COMMENT RESOLUTION

FOR THE

DRAFT NUREG/CR-XXXX

DYNAMIC RELIABILITY MODELING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR REACTOR PROBABILISTIC RISK ASSESSMENTS

Table of Contents

List of External Reviewers

As part of the review of this draft NUREG/CR has undergone three internal and two external peer reviews. Internal reviews included reviews by the staff of the Instrumentation and Electrical Engineering Branch of the Office of Nuclear Regulatory Research, the staff of PRA Support Branch of the Office of Nuclear Regulatory Research, the staff of the Instrumentation and Controls Branch of the Office of Nuclear Reactor Regulation, the staff of the PRA Licensing Branch of the Office of Nuclear Reactor Regulation, and the Advisory Committee on Reactor Safeguards. External peer reviews included a review by a panel of international experts in dynamic PRA methods, and a peer review by experts representing industry stakeholders. Below is the list of peer reviews that participated in one of the external reviews. The authors of the draft NUREG/CR would like to thank them for there efforts.

Mr. David Blanchard has more than 15 years of operations and engineering experience at Consumers Energy's nuclear facilities where he obtained a Senior Reactor Operator's certification, was reactor engineer and served as on call plant superintendent. His experience in PRA began shortly after the TMI accident when he was plant project engineer for the Big Rock Point risk assessment. Over the last 20 years, he has provided consulting services for a number of utilities in the performance and application of their plant specific PRAs, developing fully capable PRA staffs at each site that are maintaining and successfully applying their PRAs today. He has developed and applied risk and reliability techniques to a spectrum of facility types including nuclear generating plants and research reactors, economic risk analysis of coal fired stations, and reliability analyses of I&C systems at hydro facilities. Mr. Blanchard has been responsible for developing industry guidelines for a variety of electric industry generic issues including risk-informed electrical equipment qualification, generation risk assessment and most recently the performance of defense-in-depth and diversity evaluations for digital upgrades. Mr. Blanchard has a B.S. in Nuclear Engineering from the University of Missouri at Rolla and is currently President of Applied Reliability Engineering, Inc.

Mr. Robert S. Enzinna is an Advisory Engineer in Risk and Reliability Engineering at a major reactor vendor. He has been working in probabilistic risk assessment (PRA) and reliability analysis for over 28 years. He has been involved in various analysis applications involving a variety of mostly nuclear and some non-nuclear applications. His experience includes reliability analysis of electrical, mechanical, and structural systems with varying objectives related to safety, performance improvement, and licensing issues. Over the course of his career, he has developed detailed reliability and PRA models for several large instrumentation and control (I&C) systems including Reactor Protection Systems and Engineered Safety Features Actuation Systems. Applications have included analog designs as well as digital designs and have included existing plants as well as advanced reactor designs. These have included stand-alone models as well as those fully integrated with the plant PRA, and have included both time-dependent and time-averaged analysis. He has authored several topical reports involving multi-disciplinary studies to examine safety and licensing issues related to nuclear power plant designs. Mr. Enzinna was educated at Rensselaer Polytechnic Institute and graduated with a Master's Degree in Nuclear Engineering n 1979.

Dr. Stephen M. Hess is a Senior Project Manager - Safety and Asset Risk Management for the Electric Power Research Institute. He is a physicist with more than 25 years of experience

in nuclear power plant operation and maintenance, reliability and systems safety engineering, spacecraft design and thermal analysis, and technical and project management. He is expert in the fields of dynamical systems modeling and analysis, equipment and system performance analysis and reliability modeling. He holds a PhD in Physics from Bryn Mawr College. Dr. Hess previously held a Senior Reactor Operators license at the Peach Bottom Atomic Power Station. He is a member of the American Physical Society and Tau Beta Pi.

Mr. Thomas L. Sarver has over 25 years of electrical and I&C design and engineering experience in the nuclear power industry. Mr. Sarver holds a BS in Electrical Engineering and MBA, and is a Licensed Professional Engineer California and Texas. His experience includes the design and analysis of electrical systems while at Bechtel Power Corpration, I&C and mechanical system design at various engineering consulting companies. In addition to a strong foundation in system design, he has been involved in the development of plant safety analyses including deterministic analyses such as FMEAs and Appendix R safe shutdown, and probabilistic risk assessment (PRA). Mr. Sarver is currently, supporting Fire PRA development for several utilities. These efforts include implementation of NUREG 6850 with the associated requirements for explicit treatment of instrumentation required for plant operation and shutdown post fires in the plant Fire PRA.

Dr. Curtis Smith has been in the risk and reliability assessment field for over 17 years and has provided project management and technical support for diverse risk and safety assessment projects for the Nuclear Regulatory Commission (NRC), National Aeronautics and Space Administration (NASA), International Atomic Energy Agency, and the Department of Energy. With the Idaho National Laboratory since 1990, he is currently the principal investigator on several projects, is the project manager for the NRC's SAPHIRE risk analysis software, and is a lead instructor for the PRA Training program for the NRC. His current research focus is on the areas of incorporating decision-sciences into PRA and the use of Bayesian information techniques to improve the reliability and safety of complex systems. He recently served as a visiting scientist to the OECD-sponsored Halden Reactor Project performing human performance-related research. Dr. Smith has published over 65 papers and reports on risk and reliability theory and application. He has a B.S. and M.S. in Nuclear Engineering from Idaho State University and a Ph.D. in Nuclear Engineering from M.I.T.

Mr. Jeffrey L. Stone is an Engineering Supervisor in Fleet PRA Services of Constellation Energy. He is stationed at Calvert Cliffs Nuclear Power Plant in Lusby, Maryland. He has worked at Calvert Cliffs since 1985 in Operations, Operations Training, Design Engineering and Probabilistic Risk Assessment. Qualifications include Design Engineer in Civil Engineering and all aspects of PRA at Calvert and Ginna Stations. Over twelve years of experience in PRA includes fault tree, event tree, human reliability, external events, data, and Level II analysis. He has been an active representative in the Risk Management Subcommittee of the Presssurized Water Reactor Owner's Group (PWROG) since 2003. He is Chairman of the RISKMAN Users Group (Large Event Tree/Small Fault Tree software) for 2006. Education includes a BS in Nuclear Science from University of Maryland University College in 1992 and a MS in Reliability Engineering from the University of Maryland in 1998.

Dr. Atoosa P-J Thunem holds an MSc in computer science from Alborg University in Denmark, and a PhD in joint computer science, control and reliability engineering from Technical University of Denmark. She has 15 years of experience with R&D from both the

research/education community and from the telecom industry. Dr. Thunem joined the Halden Reactor Project in 2002 as principal scientist. Her main work at the Software Engineering Lab has work on dependable design and dependability analysis of computerized systems (focus on software), IT-security, model-based risk analysis and lifecycle modeling. Within these areas, she is the sole or main author of nearly 30 publications, co-author of nearly 25 publications, and additionally more than 30 reports. She has been reviewer, organizer and session chair in a number of European and international conferences and workshops. Dr. Thunem is a senior member of IEEE (Computer Society, Communications Society, Reliability Society, Robotics and Automation Society) and a member of EWICS.

Dr. Nguyen Thuy has been a Senior Research Engineer at EDF (Electricité de France) since 1994, and currently heads the Digital Systems Dependability team. The team analyzes the digital systems that are important to safety or critical to power plants and power grid performance. It also develops advanced methods, tools and guidelines for the design and verification of safe and dependable digital systems. Additionally, Dr. Thuy has worked in the US on a joint EDF-EPRI research program on digital systems important to nuclear power plants safety since 2003. Dr. Thuy is a member of several working groups of the IEC (International Electrotechnical Commission), and is a consultant for the IAEA (International Atomic Energy Agency) on instrumentation and control issues.

Dr. Enrico Zio (BSc, 1991 and PhD, 1998 in Nuclear Engineering., Politecnico di Milano; MSc in Mechanical Engineering., UCLA, 1995; PhD, in Nuclear Engineering., MIT, 1998) is the Director of the Graduate School of the Politecnico di Milano. Dr. Zio was Vice-Chairman of the European Safety and Reliability Association, ESRA (2000-2005), Editor-in-Chief of the international journal Risk, Decision and Policy (2003-2004) and is currently the Chairman of the Italian Chapter of the IEEE Reliability Society (2001-). He is also a member of the editorial board of the journals *Reliability Engineering and System Safety*, *Risk and Reliability*, *Science and Technology of Nuclear Installations*. Dr. Zio has functioned as Scientific Chairman of two International Conferences and as Associate General Chairman of two others, all in the field of Safety and Reliability. He is co-author of one book and more than 100 papers on international journals and serves as referee of 10 international journals.

Introduction

As part of the NRC's Office of Nuclear Regulatory Research continuing effort to insure the quality of its products, the draft NUREG/CR, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," under went extensive internal and external peer review. This report documents the all of the comments received as part of these peer reviews and the disposition of these comments in the final NUREG/CR.

The comments have been organized into general topical areas, general format, style and notation comments, comments on failure modeling, data collection and generation, the benchmark system, incorporation of failure models into the PRA, uncertainty analysis and comments associated with regulatory issues. For each comment, the exact comment is reproduced, the authors decision on the appropriateness of the comment (agree, agree in part, disagree) and what was done to resolve the comment is provided.

Additionally two appendixes are provided to provide additional information regarding the resolution of comments 1.1.39, 3.8 and 4.8.

General Format, Style and Notation Comments

Comment 0.1

It would be beneficial to provide a glossary of terms and abbreviations.

Response 0.1

Agree. Such a list is already provided under Abbreviations following the Executive Summary.

Comment 0.2

Section 2.3.4 - Terminology (see e.g. p. 2-29): It is difficult to find where certain terms and abbreviations are defined. Also, abbreviations are not consistently used (e.g. definition and use of MS1 / MS 1 - additionally, these terms should be defined in the paragraph on p. 2-29 which begins "The inter-computer interaction …"). It would be beneficial to provide a glossary of terms and abbreviations.

Response 0.2

Agree. Section 2.3.4, Fig.2.3.2 and Abbreviations are revised to respond to the comment.

Comment 0.3

Section 2.4.4 - Safety Assessment Model (p. 2-44): The referenced Figure 2.4.3 is missing (later figures are then mislabeled and do not mach the text descriptions).

Response 0.3

Agree. Figure 2.4.3 is corrected and later figures are then relabeled to match the text descriptions.

Comment 0.4

Section 2.5 - Introduction (pp. 2-68 to 2-69): Numbering of event sequence / assumptions is incorrect and does not match text (most likely a word processor auto numbering error).

Response 0.4

Agree. The sequence is corrected.

Comment 0.5

Section 2.5 - Figure 2.5.3 Axis Labels (p. 2-73): Typo in z-axis label; should be Re(Root2) or Re(Root3) (not roots 1 and 2).

Response 0.5

Agree. Figure 2.5.3 is corrected.

1 Failure Modeling

1.1 Dynamic Methodologies

Comment 1.1.1

While the product demonstrates a very firm knowledge about PRA generating techniques (FTs, ETs, etc.), about DFM and Markov modeling, about how they are used for certain applications and about the benchmark system example used, it lacks the same level of knowledge about other techniques and their combinations and with regard to other (more complex) systems. By means of comparison, the combination of UML notation (for pure qualitative analysis), colored Petri nets (for detailed analysis of behavior and communication patterns) and BBNs for optimization of the Petri nets have been successfully used for complex software-intensive systems with a considerable amount of type II interactions. Other applications have replaced Petri nets with SDL (a formal specification (and not V&V) technique providing both textual and graphical modeling and based on the formal language Z), also with decent level of success. As far as different system architectures are concerned, a great deal of modernization activities these days involve replacement of sub-systems with more advanced computerized systems with, e.g., more data storage capabilities, replacement of the networking part with more sophisticated units (characteristics of some also addressed by the product), and on top of all this the necessary inclusion of pure security-related systems such as IDSs. Although the majority of digital I&C systems falls into the system framework of the product (the benchmark example), it could have been beneficial for future modernization activities to have touched upon the topic. This, together with some other aspects already mentioned in this review could, for example, have been gathered in a specific chapter called "Trends and future challenges" (just meant as suggestion).

Response 1.1.1

Agree in part. Section 1.1 is revised to reflect this comment and additional references are provided. However, a more extensive survey would be outside the scope of this study. Such a survey may be included in the sequel to this report which will use a second benchmark system with mostly Type II interactions.

Comment 1.1.2

What this NUREG/CR does not do, in this reviewer's opinion, is to show that these methods will find significant failure modes that would not be found and modeled in a conventional fault tree analysis. None of the failure modes noted seemed especially hard to find in a normal FMEA. These failure modes could be accounted for in a traditional fault tree. Further, without following through with a top event (not necessarily core damage) failure probability the practicality of the analysis is not shown. An analysis method must be shown to develop reasonable and realistic failure probabilities. This has not been demonstrated here.

Response 1.1.2

Disagree. As indicated in the revised Section 1.1, the objective of this report is to illustrate the implementation of the DFM and Markov/CCMT methodology on a system representative of the

digital I&C systems used in nuclear power plants. It does not aim to demonstrate that the methods will identify new failure modes. It has already been shown in the literature that they can as described in detail in NUREG/CR-6901. The report does show, however, that the significance of the timing of faults to the system failure mode (i.e. Low Level vs. High Level for the benchmark DFWCS) which would be very difficult to identify through a conventional FMEA. It would basically involve going though the steps to generate the cell-to-cell-transition probabilities of Markov/CCMT methodology or the decision tables of DFM, except without the systematic organization of the computations and procedures to assess the consequence of the results on the system failure modes and frequencies. Regarding reasonable and realistic failure probabilities, again it is not the intention of the report to demonstrate that the use of dynamic methodologies such as DFM and Markov/CCMT methodology will produce significant changes in the predicted Top Event frequencies, but rather to provide a proof-of-concept regarding applicability of these methods. Even if the implementation of the methodologies on the benchmark DFWCS do not produce results significantly different from those that would be obtained from the conventional ET/FT approach, it would not imply that this conclusion would be true for all future upgrades and/or reactors.

Comment 1.1.3

The analysis used multiple simplifying assumptions. The system is much more complex than modeled. This makes the analysis easier to follow, but it is not clear that the methodologies can practically be used when evaluating all the interactions of the system. The number of results exceeded one million for the first ten seconds of evaluation for CCMT using the simplifying assumptions. It is not clear how this would progress when looking at the complete system without simplifications. It is also not clear why evaluating the first ten seconds of the transient will be sufficient to develop a quantification of a system for 24 hours.

Response 1.1.3

Agree in part. As indicated in the revised Section 2.5, the example initiating event is chosen for ease of illustrating the implementation of the dynamic methodologies under consideration and is not indicative of the limitations of the Markov/CCMT methodology or DFM, as well as being representative of the possible types of interactions relevant to the benchmark DFWCS which may lead to errors not easily identifiable by conventional methods. For example, power is not assumed to be constant in time which leads to the artifact described in Section 2.5. Similarly, the BFV position is function of the BC and BFV controller states and may reflect history dependence which again is not representable by the conventional ET/FT methodology. Regarding the number of scenarios, the statement is relevant for the Markov/CCMT methodology. The two methodologies that are under consideration have different strengths and are complementary. The Markov/CCMT models time explicitly so as to simulate the actual stochastic behavior of the system as closely as possible and not to miss any possible failure sequence. Its strength is forward analysis which may be important for assuring completeness is non-autonomous processes. Consequently, there are a large number of scenarios. As indicated in the revised Section 5.4.2, the user may or may not choose to use all the scenarios depending on how the system under consideration is connected to the other plant systems. For example, if the level information for the example DFWCS is not being used by other plant systems, then only the hardware/software/firmware states are relevant and Section 5.4.2 shows that only 40 scenarios can result in the system failing HIGH or LOW depending on the exact

timing of the events, and 20 can only result in the system failing LOW irrespective of the length of the planning horizon. Algorithm 2 in Section 5.4.1.2 targets this type of use. For autonomous processes, the transition matrix has to be constructed once and mission duration is not an issue (Section 4.2.5). Also, the DFM application in Chapter 3 shows how one may not consider time explicitly while still fully accounting for it and mission duration is not an issue either.

Comment 1.1.4

In general the components that will be replaced with digital components are not driving the risk of systems. What is driving these risks are components such as the pumps, valves, and relays modeled in these systems. The analog components to be replaced typically have an order of magnitude less importance than hardware such as valves and pumps. The FMEA showed this system was robustly designed and experience with digital systems has been mostly favorable. Thus, save for software common mode failures, it can be concluded that the new digital components will have a low risk significance.

Response 1.1.4

Disagree. It is not clear what the basis is for the comment. On the systems aspects of digital instrumentation and control technology, the National Academy of Sciences report has concluded that "The lack of actual design and implementation of large I&C systems for U.S. nuclear power plants makes it difficult to use learning from experience as a basis for improving how the nuclear industry and the USNRC deal with systems aspects".

Comment 1.1.5

Executive Summary: The conclusions from NUREG/CR-6901 do not have sufficient basis to justify that conventional fault tree/event tree methods are not adequate to model digital systems. The conclusions drawn from the National Academy of Sciences study are not the same as those implied by NUREG/CR-6901. While this summary states that DFM and Markov-CCMT methods are successful it does not show that similar results would not be determined by a well performed FMEA in the traditional method. Further, it does not quantify the system to show that reasonable results can be calculated.

Response 1.1.5

Disagree. The NUREG/CR-6901 does not conclude that the conventional ET/FT approach is not adequate to model digital systems but rather that it may not be adequate for such a purpose. With regard to the safety and reliability assessment methods, the National Academy of Sciences study recommends that "The USNRC should consider support of programs that are aimed at developing advanced techniques for analysis of digital systems that might be used to increase confidence and reduce uncertainty in quantitative assessments" which is one of the reasons why this study was conducted. Obtaining similar results by a FMEA would basically involve going though the steps to generate the cell-to-cell-transition probabilities of Markov/CCMT methodology or the decision tables of DFM (see revised Section 2.5), except without the systematic organization of the computations and procedures to assess the consequence of the results on the system failure modes and frequencies.

Comment 1.1.6

Section 2.3 notes a full FMEA done in Appendix B - it is not clear that the DFM or CCMT gave any additional insights into the failure modes of the system.

Response 1.1.6

Disagree. Section 2.5 shows that whether the DFWCS fails by Low or High Level may depend on the timing BFV failure. Discovery of this feature of the DFWCS would involve going though the steps to generate the cell-to-cell-transition probabilities of Markov/CCMT methodology or the decision tables of DFM (see revised Section 2.5) which is not done in the conventional FMEA. Also see *Response 1.3.5.*

Comment 1.1.7

Section 2.3.1 - The FMEA performed here reinforces the robustness of the digital design. It is notes that a failure of both sets of control (MC and BC) is significant, because operator action is required. Most of the failure cases noted cause the valve to fail in the last command position. Unless the failure occurs very early in a transient this is a relatively benign failure that can be easily recovered by operators in the time available. After the first one hundred seconds the valve position is closely matched to steam flow. This FMEA shows that for most failures it is protected far better than an analog system would be. Everything stated here notes that the digital system appears to be more reliable than an analog system and thus an improvement to plant safety. Much of the discussion on the MFRV's is only relevant for BOP and IE Frequency. These valves are required to close on a plant trip and there control becomes irrelevant.

