the system at a specified location in the system state-space at a specified time in a specified configuration. In CET, this probability is calculated from the solution of an integral equation whose inputs are the physical process model in a differential or integral form and transition rates between system hardware states. A discrete state-space version of CET is the continuous cell-to-cell-mapping (CCCM) method [90]. The CCCM defines the system states as consisting of hardware configurations and user specified intervals of the physical process variables. The probability evolution of system states is modeled using a continuous time Markovian representation. The state transition rates are obtained from the user provided system model and the Chapman-Kolmogorov equation.

Discrete-time methods include the following:

- DYLAM (Dynamical Logical Methodology) [91, 92], in essence, is a simulation driver able to generate branchings (scenarios) of system evolution at user specified time intervals and to coordinate the simulation of every branch. For each scenario, a time-dependent probability is evaluated. Any undesired consequence is identified from the generated scenarios and its probability is calculated by adding up the probabilities of contributing branches.

- DETAM (Dynamic Event Tree Analysis Method) [93], DDET (Dynamic Discrete Event Tree) method [94] and ADS (Accident Dynamic Simulator) [95] are three variants of DYLAM which can dynamically generate at each time step all the possible event trees. Branches with small probability are pruned based on some user input threshold to prevent the number of simulations to be performed from becoming unmanageable.
- Monte-Carlo (MC) simulation approach of [96, 97] uses discrete time sampling to investigate possible branchings in the system evolution due to component malfunction and follows the branches to calculate the probability/frequency of undesirable events. While the MC approach of [96, 97] can be also regarded as a dynamic event tree generation technique such as DYLAM, DETAM, DDET and ADS it differs from these methodologies in that the MC approach selects the branching times stochastically rather than using deterministic rules.
- DDET/MC hybrid simulation as described in [98] generates the branchings with a DDET engine and selects the branches to be followed by the MC approach.
- CCMT (Cell-to-Cell Mapping Technique) [99] is based on a discrete time version of CCCM and follows the probabilistic evolution of the system using a Markov chain.

Methods with visual interfaces include Petri nets [100, 84], dynamic flowgraphs [22], dynamic fault-trees [101, 102], the event-sequence diagram approach [103], and the GO-FLOW methodology [104, 105].

In a manner similar to fault-tree analysis, visual models based on Petri nets [84, 100] can be constructed to represent cause-and-effect relationships among events and yield minimal cut sets. Unlike fault-tree analysis, a Petri net model allows explicit representation of the time element in the system evolution with the use of a dynamic system model and subsequently is capable of simulation of concurrent and dynamic activities and time-delays.

The dynamic flowgraph methodology (DFM) [22] is a digraph-based technique. A process variable is represented by a node discretized into a finite number of states. The system dynamics is represented by a cause-and-effect relationship between these states. Instead of minimal cut sets, the DFM yields the prime implicants for the system. A prime implicant is any monomial (conjunction of primary events) that is sufficient to cause the top event, but does not contain any shorter conjunction of the same events that is sufficient to cause the top event.

Dynamic fault-trees use timed house events [102] or functional dependency gates [101] to represent the time varying dependencies between basic events. Such dependencies may arise because of hardware coupling through system dynamics [11, 12] (particularly in control systems), configuration changes [102] (e.g., due to maintenance) or digital control [101]. Quantification of dynamic fault-trees is performed using time dependent Boolean logic [102] or Markov models [101].

The event-sequence diagram (ESD) approach [103] uses 6-tuple of events (e.g., initiating, pivotal, delay), conditions (e.g., limiting time, competition, switch), gates (multiple input AND/OR, multiple output AND/OR), process parameter set, constraint and dependency rules to represent the probabilistic system evolution. The events represent transitions between system states. The probabilistic approach is an extension of the CET [89] approach and is based upon the Chapman-Kolmogorov equation. The output is the probability of being in a given system state as a function of time. Both cyclic and acyclic scenarios can be identified and quantified.

The GO-FLOW methodology [104, 105] is a success-oriented system analysis technique, capable of evaluating system reliability and availability. The modeling technique produces the GO-FLOW chart, which consists of signal lines and operators. The operators model function or failure of the physical equipment, a logical gate, and a signal generator. Signals represent some physical quantity or information. The analysis is performed from the upstream to the downstream signal lines, and is completed when the intensities of the final signals at all time points are obtained. GO-FLOW output includes time dependent system reliability/availability, cut sets, common cause failure analysis and, uncertainty analysis. It has been demonstrated that GO-FLOW is also capable of modeling detailed system dynamics with competing events, at least on a simple level control system [104].

Subject to given failure data and deterministic system model accuracy, the techniques that allow the most accurate and comprehensive modeling of the probabilistic system dynamics are the ones based on the Chapman-Kolmogorov equation including CET, CCCM, CCMT, and ESD approaches. Cases have been reported in the literature where accurate modeling of probabilistic system dynamics may be important for the correct quantification of competing Top Event frequencies [11, 106], particularly if there is uncertainty in the model parameters [107]. The main challenge with these techniques is computational complexity, both in model construction and implementation. Another challenge is compatibility with existing PRA structures. No system independent algorithms have been proposed to date that can generate either scenarios or minimal cut sets with these techniques.

Dynamic event-tree generation techniques are more compatible with the existing PRA structure, since the main difference between these techniques and the conventional event tree approach is that dynamic event-tree generation uses quantitative system behavior information (e.g. setpoint crossings) rather than qualitative (e.g. sequencing of system responses) for the branchings. In addition, dynamic event-tree techniques are able to generate possible scenarios of system evolution almost exhaustively. The main disadvantage is that the number of branches increases exponentially in time. Since the computational requirement of these methods is proportional to branch density, the computational demand quickly becomes prohibitive, so the methods are usually restricted to problems with small event horizons. An alternative is MC simulation, which can be faster depending on what is regarded as acceptable uncertainty on the results. The drawback is that a large number of histories may be required if the acceptable uncertainty is small. The DDET/MC hybrid approach [98] tries to combine the advantages of DDET and MC methodologies in order to reduce the disadvantages of these two methods. Still, the calculation is burdensome and the process slow. Another alternative is the Integrated Safety Assessment (ISA) method [108] which only branches every time a setpoint for system intervention is exceeded. The computational demand of ISA is less than the other

dynamic event-tree generation methods indicated above since the number of branchings is fewer.

Most of the methods with visual interfaces can be regarded as semi-dynamic, because they represent system dynamics qualitatively (e.g., dynamic fault trees, GO-FLOW) or in a coarse partitioning of the system state space (i.e. in terms of large, small or medium changes in controlled process variable such as with the dynamic flowgraph methodology). All of these methods have similar capabilities regarding process dynamics, representing it in a semi-quantitative fashion, and are capable of scenario and cut set outputs. However, cut sets may change with system evolution in time. Petri nets can be converted to fault trees [70, 109]. Again, fault-tree structure may change in time.

2.3 The Evolutionary Development of the Regulatory Framework for I&C Systems in Nuclear Power Generating Stations with Emphasis on Digital I&C Systems

2.3.1 Introduction

The objective of this section is to review the deterministic requirements associated with digital I&C systems used in nuclear power plants in the United States. It is important when modeling a systems in a PRA that the most important features of that system are included in the model. One way to assess what features that are of importance is to review the deterministic requirements associated with that system. This section will provide an historical perspective of the evolutionary development of the current regulatory framework for I&C systems in nuclear power plants and will identify and discuss the key regulations, standards and guidelines, which affect the incorporation of software-based digital I&C system into nuclear power plant PRAs.

Section 2.3.2 of this report, provides the historical perspective and overview, begining with IEEE Std 279-1971 [110], which is the basis or departure point for a majority of the regulatory guides and standards that comprise the current regulatory framework. Section 2.3.3 provides an evaluation of two NRC regulatory guides that endorse two key standards, selected regulations and an EPRI guideline.

2.3.2 Historical Perspective

IEEE Std 279-1971 (or briefly IEEE 279), AEC (Later NRC),"Criteria for Protection Systems for Nuclear Power Generating Stations"[110], describes criteria for Class IE I&C Systems (Safety-Related) in nuclear power plants. The following is a partial list of issues addressed in IEEE Std 279 [110]. The numbering scheme used is taken from IEEE Std 279:

4.1 General Functional Requirements

4.2 Single failure criterion: "Any single failure within the protection system shall not prevent proper protective action at the system level when required"

4.3 Quality of Components and Modules

4.4 Equipment Qualification

4.6 Channel Integrity

4.7 Channel Independence
4.8 Control and Protection System Interaction
4.9 Capability for Sensor Checks
4.10 Capability for Test and Calibration
4.11-4.14. Considers bypass requirements
4.15 Multiple Set Points
4.16 Completion of Protective Action
4.17 Manual Initiation
4.19 Access to Set Point Adjustments, Calibration and Test Points
4.20 Information Read-Out

As can be observed, IEEE Std 279 includes criteria that remain relevant today such as single failure criterion, isolation between safety and control systems and channel independence. IEEE Std 279 is very significant since it was the first industrial standard that addressed the requirements for safety related systems in nuclear power plants. It was prepared by many of the researchers, engineers and regulatory personnel who were instrumental in the design and approval (by the AEC) of the original I&C systems in the first operating nuclear power plants in the USA and consequently it reflects their collective experience and wisdom. Finally, the I&C systems in the majority of the current operating plants are licensed on the basis of IEEE Std 279. IEEE Std 279 is also the only industrial standard incorporated into the Code of Federal Regulations, 10CFR50.55a(h).

Standards and Guidelines Developed to Clarify Requirements in IEEE Std 279. A number of industrial standards were developed from 1971-1980 to clarify and expand on the requirements delineated in IEEE Std 279 and to address issues that were not considered in IEEE Std 279. All of these standards have undergone one or more revisions since their initial issue. IEEE Std 279, however, remains as it was originally approved. IEEE Std 603 –1980, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations" [111], is effectively an update and expansion of IEEE Std 279-1971. It has been revised several times and in 1995 IEEE Std 603 –1991 was endorsed by Regulatory Guide (RG) 1.153 [112].