Response 1.1.7

Disagree. The comment is based on qualitative understanding of plant behavior. A purpose of this analysis is to investigate relationships that may not be apparent through such a reasoning process. Also, the frequency of Low Level occurrence would affect the frequency of demand on safety systems which would affect the core damage frequency.

Comment 1.1.8

Section 2.5: The discussion of when a failure occurs has a significant impact is something any FMEA done for a traditional method of analyzing a system would have noted. (See Figure 2.5.7) The analyst would have to determine how detailed he modeled this based upon the amount of impact on the PRA. For example on the fails as is mode in the first one hundred seconds for the BFV. The FMEA noted the failure mode and a probability would be used, based on the exposure time, that it would fail when over-feeding or under-feeding the Steam Generator. These would probably be of low significance because the exposure time is very short.

Response 1.1.8

Disagree. Determination of the significance of the impact is an important reason why the PRA

is conducted. Historical evidence has shown that seemingly insignificant events in the deterministic sense can lead to quite serious consequences in the presence of right timing and combination. However, risk significance of an event or a component cannot be determined until the PRA is performed with the best available tools. Investigation of the importance of timing of failure events using FMEA would involve going though the steps to generate the cell-to-cell-transition probabilities of Markov/CCMT methodology or the decision tables of DFM (see revised Section 2.5).

Comment 1.1.9

Section 3: Even with the simplifying assumptions used the analysis is not taken to it's conclusion by quantifying the probability that the system will cause an under-fill or overfill of the Steam Generator. The technique is challenging and will take significant training for current PRA staffs to implement. Further, there are no additional insights seen by this reviewer that would not be found by an FMEA.

Response 1.1.9

Agree in part. The purpose of this NUREG/CR is to illustrate the use of the proposed methodologies only. Quantification will be provided in the next NUREG/CR (we are working on that document now and it should be available for peer review in the spring). However, this NUREG/CR does illustrate the use of dynamic methodologies by the step-by-step modeling of the example initiating event. Also, please see *Responses 1.1.5, 1.1.6* and *1.3.5*.

Comment 1.1.10

Sections 5.4.1.1 and 5.4.1.2 require coding knowledge to perform. Without practical software available this may be cost prohibitive from an engineering man hour context.

Response 1.1.10

Agree in part. The algorithms described in Sections 5.4.1.1 and 5.4.1.2 will need to be automated to interface with available PRA tools to be practical for commercial applications. However, even without automation, the interfacing can be done fairly easily as was illustrated using SAPHIRE.

Comment 1.1.11

Section 9: It is noted that fault trees and event trees cannot account for the timing of failures. This analysis showed that the timing of a failure was significant if the Bypass Valve is failed as is during the first 100 seconds that it could cause and overfill or under-fill. A detailed FMEA would have easily have noted this failure mode and the conventional method could account for that failure. Further, this failure is only significant if it occurs in the initial 100 seconds. Later in the transient the feed and steam flow mismatch would be minimal.

Response 1.1.11

Disagree. The failure referred to is significant if it occurs in the initial 100 seconds following <u>any</u>

level disturbance. Although a detailed conventional FMEA may have identified this failure mode, there is no assurance that it will identify all possible failure modes of this nature. Regarding the capabilities of FMEA, also see *Responses 1.1.5, 1.1.6.*and*1.3.5*.

Comment 1.1.12

Page 9-1 & general: The admitted challenges for these methodologies are key, especially computational demand, and lack of failure data. As pointed out by the authors, these are issues with any method used. Conventional fault tree (FT) and event tree (ET) methods have solved these problems by finding an appropriate balance between model detail and available data and computational resources. It is these very weaknesses that erase the benefit of any increased mathematical precision or theoretical advantage that Markov or other dynamic modeling may promise. As with the conventional FT and ET methods, simplifying assumptions are necessary when modeling a large-scale application such as a NPP and its I&C systems (especially so with the dynamic methods). Any theoretical difference between the dynamic methods and FT/ET methods loses its contrast in light of the uncertainties associated with modeling assumptions.

Response 1.1.12

Disagree. The balance that is being referred to has evolved over the past 30 years through operational experience. As indicated in NUREG/CR-6901, the digital I&C systems introduce new challenges. There is not sufficient operational experience with the digital I&C systems to strike the proper balance. That is why NUREG/CR-6901 has aimed to identify the state- of-the-art tools that would minimize the likelihood of misjudgement and oversight. Regarding large scale applications, it is not the intent of NUREG/CR-6901 or this report to apply dynamic methods to the whole NPP. As reflected in Requirements 9 and 10 in Section 1.2.3 and described in Chapter 6, the dynamic methodology results should be integrable into an existing PRA so that dynamic methodologies can be implemented on only a small portion of the plant rather than the whole NPP (also see *Response 1.2.6*)

Comment 1.1.13

General: It has not been demonstrated that detailed modeling of dynamic control systems is necessary in NPP PRAs. The complex dynamic control systems, for the most part, are associated with normal plant operating systems, which have little impact post-accident. The I&C systems of most importance post-accident tend to be protection systems such as RPS and ESFAS. These systems are generally not dynamic, and operate by monitoring of plant parameters, threshold comparison, voting (coincidence logic), and changing the state of an output. The NUREG should make it clear that the dynamic methodologies are not needed for protection systems.

Response 1.1.13

Disagree. Regarding “little impact” and “most importance ”, the authors do not believe that such statements can be categorically made without actually performing a PRA with the best available tools which would include dynamic methodologies. Regarding the need to use dynamic methodologies to model RPS and ESFAS, while the authors agree that dynamic

methodologies may not be needed to model the functions given as examples, it would be difficult to state that dynamic methodologies are not needed for all existing and future protection systems for all existing and future plants. As indicated in Section 1.2 of this report and Section 2.1.1.2 of NUREG/CR-6901, modeling communication and multitasking features of digital I&C systems may require explicit representation of time (also see *Response 1.3.5*). It is the authors understanding that NRC intends to conduct a second benchmark study using a RPS to determine under what circumstances dynamic models are needed.

Comment 1.1.14

The plant control systems, such as the main feedwater (MFW) control system used in the example, are not typically important contributors in the PRA, and very detailed modeling of these systems in the PRA is seldom warranted. The dynamic control systems that do impact the PRA generally affect the initiating event frequency. In other cases, there may be limited credit for post-trip response of a normal-plant control system to the initiating event (e.g., run back of MFW). The initiating event frequency (or post-trip control system failure) can usually be modeled with a point estimate. Typical PRA practice is to avoid detailed modeling of initiating events if possible; the reasons for this are the very same reasons as addressed in the NUREG. It is difficult to model dynamic control systems with hardware-based reliability models. The failure probability of these systems is not a function of the hardware reliability or even of the software reliability, but rather the performance of the plant, and the complex interaction of many factors. Consequently, the best way to model these systems is with historical operating experience, using conservative estimates, if necessary, until sufficient plant-specific data are available. When a detailed reliability model for an initiating event frequency is necessary, for example because of lack of operating experience, plant-specific initiators, or unresolved dependencies, then a more complicated model may be warranted. It is within the realm of possibility that an analyst may attempt to evaluate the initiating event and/or initiating event frequency with a Markov or DFM model, however it should be noted that there are existing PRA methodologies that are appropriate as long as they are performed according to accepted standards (such as ASME PRA Standard). It is also appropriate to assign a conservative point estimate along with conservative assumptions of the potential consequences (dependencies) of the control system failure.

Response 1.1.14

Disagree. In areas where historical data are not sufficient to completely characterize all failure modes and frequencies (such as for digital systems), it is inappropriate to assume conservatism since such an assumption may not foresee all potential combinations of failures that may lead to risk important consequences. Also, please see *Responses 1.1.8, 1.1.12, 1.2.12* and *1.3.6*.

Comment 1.1.15

DFWCS Example (see Table 5.4.2): The example produces over one million failure scenarios (equivalent to cut sets) for a ten-second mission time (i.e., ten time steps) for a failure sequence that involves three components (from a total system size of 14 components). Usefulness in a PRA is questionable, where the mission time is typically 24 hours, and the components in a system number in the hundreds. The result would be unwieldy.

Response 1.1.15

Disagree. The result would not be unwieldy. Please see *Responses 1.1.3* and *1.1.12*.

Comment 1.1.16

DFWCS example (table 5.4.3): this is a tabulation of the many "failure sequences" from the previous discussion of the DET. The table enumerates the many different paths thru random failure states of the controller. For example, in one of these sequences (1-4-5-6-7), the controller goes from operational (1) thru the states of frozen (4), arbitrary output (5), zero vdc output (6), to stuck (7) within a period of ten seconds. The many failure paths shown in this table are the various combinations and permutations through these various random states. As the accompanying text explains, the order and timing of these states determines the outcome. As the text also explains (last paragraph on page 5-40), the outcome of all of these paths is one of three valve positions: valve sticks at its old value, fails high, or fails low. In PRA lingo, this translates to the failure modes "valve fails as-is," "valve fails open," or "valve fails closed." These failure modes are intuitively obvious to any qualified PRA analyst, and are considered in every fault tree analysis. This reviewer fails to see what is gained by all of this complexity. If we also consider the probability of these failure paths (which the text apparently ignores), it is obvious that there is no practical way to put a probability on these paths (e.g., 1-4-5-6-7: operational, frozen, arbitrary output, zero output, stuck) that is any better than the failure rates assigned by a PRA analyst for "valve fails closed."

Response 1.1.16

Disagree. The statement “it is obvious that there is no practical way to put a probability on these paths” reflects reviewer’s opinion rather than fact. Section 2.4 explains how failure rates/probabilities for frozen, arbitrary output, zero output failure modes can be estimated through fault injection experiments. As indicated in the introduction of Chapter 2 and Section 2.3.4, “Stuck” refers to mechanical failure of the device and can be obtained from hardware data bases. What is gained by the complexity is the assurance that no failure scenario is missed through the intuitive or non-systematic assessment of possible failure mechanisms. Also see *Responses 1.1.12* and *1.3.6*.

Comment 1.1.17

The NUREG and its predecessor (NUREG/CR-6901) state that conventional FT methods yield conservative results. There is nothing wrong with conservatism. Conservatism is not a weakness, but a necessity. The PRA tool is an approximation, and it is necessary to approximate on the conservative side. (For example, the PRA typically ignores time dependence by calculating the time-averaged unavailability of each component separately before combining component failures at the plant/core-damage sequence level.) Conservatisms are used to account for modeling uncertainty, and the cumulative affect of these conservatisms is that they wash out the effect of mathematical subtleties. Time dependence is rarely important in light of the failures that typically dominate the PRA results, such as common cause failures and human errors, and the imprecision associated with these estimates. This reviewer does not see the benefit of trying to interface time-dependent sublogic into a non-time-dependent PRA model. There are other areas of uncertainty in the digital I&C models

that are more significant (see research suggestions in a later comment).

Response 1.1.17

Agree in part. While the authors agree with the statement that conservatism is not a weakness, they do not agree that the conventional or the typical approach to PRA is necessarily applicable to all digital I&C systems. The statement regarding what has typically dominated the PRA results is based on 30 years of experience with analog systems. Consequently, it is not clear that the conclusions regarding the significance of events based on the conventional PRA experience are also valid in the presence of digital I&C systems. Also see *Responses 1.1.4, 1.1.12, 1.1.14, 1.1.16* and*1.3.5 .*

Comment 1.1.18

Reviewer's conclusion on dynamic modeling methods: It is the reviewer's opinion that the greatest promise for these methods (Markov and DFM) is in applications that involve a stand-alone analysis of a small dynamic control system. Markov models have historically been useful only in applications of limited size. Their viability in an integrated PRA model has not been proven by the draft NUREG, and it is impossible to conclude that the proposed methods would be useful or practical with respect to a NPP PRA.

Response 1.1.18

Agree in part. This is in fact what the whole report is about, i.e., how to apply dynamic methodologies to small systems in such a way that their results can be integrated into an existing PRA. It is not clear what is meant by “practical” and “proven”. What may not be practical to an analyst due to unfamiliarity with a new methodology may be practical after proper training. That dynamic methodologies may be needed for the reliability modeling of digital I&C systems relevant to those in nuclear power plants has already been shown in the literature as discussed in NUREG/CR-6901.

Comment 1.1.19

Chapter 1: The objectives of the research should be clarified -- that it is intended only for risk-informed applications related to digital I&C systems. In addition, the specific types of applications where the methods are intended should be clarified. This would also help focus the efforts of the researchers into the most productive areas.
It should be made clear that there is a successful path to licensing of digital I&C upgrades and new designs that relies on existing deterministic regulations. While these methods may hold some future promise, it would be a mistake to allow the ongoing research and dialogue to become an impediment to digital upgrades because it is generally acknowledged that digital I&C has safety and performance benefits over analog systems.

Response 1.1.19

Agree in part. While this is a technical report and it is not the intent of the authors to comment on regulatory policy, it is also the authors’ understanding that a successful path exists to the licensing of digital I&C upgrades and new designs that relies on current deterministic

regulations. The main objective of this research is to advance the state-of-the-art on digital system risk and reliability modeling to the point where the NRC can apply risk informed decision making to digital systems. Section 1.1 is revised to reflect these points.

Comment 1.1.20

Pg 1-8: The presumption that these methods can support near-future PRA applications is incorrect. The methods described in the NUREG have historically been know to have the limitation of being useful only for systems and problems of small and limited size. These methods have never before been successfully applied to applications anywhere near the size of a nuclear power plant PRA. Hence, the burden is on the research to demonstrate that these limitations can be overcome and that the methods are applicable and practical for applications on the scale of NPP PRAs. The NUREG does not demonstrate that these methods work for large systems. In fact, it has not demonstrated that they work for the small examples in the NUREG, because the analyses were not carried to completion (with full integration and quantification). The limitations of these methods, especially with respect to system size need to be explored and explicitly stated.

Response 1.1.20

Agree in part. It is true that the methods described in the NUREG have been historically used for problems of small and limited size. in fact this is exactly what this document is proposing to do. Chapters 3 and 4 are illustrating how the small systems can be modeled using dynamic methodologies to account for the system complexity if necessary and then integrated into the overall PRA (Chapters 5 and 6). Also, please see the *Responses 1.1.3, 1.1.12,* and *1.1.18*.

Comment 1.1.21

It would be premature and debilitating to dictate regulatory requirements that cannot be met with existing methods. Dynamic modeling in PRA studies should not be required before there is a practical and proven method to implement the requirements. This would be an impediment to the safety and performance improvements that can be gained from digital technology. Consequently, this reviewer recommends that new regulatory requirements not be promulgated until the additional research recommended on page 9-2 is completed, and has demonstrated that the proposed methods provide a meaningful and cost-effective benefit. In the meantime, the industry should be encouraged to pursue risk-informed applications, if so desired, on a parallel path.

Response 1.1.21

This is a technical report and does not dictate regulatory requirements. It is also outside the scope of this report to comment on future industry applications.

Comment 1.1.22

As stated in the last paragraph of the executive summary, "the properties of the benchmark system considered in this study may not apply to all the reactor protection and control systems in nuclear power plants. For digital I&C systems which may have less complex interaction

between the failure events, the conventional ET/FT approach may be adequate for the reliability modeling of the system." This reviewer agrees that the conventional ET/FT methods are adequate for most digital I&C systems that are important in NPP PRA studies, and has first-hand experience creating such models. The use of existing methods for risk-informed applications involving digital I&C should be encouraged because evolution of these methodologies may provide another success path for the benefit of the industry and public..

Response 1.1.22

This is a technical report and cannot comment on regulatory policy. However, the authors believe that the conventional PRA methods may not be acceptable for all digital I&C applications.

Comment 1.1.23

The emphasis on dynamic failure modes is misplaced. Digital control system technology promises an improvement in dynamics (improved response time, increased sophistication). Experience (in Europe for example) has shown that digital control systems will reduce initiating event frequencies over the old analog designs. Existing regulations with respect to independence, diversity, equipment qualification, defense-in-depth, etc. provide a sound basis for ensuring the reliability and safety of digital I&C systems. They also ensure that safety-related I&C systems will not be compromised by failures within the non-safety-related I&C systems, where most of the dynamic control functions reside. The non-dynamic safety-related I&C, such as reactor protection systems (RPS) and engineered safety features actuation systems (ESFAS) protect against a multitude of failures, including those caused by failure of dynamic control systems. Because of these multiple layers of defense, it is not necessary to encumber the non-safety-related control systems with excessive licensing requirements, such as the requirement to do complete dynamic models, and the designers should retain flexibility over control system design. It is this reviewer's opinion that research could be better focused on certain areas that would have more immediate benefit to PRA practitioners and regulators. For example:

1. Quantification of software CCF and the distinction between common application program, common operating system, etc.
2. Effect of various operating system and software design features and how they impact software CCF.
3. Assessing robustness against configuration control issues
4. How to model separate functions that share a common processor
5. Generic failure rate data (or quantification methodology) for digital I&C components that do not yet have an operating history
6. Human error probabilities related to digital vs. analog displays and controls
7. Quantification of percent fault-tolerant vs test-revealed (or fail-safe vs. fail-dangerous) failure modes.

Response 1.1.23

This is a technical report and cannot comment on NRC research prioritization. However, the authors believe that use of dynamic methodologies can provide further insight into all the issues

itemized above except Issue #6.

Comment 1.1.24

The concept for the regulatory guide presented in Section 1 (Figure 1.3.2, etc.) is interesting; however it is unclear how the scores for complexity (type II) and system interactions (type I) would be determined. There are design features that can be and are employed to minimize both type I and type II interactions. If appropriate scores like this could be determined, then they should distinguish between the system design features that affect the outcome (e.g., use of deterministic programming, cyclic program execution vs. if/then/else branching, asynchronous vs. synchronous operating system, static vs. dynamic memory allocation, existence and handling of process driven interrupts, use of independent networks). Similarly, different vendor's processes for application software development may vary in robustness for an equivalent level of complexity.

Response 1.1.24

Agree. However, more research is needed to identify the criteria for ranking. Section 1.4 has been revised to highlight this point.

Comment 1.1.25

A system with low risk importance should not require dynamic modeling no matter how large or complicated it may be, or how may interactions it may have with other plant functions.

Response 1.1.25

Disagree. A methodology to determine what modeling requirements need to be met for any particular system has not been established. It may be that low risk importance systems may not require dynamic modeling. However, a conclusion would be premature until the methodology is complete.

Comment 1.1.26

A system with high risk significance (perhaps RPS or ESFAS) should not require "complete dynamic modeling" just because it may be a large system, if the functions it performs are non-dynamic (actuating safety systems when plant parameters meet certain thresholds)..

Response 1.1.26

Disagree. Please see *Response 1.1.25.*

Comment 1.1.27

With respect to Figure 1.3.1, in addition to the three attributes discussed (system importance, system interactions, and system complexity) there should be a forth attribute related to the intended PRA application. If an issue is going to be made out of model precision, then there should be a discussion of the precision and modeling attributes that are considered necessary

for each grade of application. (e.g., 1=vulnerabilities, 2=ranking, 3=risk significance, 4=sole basis of assessment per the application categories referenced in NEI 00-02, or alternately the AMSE standard).

Response 1.1.27

Agree in part. However, a methodology to determine what modeling requirements need to be met for any particular system has not been established. While this is a technical report and cannot comment on regulatory policy, it is the authors' understanding that current industry standards for needed modeling attributes and precision will be considered as part of the effort to develop regulatory guidance in this area.

Comment 1.1.28

Page 1-1: To state that ET/FT methodology may not yield satisfactory results (because NUREG/CR-6901 shows them to be a factor of 2 or 3 conservative) is not appropriate without first identifying the purpose of the analysis and defining the required precision for that application. It is good practice not to begin an analysis before first defining what it is the analysis is intended to prove. Therefore, the NUREG should clearly define what purpose such an analysis would have in PRA and licensing space, and what specifically the analysis is intended to show, before listing the attributes that such an analysis must have (page 1-7).

Response 1.1.28

Disagree. This report does not claim that the ET/FT methodology may not yield satisfactory results because NUREG/CR-6901 shows them to be a factor of 2 or 3 conservative. Rather, along with NUREG/CR-6901, it illustrates the importance of the timing of failure events in consequence evolution which cannot be captured by the conventional ET/FT methodology. Regarding the role of dynamic methodologies, the report is a technical and not a regulatory document and subsequently cannot comment on what purpose a dynamic analysis would have in the licensing space. In the PRA space, they can be helpful to assure the completeness of the scenarios and failure modes considered, as well as providing a best estimate quantification of consequence likelihoods.

Comment 1.1.29

Some of the comments made by ACRS members on this topic at the end of the recent ACRS subcommittee meeting (6/27/06) should be addressed. Summarizing:

MEMBER KRESS: … it would be nice to have some early on judgments as to which systems actually need to be modeled, and what process one would use to model those particular ones. And I think risk-importance measures would be very useful there. No use to waste time on things that are not really risk-significant.
… I was a little skeptical of having the ability to incorporate time-dependent failure rates into PRAs. I think we need to figure out how to work around that, or avoid it.
… I don't know, it seems to me that replacing analogs with digital almost automatically decreases risk. I don't know if we could make such a blanket determination or not, but that's just a thought.

MEMBER BONACA: … The area of determination of which digital systems need to be modeled and what level of detail, that's an area, of course, of interest to all of us. But I think it's also important because it will define somewhat where you need to have dynamic modeling, and where you can stay with traditional methods.… I would be responsive to Mr. Gaertner's recommendation of not forcing incorporation of digital I&C modeling in PRA.
MR. HICKEL: … My immediate thoughts are that there needs to be a more focused prioritization of where the staff is trying to develop modeling, and analysis capability. I don't know why the focus was on digital feedwater control systems. … I would think that there is a need to have more ability to project and evaluate trip systems and ESFAS logic systems than was discussed here today.
… one of the things that I see that's out there is issues of configuration control afterwards, because these are the failures that clearly are occurring. Somebody gets a bad data set and they put it into all channels of the trip system, and that's not digital. You can do the same darned thing in an analog, an old analog system… and that issue is probably more likely to occur than some very highly unusual common cause hidden software failure.

Response 1.1.29

Agree. They should be and have been. For example, regarding Member Kress' comments please see *Response 1.1.8 and 1.3.6.* Regarding Member Bonaca, please see revised Section 1.4.

Comment 1.1.30

The commercial nuclear power industry has obtained significant benefits (both in terms of safety enhancements and operational performance) from the installation of digital I&C systems in non-safety related applications (e.g. feedwater and turbine controls). Similar benefits could be derived for similar safety related applications and expanded applications to non-safety related systems. This experience (and expectation) is corroborated by extensive use of digital systems in safety critical applications both in international nuclear plants and in other industries (e.g. commercial aerospace, chemical processing, etc.). Additionally, there is a critical need to develop an acceptable regulatory basis to meet the expected deployment of new plants which will rely on digital I&C systems. Due to the pressing need to address installation of critical application digital I&C systems, the timeframe under which this research is being conducted will not support the needs of the industry, the NRC or the public interest. Although the research discussed in this report is thorough and advances the state of the art, it does not address the most pressing needs of the stakeholders mentioned above within a timeframe that meets these needs.

Response 1.1.30

Agree in part. The completion of the development of the methods presented in this report will not necessarily be complete in a very short time frame. However, it is the author's understanding that other research and programmatic efforts are underway at the NRC to address shorter term needs.

Comment 1.1.31

The report is technically good (i.e. in discussing the uses of CCMT and Markov modeling). However, the main drawback is that the lack of quantification and actual integration with a PRA precludes drawing any substantive conclusions with respect to the capability of the proposed approach to be integrated with a PRA for actual application to operating reactors. Although the authors allude to follow-up research projects which will address quantification of results, they do not give this aspect sufficient emphasis. Additionally, due to the timeliness issue (commented on above), the authors do not sufficiently address how the research described in this report is intended to be used in the regulatory framework.

Response 1.1.31

Agree in part. Please see *Responses 1.1.9, 1.1.19, 1.1.22*, and *1.1.23*.

Comment 1.1.32

The report provides a good description of the DFM and Markov modeling approaches to PRA of digital I&C systems. The description for these methods and application generally was of Satisfactory (3) and in some cases higher (i.e. Excellent (4) or Outstanding (5)) rating. However, there are several significant issues which need to be addressed and resulted in the overall scoring of Satisfactory (3) for this category.

1. The basic hypothesis of why current PRA methods (i.e. FT/ET models) are insufficient is not justified; nor is there any comparison of results obtained using the DFM and Markov models on the example applications to FT/ET methods.
2. No quantification of result is presented for the example applications. Thus, it is not possible for one to compare the results, either between the DFM and Markov approaches or to the conventional FT/ET approach. The report needs to add a discussion that quantification will be addressed in a subsequent report and caution that any conclusions presented in this report should be considered preliminary.
3. The example chosen constituted a very simplified system for demonstration. Although this is useful to demonstrate proof-of-concept, the authors do not sufficiently address the scalability of the approaches if they are to be applied to significant portions of an operating plant PRA. This is particularly critical for application of the Markov model method where it is known that an increase in the number of model elements results in a very rapid escalation in the number of transition states and required computational resources.
4. There is no discussion of how the methods discussed in the report are to be used within the regulatory framework by the NRC. The report needs to be expanded to include this discussion.

Response 1.1.32

Agree in part. Regarding Item 4, this is a technical report and can not comment on regulatory policy. However, Section 1.1 has been revised to better discuss the purpose of the report. Regarding the other Items, please see *Responses 1.1.2, 1.1.3, 1.1.9,1.2.6* and *1.3.7*.

Comment 1.1.33

Executive Summary: The major issue is whether the conclusions of NUREG/CR-6901 (i.e. the inapplicability of the conventional event tree / fault tree modeling approach to digital I&C systems) is accepted. A brief review of this report leads me to disagree with this premise. In particular, NUREG/CR-6901 explicitly states, "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." (Executive Summary p. xvii) Thus, for the purpose of regulatory decision-making, the assertion that the conventional ET/FT approach is not suitable for the evaluation of digital I&C systems is not adequately supported. In fact, NUREG/CR-6901 later states (Executive Summary p. xviii), "In all these comparisons, the ET/FT approach has been found to overestimate the Top Event frequencies". Thus, again for the purpose of regulatory decision-making, the conventional modeling approach can be viewed as somewhat conservative. Thus, from the perspective of ensuring public health and safety, if the application of the conventional ET/FT results in risk measures that are acceptable under the current regulatory framework (e.g. Regulatory Guides 1.174 or 1.177), then more detailed or sophisticated modeling should not be required. In the event these measures are not met, the licensee should have the option of modifying the design and reanalyzing using conventional techniques until an acceptable safety impact is attained.

Response 1.1.33

Agree in part. Please see *Responses 1.1.14, 1.1.19, 1.1.22*, and, *1.1.23*.

Comment 1.1.34

Executive Summary: NUREG/CR-6901 conducted a review of practices of other industries (defense, aerospace, medial technologies, telecommunications and process industries). In all cases, each of these focused efforts on applying comprehensive design, testing and quality assurance practices for ensuring digital I&C systems operate in the intended manner and ensure a desired level of system safety is obtained. Use of risk management principles typically are applied commensurate with the level of mission criticality associated with the application. In no cases was it identified that quantitative modeling of the risk impact of the digital I&C system is required as a basis for system implementation decisions. Here, it should be noted that some of these industries have potential public health and safety impacts at least commensurate with commercial nuclear power applications. Based on this evidence, a proposed regulatory approach to address nuclear power applications should be commensurate to that accepted by other federal agencies for applications that have potential public health and safety impacts or if additional requirements are imposed, the and policy bases justifying the additional requirements need to be specified.

Response 1.1.34

This is a technical report and cannot comment on regulatory policy.

Comment 1.1.35

Executive Summary - Challenges (pp. xvi - xvii): These represent real and significant challenges in the implementation of the proposed approaches. This report describes application of analytical techniques that are sophisticated and still predominantly within the realm of

research (vs. commercial application). At this stage, any attempt to apply them in the context of a regulatory decision-making framework is problematic. Based on experience with application of the conventional ET/FT PRA approach to regulatory decision-making (which required several decades to achieve broad acceptance in the US), the report should provide an acknowledgment of this issue and strongly caution that, while the research conducted presents a potentially fruitful approach to addressing any limitations inherent in current risk assessment technology, the proposed approaches cannot be applied to regulatory decisions until the analytical approaches have been sufficiently proven (at a level comparable to the conventional ET/FT approach).

Response 1.1.35

This is a technical report and cannot comment on regulatory policy. However, it is the authors' understanding that the methods presented in this report will not be endorsed for regulatory decision making until the NRC determines them to be sufficiently mature for such a purpose.

Comment 1.1.36

Chapter 1 - General: This write-up serves as a relatively brief discussion of issues identified in NUREG/CR-6901 and comparison of the approaches proposed to address them. However, all of the methods discussed (with the exception of Bayesian methodologies) have had limited (and in most cases no) application to the evaluation of nuclear plant systems and the impact of their failures on nuclear safety. This reinforces the comments made above to the discussion of Challenges in the Executive Summary.

Response 1.1.36

Agree in part. The methods discussed have had limited application in the evaluation of nuclear plant systems because of 30 years of plant operational experience regarding the validity current approach to PRA. There is no comparable operational experience with the digital I&C systems. Markov models have been used in the quantification of fault-trees in the presence of statistically dependent events. Also see *Responses 1.1.4* and *1.3.6.*

Comment 1.1.37

Chapter 1 - Discussion of DFM (bottom p. 1-5 to top p. 1-6): Many of the issues identified w.r.t. application of this approach are similar (and many identical to) issues for developing an accurate conventional ET/FT model to evaluate the system reliability.

Response 1.1.37

Agree in part. Please see *Responses 1.1.4, 1.3.5* and *1.3.6*.

Comment 1.1.38

Chapter 1 - Discussion of complexity and coupling (pp. 1-9 to 1-10): It is not clear how the concepts of internal complexity (fault tolerance, error checking, etc.) and external tight coupling (interface of control system with plant electro-mechanical equipment necessitates the need for

new evaluation techniques. Conceptually, the situation exists today (but to a lesser degree) between analog I&C systems and plant equipment used for operation and / or accident mitigation. As a specific example, from the definitions provided here, it appears Type 1 interactions / failures are possible for currently installed analog systems (such as for flow control circuitry in feedwater, auxiliary feedwater, reactor recirculation, high pressure coolant injection, etc.).

Response 1.1.38

Agree in part. Please see *Responses 1.1.4, 1.3.5* and *1.3.6*.

Comment 1.1.39

The document references NUREG/CR-6901 as indicating that the conventional event tree fault tree methodology may not yield satisfactory results when modeling a digital I&C system. NUREG/CR-6901 provides three examples in which dynamic methodologies are stated to provide more accurate results than the event tree fault tree methodology. These three examples plus the benchmark exercise from the draft NUREG do not appear to be applicable to nuclear power plant PRAs. Appendix A provides the rationale for this conclusion for each of the four examples. The report should develop examples that reflect current event tree fault tree techniques and success criteria consistent with that used in existing nuclear power plant PRAs.

Response 1.1.39

Disagree. The scope of this report is to investigate dynamic modeling methods that can be used to model digital I&C systems and which can be integrated into the existing PRAs. It is the author's understanding that other NRC research is investigating the limitation and applicability of the conventional PRA methods to digital I&C systems. Regarding the examples: a) non-coherence arising from repair and timing issues cannot be properly handled by any of the existing conventional PRA tools, b) while Type I interactions may be also relevant for analog systems, differences arising from the discrete time nature of digital systems exacerbate the effect of Type I interactions, as well as leading to new issues to be addressed (see *Response 1.3.5*), and, c) the system configurations arising from the digital nature of the I&C systems may lead to new interdependence between failure events (e.g. platform commonality). *Also see Response 1.1.8.*

Comment 1.1.40

Sections 3 and 4: Reference is made to fault tree analysis being limited to a single top event which must be reevaluated manually. The basis for this statement is not clear as most fault tree analysis codes are capable of automatically solving fault trees with multiple top events including the effects of numerous combinations of plant conditions.

Response 1.1.40

Agree in part. What is meant by the relevant statement in Chapter 3 is that each system Top Event requires a separate manual input of AND/OR gate information. The wording in Chapter 3 is revised to reflect the intention of the statement. A similar statement was not encountered in

Chapter 4.

Comment 1.1.41

The report does not indicate if the techniques presented provide significant additional risk insights into digital system implementation over an analog system. The identification of any "digital system characteristics" that may impact event frequency, common cause, or a loss of function are not presented.

Response 1.1.41

Agree in part. While there is no quantification of the impact of the digital system characteristics, Table 5.4.1 shows that BFV failure in the arbitrary output mode and subsequent loss of communication between the BFV controller and the BFV (which are both digital system features), lead to low level which will then initiate safety systems to be activated. Also, see *Response 1.1.2*.

1.2 System Representation Scheme

Comment 1.2.1

Generally, the qualitative and quantitative methods used for modeling type I and II interactions are treated together (put into the same group) and it is therefore difficult to assess what combination(s) are stronger (of course, according to a set of criteria in focus) than others. Being able to do such assessment is vital as both qualitative and quantitative modeling techniques are needed and complement one another in any reliability modeling and risk assessment..

Response 1.2.1

Agree in part. However, such an assessment is beyond the scope of this study whose intent is only to demonstrate the applicability of techniques selected in NUREG/CR-6901 to the update of the plant PRAs following an upgrade of analog I&C systems by digitial I&C systems. The use of qualitative techniques to support quantitative assessments is somewhat illustrated by the use of FMEA (Section 2.3) in support of Markov/CCMT methodology and DFM.

Comment 1.2.2

The advantage of a thorough qualitative analysis in terms of a description of the associated techniques cannot be found in the product. When it comes to type II interactions that are very complex in nature, suitable qualitative techniques seek and model real and concrete system knowledge/information. This knowledge is crucial in order for the subsequent quantitative analysis to be more trustworthy. Such knowledge is used to, e.g., estimate the most "proper" number of states for a certain system variable and with respect to a certain dependability factor in focus (say security) while using the DFM. In addition, the knowledge can also reveal the fact that several sets of states for exactly the same variable might be needed when focusing on other dependability factors, or when describing their interrelationships in different ways. An example for the latter: The description of the correlations between safety and security factors for a certain system can vary depending on how user-friendliness requirements are defined.

Response 1.2.2

Agree in part. We have tried to do such a qualitative analysis using the FMEA methodology in Section 2.3. However, it is not the intent of the authors to address security issues in the report.

Comment 1.2.3

Although highlighting features and limitations of various types of methods, the product appears less successful in providing a deeper view (also caused by the problems addressed in 1 and 2). As a consequence, the product tends (although not intentionally) to present method-specific views on system behavior as system-specific "facts". One example is the way the three-state concept used in Markov models is described (2.4.3). This concept (also used in some other techniques) does not distinguish between functional and operational characteristics of complex systems, and is practically inapplicable in modeling type II interactions for software-intensive systems. Such issues are not mentioned by the product.

Response 1.2.3

Agree. Revised Section 2.4.2 through 2.4.5 shows how the three-state model can be mapped to the failure models related to the functional and operational characteristics of the digital I&C systems.

Comment 1.2.4

The product does not offer any means to distinguish between the concepts of safety and security. One gets the impression that they are used more or less synonymously. Example: The way "system safety" is addressed in 2.4.3. Methods for the reliability assessment of "pure" security-critical systems (say the access control system at a bank) can be substantially different from those used in security-critical systems where security is defined in the context of safety (the same type of access control system at an NPP).

Response 1.2.4

Agree. However, it is not the intent of the authors to address security issues in the report.

Comment 1.2.5

In general, the level of knowledge about aspects related to type II interactions appears less convincing than that for type I interactions. One example is the erroneous definition of deadlock and starvation in 1.2. Deadlock and starvation are both phenomena merely related to multitasking systems and they occur due to granting exclusive access to shared resources (which itself is a means for avoiding race conditions). Deadlock occurs when a set of processes (or tasks) are blocked (not running) because each waits for a resource that can only be released by an already blocked process in the same set. Starvation occurs when all members of the set run indefinitely, but with no progress (no job done). While both indicate that run-time errors are not fully anticipated, starvation is almost entirely a kernel-related problem (how the kernel does its task scheduling), whereas deadlock is in most cases related to a design or coding flaw (i.e. related to inter-task communication and regardless of how the kernel prioritizes its group of application tasks). These very fundamental differences between deadlock and starvation could have been reflected by the product, to demonstrate the level of complexity for type II interactions.

Response 1.2.5

Agree. Deadlock and starvation redefined in response to the comment.

Comment 1.2.6

The report addresses a particularly difficult question that I would formulate this way: "What model(s) of manageable complexity can we use to evaluate the key safety parameters of a nuclear power plant, taking into consideration (in particular) the impact of digital systems?"

One key issue is model complexity: the plant AND the digital systems are complex entities with complex behaviors and complex states. Injecting the complexity of digital systems into plant

safety models is likely to lead to large and unmanageable models. On the other hand, oversimplifying the digital systems is likely to lead to incorrect or insufficiently founded safety evaluations. Thus, my basic approach would be to distinguish very clearly two different levels: the plant level, and the digital systems level. This is the old "divide and conquer" approach.

Response 1.2.6

Agree in part. In a way, this is in fact exactly what this document is proposing to do. Rather than redoing the whole PRA using dynamic methodologies, Chapters 3 and 4 are illustrating how the individual digital I&C system can be modeled using dynamic methodologies to account for the system complexity if necessary, Chapter 5 shows how the results of dynamic methodologies can be cast into a format that is compatible with the ET/FT approach and Chapter 6 illustrates the integration process. This process is described in Section 1.1 of the report. Section 1.4 has been revised to highlight that the scale of the digital system model that needs to be used depends on its connections with the rest of the system. The user may or may not choose to use all the scenarios depending on how the system under consideration is connected to the other plant systems. For example, as stated in Section 5.4.2, if the level information for the example DFWCS is not being used by other plant systems, then only the hardware/software/firmware states are relevant and Section 5.4.2 shows that only 40 scenarios can result in the system failing HIGH or LOW depending on the exact timing of the events, and 20 can only result in the system failing LOW irrespective of the length of the planning horizon. As indicated in Section 5.4.2, Algorithm 2 in Section 5.4.1.2 targets this type of use.