IEEE Std 323 [42] and IEEE Std 344 [43] expand and clarify section 4.4 of IEEE Std 279 and respectively describe environmental (temperature, pressure and radiation) and seismic conditions in which Class 1E Systems must perform. IEEE Std 338, "Standard Criteria for Periodic Surveillance Testing In Nuclear Power Generating Station Safety Systems" [85], which has been endorsed by RG 1.118[86], provides detailed guidance for implementation of Sections 4.9, 4.10 and parts of 4.19 and 4.20 in IEEE Std 279 and IEEE Std 379, "*Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System*" [113], which has been endorsed by RG 1.53, expands and clarifies the single failure criteria in section 4.2 in IEEE Std 279.

ISA S67.04 [114], which has been endorsed by RG 1.105 [115], describes a method for establishing instrument set points for Class 1E Systems and also provides expanded guidance

for implementing sections 4.15 and 4.19 in IEEE Std 279. ISA S67.06 [29] describes response time requirements and acceptable measurement methods for Class IE instrument channels. This standard has evolved into a general performance monitoring guideline for Class IE instrument channels. However, ISA 67.06 has not been evaluated or endorsed by the NRC as of the writing of this report. In 1975 a fire at the Brown's Ferry nuclear power plant compromised the ability of some Class 1E Systems to provide their safety function due to burned signal cables, which resulted in common mode failures. This event identified the need for further expansion and guidance for implementation of Section 4.7 in IEEE Std 279. IEEE Std 384 [116], which provides criteria for electrical and physical independence and separation of class IE equipment and circuits, addresses issues related to Brown's Ferry nuclear power plant and is endorsed by RG 1.75, Revision 1.

Following the accident at Three Mile Island in 1979 the NRC developed Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plant to Assess Plant and Environmental Conditions During and Following an Accident" [117]. IEEE and ANS have developed a standard, IEEE Std 497, "Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations", which is consistent with RG 1.97.

Soon after nuclear power plants became operational, it became obvious that a mechanism to expedite approval of minor non safety significant changes in plant equipment would be necessary. This led to a new section the CFR, 10CFR50.59 [118], which permits change if it can be shown it does change the licensing basis or does not require modification of the technical specifications. At the time of this change in the Code of Federal Regulations (CFR) a subsidiary of EPRI published NSAC 125, a guideline for the plants on how to implement what were soon to become referred to as "50.59" changes. In the typical operation of a nuclear power plant several hundred 50.59 changes may be made on an annual basis. Although the NRC audits these changes on a periodic basis, the plant typically has a rigorous procedure, which has been approved by the NRC, for approval of 50.59 changes.

In 1992 the NRC denied a requested digital upgrade of a reactor protection system in a nuclear power plant, which effectively required that all digital upgrades be reviewed by the NRC headquarters staff, and consequently disallowed them for a 50.59 change. The nuclear plant operators viewed this action, if left unchanged, as a termination of digital upgrades. They charged EPRI with the development of a guideline that would provide guidance for implementing digital upgrades using the 50.59 process. EPRI began by modifying the process in NSAC 125 to fit the requirements for a digital upgrade. They organized a committee that represented the I&C engineers at the plants and following numerous meetings and reviews, consensus approval was acquired and in 1993 EPRI published EPRI TR-102348, "Guideline on Licensing of Digital Upgrades Using the 10CFR50.59 Process" [114]. In May of 1995 NRC in their Generic Letter 95-02 endorsed EPRI 102348 -1995. In 2001 the Guideline was revised to reflect changes in the10CFR50.59 process and it was published as EPRI TR-102348 Revision 1 (NEI 01-01) [119].

The guideline on licensing of digital I&C upgrades describes an acceptable procedure for how digital I&C and the associated licensing issues can be addressed in the modification and design process and in 10 CFR 50.59 evaluations. It also provides high-level guidance on dealing with

the issue of digital common cause failures (CCF), specifically through defense-in-depth and diversity (D3) evaluation and the use of risk insights in performing D3 evaluations.

2.3.3 Regulatory Guides, Standards and Guidelines Most Relevant to Incorporation of Digital I&C Systems in Plant PRAs

The two standards, which are most relevant to incorporation of digital I&C systems into nuclear power plant PRAs, are IEEE Std 603-1998 [47] and IEEE Std 7-4.3.2-2003 [48]. NRC Regulatory Guides 1.153 [30] and 1.152 [49] have endorsed earlier versions of these two standards, respectively. These two Regulatory Guides plus Chapter 7 of the Standard Review Plan (NUREG-0800) [50] provide the most relevant guidance on the design and licensing of digital I&C systems in nuclear power plants. Consequently, any proposed methodology for incorporating digital I&C systems into plant PRAs must adhere to this regulatory framework.

RG 1.153 (IEEE Std 603-1996). "Standard Criteria for Safety Systems in Nuclear Generating Stations". IEEE Std 603 in most ways is an update and expansion of IEEE Std 279. A significant addition is provision for digital I&C systems. Although IEEE Std 603 is similar to IEEE Std 279, the I&C systems in the majority of the current operating plants are unable to meet all the provisions in IEEE Std 603, therefore, their licensing basis remains with IEEE Std 279.

In order to obtain a valid NRC perspective of this Regulatory Guide, selected sections relevant to the objectives of this report have been taken verbatim from the Discussion and Regulatory Position of RG 1.153 [30].

Discussion

IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," was prepared by the Safety Systems Working Group SC 6.3 of the IEEE Nuclear Power Engineering Committee, and it was approved by the IEEE Standards Board on June 27, 1991. IEEE Std 603-1991 establishes minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power plants.

Section 1.2 of IEEE Std 603-1991 references IEEE/ANS Std 7.4.3.2-1982. Revision 1 to Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses the 1993 version, IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Thus, Revision 1 to Regulatory Guide 1.152 constitutes an acceptable method of meeting the regulatory requirements for digital computers.

It should be noted that Section 5.8.1 of IEEE Std 603-1991 references IEEE Std 497-1981, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." In this area, Revision 3 of Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident," provides an acceptable method to meet the regulations for accident monitoring instrumentation.

Regulatory Position

Conformance with the requirements of IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" (including the correction sheet dated January 30, 1995), provides a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants.

Section 3 of IEEE Std 603-1991 references several industry codes and standards. If a referenced standard has been incorporated separately into the Commission's regulations, licensees and applicants must comply with that standard as set forth in the regulation. If the referenced standard has been endorsed in a regulatory guide, the standard constitutes a method acceptable to the NRC staff of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the Commission's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard if appropriately justified, consistent with current regulatory practice.

IEEE Std 603-1998. This standard is a revision of IEEE Std 603-1991 and will likely be endorsed by the next revision of RG 1.153. Consequently we will use IEEE Std 603-1998 as a basis for discussion of the interaction among the following issues, regulatory guides and standards for digital systems, RG 1.152, IEEE Std 352, 577 and 7-4.3.2.

Section 5.1 Single Failure Criteria cites IEEE Std 7-4.3.2, and IEEE Std 352 and 577, respectively in discussion of common cause failure and reliability analysis. This section also states that "a probabilistic assessment is intended to be used to eliminate consideration of events and failures that are not credible, however, it shall not be used in lieu of the single failure criterion."

Section 5.3, Quality. Guidance on the quality assurance program required for safety system equipment employing digital computers and programs or firmware in nuclear power plants is found in IEEE Std 7-4.3.2.

Section 5.4, Qualification. "Qualification of class IE equipment shall be done in accordance with the requirements of IEEE Std 323-1983 and 627-1980. Guidance on the qualification of safety system equipment employing digital computers and programs or firmware in nuclear power plants is found in IEEE Std 7-4.3.2".

Section 5.5, System Integrity. "The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Guidance on meeting this criterion for safety system equipment employing digital computers and programs or firmware in nuclear power plants is found in IEEE Std 7-4.3.2."

Section 5.6, Independence, 5.6.4, Detailed Criteria. "IEEE Std 384 provides detailed criteria for the independence of class 1E equipment and circuits. IEEE Std 7-4.3.2 provides guidance on

the application of this criteria for the separation and isolation of data processing functions of interconnected computers."

Section 5.15, Reliability. Guidance on performance of reliability analysis is found in IEEE Std 352 and IEEE Std 577. Guidance on the reliability of safety system equipment employing digital computers and programs or firmware in nuclear power plants is found in IEEE Std 7-4.3.2.

Section 5.16, Common Cause Failure Criteria. Plant parameters shall be maintained within acceptable limits as established for each design basis event in the presence of a single common cause failure (See IEEE 384). IEEE Std 7-4.3.2 provides guidance on performing an engineering evaluation of software common cause failures.

RG 1.152 (IEEE Std 7.4.3.2-1993), "Standard Criteria for Digital Computers in Nuclear Generating Stations". This RG and standard expands on and clarifies issues related to digital systems in RG 1.153 and IEEE Std 603. When digital systems are considered the two standards must be considered simultaneously.

In order to obtain a valid NRC perspective of this Regulatory Guide the Discussion and Regulatory Position sections have been taken verbatim from RG 1.152[49].

Discussion

Instrumentation and Control (I&C) systems that use digital computers in safety systems make extensive use of advanced technology, i.e., equipment and design practices that are expected to be significantly and functionally different from current designs. These designs include, but are not limited to, the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve the needed independence and redundancy.

IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," was jointly prepared by the Nuclear Power Engineering Committee of the Institute of Electrical and Electronics Engineers (IEEE) and the Nuclear Power Plant Standards Committee of the American Nuclear Society (ANS). The NRC staff has worked with IEEE and ANS in developing IEEE Std 7-4.3.2-1993 to ensure that the guidance provided by the consensus standard is consistent with the Commission's regulations. IEEE Std 7-4.3.2-1993 has evolved from ANSI/IEEE-ANS-Std 7-4.3.2-1982, "Applications Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." IEEE Std 7-4.3.2-1993 is a significant improvement over its 1982 version. The IEEE Standards Board approved the 1993 version on September 15, 1993. This standard identifies guidelines for digital computers (including hardware, software, firmware, and interfaces) to supplement IEEE Std 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The NRC staff recognizes that development processes for computer systems continue to evolve.

Digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the bases for many of the advantages of digital systems, it also raises a key concern with respect to its vulnerability to a different type of failure. The concern is that a design using shared data bases and process equipment has the potential to propagate a common cause failure of redundant equipment. Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against propagation of common cause failures within and between functions.

The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors will not result in an undue threat to public safety. A detailed defense-in-depth study and failure mode and effect analysis or an analysis of abnormal conditions or events should be made to address common cause failures. The Commission's position for providing defense against common cause failures in digital I&C systems for future light-water reactors is given in the Staff Requirements Memorandum of July 21, 1993, on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" (specifically in point 18: II Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems").

Section 5.15, "Reliability," of IEEE Std 7-4.3.2-1993 states, "When qualitative or quantitative reliability goals are required, the proof of meeting the goals shall include software used with the hardware." The staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the Commission's regulations for reliability of the digital computers used in safety systems. The NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals.

Software failures that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability. The NRC staff believes that quantitative reliability determination, using a combination of analysis, testing, and operating experience, provides information regarding the safety importance of the computer system and also provides an added level of confidence in its reliable performance. If quantitative software reliability goals are used, the staff believes that the amount of testing of the safety system instrumentation and control equipment will increase. The staff recognizes that the commercial dedication of "commercially" available digital systems in nuclear applications relies a great deal on quantitative methods because of the operating experience data (such as number of hours of successful operation) accumulated over the years. The staff does not intend to preclude operating experience data from the justification of a successful commercial dedication.

Section 6, "Sense and Command Features--Functional and Design Requirements," of IEEE Std 7-4.3.2-1993 indicates that no requirements beyond IEEE STD 603-1991 are necessary. IEEE Std 603-1991 specifies the need to ensure acceptable response time for the instrumentation and control system in order to accomplish necessary safety functions. Consideration of the

sampling rate of plant variables is an important aspect of the design of a digital system when satisfying this criterion.

IEEE Std 7-4.3.2-1993 includes eight annexes. This standard states that these informative annexes are not part of IEEE 7-4.3.2-1993. The NRC staff believes these annexes contain information that may be useful. However, the information in these annexes should not be viewed as the only possible solution or method. Since a consensus has not been reached in the nuclear industry, the NRC staff does not endorse these annexes.

Regulatory Position

Conformance with the requirements of IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with the exception of relying solely on quantitative reliability goals (Section 5.15), is acceptable to the NRC staff for satisfying the Commission's regulations with respect to high functional reliability and design quality requirements for computers used as components of a safety system.

IEEE Std 7-4.3.2-1993 references several industry codes and standards. If a referenced standard has been separately incorporated into the Commission's regulations, licensees and applicants must comply with the standard as set forth in the regulation. If the referenced standard has been endorsed by the NRC staff in a regulatory guide, the standard constitutes an acceptable method of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the Commission's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard if appropriately justified, consistent with current regulatory practice.

IEEE *Std* 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[48] This standard specifies additional computer specific requirements to the criteria and requirements in IEEE Std 603-1998 [47]. The criteria contained in this standard when used in conjunction with the criteria and requirements in IEEE Std 603 establish the minimum functional and design requirements for computers used in components in safety systems in nuclear power generating stations. It is expected that the next revision of RG-152 will endorse IEEE Std 7-4.3.2-2003.

Although the annexes are considered informational only, they do provide very useful information. Annex A of IEEE Std 7-4.3.2-2003 is a map between IEEE Std 7-4.3.2-2003 and IEEE Std 603-1998. Consequently, in consideration of the objectives of this report, Table 2 below reproduces Table A.1 of Annex A and is an excellent place to begin a discussion of IEEE Std 7-4.3.2, It also identifies documents that may be useful to this project.

***Upgrade of Chapter 7 (I&C) of the Standard Review Plan (NUREG 0800)*-1997 [50].** The primary objective of the upgrade was to incorporate review guidance for digital systems used in safety-related and non safety-related systems in I&C in nuclear power plants. The primary new guidance relevant to digital upgrades is found in the following Branch Technical Positions (BTP):

- BTP 14, "Guidance on Software Reviews for Digital Computer-Based I&C Systems" [120] Describes the NRC position on an acceptable development method and specifies acceptance criteria for safety critical software. The methodology is prescriptive in terms of the development process and acceptance criteria. The acceptable development process focuses on high quality development and the acceptance criteria focus on testing to meet the design requirements of individual subsystems. The method is weighted toward production and does not necessarily require testing for all expected operational conditions.
- BTP 18, " Guidance on the Use of Programmable Logical Controllers in Digital Computer-Based I&C Systems" [121].
- BTP 19 "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems" [122] Describes the NRC position on D3, describes an acceptable method for performing D3 evaluations and specifies acceptance criteria.
- BTP 21, "Guidance on Digital Computer Real-Time Performance" [123].

***EPRI TR1002835** "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades Applying Risk-Informed and Deterministic Methods" [124], September 2004.* This guideline is intended to be an alternative approach to BTP 19. It recommends an integration of deterministic methods such as prescribed in BTP 19 and risk informed methods, which use the plant PRA to determine the potential risk of a change in the licensing basis posed by a proposed digital upgrade and RG 1.174 for acceptance criteria of the change. This guideline has not been endorsed by NRC.

Table 2: Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003[48]

IEEE Std 603-1998 Criteria	**IEEE Std 7-4.3.2-2003 Additional requirements**	**Annex for Guidance**
4. Safety System Design Basis	4. Safety System Design Basis	Annex B
5. Safety System Criteria	None	Annex B
5.1 Single Failure Criterion	None	
5.2Completion of protection action	None	
5.3 Quality	Software development (See 5.3.1) Software tools (See 5.3.2) Verification and validation (V&V) (See 5.3.3) Independent Verification and validation (IV&V) (See 5.3.4) Software Configuration management (See 5.3.5) Software project risk management (See 5.3.6)	Annex D and F
5.4 Equipment qualification	Testing software and diagnostics (See 5.4.1) Qualification of existing compilers (See 5.4.2)	Annex C
5.5 System integrity	Design for computer integrity (See 5.5.1)	Annex B and C

	Design for test and calibration (See 5.5.2) Fault detection and self-diagnostics (See 5.5.3)	
5.6 Independence	Independence (See 5.6)	Annex E
5.7 Capability for test and Calibration	None	
5.8 Information Displays	None	
5.9 Control of access	None	
5.10 Repair	None	
5.11 Identification	Identification (See 5.11)	
5.12 Auxiliary features		
5.13 Multi-unit stations	None	
5.14 Human factor considerations	None	
5.15 Reliability	Reliability (See 5.15)	Annex F
6. Sense and command features-Functional design requirements	None	
7. Execute feature-Functional design requirements	None	
8. Power source requirements	None	

RG 1.174, "*An Approach for Using Probabilistic Risk Assessment in Risk-Inform Decisions on Plant-Specific Changes to the Licensing Basis*" [125]. This is not a Regulatory Guide specifically for I&C but a regulatory guide for any change in the plant licensing basis, therefore, it can be and often has been applied to accessing the risk that a proposed change in the I&C system will introduce and the acceptability of that change in risk. The guidance provided in EPRI TR1002835 makes use of the approach and criteria described in RG 1.174 to support application of risk insights when performing D3 evaluations and the acceptability of any proposed changes.

NUREG/CR-6303 [126], This NRC contractor report describes the method for performing D3 evaluations that is referenced in BTP-19. It also includes guidance for determining whether there is sufficient diversity between different portions of an I&C system such that they would not be subject to the same digital CCF. This report presents an approach that addresses digital design features, which impact the potential for CCF, and incorporates the use of risk-informed insights

2.3.4 Conclusions

Sections 2.3.1-2.3.3 of this report presented a description of the evolutionary development of the current regulatory framework for safety-related I&C systems in nuclear power plants. It emphasized those regulatory guides and industrial guidelines that address software based digital I&C system used in safety-related components and systems, which can impact safety systems. For a model of a digital I&C system to be used in a risk-informed application it needs to be developed to a sufficiently low level that it includes the details of how the system is meeting the regulatory guidance outlined here. As part of the guidance provided in RG 1.174, a system must continue to meet current regulatory requirements. A model of a digital system should be at sufficiently low level to include the design details associated with how the systems is meeting the independence requirement of IEEE std 603, for example. If the model is not at

this level of detail it would not be possible to ensure that the most important, from a regulatory view point, system features are correctly modeled.