Comment 1.2.7

Section 2.1: Two types of interaction between digital systems are considered: type I through process, and type II through direct interactions. Other types of interaction should be included, in particular interactions through causally related specification, design or operation / maintenance errors.

Response 1.2.7

Agree in part. Specification, design or operation/maintenance errors can be contributors to the risk importance of the digital I&C systems. However, these types of errors are not within the scope of the study. Section 1.1 of the report is revised to clarify the scope.

Comment 1.2.8

Sections 2.1 and 2.2: The architecture and the internal functioning of the digital feedwater controller need more detailed and formal description. The objective of the description would be to identify and characterize "digital failure units" and their failure modes, analyze defensive measures and failures propagation, and the units failures that must occur in order to obtain given system failure modes.

Response 1.2.8

Agree in part. The digital failure units are defined in Sections 2.1. and 2.2 (i.e., main and backup computer, BFV, MFV, PDI controllers). The level of detail provided and failure modes

for the units identified are based on the available benchmark DFWCS documentation.

Comment 1.2.9

The results of Markov methodology and DFM need to be compared and the differences resolved.

Response 1.2.9

Agree. Section 5.5 of the report is included to provide such a comparison and resolution.

Comment 1.2.10

The differences between the Markov models used in Section 2.4 and Chapter 4 need to be explained.

Response 1.2.10

Agree. Section 4.1 of the report is revised to indicate that Section 2.4 uses the Markov models to obtain a better understanding of the hardware/software/firmware structure of the system to plan for fault injection experiments for failure data generation whereas the Markov methodology of Chapter 4 utilizes the data generated by these fault injection experiments, as well as obtained from other databases and CCMT to quantify the likelihood of Top Event occurrence. Also, the Markov models used for the latter purpose are referred to as Markov/CCMT models in the entirety of the report and a new Section 2.4.3.1 is provided to clarify the difference.

Comment 1.2.11

Section 2.3 discusses many computer and controller failure modes - however there appears to be no discussion on probability of these combinations. It is not clear how risk significance of each combination is determined. It would be helpful to see how each failure mode (arbitrary signal to a controller for example) is developed into a probability for a sequence.

Response 1.2.11

Agree in part. Chapters 3 and 4 show how the reliability models for the DFWCS can be constructed using these modes, respectively, with the DFM and Markov/CCMT methodology. Chapters 5 and 6 how these reliability models can be integrated into PRA quantification tools to determine the minimal cut sets for selected Top Events. The risk significance of each combination using different measures (e.g., Fussel-Vesely, Birnbaum) can be then determined using the standard features of these tools as clarified in the revised Section 5.1 and data from Section 2.4.

Comment 1.2.12

Section 3: One failure mode noted in the DFM Analysis is the BFV failing in the arbitrary mode. This is a failure mode, but what is important to the PRA is in which direction the valve fails. The different failure modes within arbitrary require quantification. It is conservative to assume

always failing in the insufficient flow direction.

Response 1.2.12

Agree in part. While the authors agree with the comment for the example initiating event, it is not clear that such a conservative direction can be inferred in all applications.

Comment 1.2.13

Tables 5.4.2 and 5.4.3 - It is unclear if any screening is done for scenarios that are unrealistic or extremely improbable. For example if a controller gives a zero output it would seem very likely to continue to give a zero output and not randomly switch to other failure modes.

Response 1.2.13

Agree in part. The FMEA analysis (Section 2.3) does consider possible outcomes of component state changes and eliminates outcomes that are not possible based on the available system documentation. However, the type of screening based on likelihoods is not done since it would anticipate data. In DET analysis pruning can be done using user specified cut-off probabilities. For the particular example of zero output in the comment, Fig.2.3.3 shows that the only possible state zero output leads to is Device Stuck which is possible due to mechanical failure of the device and is independent of the controller failure mode (see revised Section 2.3.4).

Comment 1.2.14

In digital I&C especially, conservatisms are an effective way to proceed with the current analysis technology. For example, unlike analog systems, digital systems typically process several related or unrelated functions on the same processor. Until practical methods are available to separate and quantify failure of the different functions individually, it is appropriate to model the computer processor failure in the digital I&C system as an all-or-none proposition. In other words, conservatively assume that all of the functions on the common processor fail simultaneously in the worst case configuration. This is a practical alternative to trying to identify and assign a probability to all of the combinations of all of the states of all of the outputs of the processor. Before prescribing the attributes that an analysis should possess (Section 1.2.3), the analyst should ask whether that level of detail is even necessary. For an application where there is abundant defense-in-depth, independent backup systems, and/or low probability of failure, the conservative approach may be entirely tolerable.

Response 1.2.14

Disagree. The authors believe that the approach proposed would have a lot of subjective elements which may or may not prove to be justified when measured against more objective methods such as proposed in this report. Also, see *Responses 1.1.14* and*1.2.12*

Comment 1.2.15

Sections 3 and 4 : The success criteria for the FW control system is inconsistent with what is assumed in nuclear power plant PRAs (which ranges from above steam generator dryout to below the steam lines).

Response 1.2.15

Agree in part. While from the viewpoint of additional actions to be taken, it is true that the failure criteria for the feedwater system ranges from above steam generator dryout to below the steam lines, the choice of the HIGH LEVEL and LOW LEVEL bounds are based on: a) the functional requirements of the DFWCS, and, b) the fact that the choice does not impact the ultimate outcome of the scenarios.

Comment 1.2.16

One central problem with the reliability modeling of digital instrument and control (I&C) systems is that of software reliability, which was outside the scope of the subject report (See “Challenge 3" on page xvii of the subject report). However, the complete solution of the reliability modeling of digital I&C systems requires a solution of the problem of software reliability.

Response 1.2.16

Disagree. As indicated in Section 1.2.3 of the report, there is no consensus in the reliability community about how the reliability of software systems should be modeled, measured, and predicted, and even whether such a concept makes sense for software. Section 2.1.2.1 of NUREG/CR-6901 describes in detail the fundamental issues associated with the concept of software reliability. That is why NUREG/CR-6901and this report treats software as an entity embedded in hardware. As indicated in Section 2.4.4.1 of this report, the methodology used for quantification of the reliability of embedded software builds upon 20 years of research and is a well accepted methodology.

Comment 1.2.17

Software reliability has not been addressed. This is stated as challenge 3 on page xvii, which correctly states that “there is no consensus in the community on how software reliability should be quantified and, in fact, whether such a concept is appropriate at all.” While possibly allowing some comparison of reliability based on system architecture and complexity, the need for an integrated evaluation of software and hardware prevents the reliability models from being used in licensing activities.

Response 1.2.17

Agree in part. While this technical report is not a regulatory document and as such cannot comment on the suitability of the proposed approaches for licensing activities, the methodology used for quantification of the reliability of embedded software builds upon 20 years of research and is a well accepted methodology. *Also see Response 1.2.16*.

Comment 1.2.18

The software architecture was not modeled. There was some discussion on general software failure concepts and fault injection methods, the actual software used in the system being modeled was either not considered, or not discussed in this report.

Response 1.2.18

Agree in part. Please see *Response 1.2.16*

Comment 1.2.19

The following assumptions should be evaluated and corrected as appropriate for the final NUREG:

A. In the discussion of fault tolerant features, the watchdog timer is discussed on page 2-17. This discussion would lead to the understanding that in the presence of a software failure or other computer failure, the watchdog timer will not be reset, and would therefore announce the failure. In fact, only failures which result in the processor being stopped would result in the watchdog timer not being reset and therefore announcing software failure. Other types of software failure, such as an incorrect calculation or a jump over critical portions of the software, would have no effect on the watchdog timer.

B. In Table 2.3.1, “Abbreviated FMEA for the MC”, a failure of both sensors is shown as resulting in a worst case failure of the main computer, resulting in the backup computer taking control. In Figure 2.4.9, “Architectural View of the Benchmark DFWCS”, it is shown that the same sensors are used by both the main and the backup computers. Failure of these sensors would cause both computers to fail. It is only in the limiting case of the sensors operating correctly, and the fault being in the input portion of the main computer, where the backup computer would continue to receive correct sensor information and allow the backup computer to take control.

Response 1.2.19

A. Agree in part. There are numerous types of software failures that may result in a watchdog timer not being reset properly. It is correct to state that there are software failures that would not result in the failure to reset the timer, as well. As indicated in the comment, an inaccurate calculation in and of itself may not cause the watchdog timer to be reset. The watchdog timers are very rudimentary devices to determine if the CPU is "healthy." However, there are many other situations in which a watchdog timer will not be reset without a halted processor . For example, a runaway process that consumes fully the CPU would result in the watchdog timer not being reset. Also, incorrect interrupt handling may cause the watchdog not be reset without the CPU being stopped. Finally, simply an incorrect implementation may not always be able to complete in time due to unexpected load on the system. We have added a sentence in Section 2.2 to make this more clear.

B. Agree. While this failure mode is included in the model in Section 2.3, it was an oversight not to include the common modes within the Tables 2.3.1, 2.3.2 and B.1. These modes have been added to the tables.

Comment 1.2.20

The executive summary, pages xv - xvii, and the report summary and conclusion, chapter 9, could be misinterpreted in that each states that this study shows that digital systems can be modeled, and that the results can be integrated into an existing plant PRA. The limitations to this methodology are mentioned as possible challenges, but are not as prominent as may be desirable, and therefore potential users of this report may be lead to believe that the methodologies are sufficient for use in risk based licensing of digital systems for safety related use in nuclear power plants.

Response 1.2.20

Agree. The Executive Summary, Abstract and Summary and Conclusion chapter have been revised.

1.3 Suitability of Selected Methods

Comment 1.3.1

The 11 requirements underpinning the present work are inherited from the previous review of NUREG/CR-6901. Such requirements have limited the scope of the work to the DFM and Markov modeling methods. Possibly, a more comprehensive (and significantly larger effort) could have been to test all the possible methods considered in NUREG/CR-6901 on a benchmark system (the one described in this new report or even a simpler one), with respect to the 11 criteria chosen. This might have reduced the subjectivity of the selection of the fittest methods for the I&C digital control reliability problems under study.

Response 1.3.1

Agree in part. The authors believe that the requirements of NUREG/CR-6901 do represent the necessary features a methodology needs to have for the reliability modeling of digital I&C systems if this reliability model is to be incorporated into an existing plant PRA. However, the authors also agree with the need for benchmark that will allow a more objective selection of the fittest methodology. As was also indicated in NUREG/CR-6901, the selection of the Markov/CCMT and DFM as the methodologies of choice is purely based on the applications reported in the literature due limitations of resources. This report provides such a benchmark system.

Comment 1.3.2

I believe an evaluation by an different group may rank other methods such as simulation-based ones as or more likely to succeed as compared to DFM and/or Markovian-based ones.

One quantitative result to back up this claim can be produced simply by using Google, as noted below:

Search String	# Results
"dynamic flowgraph methodology DFM"	247
"Markov"	22,100,000
"Simulation"	273,000,000

Simulation is an order of magnitude more discussed/applied/researched/etc., than Markovian methods. DFM methods are far and away NOT discussed/applied/researched/etc.

For the NRC to "place all its (research) eggs in one/two baskets" such as DFM (unknown efficacy) or Markovian (rarely used in PRA, even though it has a 40 year incubation period) may not provided the intended outcome at the conclusion of the research/application/development.

However, this comments should be tempered with the fact that other methods such as simulation have associated complications themselves.

Response 1.3.2

Agree in part. As indicated in Section 3.1.2 of NUREG/CR-6901, simulation 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.

Comment 1.3.3

There needs to be more discussion on the "cons" of the proposed methods. For example, in the DFM discussion in section 3, the pros are discussed. However, when one gets to Figure 3.4.1, one limitation (as compared to fault trees) is evident in that the model is fairly intractable. Most engineers can follow the flow of a fault tree to divine the ways a system can fail and how it is modeled, but I suspect that an engineer would have a very difficult time understanding of the FM model (even upon much reflection). It is somewhat easy to catch errors in fault tree and event tree models, but again I suspect that many of the authors of the NUREG report would not be able to figure out simply by looking if the DFM model is "correct" or not. Note that this comment is just as applicable to the Markov approach since there we see bits and pieces of the model, but we do not see the big-picture and how all the parts fit together (or if they even do...).

Response 1.3.3

Agree. However, the authors are not aware of any promising alternatives with equal capabilities.

Comment 1.3.4

The product has a clear manner of communication, although it contains a number of errors/mistakes and needs a final proof-reading (example: the first line in 1.2.2, the first line in the first bullet in 8, etc.). It could have been better organized regarding the amount of information, which from time to time appears confusing. Admittedly, such problems are difficult to avoid.

Response 1.3.4

Agree. The document is proofread again in response to the comment.

Comment 1.3.5

I am not sure that I fully understand why the sole presence of digital systems would require more advanced plant models than the current PRA models. Such advanced models may very well be necessary, due to the complexity of the plant itself and the necessity to take into consideration aspects such as the physical process(es), the plant systems & equipment and their failures, the plant situations (normal and abnormal), human factors, etc., independently of the presence of digital systems. The choice of the plant safety model(s) being made, a subsidiary question is: "What 'parameters' should be used to represent the effects of digital systems in the model(s)?" For traditional PRA models, these parameters could probably be divided into three main classes:

- Parameters influencing the occurrence and frequency of initiating events. The influence can be detrimental: particular failure modes in particular plant conditions could lead to initiating events, either directly (e.g., a spurious actuation) or indirectly (e.g., incorrect or misleading information provided to operators). The influence can also be beneficial (and this does not seem to be addressed in the draft report): digital systems can provide advanced monitoring functions that could improve equipment reliability, or can provide advanced operator support that can reduce human errors.
- Parameters influencing the execution of mitigating actions after the occurrence of an initiating event. The influence can be direct (when the mitigating actions are performed automatically by the digital systems) or indirect (when the mitigating actions are triggered by the operators with the assistance of, or through, digital systems). The parameters are mostly the probabilities of specific failure modes in the specific context where each mitigating action is required.
- Conditional probabilities of failure (beta factors) between significant digital systems failures. These beta factors represent the coupling of digital systems through various interactions mechanisms (which are more extensive than the two types listed in page 1-2).

These parameters could be evaluated using models of the digital systems distinct and separated from the plant model(s). Since this subsidiary question is itself a very difficult one with little scientific consensus, my approach would be to make use of all information that is available regarding the digital systems. In particular, for highly critical digital systems, system designers and software programmers take great care in designing in so-called "defensive measures" to avoid or eliminate specification and design errors, to avoid or reduce conditions that could activate possible residual errors, and to prevent postulated components failures causing system failures. The analysis of these measures, together with a systematic typology of errors, could help the analyst in identifying the credible residual errors and system failure modes, and in providing more focused scoping contexts to probabilistic quantitative evaluations. Thus, it is important to have digital systems experts closely involved.

Response 1.3.5

Agree in part. A key premise of this comment is that stochastic behavior of the system is separable from controlled/monitored process. NUREG/CR-6901 has illustrated that this premise is not necessarily true for systems relevant to reactor protection and control systems. Section 2.5 of the report shows that the failure mode of benchmark DFWCS may be intimately related the timing of the failure of the components through the controlled process. While such connectivities are also true for the traditional analog I&C systems and separation is allowed under the current ET/FT approach to PRA, it is not clear that separation is still allowable under certain features of the digital I&C systems. For example, the revised Section 2.5 explains that position of the level and the magnitude of the other variables used by the controller (e.g., compensated level, level error) at a sampling point in time are no longer the same at the next sampling point. In that respect, timing becomes a key source of uncertainty within the context of Reg Guide 1.200 since it is a source of uncertainty where "the choice of approach or model is known to have an impact on the determination of PRA results in terms of introducing new accident sequences, changing the relative significance of sequences, or affecting the overall CDF or LERF estimates that might have an impact on the use of the PRA in decision-making." For the DFWCS under consideration in this NUREG/CR, this uncertainty partly originates from

the dependence of the DFWCS failure mode (i.e., LOW LEVEL or HIGH LEVEL) on the level as a function of system configuration (which is stochastic and cannot be modeled by traditional methods) but also partly from the discrete time nature of the digital controller. The cell-to-cell transition probabilities of the Markov/CCMT and decision tables of DFM account for such uncertainties through the discretization of the continuous controlled variables. In principle, the discretization may also account for delays in hardware response or inertia by choosing the cells large enough so that the system resides in the cells sufficiently long time. The issues related to the discrete time nature of the digital I&C systems introduce new uncertainties that are not simply "add on"s that can be separated from the uncertainties relevant to analog systems. Another point to keep in mind regarding the suitability of the conventional ET/FT approach for the digital I&C systems is that the tools to implement the conventional ET/FT approach (e.g., CAFTA, RISKMAN, SAPHIRE) are not designed to handle the non-coherence that may arise from the recuperation and multiplexing capability of digital I&C systems (see revised Section 1.1).

Comment 1.3.6

I am not sure that a single quantification method or technique would be suitable to all types of residual errors and failure modes. We will probably need to evaluate separately the potential for each residual safety-significant failure mode, focusing on those that are likely to dominate the various failure probabilities/frequencies and beta-factors of interest.

Response 1.3.6

Agree in part. The authors agree with the statement that a single quantification method or technique may not be suitable to all types of residual errors and failure modes. In fact, Chapter 9 (Summary and Conclusion) of the report states: “Finally, the properties of the benchmark system considered in this study may not apply to all the reactor protection and control systems in nuclear power plants. For digital I&C systems which may have less complex interaction between the failure events, the conventional ET/FT approach may be adequate for the reliability modeling of the system.” Section 1.3 of the report also addresses this issue. The authors do not believe, however, that the safety-significance of a failure mode can be necessarily inferred from the existing scarce operational experience with digital I&C systems in nuclear plants or an existing PRA which may not account for the type of dependencies illustrated in Section 2.5 of this report and discussed at length in Section 2.1.1 of NUREG/CR-6901. Also see *Responses 1.1.4* and *1.3.5*.

Comment 1.3.7

Table 5.4.2 shows over one million failed results for the first ten seconds. This is given the very significant simplification of the analysis (MC failed, FRV closed, Feed Pump is at a fixed speed, and only modeling one Steam Generator, etc.). Without the simplification the number of results would increase significantly and may fail the engine. Of further concern is that this only addresses the first ten seconds of a standard 24 hour mission time. There is no convincing analysis here that shows that the analysis method is viable if the system is fully modeled and consideration for how to cover a full mission time is included. The classification of failure paths noted helps in post-processing, but it is not demonstrated with a full system analysis.

Response 1.3.7

Agree in part. Please see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6* and *1.3.6*.

Comment 1.3.8

Section 6.2: The method for incorporating cutsets into SAPHIRE may not viable for CAFTA and RISKMAN - the dominant risk tools being used by the industry at this time.

Response 1.3.8

Disagree. Both CAFTA and RISKMAN have similar graphical and textual interfaces which should allow input in an analogous fashion as indicated in revised Section 6.2.

Comment 1.3.9

Page 9-1 & general: The problems with computational demand have plagued the proponents of Markov modeling for several decades. These models become unwieldy on large complex applications. I&C system designs have become even larger and more sophisticated in the meantime, especially with the advent of digital I&C. The example used in the NUREG (Digital feedwater control system, DFWCS - see other comments below to illustrate these points) is simple compared to other recent I&C system examples, such as a full system replacement or a new plant design. The NUREG repeatedly expresses difficulties with the model size for even this relatively simple example (e.g., page 5-38 notes "even for relatively shallow DETs there are a large number of possible scenarios"). There is no evidence in this NUREG to indicate that the problem of scale has been overcome.

Response 1.3.9

Agree in part. It is the authors' understanding that the NRC intends to test the proposed methods using a system similar to a recently proposed reactor protection system. Also see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6* and *1.3.6*.

Comment 1.3.10

DFWCS example (figure 5.4.4): In the case of the Markov example, the dynamic event tree (DET) is just an enumeration of every combination of every state of every component in the system. Enumeration of every failure combination is a brute-force methodology. Methodologies such as this have long ago been abandoned by the PRA community for more useful methods. (For example, a similar brute-force fault tree solution methodology, PREP-KITT, was used in the mid 1970s and it was very limited in its solution power; much more sophisticated and efficient fault tree solution methodologies have evolved since.) The difficulty with this is easily seen in the example. The number of failure states involved in just this simple 14-component example verges on being overwhelming - over 100 million combinations (page 4-13). This is reduced through simplifying assumptions to 76,800 combinations (before time steps are applied). In this case, the simplifying assumption is to combine the sensors with the computers (this would not be advisable in a full-scale application, because the sensors are often a point of commonality between functions). As has been proven time and again with

Markov methodologies, the results blow up exponentially as the number of components considered increases. It is this reviewer's opinion that this process would not work on any large application.

Response 1.3.10

Disagree. The statement that "...(DET) is just an enumeration of every combination of every state of every component in the system" is incorrect. The authors believe that Sections 4.3 and 5.4.1 sufficiently explain why the DETs in this study are not just an enumeration of every combination of every state of every component in the system. For example, Fig.4.3.2 which the DETs are partially based upon shows that there are a large number of impossible transitions (indicated by 0 in Fig.4.3.2) which are not considered in DET construction from the Markov/CCMT methodology results. Regarding "brute force," and "much more sophisticated and efficient fault tree solution methodologies", the analogy to PREP-KITT is incorrect. This report is not proposing a fault-tree methodology but rather how to perform an analysis using dynamic methodologies and incorporate the results into an existing PRA, as indicated in Section 5.1. The capabilities of dynamic methodologies cannot be duplicated by the fault tree methodology no matter how efficient a fault tree solution technique is (see NUREG/CR-6901). Methods similar to the dynamic methods presented in this report are used by the aerospace industry whenever there is a need as indicated in NUREG/CR-6901. Regarding "simplifying assumption is to combine the sensors with the computers", this is not an assumption but allowable representation scheme for the system under consideration. If the sensors are a point of commonality between functions, then we don't combine the sensors with the computers. Also see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6* and *1.3.6*.

Comment 1.3.11

Section 2.5 - Discussion of Compensated Level (pp. 2-73 to 2-75): The discussion with respect to Figures 2.5.4 through 2.5.6 describes the anticipation of steamflow / feedflow mismatch to the steam generator as a factor in the control of SG level. For the analyzed condition (e.g. low power / post reactor trip / control via BFV), I would expect the system design would revert to control using SG level only (i.e. a "single" element control scheme). This would be due to the low levels of steamflow and feedflow present that preclude good control stability for three element control in this region (due to the square root conversions of the steam and feedwater flows). This comment is based on my recollection of operational feedwater control systems with which I have past experience. It also emphasizes an important point in that is applicable to any modeling approach (including the conventional FT/ET approach or the approaches discussed in this report). This point is that the conclusions obtained are dependent upon the modeling assumptions and the extent to which the models accurately reflect the physical system and an essential element must include a validation of this fidelity.

Response 1.3.11

Agree in part. While the reviewer's recollection may be correct, the equations used in Section 2.5 for the analysis of the example initiating event are taken from the actual control algorithm of the DFWCS of an operating PWR. In that respect, there are no modeling assumptions in the representation of the DFWCS, Assumption 1-7 posed in the beginning of Section 2.5 refer to the example initiating event only.

Comment 1.3.12

Section 2.5 - Discussion of Failure Timing (pp. 2-75 to 2-76): The discussion of failure timing of the BFV "as is" failure (and subsequent time series plot displayed on Figure 2.5.7) indicates a bifurcation point occurs somewhere between 43s < t < 44s. The analysis of this sequence presented in this report does not provide enough depth to permit the reader to draw useful conclusions. In particular, since the model used is nonlinear, bifurcations of this type are possible. However, there are several key elements that require significant additional investigation before conclusions can be drawn.

- Since the result presented is based on a numerical simulation, the conformity of the model to operational data of actual system performance needs to be obtained and analyzed to ensure the model is an accurate representation of system behavior.
- For models of nonlinear systems, the behavior of the system near bifurcation points may be extremely sensitive to the values of both the model parameters and the system initial conditions. The authors provide no discussion of this, nor of how the model coefficients were selected (or of their accuracy).
- Based on the trace provided in Figure 2.5.7, prior to failure, the model indicated oscillations were damping out. However, the authors provide no discussion of the physical effects that would lead to the behavior. For example, since the level trace undergoes oscillations for all time t > 0, one could reasonable postulate that this particular failure could result in the observed behavior for any t > 0 with the outcome dependent solely on whether the failure occurred while the system was in an up trend (high failure) or down trend (low failure) portion of the cycle with the only difference being the time required to reach the high or low level state. Note that this will occur for all t > 0 in the model (since for nearly all times there will be some deviation between the setpoint and the control variable). But in the real physical system, after some time, the deviations become of the same order of magnitude as statistical fluctuations in the parameters and thus the system will not actually proceed to the high or low failure state.

- Finally, note that the same issues are inherent in the modeling and evaluation of this system if an equivalent analog control system was used. Thus, none of the discussion provided is unique to digital systems.

Response 1.3.12

Agree in part:

- While it is true that the system behavior is represented through a model, Eqs. (2.5.1) through (2.5.7) are taken from the DFWCS algorithm of an operating PWR (see revised Section 2.2.2), and subsequently are expected to be reflecting the actual operation of the DFWCS.
- As it is the case with the tuning of any controller, the model coefficients in Eqs.(2.5.17) through (2.5.21) were chosen so as to stabilize the level after a disturbance as has been demonstrated through Figs.2.5.2 through 2.5.6. However, all possible disturbances/times cannot be preconceived and an unforseen bifurication may occur, as it did in La Salle Unit 2 on March 9, 1988, and as has been indicated in Section 2.5.

- Whether the change in system failure mode originates from the failure occurring while the system was in an up trend (high failure) or down trend (low failure) portion of the cycle with the only difference being the time required to reach the high or low level state or due to a bifurication is immaterial since both have their origins in the sensitivity of system dynamics to the time of BFV failure, which is not exhaustively explored in the conventional FMEA (also see *Responses 1.1.5* and *1.1.6*.)
- For the differences in the issues for this event between the analog and digital systems, please see *Responses 1.1.3, 1.1.41,* and 1.3.5.

Comment 1.3.13

Section 3.2.1.1.1 - Discussion of DFM Benefits (p. 3-7): I agree conceptually with the discussion of the potential advantages of DFM over FT/ET methods. However, I believe the authors (1) overstate the benefits (e.g. there is a tradeoff in the advantages, particularly the potential versatility of the DFM approach, against the significant increase in model complexity and computational resources, (2) fail to discuss the additional data requirements which include the need for time dependent failure data necessary for model quantification and (3) fail to discuss that although it would be useful to have models that can evaluate multiple situations (top events), there is no requirement that models used to evaluate nuclear safety possess this feature.

Response 1.3.13

Agree. However, complex systems may require complex modeling methods. The authors believe that until we have sufficient operational experience with such complex systems, the most comprehensive modeling tools need to be used.

Comment 1.3.14

Section 3.5.2.1 - Tracing of Inductive DFM Model (pp. 3-20 to 3-27): The authors briefly mention how the analyzed event could be quantified. However, no quantification is performed. Thus, the authors do not demonstrate that one will obtain results that are accurate and defensible. Failure to perform and report results from an actual quantification also prohibits the authors from providing any conclusions or "lessons learned". Additionally, without a quantification and comparison to a similar analysis using conventional FT/ET techniques, a determination of the relative strengths and weaknesses of the two approaches cannot be performed and previous statements in the report of the need to replace the conventional FT/ET analysis approache remains an unsubstantiated conjecture. The authors should note these limitations, both here and in the conclusions (Chapter 9). Additionally, they should state that further research is being performed to perform quantification of results for the DFWCS system modeled here and other systems discussed in NUREG/CR-6901, and that any conclusions with respect to the necessity or applicability of these methods for nuclear safety evaluations of digital I&C systems presented in this report should be considered preliminary in nature.

Response 1.3.14

Agree in part. The Abstract, Executive Summary and Chapte 9 have been revised to reflect the fact that this report only constitutes a proof-of-concept study. Also see *Response 1.1.9.*

Comment 1.3.15

Section 3.5.2.2 - Quantification of Deductive DFM Model (pp. 3-23 to 3-27): The authors present two examples of how the process can be used inductively. Again, no quantification is performed. Additionally, the authors provide no discussion that similar results could be obtained using conventional FT/ET/FMEA techniques nor is any comparison attempted.

Response 1.3.15

Agree. Please see *Responses 1.1.9* and *1.1.39*.

Comment 1.3.16

Section 4.2.3. - Markov Model General Comment (pp. 4-5 to 4-15): The authors do not note that the Markov models are developed using and are dependent upon the results of the component level FMEAs and that this is similar to the process used to develop classical FT/ET models. Thus, just as in the classical approach, the Markov model only will be as accurate and robust as the underlying FMEA (or other qualitative method to identify applicable component failure modes and effects) from which it is derived.

Response 1.3.16

Agree in part. It is true that the Markov model will be only as accurate and robust as the underlying FMEA (or other qualitative method to identify applicable component failure modes and effects) from which it is derived. However, Section 4.2.3 does state that "The choice of the failure states is based on the FMEA tables presented in Section 2.3." On the other hand, although the ET/FT approach also uses similar FMEA tables, the Markov methodology has the capability to represent statistically dependent failure events while the classical ET/FT approach does not, as indicated in the revised Section 4.2.3.

Comment 1.3.17

Section 4.2.3. - Markov Model General Comment (pp. 4-5 to 4-15): The authors also do not present a discussion of how common cause failure mechanisms will be treated. (Note - in the remainder of the report, I could only find 4 instances of where common cause was mentioned (in the context of sensor common cause failure) but no discussion of how this would be quantitatively addressed).

Response 1.3.17

Agree. The revised Section 4.2.3 indicates that "software is not being treated separately but as embedded in hardware as indicated in Sections 1.2, 8, and throughout Section 2.4. In that respect, conventional common caused failure methods are applicable. For example, platform commonality can be accounted for using the beta factor method if data are available for system failure due to platform based failure modes."

Comment 1.3.18

Section 4.2.3. - Markov Model General Comment (pp. 4-5 to 4-15): The descriptions of the various Markov models and their underlying bases generally are concise and easily understood.

Response 1.3.18

None required.

Comment 1.3.19

Section 4.2.3.2 - Markov Model for FP (p. 4-6): This section is actually the Markov transition state model for the Feedpump Controller (FPC) (see corresponding FMEA Table 2.3.5 on pp. 2-24 to 2-25). (Mechanical) Failures of the Feedwater Pump (e.g. inadvertent trip) are not included here. This section should be revised for clarity.

Response 1.3.19

Agree. Mechanical failures are modeled through the relevant controller failing high or low (e.g. inadvertent FP trip). For example, an inadvertent pump trip is modeled through the FP controller failing low and an inadvertent BFV opening is modeled through BFV controller failing high. Both the general comments regarding Markov modeling of components in Section 4.2.3 and the section on controllers (Section 4.2.3.5) have been revised for clarity.

Comment 1.13.20

Section 4.2.3.3 - Markov Model for MC and BC (pp. 4-6 to 4-7): Here the authors note that for these components they are modeling at a supercomponent level. This is similar to approaches taken under similar conditions in a classical FT/ET approach. However, the authors do not note this, nor do they note that the resultant Markov model will possess similar limitations that a classical FT/ET model will have due to this simplification.

Response 1.3.20

Disagree. Although the classical ET/FT approach uses the concept of macro-components, the Markov methodology has the capability to represent statistically dependent failure events while the classical ET/FT approach does not. Also see *Responses 1.1.5,1.1.6* and *1.3.16*.

Comment 1.3.21

Section 4.2.3.7 - Number of Modeled States (pp. 4-13 to 4-15): Here the authors note that the number of component state combinations and the analytical approach was selected to reduce the size to one that is computationally tractable. However, even for this very simple system, the number of states that require evaluation (and supporting state transition estimates / data) is very large. Additionally, as the system complexity (e.g. number of components increases) and the corresponding model complexity grow, the number of component state combinations will increase geometrically. This fact will limit the potential utility of the modeling approach to very simple systems or simplified representations of complex systems.

Response 1.3.21

Agree in part. The example event was not selected to reduce the size to one that is computationally tractable but rather "...to provide clarity in illustrations..." as stated in Section 2.5. Also see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18* and *1.3.6*.

Comment 1.3.22

Section 4.3.5 - Quantification of Deductive DFM Model (p. 4-23): Similar to the note concerning model quantification in Section 3.5.2.1, the authors briefly mention how the analyzed event could be quantified. However, no quantification is performed. Thus, the authors do not demonstrate that one will obtain results that are accurate and defensible. Failure to perform and report results from an actual quantification also prohibits the authors from providing any conclusions or "lessons learned". Additionally, without a quantification and comparison to a similar analysis using the conventional FT/ET techniques, a determination of the relative strengths and weaknesses of the two approaches cannot be performed and previous statements in the report of the need to replace conventional FT/ET analysis approaches remains an unsubstantiated conjecture. The authors should note these limitations, both here and in the conclusions (Chapter 9). Additionally, they should state that further research is being performed to perform quantification of results for the DFWCS system modeled here and other systems discussed in NUREG/CR-6901, and that any conclusions with respect to the necessity or applicability of these methods for nuclear safety evaluations of digital I&C systems provided in this report should be considered preliminary in nature.

Response 1.3.22

Agree in part. Please see *Response 1.3.14*.

Comment 1.3.23

Section 5.4.2 - Example Failure Scenario Table 5.4.1 (pp. 5-36 to 5-37): In the discussion leading up to the example, the authors (correctly) mention the number of partitions and ranges selected for the process variables determine the level of modeling accuracy (see discussion on p. 5-34). They also mention (again correctly) that this represents a tradeoff between accuracy and cost / computational resource requirements. However, in my opinion, they do not sufficiently stress the importance of this aspect with respect to the need for verification of model results to expected physical system response. For example, in Table 5.4.1, from time t = 2 (sec) to t = 3 (sec), failure of the BFV controller causes level to decrease from a high to a low condition. Given the very short time (?t = 1 sec) and the significant inertia of the valve / system (large diameter air operated valve / high system pressure and large mass flowrate), it is questionable whether the model accurately reflects the actual valve and system dynamics. For example, in the discussion of minimum failure time, a consistency check should be that this time not be less than the actual physical stroke time of the valve. Although this does not impact the ultimate outcome of the scenario, it leads me to question whether the model outcomes and results have been evaluated for reasonableness based on the expectation of how the system would physically respond. I believe the authors should provide discussion to address this point.

Response 1.3.23

Agree in part. The DFWCS model equations are taken from the actual control algorithm of the DFWCS of an operating PWR and the outcomes are reasonable regarding the DFWCS design function of controlling the level at the specified setpoint as illustrated by Fig.2.5.5. The system inertia is not accounted for in the control algorithm and subsequently is not accounted for in their continuous time counterparts Eqs.(2.2.2) - (2.2.9) or (2.5.2) - (2.5.5). The system inertia is partially taken into account in Eq.(2.2.1) though the constant *A* which in Eq.(2.5.1) is taken to be1/109.0 ft^{-2} as shown in Table 2.5.1 and which corresponds to a maximum rate of level change of 140/109.0 = 1.28 ft/s when the MFV/BFV is fully open (see Fig.2.5.1). In principle, valve inertia can be taken into account through Eqs.(2.2.11) or (2.2.12), but was not due to lack of reliable data. The level change being referred to corresponds to a minimum BFV aperture change of 40%/s (i.e. difference in the high BFV position of S_{Bn}=30% at t=2 s vs. low BFV position of S_{Bn}=70% at t=3 s in Table 5.4.1). As indicated in the comment, whether this is too high or not does not impact the ultimate outcome of the scenario. Section 5.4.2 is suitably revised to reflect this explanation.

Comment 1.3.24

Section 5.4.2 - Example Failure Scenario Table 5.4.2 (pp. 5-37 to 5-38): In this table the number of scenarios appears to grow exponentially with time. A quick calculation using the data in the table confirms this. Thus, for any reasonable mission time, the method will need to quantify so many scenarios as to be totally impractical (if not impossible), even for this relatively simple model. As a quick estimate, extrapolating from the data in the table, after 10 min (only 1.2% of the typical PRA evaluated mission time), the number of scenarios ~ 10260. (Note that for advanced reactor concepts, this issue is exacerbated even further by the need to evaluate mission times much longer than 24 hours). The authors should provide a discussion of how much time needs to be run in the simulation to provide sufficient information to conduct an effective evaluation and how this evaluation should be performed.

Response 1.3.24

Agree in part. Please see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18*, *1.3.6* and *1.3.30*.

Comment 1.3.25

Section 5.5.4 - First Paragraph of Comparison Section (p. 5-43): See previous note to Section 2.5 - Discussion of Compensated Level (pp. 2-73 to 2-75). The dependence on steamflow / feedflow mismatch is true for power operations. However, for post-trip operations where SG level is the sole controlling variable, the conclusion presented is incorrect.

Response 1.3.25

Agree in part. Please see *Responses 1.3.11* and *1.3.23*.

Comment 1.3.26

Section 2.5 provides a relatively rigorous deterministic evaluation of steam generator level as a function of time for FW control system failure modes. One of the conclusions of this section is

that the exact timing of specific component failures can have an impact on the failure mode of the system. The timing of the failure of the FW bypass valve is given as an example, in one scenario the steam generator level rising and in the other scenario (with failure occurring only a second later) steam generator level falling.

Response 1.3.26

None required.

Comment 1.3.27

A discussion of common cause/mode failures has not been included. Some of these may be included in the "Design Fault" category, however, it is anticipated that a large component of this may be in the SW. The common cause failure of identical systems and processors should be addressed as this information is essential to the plant PRA risk assessment.

Response 1.3.27

Agree. Please see Response 1.3.17.

Comment 1.3.28

The NUREG/CR notes that large quantities of data are generated with minimal analysis. The value of this voluminous output as input to the Plant PRA appears limited. This is consistent with the authors' processing of the events down to 40 states; 20 up and 20 down. It seams that further refinement of this data could yield a manageable number of states that could be incorporated into the existing plant PRA models. Given that the authors propose processing this data partial in the PRA, with subsequent manipulation, and then re-insertion for quantification and uncertain analysis, it seems that a simpler approach could be employed. A comparison of results is required to demonstrate the greater accuracy or reduction of uncertainty.