3. DISCUSSION OF MINIMUM REQUIREMENTS A DIGITAL SYSTEM MODEL MUST MEET

Based on the material presented in Sections 1 and 2, the digital I&C systems differ from their analog counterparts in the following respects:

1. The firmware and software components of digital I&C system do not demonstrate any wear characteristics in the conventional sense. Consequently, these elements of digital systems do not respond to accelerated life testing, stress testing, etc.
2. The firmware/software reliability cannot be accurately modeled using a bathtub curve approach [38].
3. Digital I&C systems operate in discrete time steps, while analog systems operate in continuous time.
4. There may be complex interactions between the components of the digital I&C system and between the digital I&C system and process physics which may lead to potentially significant dependencies between failures events [8].
5. The failure modes of digital I&C system are not well defined [40].
6. Digital I&C systems may have a much smaller operating environment temperature range than analog counterparts. Also, digital systems may be affected differently than analog systems by external stressors such as electromagnetic/radio frequency interference, temperature, pressure, vibration and radiation. Consequently, they must be qualified to operate in all expected condition as specified by IEEE Std 323 [42], IEEE Std 344 [43] and NRC Regulatory Guide 1.180 [127].
7. Software may be able to mask intermittent failures in hardware. For example, a protocol for Ethernet is able to coordinate collision of packets transmitted when more than one node on the network attempts to transmit [33]. Similarly, error detection and correction codes and methods may be able to mask hardware failures due to "stuck" bits, corrupted data transmission, etc.
8. Digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to their vulnerability to common cause failure (CCF).
9. It is possible for digital I&C systems to introduce new failure modes.
10. Software is not a physical entity and testing alone is not sufficient to verify that software is complete and correct [39].
11. Software defects may remain hidden for long periods after a product has been in general use and failures may occur without any advance warning when a particular execution path is exercised [39].
12. Digital systems use binary approximation of real numbers. The approximations and subsequent math operations on the represented values may introduce significant round-off or truncation errors on the resulting values. Analog systems employ continuously varying voltages to represent real numbers and no such truncation and round-off errors are introduced.

Regarding Items 6 and 8, RG 1.152 (IEEE Std 7-4.3.2) Section 5.16, Common Cause Failure Criteria states that plant parameters shall be maintained within acceptable limits as established for each design basis event in the presence of a single CCF. IEEE Std 7-4.3.2 provides guidance on performing an evaluation of software CCFs [48,49].

Particularly due to Items 1, 2, 7, 10 and 11 above, reliability treatment of digital systems tends to include firmware and software as a largely invisible element of the hardware that encapsulates it. Items 3, 4, 6, 7, and 9 may require the use of dynamic modeling techniques.

3.1 Discussion of Requirements Identified for Digital I&C System Models and Their Successful Integration into Existing PRAs

Sections 1 and 2 of this report provide some general requirements for the reliability modeling of digital I&C systems and its incorporation into existing PRAs. Sections 3.1.1 and 3.1.2 discuss, respectively, the requirements that relate to the correct representation of the stochastic digital I&C system behavior and integration of the stochastic digital I&C system model into existing PRA studies.

3.1.1 Discussion of Requirements for the Digital System Model

1. *The model must be able to predict future failures as well as failures encountered in the past:* The model cannot be purely based on previous experience and must have capability to recognize and account for situations not encountered in the past. For example, response surfaces which are "black-box" models to describe the deterministic system response to inputs, and neural nets, which are a special form of response surfaces are often used as surrogate system models in situations where the physical phenomena governing the system evolution are not well known or to reduce computational time if the system model is complex. However, a response surface or a neural net digital I&C system model trained only with operational experience may not be able to predict the consequences of event sequences that were not part of the training data. Similarly, failure data based on operational experience may not be able to account for the aging of the digital I&C system hardware and inputs into the system that fall outside the design domain of the digital I&C system.
2. *The modeling must account for relevant features of the system under consideration:* Due to the different types of digital I&C systems used in nuclear power plants, the modeling requirements can change substantially. If the digital I&C system is used strictly for data collection with no processing of data or decision making, then the ET/FT approach can often be satisfactory. However, data collection from sensors may require analog to digital conversion. Such conversion may introduce errors or artifacts. These errors and artifact may occur if the sampling rate is not sufficiently high [41] or through the failure to use proper anti-aliasing techniques. Also, sampling rate, algorithm selection, and processor speed must be selected and matched carefully to ensure that the response time performance requirements are met. Subsequently, explicit representation of the time element may be important in the digital I&C system model even if the system is used strictly for data collection with no processing of data or decision making. If sequence dependent failure modes exist, a state-based technique (such as Markov) models may need to be used. Extensive interaction of the digital I&C system with process physics may require more complicated modeling procedures (such

as CET [89] or CCMT [99]). It has been experimentally shown that [128] techniques based on digraphs (such as DFM [22]) are effective for proportional controllers but not necessarily for proportional-integral or proportional-integral-derivative controllers. Using a simple level controller, [11] shows that the time and process variable magnitude discretization used in the reliability model construction can change the probability of failure in different models substantially.

3. *The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified:* The conventional ET/ FT approach assumes that faults occurring in system components propagate instantaneously throughout the system. There is evidence that such an assumption leads to overestimation of Top Event frequencies in control systems with more than one failure mode [18, 19]. There is also evidence that the assumption (along with qualitative representation of the process physics in the ET/FT approach) may lead to incomplete identification of the scenarios leading to the Top Event [93, 19] and incorrect quantification of the statistical importance of component failures with respect to the Top Event [17].

4. *The model must be able to quantitatively represent dependencies between failure events accurately, including common cause failures and those arising due to interaction of the digital I&C system with process physics:* Dependencies between failure events may arise due to complex hardware-software-process interactions that may be present in the digital I&C system. For example, there may be complex interaction between the components of a digital I&C system which may propagate to the process physics. In the level controller example of Section 2.1.1.3.3, the inlet and drain systems are tightly-coupled through the supervisory controller whose behavior is affected by the water level in the reservoir and whose malfunction in turn may affect the behavior of the water level in the reservoir. If setpoints are determined by software, software errors can directly affect the process physics. Hardware failure data may be a function of pressures and temperatures of the physical process that is being controlled. In fact, such hardware-software-process interdependencies may be so strong that a change in the physical parameters can strongly affect the overall system failure characteristics. For example, [18] shows that not only the direction of a level setpoint drift but also the magnitude of the setpoint drift can affect the predicted probability of system overflow in a level-control system (also See Section 1.3.2). Again, [18] shows that a change in the outflow rate may also strongly affect the overflow probability in the same system. Using the feed-bleed cooling of the reactor core following a small-break loss of coolant accident (SBLOCA) in a BWR/6, [17] shows that exact magnitude and direction of change of the physical process variables at the time of hardware failure can affect whether system failure occurs by reactor vessel overpressure or core uncovery (also see Section 1.3.1). Using the same system, [107] shows that: a) there is a threshold for the SBLOCA size beyond which the demand rates for some plant safety systems changes by one order of magnitude, and, b) such effects cannot be accounted for by failure modeling techniques that use static or qualitative plant models (e.g., ET/FT and DFM, respectively).

5. *The model must be designed so it is not hard for an analyst to learn the concepts and not hard to implement:* While methodologies such as CET [89] and CCMT [99] satisfy Requirements 1 through 4 above, it is very difficult (if not impossible) to obtain the necessary input data for these methodologies from an existing ET/FT, such as exact magnitude of process variables at coupling points and exact timing of events. Similar arguments can be made for the Monte Carlo methodology. Dynamic methodologies are

also mathematically very complex, in general, have steep learning curves and are often computationally very challenging. The dynamic event tree generation techniques such as DYLAM [91, 92], DETAM [93], DDET [94] and ADS [95] yield minimal cut sets, are relatively easy to learn but may not be easy to implement if branching probabilities are statistically dependent. Tools such as SAPHIRE (Section 3.1.2) can account for statistically dependent branching probabilities if cut sets leading to these probabilities are provided. Methods with visual interfaces may offer feasible options if highly mechanized for model construction (such as GO-FLOW [104, 105]). However, among these methods, only DFM has been implemented for digital I&C system reliability modeling [22].

6. *The data used in the quantification process must be credible to a significant portion of the technical community:* There is little operational experience with digital I&C system and field data. Subsequently, most of the data to be used in the reliability modeling of digital I&C systems need to be generated or estimated from generic digital processor data. As described in Section 2.1.3 techniques have been proposed to accomplish this need. However, as also indicated in Section 2.1.3, data generation may take an unreasonable amount of time to create, run, and justify its correctness, and test cases might not be representative of real work loads. If software is treated as a separate entity, the validity of the software failure data estimated may be debatable. Finally, if failure data obtained as probability of failure upon demand need to be converted to failure rates for implementation in the model (e.g., in a continuous time Markov model), the conversion process may lead to overestimation of system reliability [107, 129].

3.1.2 Discussion of Requirements for the Procedure to Incorporate the Model into the PRA

The SAPHIRE code [130, 131] is used as an example to determine the requirements for the procedure to incorporate the digital I&C system model into the PRA. SAPHIRE is a PRA software tool developed by Idaho National Laboratory. SAPHIRE utilizes fault trees and event trees to generate and quantify cut sets. In addition, SAPHIRE can perform importance analysis, uncertainty analysis using either Monte Carlo or Latin Hypercube sampling techniques, and can calculate the sensitivity of the system due to changes in basic event frequencies.

To integrate a digital I&C system model into SAPHIRE, it is essential to understand its role in the larger system, so the system may be accurately modeled and failures may be traced through the fault trees and event trees. In other words, when an analog system is updated to include digital subsystems, it is necessary to know how a digital I&C system affects and is affected by the other subsystems, so that the system fault trees and event trees may be changed accordingly to accommodate the new subsystem. Additionally, it is necessary to know whether the new digital I&C system replaces older analog systems (which requires the analog systems to be removed from the existing ET/FT), or is incorporated to work alongside the older systems which may require augmentation of the ET/FT to accommodate the possible new failures attributable to the digital I&C system. When the new system is described, certain fault trees may have additional events added to account for the new digital I&C system, while other events may be removed if the digital I&C system completely replaces them. Furthermore, there may be changes to the fault tree logic. For example, if the digital I&C system and certain analog systems perform the same or similar functions, new logic gates would be added to the fault trees to represent this redundancy. Subsystems of a large digital I&C system may be

interacting with different components of the nuclear power plant which would then require the system to be broken down by subsystems for the incorporation of its failure model into the PRA. The changes in the PRA can be accomplished either by modifying the existing ET/FT or by replacing/appending the minimal cut sets. In either case, basic event data for the new/changed failure modes will need to be provided.