Response 1.3.28

Disagree. Please see *Responses 1.1.2, 1.1.3, 1.1.12*, and *1.1.13*.

Comment 1.3.29

Section 2.5 includes an example implementation. Some of the identified model features raise specific concerns.

- Figure 2.5.7 and the associated text indicate that a valve failing "high" at 43 sec will fail "low" at 44 sec. Does this mean that the PRA must address sub-sec intervals so that the CS can be modeled properly? The ability to include this level of timing in the plant PRA would be problematic. The definition of time zero is not clear and how this would correlate with the Plant PRA Sequence is not known.
- Figures 2.5.8, .9 and .10 include control system anomalies (oscillations) at approximately 900 sec. This is used as a justification for the dynamic modeling. This is valuable information that is pertinent to the design of the system; however, again without

a better understanding of the phenomenon or interactions (which is not included) the inclusion of such items in the Plant PRA model would be problematic.

Response 1.3.29

Agree in part. It is true that without a better understanding of the phenomena or interactions, the inclusion of items such as timing issues in the plant PRA model would be problematic. The dynamic methodologies under consideration are doing precisely that within the context of PRA. In view of the research to date on the modeling of Type I and Type II interactions (Section 1.2.2) and the features of the digital I&C systems relevant to nuclear power plants (Section 1.2.1), the authors do not believe that it is always possible to analyze the stochastic and deterministic behavior of the digital I&C systems with regard to their quantitative impact on PRA. A careful FMEA may yield information regarding their qualitative impact, however, such a PRA would amount to the analysis required to generate the cell-to-cell transition probablities of Markov/CCMT or the decision tables of DFM (see *Response 1.1.5*). Regrading the practicality of dynamic modeling, they are not intended to be applied to the whole PRA, but only to selected systems. That is why Chapter 6 illustrates the mechanics of incorporating a dynamic model to the existing PRA. In the incorporation process, one way of coupling quantitative information regarding plant dynamics to a qualitative event would be to branch out the qualitative event in terms of the conditionals present in the dynamic analysis. For example, the trajectory bifurcation in Fig.2.5.7 could be represented as a 2-branch event, conditional upon the timing of BFV failure as illustrated in Fig.6.3.1 of the revised Section 6.3.

Comment 1.3.30

The methods used for reliability modeling of digital I&C systems, although they worked well for the sample problem, may not work well for larger, more complex systems. At least superficially, it would appear that the computer time needed to solve the problem increases with the size of the problem at a rate greater than any polynomial in an index of the size of the problem (that is, the problem belongs to complexity class NP). An analogous situation is the solution of non-coherent fault trees. If it turns out that the number of component states must be increased in order to model the system faithfully , then this exacerbates the problem. It is possible, but not certain, that probabilistic methods of solving the problem (Monte Carlo methods) may be helpful here.

Response 1.3.30

Disagree. The problem is not NP for the Markov/CCMT methodology because the DETs are terminated if: a) scenario time exceeds system mission time, b) controlled/monitored variables fall outside allowed ranges (i.e. system fails), c) scenario probability falls below a user specified number, and, d) if the system is restored to its nominal state (see revised Section 5.4.1.1). It is a non–issue for DFM, since it searches possible paths between specified initiating events and consequences (Chapter 3). Furthermore, neither methodology is intended to be used for the full PRA (see *Responses 1.2.36*, *1.3.29*, *4.4,* and *4.5*).

Comment 1.3.31

There is limited discussion on how well the methodologies "scale up." The conclusion

that It may be possible to meet most of the challenges by linking current event/fault trees to dynamic methodologies through new interfaces and distributed computing does not suggest a practical application of the methodologies in the short term. Actual digital systems to be modeled are significantly more complex.

Response 1.3.31

Agree in part. Please see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6, 1.3.6,* and *1.3.30.*

2 Data Collection and Generation

Comment 2.1

The problem of reliability data seems not to have been dealt with in sufficient depth, albeit the recognition of being very relevant

*Response 2.*1

Section 2.4 was revised to address sources of data uncertainties and possible resolutionary measures. Data uncertainty is also addressed in Section 7.1.

Comment 2.2

Page 2-28 first paragraph: The quoted statement "...it's functions in a manor that does not compromise the safety of the ? Associated with the system..." may be out of context. Can you provide the complete sentence or paragraph so that I can confirm usage and proper reference? The missing word where the ? Is important.

Response 2.2

Agree. The missing part is "...safety of any people..." and is corrected in the revised Section 2.4.2.1.

Comment 2.3

Page 2-28 first paragraph: When describing the third state of the model, the term "its function" is used. I think that this usage is too vague. Digital systems typically perform many functions which can be classified into many categories. Some are CRITICAL, while others may be SAFETY, and still others are inconsequential. For a failure mode to qualify as a Fail Unsafe mode, the systems specified SAFETY function is what not being performed.

Response 2.3

Carl

Comment 2.4

Page 2-28 second paragraph: I'm not sure how one would quantify term Rate at which the Failure occurs or Failure Transition Rate. Fault injections and system responses are generally instantaneous (< 1 second). There does not seem to be any guidance on this..

Response 2.4

Agree. Failure rate is the expected number of failures of a type of device or system per given unit of time. Failure rates are usually estimated from field data, life testing methods, and vendor component databases. Fault injections do not estimate or approximate failure rate data.

The purpose of a fault injection test or observe the systems "response" to a simulated failure of interest - e.g. the fault injection. Section 2.4.4 has been revised to respond toi the comment.

Comment 2.5

Page 2-28 second paragraph: General comment - Non-Safety Related control systems, by definition, do not have an "Unsafe" state though they can contribute to the probability of an unsafe condition occurrence or to the severity of an unsafe condition. This is just my perception. I'm not a PRA guy so you may be able to just explain the wording to me.

Response 2.5

Agree in part. It is true that the DFWCS is not a safety critical system. However, we assume for the purposes of this report that an undetected error caused by a fault is unsafe. We have changed the semantics of the unsafe state to a undetected or uncovered error state. This semantic more appropriately reflects the non-safety aspect of the system. Of course the consequences of a undetected error can have impact on the safety of the plant, however, that must be taken into account by the overall PRA. See Section 2.4.4

Comment 2.6

Page 2-29 First paragraph: The first step toward this process is; (1) deciding what are the appropriate failure modes to represent, and, (2) are they inclusive and complete. This implies that the first step in the process is to make an inclusive and complete list of failure modes for the system. I contend that it is not possible to create a truly "inclusive and complete" list of failure modes for a digital system. Even the most basic of digital systems contains thousands of potential failure modes and there may be several variations of each of them. At best, we would be able to compose a list of potential failure types or categories which encompass the majority of credible failure modes that can occur to the system. It is just not possible to identify all failure modes..

Response 2.6

Agree in part. The observation that a digital system (programmable) could manifest a large number of failures (potentially infinite) is essentially correct. Finding a inclusive and complete list of all failure modes and causes would be infeasible. However, enumerating the classes of potential failure modes that would be important to and appropriate for a specific PRA is feasible. This is what we essentially mean when we say "inclusive and complete". We are trying to be inclusive and complete with respect to the classes of failures as defined by a FMEA or generalized failure mode taxonomy. See Section 2.4.3.2 for a clearer definition of the fault injection domain.

Comment 2.7

Page 2-31 first line: Should there be a distinction between the "Unsafe Undetected" Failure mode state and the "Unsafe Detected" state? It seems that these are two very different paths which will have different probabilities of occurrence. Should the Markov model be expanded to reflect this?.

Response 2.7

Agree. The underlying assumption is that a detected error by the DFWCS initiates the proper recovery or mitigation action. Thus, we assume in this analysis that detected errors do not lead to a unsafe state. On the other hand, it is certainly feasible that undetected errors may lead to failures that do not adversely affect the safety of the plant. For the sake of conservative and cautious engineering judgment, we assume that a undetected error is unsafe. The assumption that a detected error will initiate a proper mitigation action could be relaxed to include the recovery or mitigation coverage. That is, given that a detected error has occurred, what is the probability the recovery action will be successful. See Section 2.4.4 has been revised to respond to this comment.

Comment 2.8

Section 2.4.4 Modular Markov Chain Modeling of the DFWCS: At some point you should spell out Digital Feedwater Control System. Other plants may not be familiar with this acronym..

Response 2.8

Agree. The acronym has been defined in the Abbreviations section.

Comment 2.8

Section 2.4.4: Replace the term "PID controllers" with OCS or Operator Control Station. The PID stands for Proportional, Integral, Derivative control and these devices do not perform these functions. The OCS term more accurately describes the functions of these devices. This comment applies to Figure 32(5) as well..

Response 2.8

Agree in part. The PID controllers essentially act as "checker" or "monitors" for the computed commands from the control computers. In the DFWCS. These checkers are implemented using programmable PIDS. The PID nomenclature is carried forward from historical documentation of the system.

Comment 2.9

Section 2.4.4 third sentence from the end of the first paragraph: Replace "fails operate" with "transfers to a tracking mode of operation" to more accurately describe the system response.

Response 2.9

Agree in part. “Fails operate” is removed.

Comment 2.10

Section 2.4.1: The limits of faults injection with respect to safety & reliability quantification should be highlighted alongside its merits. Though it may help determine the digital system behavior in the presence of certain types of faults, I don't think it can satisfactorily address specification or design faults.

- Fault injection is unlikely to help us assess the potential for incomplete or incorrect specifications, and we have to remember that experience shows that specification faults are the dominant cause of systematic failure for highly reliable digital systems.
- I also doubt that injected faults can really represent the range of possible design faults.

Response 2.10

Agree. We have always maintained, and we should state more clearly, that fault injection is but one crucial technique in a comprehensive framework for dependability assessment. Fault injection has it's limitations. It does not represent design flaws, specification flaws very well, or at all. We advocate contemporary design assurance and fault avoidance methods, such as, formal specifications analysis, model checking, and dynamic code analysis methods to minimize the impact of design faults. However, it is generally accepted and demonstrated that fault injection methods are useful in finding design flaws in fault tolerant systems. Fault injection stresses the error detection mechanisms (both SW and HW) of a fault tolerant system. In most fault tolerant systems, anywhere from 15% to 50% of the resident binary code or hardware resources on the machine is dedicated to Fault Detection, Isolation, and Recovery (FDIR) functions. This code is rarely exercised in the real world because failures, off-nominal conditions are infrequent. Fault injection is specifically designed to exercise and stress the FDIR mechanisms of the system under a variety of conditions - both nominal and off-nominal. We have a number of experience reports from academia, industry, and government where fault injection has found design flaws in the fault tolerance mechanisms of computer based safety critical systems. While fault injection has its limitations, and these are well-known, we view it as a natural partner to contemporary design assurance techniques, testing and fault avoidance methods. Sections 2.3 and 2.4 have been revised to incorporate these remarks.

Comment 2.11

Section 2.4.2: I don't think that a digital system failure is always associated with the system being in a failed state. Of course, most hardware failures and many software failures (e.g., deadlocks, overflows or divisions by zero) clearly correspond to failed states. For failures resulting from incorrect or incomplete specification, this is a different story: the same system behavior can be interpreted as appropriate and correct in certain plant situations, and inappropriate and incorrect in other situations. In such cases, a failure is not intrinsic to the digital system: it is a combination of system behavior and plant situation.

Response 2.11

Agree. The occurrence of failure due to an underlying fault in the computer based I&C system is manifest iff the plant and the control interactions activate the fault and propagate the error, and produce the failure. For instance, if a certain memory location that holds a non-zero variable is corrupted to zero or a negative value the fault is only activated when the processor fetches the value and uses it in a computation. Thus, it is important in fault injection campaigns

and for that matter all types of testing to vary the workload and plant conditions to stimulate these conditions. Context is important. In our methodology, we use a several methods to address this problem. First, we generate a fault list that will cause a specific failure mode to occur. This is called malicious fault list generation. See reference xx in the report and section xx of the report. The idea is to use backward inference and tracing through the hardware and software execution of program to produce a tree of possible fault corruption locations wrt to the timing of the program. Secondly, we vary the input conditions of the computer under test. These, may ramping from one mode to another mode, off-nominal conditions, out of range conditions, etc.... Third, we use real input data from various operating scenarios. Taken all together, these methods attempt to create a realistic representation of the system operating conditions, that is, it gives context to the testing. Sections 2.3 and 2.4 have been revised to incorporate these remarks.

Comment 2.12

Section 2.4.2.2: I don't think that the fault injection approach described here can help us evaluate the likelihood of being in an undetected unsafe failure mode. First, let's be more precise in our terminology:

- Fault: a defect, a "bug".
- Deviation: deviation from the intended behavior; it's not necessarily a failure, if the deviation remains within acceptable limits; in software, some deviations have no or little visible effects on overall system behavior
- Failure: the system does not provide the expected service

In many cases, "fault injection" really means "injection of deviations" (e.g., changing a value internal to the digital system), not "injection of design or specification faults". Injection of deviations may help us evaluate the effectiveness of surveillance, healing or tolerance mechanisms, once a deviation has occurred. (Even for this task, it remains an imperfect tool since it will not help for specification faults, and will not properly cover the range of possible design faults). It will not help us evaluate the likelihood of deviations occurring. Injection of design or specification bugs is very unlikely to be representative of residual bugs, since these residual bugs are precisely what the designer didn't think of.

Response 2.12

Agree in part. In general, fault injection does not inject design errors or specifications errors into the system. We agree that the injection of residual design errors into the system to test the system response would not be the most productive use of fault injection. In this work we do not inject or emulate design and specification errors of the system. However, If one wanted to evaluate the effectiveness of a test suite or procedure designed to detect certain design or specification flaws, then some form of "failure" injection based on code modification or mutations may be appropriate. Section 2.3 has been revised to incorporate these remarks. Also, see *Response 2.10.*

Comment 2.13

Section 2.4.3: I think digital failures are much more subtle than what is implied by figure 2.4.2:

- We may need to distinguish the different possible failure modes, because different failure modes may lead to different consequences. For example, let's consider a digital protection system, the output of which is a single Boolean protection signal. Since a simple hardware watchdog raises the protection signal in case of timeout, two failure modes need to be considered: the signal is raised spuriously, or the signal is not raised when plant situation demands it.
- As previously said, failure is not always an intrinsic state of the digital system, but a combination of system behavior and plant situation.
- The λ(t)-s and the C(t)-s may depend not only or not necessarily on time but also on plant and digital system conditions
- I am not sure that failures are either safe or unsafe. If we take the previous example, a spurious actuation during normal plant operation is not as unsafe as a failure to actuate, but it still has safety significance. On the other hand, failures occurring only when there is no nuclear fuel can be viewed as truly safe failures.

Response 2.13

Agree in part. Figure 2.4.2 is used to define the terms fault, error, and failure. Depending on the community, these terms take on different meanings. The safety critical systems community, the dependable systems community, fault tolerance community and certain standards organizations (IEC and I believe IEEE) have has adopted the definitions given with respect to Fig.2.4.2. Figure 2.4.2 does not imply that there is a single failure mode for a digital system. Perhaps changing the word failure to "failures" or "failure modes" would be better. In fact there are countable infinite failure modes. All of the terms fault, error, and failure should be interpreted in plural form. Looking at the definition of "failure", a deviation from expected service implies that a failure mode is function of environment conditions, plant state, and digital controller state. Changes to Fig.2.4.1 incorporate these remarks.

Coverage is defined as the conditional probability that a failure or fault is detected/recovered given that a fault has occurred. The detection and recovery of a fault can be dependent on the workload of the computer. The workload of the computer in control applications is plant dependent. We discuss the importance of workload for fault injection and coverage estimation in revised Section 2.4.4. Also see *Responses 2.5 and 2.7.*

Comment 2.14

Table 2.4.2: No demand failure probabilities are used. A significant portion of a demanded failure components failure probability is due to "shock" failures and is independent of the hourly failure rate associated with degradation. The industry will need standard estimates for these failures if accurate digital modeling is to be performed. The degree of uncertainty in these failure probabilities is as significant as the modeling methods.

Response 2.14

Disagree. First, we will address the uncertainty issue. Hardware failure data (from databases, vendor specific databases, and actual failure data from plant operations) for I&C systems, components, and microelectronics have a measure of uncertainty associated with it. This has

been known for many years. The issue at hand is to understand: (1) how this uncertainty effects the system failure probability, and (2) how to account for the uncertainty in modeling process. They are established and accepted methods used by the reliability community to deal with uncertainty in failure rate estimates (see Section 2.2.4). The reviewer asserts that failure rate uncertainty is at "high levels". We are not sure that assertion can be generalized. Most computer based safety critical I&C systems are fairly conservative in their use of technology and design. As a result, the failure rates for the chip level components systems are low. It is not uncommon for the mean time to failure of contemporary embedded microprocessors chips, FPGA's, memory devices to be on the order about 500,000 hours of operation before failure or greater. Bottom line, the reliability of contemporary microelectronics is exceedingly high. The variance of the MTTF of most chip level devices is small compared to the mean, on the order 10,000 hours or so. See Section 2.4.4 on failure rate estimations.

On the other hand, failures due to software flaws or design defects in computer based I&C systems are difficult to estimate apriori. This effort does not address the estimation and uncertainty analysis of software or hardware design flaws in computer based I&C systems. See *Response 2.10* for more detail. Design assurance techniques, formal methods, fault avoidance techniques a more appropriate methods to deal with design defects (see Section 2.4.3).

Comment 2.15

Section 2.4.7: This reviewer has insufficient knowledge to understand the impacts of the researcher's inability to generate "Symbolic" information. It is stated that this required using assembly instructions. The document does not state how this impacted the viability of the remaining analysis. The reviewer does not have sufficient knowledge of the software coding issues to determine the impact of this work around and the NUREG does not state what impact this has. How this impacts the results and uncertainties should be directly noted.

Response 2.15

Agree. We have revised Section 2.4.5 to respond to this comment.

Comment 2.16

The primary uncertainties with the approach are described in the NUREG, i.e., computational demand, and data to support the calculation. What is not clear is whether these uncertainties can be overcome. Therefore, there is considerable uncertainty as to whether the research can produce usable results.

Response 2.16

Disagree. As stated in Response 2.14, the uncertainties with regard to failure rate data do not appear to be considerable. The safety critical systems community has been using the methods described in the document or similar to those for a number of years across a variety of applications to produce tractable results. See Section 2.4.4

Comment 2.17

DFWCS Example (Table 5.4.1): An example "dynamic" failure scenario is presented in more detail (this is just one of the one-million-plus scenarios discussed above), and it is difficult to see the relevance of this failure scenario to a PRA. In the example, the hypothetical controller failure mode is that it starts generating arbitrary outputs (but the outputs stay on scale), the failed output alternates between an arbitrary high and low value. Then there is a failure of the controller to communicate with the valve, and the valve continues in the direction of the last known command (in this case closed). What are the failure probabilities for this hypothetical changing of state between high, and low, and then off? How can they be quantified? Quantification of this scenario (page 2-59) requires partitioning of the controller's failure rate into the various states (e.g., arbitrary output high, arbitrary output low, off) and determining probabilities for the state transitions. In this particular example, a uniform fault distribution is assumed for all of the failure states (i.e., all failure modes have equal likelihood) and they are assumed to change from state to state randomly from time step to time step. Even if realistic probabilities could be assigned to the different states and to the transitions between these states, and if the sequence in this example is even credible, it is difficult to envision why this level of detail is necessary. Quantification of the total probability of failing closed within 10 seconds requires combining this sequence with the other million-plus scenarios that cause the valve to fail closed. This process requires substantial computation for no apparent benefit. In the end, the model is no better than the probabilities assumed for its inputs. In a conventional fault tree model, all these one-million-plus scenarios could be one simple basic event called "valve closes spuriously," which can be assigned a probability from a generic database or plant-specific experience.