Another key element to successfully modeling systems incorporating digital I&C system is whether or not the system has any dependencies on outside systems, or failure modes common to systems outside the system boundaries, and what these dependencies may be. It may be possible for a digital I&C system to fail under conditions that would not have caused the failure of previous analog systems. For such a case an entirely new fault-tree and/or event tree (for sequence dependent failures) may need to be generated to analyze this new failure mode. For example, if the digital I&C system fails one safety check, one branch point in the relevant event tree may be affected. If the system fails multiple checks, more than one branching point may be affected. Similarly, an intermittent failure may affect one or few branch points. A function failure may need to be modeled as a common cause failure.

An important consideration in the integration of a digital I&C system model into SAPHIRE will be describing the basic event occurrence data. However, since SAPHIRE can handle several different types of failure distributions, there is some flexibility allowing for a more accurate model to be used in each component.

Using SAPHIRE as the example PRA tool, the requirements to incorporate the digital I&C system model into the PRA can be summarized as follows:

1. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
2. The model must be able to differentiate between faults that cause function failures and intermittent failures.
3. The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
4. The methodology must be able to model the digital I&C system portions of accident scenarios to such a level of detail and completeness that the non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed.
5. The model should not require highly time-dependent or continuous plant state information.

Since most existing PRA do not contain time dependent system information, Requirements 4 and 5 are particularly important to incorporate the results of dynamic methodologies into an existing PRA. An implicit assumption in Requirement 3 is that obtaining the relevant information will not require excessive effort on the part of the user. For example, Monte Carlo methods will yield information to deduce the minimal cut sets (as well as information on partial failure or degradation), however, converting this information to a form that can be incorporated into an existing PRA study may not be a trivial task. Similar remarks can be made about the information obtained from Markov models.

3.1.3 Discussion of Current Availability of Tools

Table 3 below gives an overview of how the methodologies reviewed in this report meet the requirements listed in Sections 3.1.1 and 3.1.2. Due to the lack of objective criteria, classification of compliance with the requirements is subjectively based on the examples provided in the available literature. From Table 3 it is clear that there is no single methodology available which satisfies all the requirements. Also, it is not clear that the data used in the quantification process would be credible to a significant portion of the technical community for any methodology. Since it is highly unlikely that issues related to data credibility will be resolved in the near future, investigation of the impact of digital systems on PRAs will need to include the sensitivity of the results to the data used and proposed resolutions. The methodologies that rank as top three with most positive features (X marks) and least negative (O marks) or uncertain (? marks) features are the DFM, dynamic event tree approach or Markov approach and ESD. GO-FLOW is a strong competitor.

Table 3: Methodologies and Requirements

Requirement/ Methodology	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees [89]	X	X	X	X	O	?	?	X	?	?	O
Dynamic Event Trees [91-95, 98]	X	X	X	?	X	?	?	?	X	X	O
Markov Models [13, 90, 99]	X	X	X	X	O	?	X	X	?	?	O
Monte Carlo Simulation [96]	X	X	X	X	?	?	?	?	?	?	O
Petri Nets [69, 70, 71, 84, 100]	X	X	X	X	O	?	?	?	?	?	O
DFM [22, 83]	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees [101, 102]	X	?	?	?	X	?	X	?	X	?	X
ESD [103]	X	X	X	X	O	?	?	?	X	X	O
GO-FLOW [104,105]	X	?	X	?	O	?	?	?	X	X	X
Bayesian Methodologies [67, 68]	X	?	?	?	O	O	?	?	?	?	X
Test Based Approaches [75]	?	?	X	O	X	?	X	X	?	O	X
Software Metric Based Approaches[76]	O	?	O	O	?	?	X	X	O	O	X
Schneidewind Model [53,77]	X	?	?	?	?	?	?	?	O	O	X

X: Fulfills requirement

O: Does not fulfill requirement

? Needs further study to determine whether or not the methodology fulfills the requirement

Requirements

1. The model must be able to predict encountered and future failures well.
2. The model must account for the relevant features of the system under consideration.
3. The model must make valid and plausible assumptions.
4. The model must quantitatively be able to represent dependencies between failure events accurately.
5. The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement.
6. The data used in the quantification process must be credible to a significant portion of the technical community.
7. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
8. The model must be able to differentiate between faults that cause function failures and intermittent failures.
9. The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.

10. The methodology must be able to model the digital I&C system portions of accident scenarios to such a level of detail and completeness that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed
11. The model should not require highly time-dependent or continuous plant state information.

While the DFM ranks as the most preferable methodology, it is not clear that it can satisfy Requirement 4 for all digital I&C systems. As discussed in Section 3.1.1 under this requirement, the exact magnitude and direction of change of the physical process variables at the time of hardware failure can affect the mode of system failure in systems relevant to nuclear engineering. Based on the digraph approach, the DFM works with only qualitative changes in physical variables. Similarly, if the branching probabilities are provided by fault–trees in dynamic event-tree construction, it is not clear that dependencies between basic events can be completely accounted for. Such problems can be avoided by using Markov models, but digital processor failure data generation can be problematic for Markov models as indicated in Section 2.1.3.1. Also, Markov models require highly time-dependent or continuous plant state information (Requirement 11) and it is not clear that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed with output from Markov models. Finally, ESD, in principle, avoids some of these problems by combining the continuous event tree approach with a graphical interface, but an application to digital I&C systems has not been encountered in the literature. Current implementations of ESDs (e.g. NASA's QRAS Version 1.7 [130]) treat ESDs as simple logic models and are analogous to event trees.

The above arguments indicate that a comparison of the most promising methodologies is needed using benchmark systems of interest to nuclear power plants on an existing full scale PRA to resolve the existing uncertainties with their capabilities. The benchmark systems should be representative of the licensing issues arising from the differences between digital I&C systems and their analog counterparts.

4. CONCLUSIONS

Reliability modeling of digital I&C systems cannot be addressed purely in terms of hardware and software. The reliability model needs to account for the possible dynamic interactions among the digital I&C system components, as well as between the controlling (supervising) system and controlled (supervised) process. Section 2 of this report reviews the dynamic and semi-dynamic methodologies proposed to date that attempt to represent this dynamic interaction. Only the spacecraft industry, under NASA's guidance, appears to be moving to a true risk evaluation system using such methodologies.

While there are a number of available dynamic methodologies, it appears that all of these approaches have limitations that may preclude them from being used as the technique of choice without modification. Lack of benchmark (a known model of system supported by operational data) against which these methodologies can be evaluated, as well as the ET/FT approach, makes comparison difficult. Each of the methods surveyed, however, did have unique points that may be able to be extended, enhanced, and/or integrated with other models. Such modification to the proposed approaches may result in techniques that can model digital systems to the level of detail required and in a quantitative manner.

The modeling method that is used needs to be able to model the digital system to a level sufficient to ensure that all risk important interaction are included, as well as, all of the systems features that are required by current regulatory guidance, as discussed in section 2.3. Almost all the methods reviewed in this report are capable of modeling a digital system to this level of detail, in the sense that they are probabilistic methods capable of describing common cause failures, and can model software integrated with hardware.

Regarding acceptance criteria for the methodologies to be used for digital systems assessments in nuclear power plants, the methodologies should demonstrate satisfactory compliance with the following requirements as a minimum:

1. The methodology should account for possible dynamic interactions between: a) the digital system and controlled/supervised plant physical processes, and, b) the components of the digital system itself.
2. The model must be able to predict future failures well and cannot be purely based on previous experience.
3. The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified.
4. The data used in the quantification process must be credible to a significant portion of the technical community.
5. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
6. The model must be able to differentiate between faults that cause function failures and intermittent failures.

7. The model must have the ability to provide uncertainties associated with the results.

Item 1 is particularly important in view of:

- the requirement of the standards cited above that the methodologies to be used in the probabilistic assessment of the digital I&C systems be capable of identifying the new failure mechanisms/scenarios, and,
- the conclusion of the National Academy of Sciences Committee on the Safety and Reliability Issues of Digital Instrumentation and Control Systems in Nuclear Power Plants that digital I&C systems (and digital systems in general) should not be addressed only in terms of hardware or software, but rather that the system as a whole be modeled to account for interactions between hardware and software.

No single methodology has been identified that satisfies all the requirements. Also, none of the methodologies reviewed have been shown to satisfy Item 4.

The methodologies that rank as the top two with most positive features and least negative or uncertain features (using subjective criteria based on reported experience) are the DFM and dynamic event tree approach or Markov approach (each with different advantages and limitations). While the DFM ranks as the most preferable methodology, it is not clear that it can properly account for Type I and Type II interactions due to its semi-quantitative representation of these interactions. In that respect, the next phase of this research will likely involve the following:

- Two benchmark problems should be defined that respectively capture important features of the existing analog I&C systems and their digital counterparts expected to be encountered in license applications.
- The benchmark problems should be used to compare the DFM and the Markov methodologies with regard to the modeling of Type I and Type II interactions using a common set of hardware/software/firmware states and state transition data.
- If the DFM and Markov methodologies produce similar results, then the impact of analog to digital I&C conversion should be investigated on a full PRA using prime implicants from DFM results and the state transition data used for the benchmark problem.
- If the DFM and Markov methodologies do not produce similar results, possible origins of the differences should be investigated.
- The feasibility of developing a dynamic methodology on a platform compatible with the current ET/FT approach (e.g. SAPHIRE) should be also investigated.

It should be indicated that there is no regulatory requirement for a single methodology to be applicable to all digital I&C systems relevant to the reactor protection and control systems. All the methodologies reviewed in this report, as well as the conventional ET/FT approach, have features that can make them preferable over the others depending on the system under consideration. The availability of a single methodology that is applicable to all digital I&C systems of interest provides convenience from a regulatory viewpoint in the sense that it can be used as a common platform to evaluate the validity of the analyses performed by different methodologies.

Regarding the applicability of the conventional ET/FT approach to digital I&C systems, no actual comparisons to dynamic methodologies have been encountered in the literature. The extrapolation of existing computational evidence based on a few comparative studies on dynamic systems seems to indicate that the ET/FT approach may yield satisfactory results when a digital I&C system does not:

- interact with a process that has multiple Top Events, logic loops and or substantial time delay between the initiation of the fault and Top Event occurrence,
- rely on sequential circuits which have memory,
- have tasks which compete for the I&C system resources, and,
- anticipate the future states of controlled/monitored process.

In all these comparisons, the ET/FT approach has been found to overestimate the predicted Top Event frequencies. However, the overestimation can be very large (by a factor of 2 or 3 [17] or even by an order of magnitude [18]). The ET/FT approach may also not be able to identify possible dependencies between failure events due to the omission of some failure mechanisms [19].

5. REFERENCES

1. Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades - Applying Risk-Informed and Deterministic Methods, Report#1002835, EPRI, Palo Alto, CA (2004)
2. Final Policy Statement, " Federal Register, Vol. 60, P.43622, August 16, 1995.
3. National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, National Academy Press (1997)
4. ACRS Letter Report to L. Joseph Callan, "Regulatory Guidance on Implementation of Digital I&C Systems", June 23, 1997
5. S. K. KHOBARE, S. V. SHRIKHANDE, U. CHANDRA AND G. GOVINDRAJ, "Reliability analysis of microcomputer circuit modules and computer-based control systems important to safety of nuclear power plants," *Reliability Engineering and System Safety, 59,* 253-258 (1998)
6. A. BOBBIO et al, "Sequential application of heterogeneous models for the safety analysis of a control system: a case study," *Reliability Engineering and System Safety, 81,* 269-280 (2003)
7. E. PLIJUGIN, "Development on probabilistic methods for a quantitative reliability assessment of software-based I&C systems", Proc. NPIC&HMIT 2004, 1394-1401, American Nuclear Society, LaGrange, IL (2004)
8. T. ALDEMIR, N. SIU, "Guest Editorial", *Reliab. Engng & System Safety*, 52, 181-184 (June 1996)
9. P. K. ANDOW, *Trans. IChemE*, 59, 125-128 (1981).
10. J. MARCH-LEUBA, *Trans. Am. Nucl.Soc.*, 60, 345-346 (1989).
11. N. SIU, "Dynamic approaches – issues and methods: An overview", *Reliability and Safety Assessment of Dynamic Process Systems,* T. Aldemir, N. S. Siu, A. Mosleh, P. C. Cacciabue, B. G. Göktepe (Eds.), 3-7, NATO ASI Series F, Vol 120, Springer-Verlag, Heidelberg (1994)
12. T. ALDEMIR, "Dynamic Approaches - applications: An overview", *Reliability and Safety Assessment of Dynamic Process Systems,* T. Aldemir, N. S. Siu, A. Mosleh, P. C. Cacciabue, B. G. Göktepe (Eds.), 81-84 NATO ASI Series F, Vol 120, Springer-Verlag, Heidelberg (1994)
13. D. TODD SMITH, TODD A. DELONG, AND BARRY W. JOHNSON, "A Safety Assessment Methodology for Complex Safety-Critical Hardware/Software Systems", *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies,* Washington, DC, November, 2000
14. D. M. RASMUSON, N. H. MARSHALL, Preliminary User's Guide to the Reliability Analysis System, RE-S-76-177, Idaho National Engineering Laboratory (1976).
15. S. A. EIDE, "Historical Perspective on Failure Rates for U.S. Commercial Components, *Reliab. Engng & System Safety*, 80, 123-132 (2003)
16. L. XING, K. N. FLEMING, W. T. LOH, "Comparison of Markov Model and Fault Tree Approach in Determining Initiating Event Frequency for Systems with Two Train Configurations", *Reliab. Engng & System Safety*, 53, 17-29 (1996).

17. M. HASSAN, T. ALDEMIR, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", Reliab.Engng & System Safety, 27, 275-322 (February 1990)

18. T. ALDEMIR, "Quantifying Setpoint Drift Effects in the Failure Analysis of Process Control Systems", Reliab. Engng & System Safety, 24, 33-50 (January 1989)

19. P. C. CACCIABUE, A. AMENDOLA, G. COJAZZI, "Dynamic logical analytical methodology versus fault tree: The case of auxiliary feedwater system of a nuclear power plant", Nucl. Technol., 74, 195-208 (1986)

20. S. A. ARNDT, E. A. THORNSBURY, AND N. O. SIU, "What PRA needs from a digital system analysis", *Probabilistic Safety Assessment and Management,* E. J. Bonano, A. L. Camp, M. J. Majors and R. A. Thompson (Eds.), 1917-1922, Elsevier Science Publishing Co., New York (2001)

21. A. IANNINO, J. D. MUSA, AND K. OKUMOTO, "Criteria For Software Reliability Model Comparisons", ACM Sigsoft Software Engineering Notes, Vol 8 No 8 Jul 1983, pg. 12

22. C. J. GARRETT, G. E. APOSTOLAKIS, "Automated hazard analysis of digital control systems", Reliab. *Engng & System Safety,* 77, 1-17 (2002)

23. M. STAMATALETOS et.al., "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," Version 1.1, August, 2002.

24. Definition of "Hard-coded," http://www.techdictionary.com

25. Definition of "Hard-coded," http://www.hyperdictionary.com.

26. R.L. CAMPBELL, "What Is Built-In Self Test And Why Do We Need It?," http://www.evaluationengineering.com/archive/articles/0396desn.htm.

27. J.BULLOCK, "Ladder Logic," Encoder, May 1997, http://www.seattlerobotics.org/encoder/may97/ladder1.htm

28. R.WALKER, "Intel 8080 Central Processing Unit," 1980, available at http://www.ordersomewherechaos.com/ rosso/fetish/m102/web100/docs/intel-8085-preface.html.

29. ISA-SP67.06, "Performance Monitoring for Nuclear Safety-Related Instrument Channels in Nuclear Power Plants", The Instrumentation, Systems, and Automation Society 67 Alexander Drive, Research Triangle Park, NC 27709 USA, 1999

30. RG 1.153, "Standard Criteria for Safety Systems in Nuclear Generating Stations ", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, 1996

31. IEEE Standard 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology," February, 1991.

32. J.HEFLER, "PWR Feedwater Upgrade, Breakout Session #3." EPRI Workshop on Licensing Digital Upgrades, Annapolis, MD, June 14-15, 1994.

33. KUROSE, J. F. AND ROSS, K. W. 2003. Computer Networking A Top-down Approach Featuring the Internet. Boston:Addison Wesley Pg. 460-466.

34. C. PERROW "*Normal Accidents, Living with High-Risk Technologies*", 1999 Princeton University Press, New Jersey

35. Definition of "Computer Worm," http://en.wikipedia.org/wiki/Computer_worm

36. K. POULSEN, "Slammer worm crashed Ohio nuke plant network", http://www.securityfocus.com/news/6767

37. NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/apr/apr.htm.

38. R.S. PRESSMAN, "*Software Engineering: A Practitioner's Approach,*" *6th Edition* McGraw-Hill, 2005.

39. "General Principles of Software Validation; Final Guidance for Industry and FDA Staff," January 11, 2002, http://www.fda.gov/cber/guidelines.htm

40. KANG, H., SUNG, T. "An Analysis of safety-critical digital systems for risk-informed analysis", *Reliability Engineering and System Safety,* 78, 307-314, 2002

41. JOHNSON, D., "The Sampling Theorem", Retrived January 10, 2004, from Connexions at Rice University: http://cnx.rice.edu/content/m0050/latest/

42. IEEE 323-1999 "Recommended Practice for Environmental (Temperature, pressure and radiation) Qualification of Class 1E Equipment for Nuclear Power Generating Station", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1999.

43. IEEE 344-1998, "Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1998

44. RG 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," ", U.S. Nuclear Regulatory Commission,, Washington D.C., 20555-0001, January, 2000.133.M. R. Lyu, *Handbook of Software Reliability Engineering*, McGraw-Hill, 1996.

45. Definition of Failure Mode, http://en.wikipedia.org/wiki/Failure_mode

46. M. SINGHAL, N. G. SHIVARATRI, *Advanced Concepts in Operating Systems*, New York: McGraw-Hill, Pg.297-366

47. IEEE 603-1998 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1998

48. Regulatory Guide (RG) 1.153, Standard Criteria for Safety Systems in Nuclear Generating Stations", U.S. Nuclear Regulatory Commission,, Washington D.C., 20555-0001, 1981

49. RG 1.152, "Standard Criteria for Digital Computers in Nuclear Generating Stations", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, 1997

50. Update of Chapter 7 (I&C) of NUREG-0800, Standard Review Plan, U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1997.

51. "Software Considerations in Airborne Systems and Equipment Certification,"DO-178B, RTCA, Inc. (1992).

52. Final Annual Report For Clarification of DO-178B "Software Considerations In Airborne Systems And Equipment Certification", DO-248B, RTCA, Inc (2001)

53. N.F. SCHNEIDEWIND and T.W. KELLER, "Applying Reliability Models to the Space Shuttle," *IEEE Software,* July 1992, pp. 28-33.

54. GAO/IMTEC-92-26, "Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia" (1992)

55. W.S. HUMPHREY, "Characterizing the Software Process A Maturity Framework," Technical Report, CMU/SEI-87-TR-11, June 1987.

56. "CMMI for Software Engineering Continuous Representation," Technical Report, CMU/SEI-2002-TR-028, August, 2002.