Response 2.17

Agree in part. The revised Section 2.4 shows how the data to different failure modes can be generated. Also, see *Responses 1.112 - 1.1.14, 1.1.17*, and*1.3.6*.

Comment 2.18

Section 2.4.2 - Discussion of Faults / Errors / Failures (pp. 2-41 to 2-42): I agree with the paradigm Faults ' Errors ' Failures. However, I do not think the linkages to physical / information / external universes makes a great deal of sense nor is it presented well. For example, is the viewpoint being taken that of thermodynamics (e.g. system and environment with an interaction between them) or is something else intended? I also think the emphasis the authors provide for the purpose of fault injection (testing) is incorrect. The purpose of a fault injection "campaign" is to validate the operation and capability of the FDIR software; its purpose is not to validate the applicability or fidelity of the model (although data gathered from this testing can be used to support this goal).

Response 2.18

Disagree. The linkages between physical, information, and external universe is an abstract point of view. Basically, the physical represents the hardware of the system. Semiconductors, microelectronic devices, power supplies, data distribution networks, etc... Thus, a fault is physical defect or alteration of a component. The second universe basically represents the execution behavior of the digital system. Because execution of digital system is carried out on units of information, we call it the information universe. Errors occur on data words within the

computer, instructions, or transmission of information from place to another. The external universe (or users universe) is where the user or another system see's the effect of faults and errors. This where failures manifest, failure is any deviation from the expected or desired service/behavior of the system. Fault injection provides the data to the models that will validate the capability of the FDIR mechanism. These remarks were reflected in the revised Section 2.4.3

Comment 2.19

Section 2.4.4 - Discussion of Model Based Testing (p.2-44): The authors imply that for digital I&C systems, a model based testing approach is needed. However, they do not provide sufficient information to justify this claim. In particular, there is only superficial description of why current practices are not sufficient (i.e. lack systematic engineering methodology, inadequate tool support). Based on the use of digital I&C systems in critical applications in other industries, if this were true, one would expect a significant number of events due to failures of the digital systems would be reported and the respective regulatory authority (e.g. FAA, etc.) would require application of a model based testing approach to reduce these events.

Response 2.19

Agree in part. While notable industries have adopted the model based approach to dependability assessment, including the avionics and airframe industry, railway, security, and certain biomedical industries, Section 2.4.4 has been revised to respond to the comment.

Comment 2.20

Section 2.4.7.6 - Data Collection (p.2- 67): The first sentence refers to "Figure 1" showing a data dump interconnection. There is no such figure close to this page and it is not clear if this refers to a previous or subsequent figure.

Response 2.20

Agree. Corrected.

Comment 2.21

Section 2.4.7 - Experimental Design: General comment - this section provided a good description of the experimental approach selected and the bases for it. This represents a strength in this report.

Response 2.21

None needed.

Comment 2.22

Section 2.4.8 - Preliminary Conclusion: Several comments with respect to these conclusions (pp. 2-67 to 2-68):

- Conclusion 1: I think the authors need to be clear here in the purpose of having a "predictive model". For the purpose of regulatory decision-making (i.e. acceptance of installation and use in a safety related or risk-informed application), the model only needs to demonstrate that the anticipated system failure modes, frequencies and consequences are acceptable (for example, they are no worse than that of a corresponding acceptable analog system). With respect to use of the model as a predictive tool, this is not required, but could be desirable for use by plant management as an early detection mechanism to alert responsible personnel to degraded performance at an incipient stage.
- Conclusion 2: This is very poor English (it is not a sentence). I interpret the intent to be, "The method is applicable to …"
- Comment 5: To me, this is written to indicate that actual fault injection experiments will be conducted at an operating commercial nuclear plant. Is this true, or is the experiment to be conducted on a mockup system? If applied on the operational DFWCS, it appears there may be an inherent contradiction between the concern on the safety impact of digital I&C system failures (on the one hand) and the plan to run the experiments that inject faults into an operational system where an unanticipated error (either in the digital I&C system or the testing procedure) could result in a loss of feedwater event.

Response 2.23

Agree. The referred section has been revised to respond to the comment.

Comment 2.24

Section 2.4: What is not clear from this section is:

- How fault injection is related to plant conditions that presumably would cause these faults
- How the combination of hardware failure rates and fault coverage represents system reliability (referring to the definitions provided in section 2.4.2).

Response 2.24

Agree. Section 2.4 has been revised to respond to the comment.

Comment 2.25

Even with the additional discussion of fault injection provided in this section, it is still not clear how it is appropriate for the development of failure rates to be assigned during accident sequence quantification. The approach proposed by this draft NUREG appears to be directed largely at modeling hardware and its failure modes. While not stated, the effects of software failure would appear to be represented by fault coverage. The conversion of dependability to a failure probability is not described and, as it is at the system level, how the dependability results are assigned to basic events is not clear. Explicit representation of software is not a part of the

proposed approaches. As a result, there does not yet appear to be a means available to capture the effect of common software failures in redundant systems with these techniques. The comment regarding uncertainty should be expanded to recognize that many of the qualitative insights important to the outcome of a nuclear power plant PRA that can be derived from a dynamic analysis can also be derived from other probabilistic and deterministic approaches including fault trees and FMEAs.

Response 2.25

Agree in part. While explicit representation of software is not a part of the proposed approaches, software failure is included in coverage. Common mode software failures in redundant systems (e.g. platform based) can be captured with coverage since system failure due to common mode is also part of uncoverage. Section 2.4 has been revised to highlight this point. Regarding insights important to the outcome of a nuclear power plant PRA, please see *Responses 1.1.2, 1.1.5, 1.1.6*, and, *1.18*.

Comment 2.26

The document provides the details of methods to determine the 'Dependability" of the Control system. It appears that this is the metric that is tied to the failure probabilities in the PRA. The translation of the dependability to failure rate that can be assigned to a basic event is not discussed. Sections discussing the connection to various PRA models (specifically SAPHIRE) do not address how this will be accomplished. The work appears to focus on HW especially with the failure injection. The NUREG/CR documents that the treatment of SW is not settled. It is understood that this is problematic; however, it must be addressed.

Response 2.26

Agree in part. Section 2.4 has been revised to include the translation of the dependability to failure rate that can be assigned to a basic event. Regarding software reliability, please see Response 2.25.

Comment 2.27

In development of the model with the use of fault injection, coverage of the Type I faults is well documented. However, it is not clear how the Type II (communication) faults are captured in the analysis.

Response 2.27

Disagree. Type II faults are part of uncoverage. Section 2.4 has been revised to respond to highlight this point.

Comment 2.28

The acceptability of failure data has limited justification and is recognized by the report as a significant limitation to the methodologies presented. The applicability of generic failure data and its applicability to various digital systems is also a limitation in the modeling presented and

is not discussed in the report. This is especially true for software, which is not specifically included in the models.

Response 2.28

Agree in part. However, the data challenge is not specific to the methods described in this report but to all existing methods. the data challenge is not specific to the methods described in this report but to all existing methods. Chapter 9 has been revised to highlight this point.

Comment 2.29

The acceptability of the fault injection technique to provide failure data generation is implied by the report. However, practical limitations in its application to digital systems look to be significant in time, scope, generic applicability, modeling, and number of fault tests required. Although this method is presented as a means to generate needed failure data, the fault-injection portion of the report is not necessary to demonstrate the report's digital system modeling methodologies. Based on this, it is suggested that the fault injection portion of the report be presented/treated separately.

Response 2.29

Agree in part. Section 2.4 has been revised to clarify that fault injection is one possible and not the only way to generate the failure data. However, the author's also believe that data requirements are also part of the modeling methodology and the description of at least one possible procedure to generate the needed data has to be resented as part of the proposed methodologies.

3 Benchmark System

Comment 3.1

While in the background information the reasons for the potential failure of ET/FT methodologies are given explicitly (interaction with a process, memory of sequential circuits, multitasking, process future states anticipation)), leading to the definition of Types I and II interactions, there is a lack of explicit connection to these in the successive benchmark problem; in other words, it would render the benchmark more effective if its characteristics were explicitly and directly associated with the peculiar aspects indicated as relevant for the digital I&C.

Response 3.1

Agree in part. The authors believe that such references for every benchmark DFWCS characteristic indicated in Chapter 2 would impair the readability of the report. Chapter 8 was included in the revised report to make this connection.

Comment 3.2

Executive Summary - Last paragraph p. xvii: The report authors acknowledge that the techniques were applied to a complex system and that the conventional ET/FT approach may be sufficient for other applications. What is not mentioned is that the chosen application (i.e. digital feedwater control) is applicable to a non-nuclear safety system for which regulatory review for plant installation is not required (and numerous installations have been performed both in the US and internationally).

Response 3.2

Agree in part. However, the author's believe that the concept of a safety/non-safety system may not be applicable in the PRA domain. In principle, all failures may contribute to CDF and LERF. In that respect, it is difficult to decide on the risk importance of a system prior to performing the PRA with the best available tools.

Comment 3.3

Section 2.3 - Discussion of system operation under abnormal conditions: The FMEA's appear to be comprehensive and well executed. However, the discussion does not provide any comparison to the similarities and differences to corresponding analog systems that are in use at operational nuclear plants. In particular:

- Section 2.3.1 - Discussion of MC /BC failures (p. 2-20): The discussion of the potential impact of simultaneous failures of the MC and BC is accurate. However, it is not mentioned that these failures are similar to but do not appear to be as significant as a master controller failure in a conventional analog feedwater control system (due to the system design for the MFV, BFV and FP controllers).
- Section 2.3.2 - Discussion of MFV / BPV / FP / PDI (digital) controller failures (pp. 2-22 through 2-26): The discussion does not mention that the impact of these failures is

similar to failures in the corresponding components in a conventional analog feedwater control system.

Response 3.3

Agree in part. Please see *Response 1.3.5.*

Comment 3.4

Section 2.3.3 - Discussion of EMI induced communications errors (p. 2-27 first full paragraph): This discussion does not acknowledge the fact that current analog systems are subject to EMI induced errors also. Nor is there any mention of the controls currently in place to limit the potential for these events or to compare the possible differences (in terms of occurrence frequency and event impact) between digital and analog systems.

Response 3.4

Agree in part. Section 2.3.3. has been revised to acknowledge that there is regulatory guidance to reduce the likelihood of EM interference. However: a) the extent to which the digital and analog systems are affected by EMI is not the same (e.g. a bit flip cannot happen in an analog system), and, b) existing controls for the prevention of an event does not mean that it will not happen.

Comment 3.5

Section 1.2 identifies failure modes of hardware/software/firmware systems that may be coupled through the process being controlled (Type I interactions) or through communication among components within the system (Type II interactions). Given a combination of current digital system design processes and regulatory requirements, the identified failure modes would not appear to be applicable to digital systems installed in critical applications within a nuclear power plant. For each failure mode listed in Section 1.2, the report should include examples of applications and/or systems currently found in nuclear power plants that would be expected to have these characteristics.

Response 3.5

Agree in part. Such examples were provided in NUREG/CR-6901. However, complete categorization of all the systems in nuclear power plants is outside the scope of this report.

Comment 3.6

Section 1.2.3 provides a list of characteristics desirable in methods used to model digital systems. Expanding the discussion to provide the rationale for these characteristics is desirable as not all are intuitive (nor can the basis necessarily be found in NUREG/CR-6901). For example:

1. The model must be able to predict encountered and future failures as well. (I assume this means that the resulting failure probability and dominant contributors should be

representative of failure modes that have not yet occurred in addition to historical experience).

2. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones. (The definition of 'fails a safety check' is not clear. it is assumed that what you are after here is the change in success criteria resulting from a failure).
3. The model must be able to differentiate between faults that cause function failures and intermittent failures. (It is assumed the key word in this characteristic is 'intermittent'. A statement as to when intermittent failures are important to the system would be of value here).

Response 3.6

Agree in part. However, these requirements were taken from the literature and an explanation is provided in the literature cited in NUREG/CR-6901.

Comment 3.7

The benchmark problem should be modified such that the focus of the analysis is the manual portion of the FW control system and/or any automated controls which are actuated in preference to normal FW control. The level range over which the FW control system is considered to be successful should be consistent with that typically assumed in nuclear power plant PRAs.

Response 3.7

Agree in part. Please see *Response 1.3.7*.

Comment 3.8

Section 5.2: Up to this point in the draft NUREG, the modeling has been directed at the FW control system. However, this section provides a detailed description of the AFW system. In most nuclear plants, FW control is a balance of plant control system while AFW is actuated by an ESFAS (often classified as safety related). These are typically two independent systems (with the possible exception of selected supporting systems). In addition, the written description of this system appears to be inconsistent with the line diagrams and fault trees presented in the report (e.g., contrary to the last sentence on pg 5-10, AFW actuation is included in the fault tree, the MOVs to the steam generators appear to be normally open and do not require an actuation signal,…). It is suggested that the AFW example be replaced with the FW system for this for this plant so as to make it more consistent with respect to manner in which these systems are installed in most nuclear plants. See Appendix B.

Response 3.8

Agree in part. The available plant PRA does not contain a model of the MFW system. In that respect, the DFWCS equipment have been mapped onto analogous AFW system equipment for the purposes of demonstrating how the linkage of dynamic models to static PRA models can

be accomplished. Section 5.2 and Chapter 6 have been revised to reduce the inconsistences referred to in the comment.

Comment 3.9

Sections 8 and 9 propose further benchmarking. If these additional benchmarks are undertaken, it is suggested:

- The systems to be benchmarked be modeled in a manner that reflects how the plant responds post-trip, considers what the EOPs instruct the operators to do with the system and recognizes the success criteria for the system as modeled in nuclear power plant PRAs. Consultation with industry operations and engineering personnel familiar with representative power plants would be useful in this regard.
- The analysis should be directed at addressing current industry issues with respect to the modeling of digital I&C in PRA. That is
    - Evaluating the effects of common cause failures for digital systems
    - Analyzing the effects of the system on the plant as a whole as opposed to the digital system itself or just a single system in which it is installed
    - Selecting potentially risk significant accident scenarios that may be unevaluated under the current deterministic approach to evaluating digital systems
    - Identifying potential unnecessary conservatisms in the design of the system (particularly those that may increase risk).

Response 3.9

Agree. While this report cannot comment on NRC research priorities, it is the authors' understanding that next benchmark will address some of these recommendations.

Comment 3.10

The complexity of the system modeled is not representative of the type of digital systems being used or proposed by licensees. The digital feedwater system modeled is fairly simple. Digital systems such as the Westinghouse Common Q and the Areva TXS are significantly more complex, and this complexity may make application of the methods shown in this NUREG to actual systems impractical. It is suggested that a future research effort attempt to model a system similar to those currently under review.

Response 3.10

Agree. While this report cannot comment on NRC research priorities, it is the authors' understanding that next benchmark will be similar to a recently proposed reactor protection system.

4 Incorporation of Failure Models Into PRA

Comment 4.1

In spite of the fact that the conclusions given are well supported by the information provided and that they are well balanced, another issue which may deserve more discussion is that of the post-processing of the results which may be required after the integration of the digital I&C systems reliability models in the plant PRA models.

Response 4.1

Agree. Section 6.3 was modified to include why post processing may be required due to timing inconsistencies in the output cut sets and how these inconsistencies may be removed.

Comment 4.2

The actual incorporation of the DFM and Markov models output into the Example Plant PRA (Section 5.1) remains somewhat at a high level (more so for the DFM than for the Markov approach).

Response 4.2

Agree in part. However, Sections 5.3.2 and 5.4.2 provide concrete examples of conversion of the DFM and Markov/CCMT results into dynamic event trees.

Comment 4.3

The interfacing with SAPHIRE also remains at a high level.

Response 4.3

Disagree. Figure 5.3.1 shows how the dynamic methodology results can be integrated into SAPHIRE using the SAPHIRE graphical interface. Section 6.2 shows the integration using the SAPHIRE textual interface, with actual interface scripts used for the integration provided in Section 6.2.

Comment 4.4

Integration with the PRA (pages 5-30 to 6-5): Successful integration of the example dynamic model with the main PRA model has not been adequately demonstrated. Integration with the PRA is developed only conceptually and is not practical nor useful. The concept described essentially involves appending the minimum cut sets (or prime implicants) from the DFM or Markov analysis results onto the PRA's minimum cut sets, after converting them to a graphical fault tree format. The proposed "fault tree" interface is a listing of all the Markov-derived cut sets (or sequences from the DET) converted to fault tree format. There are several problems with this approach:

1. This "linking" does not satisfy the intent of the linked fault tree methodology. There are no subtrees to resolve dependencies between the I&C model, its support systems, and other systems, such as for power supplies, HVAC, or common sensor input.
2. It would make the PRA's fault trees very cumbersome, complicate understanding, and for a large PRA model, it probably would not solve.
3. This type of interface also serves no benefit because it is no different than merging the cutsets directly with the PRA's cut sets. The cut sets are the answer (solution) of the PRA; there is no benefit to converting cutsets back into and-gates and or-gates, and re-solving.
4. If there are no dependencies between the dynamic model and the fault tree, then the dynamic model is independent and can simply be solved and reduced to a point estimate value before combining with the fault tree. If on the other hand there is "coupling," then (as described on pages 5-27/28) the integration is "complicated" and there are "issues," which are not resolved in this NUREG.
5. By far the most important aspect of integrating (linking) fault trees is the resolution of dependencies. Individual random failures are seldom of any importance in a PRA. Almost all PRAs are dominated by dependencies (power supplies, CCWS, etc.) and common cause failure (CCF). To the extent that an I&C system is relied on by different safety systems, this is what needs to be captured rather that the specific failure state sequence that gets you there.

Response 4.4

Agree in part. The authors agree with all the points made in the comment as they pertain to the PRA model used in Chapter 6 and the example initiating event. The PRA model used in Chapter 6 is necessitated by the requirement that this report needs to be publicly accessible. The reasons for the choice of the example initialing event were discussed in Section 2.5 and are further elaborated upon in *Responses 1.1.3* and *1.2.6.* However, the purpose of Chapter 6 is not to demonstrate that there will be additional dependencies but rather to illustrate the mechanics of incorporating initiating events of interest for the digitial I&C system under consideration to the existing PRA model. If there are dependencies between the elements of these events and the rest of the plant PRA model, such dependencies will be automatically resolved though the use of a similar naming convention for basic events and Boolean algebra rules by the PRA quantification tool used (see the introduction to Section 6.1 in the revised Chapter 6). If the resulting tree becomes complicated, it is simply reflecting system topology.

Comment 4.5

Assuming that it is feasible to include a dynamic control system model in the PRA, it is not clear what parameters in the Plant PRA would be used as inputs to the dynamic control system model. It appears that the appropriate link for the dynamic control system model is a thermal hydraulic model that would provide input data that would be of value to the control system simulation. If the dynamic control system does not have extensive input from other parts of the PRA, then the usefulness of inserting the model, v. the externally solved results, is not demonstrated.