57. "CMMI for Software Engineering Staged Representation," Technical Report, CMU/SEI-2002-TR-029, August, 2002.

58. R.L. VAN SCOY, "Software Development Risk: Opportunity, Not Problem," Technical Report, CMU/SEI-92-TR-30, September 1992.

59. M.C. PAULK, ET. AL., "Key Practices of the Capability Maturity Model, Version 1.1," Technical Report, CMU/SEI-TR-*93-025.*

60. "American National Standard Quality Systems—Model for Quality Assurance in Design/Development, Production, Installation, and Servicing," ANSI/ASQC Q91-1987, American Society for Quality Control, 611 East Wisconsin Ave., Milwaukee, WI 53202, June 19, 1987.

61. "American National Standard Quality Management Systems—Requirements," ANSI/ISO/ASQ Q9001-2001, American Society for Quality, P.O. Box 3005, Milwaukee, WI 53201, December 2000.

62. TRAVERS, W. D. "Approaches for Adopting More Widely Accepted International Quality Standards" Available at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2003/secy2003-0117/2003-0117scy.html

63. "American National Standard Quality Management Systems—Requirements," ANSI/ISO/ASQ Q9001-2001, American Society for Quality, P.O. Box 3005, Milwaukee, WI 53201, December 2000.

64. Department of Health and Human Services, Food and Drug Administration, 21 CFR Parts 808, 812, and 820, "Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation," Federal Register, 61,. 195, Monday, October 7, 1996 / Rules and Regulations, pp. 52601-52662.

65. N. E. FENTON, M. NEIL, "A Critique of Software Defect Prediction Models", IEEE *Transactions on Software Engineering*, 25, 675-689 (1999).

66. B. LITLEWOOD, L. STRIGINI, "Software Reliability and Dependability: a Roadmap", ICSE 2000: Proceedings of the Conference on The Future of Software Engineering, 175-188, ACM Press, New York (2000).

67. Y. ZHANG, AND M. M GOLAY, "Development of a Method for Quantifying The Reliability of Nuclear Safety-Related Software", PSAM6: Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version, Elsevier Science Ltd. 2002

68. G. PAI, S. DONOHUE, J. DUGAN, "Estimating Software Reliability From Process and Product Evidence", PSAM6: Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version, Elsevier Science Ltd. 2002

69. P. L. GODDARD, "A Combined Analysis Approach to Assessing Requirements for Safety Critical Real-Time Control Systems", Hughes Aircraft Company, IEEE Proceedings Annual Reliability Maintainability Symposium, 1996

70. A. RAUZY, "Mode automata and their compilation into fault trees", Reliab. Engng & System Safety, 78, 1-12 (2002)

71. M. BALAKRISHMAN, K. TRIVEDI, "Stochastic Petri Nets for reliability analysis of communication network applications with alternate routing", Reliab. Engng & System Safety , 53(1996) pp. 243-259

72. J. L. PETERSON, "Petri Nets", Computing Surveys, Vol 9, No 3, September 1977.

73. M. MARSAN and G. CONTE, "A Class of Generalized Stochastic Petri Nets for the Performance Evaluation of Multiprocessor Systems", ACM Transactions on Computer Systems, Vol 2, No. 2, May 1984, Pg. 93-122.

74. T. S. LIU and S. B. CHIOU, "The application of Petri nets to faiulre analysis", Reliability Engineering and System Safety, Vol 57, February 1997, Pg. 129-142.

75. B. LI, M. LI, C. SMIDTS, "Integrating Software into PRA: A Test-Based Approach", PSAM 7-ESREL'04, C. Spitzer, U. Schmocker, V. N. Dang (Eds.), Springer – Verlag, London, U.K. (June 2004)

76. C. SMIDTS, AND M. LI, "Validation of A Methodology For Assessing Software Quality", Report UMD_RE_2002-07, February 2002

77. N. F. SCHNEIDEWIND, "Analysis of Error Processes in Computer Software", Proc. Int'l Conf. Reliable Software, IEEE CS Press, Los Alamitos, Calif., 1975, Pg. 76-78.

78. L. M. KAUFMAN, B. W. JOHNSON, "Embedded Digital System Reliability and Safety Analyses", NUREG/GR-0020, U.S. Nuclear Regulatory Commission, Washington, D.C. (2001)

79. R. Slater "Fault Injection" available at www.ece.cmu.edu/~koopman/des_s99/fault_injection/

80. J. VOAS, G. MCGRAW, "Software Fault Injection: Inoculating Programs Against Errors", John Wiley and Sons, inc. New York, 1998, page 37

81. J. VOAS, G. MCGRAW, "Software Fault Injection: Inoculating Programs Against Errors", John Wiley and Sons, inc. New York, 1998, page 34

82. T. DELONG, C. ELKS, J. DUGAN, M. STOVSKY, T. ALDEMIR, S. ARNDT, Teleconference, 12/15/2004

83. S. GUARRO, M. YAU and S. OLIVA, "Conditional Risk Model Concept for Critical Space Systems Software," Probabilistic Safety Assessment and Management: PSAM 7-ESREL'04, C. Spitzer, U. Schmocker, V. N. Dang (Eds.), 158-163, Springer – Verlag, London, U.K. (June 2004)

84. Y. DUTUIT et al, "Dependability modeling and evaluation by using stochastic Petri nets: application to two test cases", Reliab. Engng & System Safety , 55, 117-124 (1997)

85. D. L. PARNAS, "Software Aspects of Strategic Defense Systems", Communications of the ACM , Volume 28, Number 12 (December 1985)

86. C. SMIDTS, M. LI, "Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems", NUREG/GR-0019, UMD-RE-2000-23, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (2000).

87. C.SMIDTS, M. LI, Preliminary Validation of a Methodology for Assessing Software Quality, NUREG/CR-6468, U.S. Nuclear Regulatory Commission (2004).

88. J. A. RICE, "Mathematical Statistics and Data Analysis" 2nd Edition, Duxbury Press, Belmont, California, 1995 pg. 44

89. J. DEVOOGHT, C. SMIDTS "Probabilistic Reactor Dynamics I: The theory of continuous event trees", Nuclear Science and Engineering: 111, 229-240 (1992).

90. B. TOMBUYSES, T. ALDEMIR "Dynamic PSA of process control-systems via Continuous Cell-To-Cell-Mapping", in: P.C. Cacciabue, I.A. Papazoglou (eds.), Probabilistic Safety Assessment and Management PSAM3: 1541-1546, New York Elsevier (1996)

91. A. AMENDOLA, G. REINA "Dylam-1, a software package for event sequence and consequence spectrum methodology", EUR-924, CEC-JRC. ISPRA: Commission of the European Communities(1984)

92. G. COJAZZI, "The DYLAM approach to the dynamic reliability analysis of systems", Reliab. Engng & System Safety , 52, 279-296 (1996).

93. C. ACOSTA, N. SIU "Dynamic event trees in accident sequence analysis: Application to steam generator tube rupture", Reliab. Engng & System Safety, 41, 135-154 (1993).

94. C. SMIDTS, S. SWAMINATHAN "Improvements to discrete dynamic methodologies", PSA-96, 159-166, American Nuclear Society (1996).

95. H. KAE-SHENG, A. MOSLEH, "The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants", Reliab. Engng & System Safety , 52, 297-314 (1996)

96. P.E. LABEAU "A survey on Monte Carlo estimation of small failure risks in dynamic reliability", Int. J Electron Commun: 52(3):205-211 (1998).

97. S. MARCHAND, B. TOMBUYSES, P. LABEAU "DDET and Monte Carlo simulation to solve some dynamic reliability problems", PSAM 4, vol. 3: 2055-2060, New York, (1998).

98. M. MARSEGUERRA, E. ZIO, "Monte Carlo Approach to Psa for Dynamic Process Systems", *Reliab. Engng & System Safety*, 52, 227-241 (1996)

99. T. ALDEMIR "Utilization of the Cell-to-Cell-Mapping Technique to construct Markov failure models for process control systems", in: G. Apostolakis (ed.), Probabilistic Safety Assessment and Management PSAM1: 1431-1436. New York Elsevier (1991).

100. M. GRIBAUDO et al, "Fluid Petri Nets and hybrid model-checking: a comparative case study", Reliab. Engng & System Safety, 81, 269-280 (2003)

101. J. D. ANDREWS, J. B. DUGAN, "Dependency modeling using fault-tree analysis", Proceedings of the 17th International System Safety Conference, 67-76, The System Safety Society, Unionville, Virginia (1999)

102. M.CEPIN, B. MAVKO, "A dynamic fault-tree", Reliab. Engng & System Safety, 75, 83-91 (2001)

103. S. SWAMINATHAN, C. SMIDTS, "The mathematical formulation of the event sequence diagram framework", Reliab. Engng & System Sa, 65, 103-118 (1999)

104. T. MATSUOKA, M. KOBAYASHI, "An analysis of a dynamic system by the GO-FLOW methodology", in: C. Cacciabue, I.A. Papazoglou (eds.), Probabilistic Safety Assessment and Management'96: 1547-1436. Elsevier, New York (1991).

105. T. MATSUOKA, M. KOBAYASHI, "GO-FLOW: A New Reliability Analysis Methodology", Nuclear Science and Engineering, 98, 64-78 (1988)

106. M. BELHADJ, M. HASSAN, T. ALDEMIR, "On the Need for Dynamic Methodologies in Risk and Reliability Studies", Reliab. Engng & System Safety, 38, 219-236 (June 1992)

107. T. ALDEMIR, M. BELHADJ, L. DINCA, "Process Reliability and Safety Under Uncertainties", Reliab. Engng & System Safety, 52, 211-225 (June 1996)

108. J.M. IZQUIERDO, J. HORTAL, J. SANCHES-PEREA, E. MELENDEZ "Automatic generation of dynamic event trees: A tool for integrated safety assessment", Reliability and safety assessment of dynamic process systems, T. Aldemir, N. S. Siu, A. Mosleh, P. C. Cacciabue, B. G. Goktepe (Eds.), 135-150 NATO ASI Series F, Vol 120, Springer-Verlag, Heidelberg (1994).

109. T. S. LIU, S. B.CHIOU" The application of Petri nets to failure analysis", Reliab. Engng & System Safety, 57, 192-142 (1997)

110. IEEE 279, "Criteria for Protection Systems in Nuclear Generating Stations". Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1971

111. IEEE 603, "1980 "Standard Criteria for Safety Systems for Nuclear Power Generating Stations" , Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1980

112. Regulatory Guide (RG) 1.153, Standard Criteria for Safety Systems in Nuclear Generating Stations", U.S. Nuclear Regulatory Commission,, Washington D.C., 20555-0001, 1981

113. IEEE 338, "Standard Criteria for Periodic Surveillance Testing In Nuclear Power Generating Station Safety Systems", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 1980

114. EPRI TR-102348, "Guideline on Licensing Digital Upgrades", EPRI, 3412 Hillview Avenue, Palo Alto, CA 94303, September 1995.

115. RG 1.105, 'Setpoints for Safety-Related Instrumentation Used in Nuclear Power Plants", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, 1997

116. IEEE 384-2002, "Standard Criteria for Independence of Class IE Equipment and Circuits", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 2002

117. Regulatory Guide 1.97, " "Instrumentation for Light-Water-Cooled Nuclear Power Plant to Assess Plant and Environmental Conditions During and Following an Accident"" U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, 1981

118. Code of Federal Regulations, Title 10, Part 50.59: "Changes, Test and Experiments"

119. EPRI TR-102348 Revision 1 (NEI 01-01), "Guideline on Licensing Digital Upgrades – A Revision to EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule", EPRI, 3412 Hillview Avenue, Palo Alto, CA 94303, March 2002

120. Branch Technical Position HICB-14, "Guidance on Software Reviews for Digital Computer-Based I&C Systems", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1997

121. Branch Technical Position HICB-18, " Guidance on the Use of Programmable Logical Controllers in Digital Computer-Based I&C Systems, U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1997

122. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1997

123. Branch Technical Position HICB-21, "Guidance on Digital Computer Real-Time Performance", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1997

124. EPRI TR1002835 "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades Applying Risk-Informed and Deterministic Methods", EPRI, 3412 Hillview Avenue, Palo Alto, CA 94303 September 2004.

125. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, July 1998

126. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems", U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, December 1994

127. IEEE 352, 'Guidance on Reliability Analysis of Safety-Related in Nuclear Generating Stations"s", Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, New York 10016-5997 USA, 2003

128. M. GALLUZO, P. K. ANDOW, "Failures in Control Systems", Reliability Engineering, 7, 125-128 (198)

129. M. HASSAN, T. ALDEMIR, "Dynamic System Reliability Analysis With Mixed Component Failure Data", Use of Probabilistic Safety Assessment for Operational Safety: PSA '91, IAEA-SM-321, 775-77, International Atomic Energy Agency, Vienna, Austria (1992)

130. *Quantitative Risk Assessment System (QRAS) Version 1.7 User's Guide*, NASA (2004)

131. K.D. RUSSELL ET AL., Systems analysis programs for hands-on integrated reliability evaluations (SAPHIRE), version 6.0: System overview manual, NUREG/CR-6532, U.S. Nuclear Regulatory Commission (1999)

APPENDIX A

Nuclear Safety-Related I&C Standards Listed on the IEEE and ISA Websites

A.1 IEEE Nuclear Safety-Related Standards on IEEE Website

The following is a complete list of the IEEE Nuclear Safety-Related Standards as listed on the IEEE website. This list demonstrates the breadth of the IEEE Standards for nuclear power plant safety-related I&C systems.

IEEE Std 323-1999	Recommended Practice for Environmental (Temperature, pressure and radiation) Qualification of Class 1E Equipment for Nuclear Power Generating Station
IEEE Std 344-1998	Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE Std 352-1987 (R1993)	IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems
IEEE 379-1987	Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System
IEEE Std 382-1996 (R2004)	IEEE Standard for Qualification for Actuators for Power Operated Valve Assemblies with Safety-Related Functions for Nuclear Power Plants
IEEE Std 383-1974 (R1992)	IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations
IEEE 38 Std 4-2002	Standard Criteria for Independence of Class IE Equipment and Circuits
IEEE Std 387-1995 (R2001)	IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations
IEEE Std 420-2001 Std	IEEE Standard Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations
IEEE Std 484-2002	IEEE Recommend Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications
IEEE Std 485-1997	IEEE Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations
IEEE Std 572-1985 (R1992, 2004)	IEEE Standard for Qualification of Class 1E Connection Assemblies for Nuclear Power Generating Stations
IEEE Std 577-2004	IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations
IEEE Std 603-1998	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE Std 622-1987 (R1994)	IEEE Recommended Practice for the Design and Installation of Heat Tracing Systems for Nuclear Power Generating Stations

IEEE Std 622a-1984 (R1994)Std	IEEE Recommended Practice for the Design and Installation of Electric Pipe Heat Tracing Systems for Nuclear Power Generating Stations
IEEE Std 628-2001	IEEE Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations
IEEE Std 649-1991 (R1999, 2004)	IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations
IEEE Std 650-1990	IEEE Standard Qualification of Class 1E Battery Chargers and Inverters for Nuclear Power Generating Stations
IEEE Std 690-1984 (R1996, 2002)	IEEE Standard for the Design and Installation of Cable Systems for Class 1E Circuits in Nuclear Power Generating Stations
IEEE Std 692-1997	IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations
IEEE Std 741-1997 (R2002)	IEEE Standard Criteria for the Protection of Class IE Power Systems and Equipment in Nuclear Power Generating Stations
IEEE Std 765-2002	IEEE Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations
IEEE Std 803.1-1992 Std	IEEE Recommended Practice for Unique Identification in Power Plants and Related Facilities--Component Function Identifiers
IEEE Std 805-1984 (R1992)	IEEE Recommended Practice for System Identification in Nuclear Power Plants and Related Facilities
IEEE Std 833-1988 (R1994)	IEEE Recommended Practice for the Protection of Electric Equipment in Nuclear Power Generating Stations from Water Hazards
IEEE Std 845-1999	IEEE Guide for the Evaluation of Human-System Performance in Nuclear Power Generating Stations
IEEE Std 933-1999 (R2004)	IEEE Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations
IEEE Std 944-1986 (R1996)	IEEE Application and Testing of Uninterruptible Power Supplies for Power Generating Stations
IEEE Std 1023-1988	IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations
IEEE Std 1050-1996	IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations
IEEE Std 1082-1997 (R2003)	IEEE Guide for Incorporating Human Action Reliability for Nuclear Power Generating Stations
IEEE Std 7-4.3.2-2003	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

A.2 ISA Nuclear Safety-Related Standards on the ISA Website

The following is a complete list of the ISA Nuclear Safety-Related Standards as listed on the ISA website:

ISA-SP67.01 Transducer and Transmitter Installation for Nuclear Safety Applications

ISA-SP67.02 Instrument. Sensing Line Piping and Tube Standards for Use in Nuclear Power Plants

ISA-SP67.03 Reactor Coolant-Pressure-Boundary Leak Detection

ISA-SP67.04 Setpoints for Safety-Related Instrumentation Used in Nuclear Power Plants

ISA-SP67.06 Performance Monitoring for Nuclear Safety-Related Instrument Channels in Nuclear Power Plants

ISA-SP67.14 Qualification and Certification of Instrumentation and Control Technicians in Nuclear Power Plants

ISA-SP67.16 Safety-Related, Digital-Based System Upgrades in Nuclear Power Plants

ISA-SP67.17 Fiber Optic Cable for Nuclear Power Plants and Other Nuclear Facilities

NRC FORM 335 (9-2004) 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-6901

2. TITLE AND SUBTITLE

Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria forNuclear Power Plant Assessments.

3. DATE REPORT PUBLISHED

MONTH	YEAR
February	2006

4. FIN OR GRANT NUMBER

K6472

5. AUTHOR(S)

T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A.W. Fentiman and L.T. Mangan

6. TYPE OF REPORT

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 Ohio State University
Columbus, Ohio 43210

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 Fuel, Engineering and Radiological Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

S. A. Arndt, NRC Project Manager

11. ABSTRACT *(200 words or less)*

Digital systems offer the potential to improve plant safety and reliability through features such as increased hardware reliability and stability and improved failure detection capability. Because of these advantages and obsolescence issues with current analog systems there is a desire to use more digital systems in both safety and non-safety systems in nuclear power plants. However there are currently limited guidance and consensus on the reliability modeling of digital systems, which prohibits the use of risk informed regulatory reviews of digital systems. While the static event-tree/fault-tree (ET/FT) approach has been used in the reliability modeling of digital I&C systems in nuclear power plants, numerous concerns have been raised in the reliability literature in the past about the capability of the ET/FT approach to properly account for dynamic interaction between the digital system and the rest of the plant processes and within the hardware and software of the digital system itself. Any modeling method that is used should be capable of modeling the digital system to a level sufficient to ensure that all risk important interaction are included, as well as, all of the systems features that are required by current regulatory guidance. This report describes the issues that need to be addressed both in the reliability modeling of digital instrumentation and control (I&C) systems and in the incorporation of the digital I&C system reliability models into existing PRA models for improved risk-informed decision making with regard to a digital system's contribution to plant risk. The report also outlines the acceptance criteria to be used for the digital I&C system models prior to the implementation in regulatory applications.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Instrumentation and Control (I&C)
Risk-Informed Regulation
Digital Systems
Probabilitic Risk Assessment (PRA)

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program