Response 4.5

Agree in part. If the dynamic control system has no input from other parts of the PRA and has not output to other parts of the PRA, then the control system can be treated as a standalone component and there is no need to insert the dynamic reliability model into the PRA (see revised Paragraph 2 of Chapter 6). If the dynamic model needs input from the rest of the PRA, this information can be provided to the dynamic PRA in the form of multiple branches. For the example initiating event, the branch information is generated using the plant dynamics model. In other applications, a simpler representation of the interactions between the digital system and rest of the plant may be adequate (e.g. in tghe form of tabular data). Figure 6.3.2 shows the trajectory bifurication in Fig.2.5.7 can be incorporated into a conventional PRA, given that the level is normal at t=0. If the level location is not known, a partitioning similar to that given in Fig.4.3.1 can be used to represent the level and branchings similar to Fig.6.3.2 that are constructed for the other level intervals (see revised Section 6.3).

Comment 4.6

Section 5.2 - Discussion of Plant PRA (p. 5-10): The authors (correctly) state that the PRA analyzed (from NUREG-1150) does not include modeling of the feedwater control system. However, there is no discussion whether the inclusion of these elements in the model would significantly impact the PRA results obtained. Since no quantification was performed, it is not possible to ascertain if this would represent a significant contributor to CDF or not. However, qualitative experience with installation of DFWCS at operating plants indicates that these installations have dramatically reduced the number of control system induced feedwater events. Thus, my first thought is that events due to DFWCS failures would constitute a very small fraction of the core damage risk incurred from the FW and AFW systems.

Response 4.6

Agree in part. The commenter's assessment may be correct, however, the objective of this proof of concept study is only to demonstrate the applicability of techniques selected in NUREG/CR-6901 to the update of the plant PRAs following an upgrade of analog I&C systems by digital I&C systems, not to assess the contribution of the DFWCS to the overall risk (see Section 1.1).

Comment 4.7

Section 5.3 - SAPHIRE as PRA Tool of Choice (p. 5-26): FT/ET models will remain the method of choice for nuclear plant PRAs; however, this sentence should delete any reference to SAPHIRE as a tool of choice since there are numerous COTS tools available for conducting FT/ET analyses and individual practitioners have significant embedded costs in their current selected software applications. The paragraph should then be rewritten to discuss the limitations inherent in the SAPHIRE tool (if desired) or eliminate all references to SAPHIRE and discuss the issues presented in a generic manner.

Response 4.7

Agree. Section 5.3 has been revised to indicate that SAPHIRE was only used as an example of automated PRA tools.

Comment 4.8

The conclusions of this section are correct in that the timing of the FW bypass valve in a stuck position can have an effect on how steam generator level behaves in response to FW control failures. However, this particular failure mode has no relevance to the outcome of a nuclear power plant PRA. As noted in Appendix A:

- the success criteria for the feedwater system is to maintain steam generator level between two extremes (above steam generator dryout but below the steam lines).
- Control of FW flow generally does not credit the control system but manual action or backup systems which regulate FW flow preferentially to the normal feedwater control system.
- Regardless of the timing of the failure, the PRA would model the FW bypass valve as functionally failing to regulate flow. If this resulted in a fall in steam generator level, the feedwater system would not be considered effective in removing heat from the steam generators. If an uncontrolled rise in steam generator level occurred, then the feedwater system would trip. For either failure mode, the PRA models the feedwater system as having failed with the same resulting consequences.

Response 4.8

Disagree. The DFWCS failure mode would affect the frequency of the remedial action to be taken.

Comment 4.9

The NUREG/CR argues that a dynamic model of the control system is required to determine the "dependability" of the system and to identify potential failure states and sequences. As digital control systems grow more complex in hardware and software and the interconnection of systems via external communication networks, the current FMEA methodologies may not be adequate and new tools will be required. Whereas this may have merit for the development and analysis of the system and ultimate regulatory acceptance of the digital control system, a nexus to the need for the integration of a dynamic control system model into the plant PRA is not demonstrated. The proposed methods require further development and demonstration of viability, as well as a baselining against current methods to allow a cost benefit balance.

Response 4.9

This is a technical report and cannot comment on regulatory policy. However, it is the authors' understanding that the methods presented in this report will not be endorsed for regulatory decision making until the NRC determines them to be sufficiently mature for such a purpose.

Comment 4.10

The export compatibility to the systems analysis program for hands-on integrated reliability evaluation (SAPHIRE) code is presented and various limitations identified. The concern is more generic in that the linking to traditional PRA logic models (event trees and fault trees) is a

generic issue not specific to SAPHIRE (e.g., the same problem exists for cutset and fault tree analysis, etc.).

Response 4.10

Agree. SAPHIRE is only used as an example of automated PRA tools. Section 5.2 has been revised to highlight this intention.

5 Uncertainty Analysis

Comment 5.1

In spite of the fact that uncertainty information is part of Requirement 9 for the modeling tool, this issue is not addressed in the benchmark problem.

Response 5.1

Agree. Chapter 7 was incorporated into the revised report to respond to this comment.

Comment 5.2

In general, the findings of the work contained in the report are presented in a balanced way, with attention devoted also to pointing out the limitations of the approaches suggested, i.e. the DFM and Markov modeling approaches. A deeper discussion of the consequences of these limitations could have been dared.

Response 5.2

Agree in part. Current Chapter 7 (Uncertainty Quantification) was added to address this issue. The consequences of modeling the digital I&C system as a finite state machine, including the partitioning scheme of the continuous variables, abstraction of the interaction between components and the uncertainties associated with data generation, as well as issues specific to the DFM and Markov/CCMT methodologies are discussed. Some remediation approaches are proposed.

Comment 5.3

The whole area of uncertainties are mentioned, but purely in a "to be determined" fashion. Further, I was disappointed that after all the nice discussion on the two methods, I expected to see a "results table" where I could compare the two methods side-by-side for the example problem. I did not see this table in the report.

Response 5.3

Agree. Chapters 7 and Section 5.5. respond to these comments, respectively.

Comment 5.4

There are multiple causes for a high level of uncertainty in the failure probabilities for digital systems. The greatest source of this uncertainty is from lack of data on component failure probabilities, especially demand failure probabilities, and from lack of data on software common mode failure probabilities. It is this reviewer's opinion that these have a much greater impact on system failure probability than the methods used for modeling the digital system. Section 2.4.9 stated that due to time and budget constraints the scope of the study was limited. This insinuates that this type of analysis requires extensive resources (as well as requiring a wide range of expertise including IT and PRA). Also, the FMEA in Section 2.3.1 shows that the

system is very robust and apparently more fault tolerant than an analog system. There has been no cost benefit analysis performed to determine that these analysis methods are needed or have sufficient benefit to account for the costs to the industry to incorporate them. The continuing research noted in the conclusions may provide more information regarding this concern.

Response 5.4

Agree. However, this is a technical report and cannot comment on NRC research priorities.

Comment 5.5

The NUREG did clearly discuss uncertainties involved with the DMF and CCMT/Markov methods in the uncertainty section. However, it failed to quantify the top events to allow any study of how these uncertainties impacted the methods quantification.

Response 5.5

Agree. However, the objective of this proof of concept study is only to demonstrate the applicability of techniques selected in NUREG/CR-6901 to the update of the plant PRAs following an upgrade of analog I&C systems by digital I&C systems, not to assess the contribution of the DFWCS to the overall risk (see Section 1.1).

Comment 5.6

Section 5.3: Uncertainty Analysis - addresses the mathematical uncertainties but does not address the uncertainties related to the assumptions used in the quantification of the DFWCS.

Response 5.6

Agree. Both epistemic and aleatory uncertainties in modeling as well as quantification are discussed Chapter 7 in the revised document.

Comment 5.7

Section 7 - First Paragraph of Uncertainty Quantification (p. 7-1): This paragraph is the most succinct and useful characterization of aleatory and epistemic uncertainties that I have seen. This represents a strength in this report.

Response 5.7

None needed.

Comment 5.8

Section 9 - General Note with respect to Quantification (pp. 9-1 to 9-2): The comments previously provided with respect to quantification of results should be repeated here. In particular, the authors should restate the limitations provided previously in comments to

Sections 3.5.2.1 and 4.3.5. Additionally, they should state that further research is being performed to perform quantification of results for the DFWCS system modeled here and other systems discussed in NUREG/CR-6901, and that any conclusions with respect to the necessity or applicability of these methods for nuclear safety evaluations of digital I&C systems should be considered preliminary in nature.

Response 5.8

Agree. Chapter 9 has been revised to indicate that this report presents a proof-of-concept study only.

Comment 5.9

Section 5.3 discusses the integration of DFM results and 5.4 the Markov/CCMT results. The distinction between steam generator level low and steam generator level high is not relevant to nuclear power plant PRAs as they will both functionally lead to loss of the FW makeup function. With the possible exception of the FW bypass valve failure, the detail included in the models for level, compensated level and error are not consistent with the success criteria for the FW system as modeled in a nuclear power plant PRA.

Response 5.9

Agree in part. Please see *Response 3.8*.

Comment 5.10

Section 5.5 provides a comparison of the results. A quantitative comparison should be added to this section as well as a comparison of the overall FW system and accident sequence frequency results to that which would be obtained from the static ET/FT approach.

Response 5.10

Agree in part. The purpose of this NUREG/CR is to illustrate the use of the proposed methodologies only. Quantification will be provided in the next NUREG/CR (we are working on that document now and it should be available for peer review in the spring).

Comment 5.11

Without an example of the integration of these techniques into a full scope accident sequence analysis, it cannot be concluded that the practicality of the approach has been demonstrated. At a minimum, this section should be expanded to include an estimate of the number of prime implicants (or cut sets) that would be expected for various problems as well as the level of effort and resources needed for performing a full scope analysis including modeling and integration of the results.

Response 5.11

Agree in part. The purpose of this NUREG/CR is to illustrate the use of the proposed methodologies only. However, this NUREG/CR does illustrate the use of dynamic methodologies by the step-by-step modeling of the example initiating event and has provided a proof-of-concept for the implementation of the proposed methods. The authors' understanding is that further research will address the practicality issues.

Comment 5.12

The impact on uncertainty is not incorporated in the report findings but is recognized by the report as a limitation. Although a digital system model is proposed - software is not discussed as a specific source of uncertainty.

Response 5.12

Agree in part. As indicated in Section 1.2.3 of the report, there is no consensus in the reliability community about how the reliability of software systems should be modeled, measured, and predicted, and even whether such a concept makes sense for software. Section 2.1.2.1 of NUREG/CR-6901 describes in detail the fundamental issues associated with the concept of software reliability. That is why NUREG/CR-6901and this report treats software as an entity embedded in hardware.

6 Regulatory Issues

Comment 6.1

Is the expectation that this research be applicable for use in applications such as the Maintenance Rule? What, if any, ties does it have to guidance such as Reg Guide 1.174 and 1.200?

Response 6.1

This is a technical report and cannot comment on regulatory policy. However, it is the authors' understanding that the methods presented in this report will not be endorsed for regulatory decision making until the NRC determines them to be sufficiently mature for such a purpose.

Comment 6.2

The report states: "As part of a cooperative agreement between the NRC and The Ohio State University (OSU), a study was initiated in 2004 to develop both policies and methods for inclusion of reliability models for digital systems into current generation nuclear power plant PRAs." One thing that was missing was much discussion on the topic of "inclusion...into current generation...PRAs." The report needs to be explicit on this aspect, for example are we talking for inclusion into utility PRA or the NRC SPAR models? SPAR models are intentionally streamlined, concise, and tractable, which may call into question one or more methods that are described. While the report does describe the mechanisms for loading PRA-type information into a code such as SAPHIRE, there are other aspects that more important bearing on the "inclusion" facets such as those I mentioned and others (size of the model, running time of the model, availability of importance measures, use of the model during precursor evaluations).

Response 6.2

Agree. However, further research is needed to resolve these issues.

Comment 6.3

More complete analysis with these techniques is needed to allow a detailed regulatory guide to be developed. The future research noted for direct comparison of these methods with full quantification should be complete prior to development of a Regulatory Guide on this issue. It is this reviewer's opinion that this further research is crucial to a better understanding of what is needed in future regulations. Anything drafted prior to that would be based on insufficient knowledge of the implications and practicalities associated with modeling techniques for digital systems.

Response 6.3

This is a technical report and cannot comment on regulatory policy.

Comment 6.4

The continuing research, which includes quantifying a system and comparing it to a quantification using a conventional method, will provide a much more complete insight the benefits of these advanced methodologies. Any regulations developed for risk assessment of digital systems must consider the results of the studies.

Response 6.4

Agree. However, this is a technical report and cannot comment on regulatory policy.

Comment 6.5

If future regulations require the advanced modeling methods noted the screening process shown in Figures 1.3.1 and 1.3.2 has merit and should be developed further via a combined effort with the industry (NEI).

Response 6.5

Agree. However, this is a technical report and cannot comment on NRC research priorities.

Comment 6.6

Figures 1.3.1 and Figures 1.3.2 which discuss conceptual models for categorizing digital systems appear to be a logical screening method for these requirements. If further developed it must be recognized that there must be a floor for system importance. In other words, a system with very low importance should be screened even if it is complex. How low this threshold should be can be evaluated.

Response 6.6

Agree in part. However, a methodology to determine what modeling requirements need to be met for any particular system has not been established.

Comment 6.7

Section 2.4.9: This section stated that due to time and budget constraints the scope of the study was limited. This insinuates that this type of analysis requires extensive resources. No considerations for a cost-benefit analysis have been noted by the reviewer..

Response 6.7

Agree in part. The authors' understanding is that further research will address the practicality issues.

Comment 6.8

Section 2.5: It notes that this is a "Level 2" Analysis. It appears to be a level 1 analysis and does not relate to Containment Release. The analysis assumes the Main Computer fails and states that this is for clarity. However, this results in failing to show that the methodology can

successfully be implemented under a full system which is more complex. It fails to address the methodologies practicality for analyzing the additional interfaces between the computers. This is reinforced by the additional simplifications noted in Section 2.5.1. Further, to prevent core damage only one Steam Generator is required to maintain level. Top event level would require an analysis with common cause between the two trains as success criteria only requires one train to succeed. This analysis only includes the failure probability to one SG. The purpose of the publication is to show the viability of these methods. This is not done if multiple simplifying assumptions are done. It does make the analysis easier to follow, but does not allow this study to prove practicality.

Response 6.8

Agree in part. Please see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6, 1.3.6* and *6.7*.

Comment 6.9

Section 3: Without quantification a comparison of the failure modes probabilities cannot be performed. It is this reviewer's opinion that if this quantification were performed, without the simplifying assumptions used, that the actual valve and pump failure modes would dominate the failure probabilities and the digital system's failure modes would be relatively insignificant.

Response 6.9

Agree in part. However, the statement is the reviewer's opinion and needs to be confirmed by such a quantitative analysis.

Comment 6.10

Section 4: This is an excellent, but broad, description of the Markov/CCMT methodology. However, it is not practically applied to quantify the probability that the DFWCS fails.

Response 6.10

Agree in part. The purpose of this NUREG/CR is to illustrate the use of the proposed methodologies only. However, this NUREG/CR does illustrate the use of dynamic methodologies by the step-by-step modeling of the example initiating event and has provided a proof-of-concept for the implementation of the proposed methods. The authors' understanding is that further research will address the practicality issues.

Comment 6.11

Section 5.4.2 - Same comments as Section 2.5. The simplifying assumptions make it easier to describe the process, but prevent showing that a full analysis of DFWCS is practical using this method.

Response 6.11

Agree in part. Please see *Response 6.10*.

Comment 6.12

Conclusion of future activities 1, 2, and 3 listed in the summary are vital inputs to any decisions made of future regulation on risk assessment of digital systems. This analysis has not shown that a complete quantification is viable and it has not shown the inadequacy of conventional methods. The methods must be compared objectively via a comparison of evaluations on the same system with the same level of effort on the FMEA.

Response 6.12

Agree in part. It is the author's understanding that quantification will be performed in a subsequent study. However, this is technical report and cannot comment on regulatory policy. Also, see *Responses 1.1.5, 1.1.6,* and *1.1.9*,

Comment 6.13

The authors are technically capable and appear to be very knowledgeable of their topic. However, the reviewer takes issue with whether the methodology is useful for plant PRAs or in regulatory decision-making.

Response 6.13

Agree in part. This is a technical report and cannot comment on regulatory policy. However, it is the authors' understanding that the methods presented in this report will not be endorsed for regulatory decision making until the NRC determines them to be sufficiently mature for such a purpose.

Comment 6.14

It is unclear what safety issue(s) the analysis methodology addresses..

Response 6.14

Disagree. The intent of this report is to advance the state-of-the-art in risk and reliability modeling of digital systems within the context of nuclear plant PRAs.

Comment 6.15

It is not clear whether the suggested performance criteria (see Section 1.2.3) are achievable by any method, nor is it clear that these criteria are necessary to ensure the adequate health and safety of the public. In this reviewer's opinion, there is a real possibility that this activity will dissuade licensees from implementing digital I&C upgrades that have a real benefit to public health and safety.

Response 6.15

This is a technical report and cannot comment on regulatory policy.

Comment 6.16

The NUREG does a good job of describing the work performed to date. Significant additional work is needed to complete the project.

Response 6.16

None needed

Comment 6.17

Chapter 1 - Section 1.2.3 provides a useful set of criteria applicable to selection of appropriate modeling methodologies for application to the reliability modeling of digital I&C systems. The list of criteria appears reasonable and comprehensive. However, three observations are pertinent. First, the objective, from a regulatory viewpoint, should be the specification of criteria with the express intent of their application to regulatory decision-making. This important modifier is not included in the development of the requirements. Second, since many of the modeling techniques are complex and employ advanced technology and / or mathematics, it is difficult to see how any of them will satisfy Criterion 5 (ease of understanding and application by a typical (industry or NRC) practitioner), at least within the timeframe needed to support necessary digital I&C upgrades in currently operating plants and deployment in the first wave of new COL plants. Note that since a primary purpose of these evaluations is to support regulatory decision-making, this criterion should have very high weighting in the selection of appropriate analysis methods. Finally, in NUREG/CR-6901, the classification of the methods evaluated is incomplete in that (1) no basis for the conclusions provided in Table 3 (characterization of the potential method's capability to meet the proposed criteria) is given and (2) no comparison to the capabilities of the ET/FT approach is provided. Based on the perspective provided here, I disagree with the authors stated conclusion that the proposed techniques can support near-term future applications.

Response 6.18

Agree in part. While this is a technical report and it is not the intent of the authors to comment on regulatory policy, it is the authors' understanding that a successful path exists to the licensing of digital I&C upgrades and new designs that relies on current deterministic regulations. The main objective of this research is to advance the state-of-the-art on digital system risk and reliability modeling to the point where the NRC can apply risk informed decision making to digital systems. Section 1.1 is revised to reflect these points. It is also the authors understanding that there are other NRC activities ongoing to support near-term future applications.

Comment 6.19

Chapter 1 - Discussion of complexity and coupling (p. 1-10): Attributes 1-4 that determine the modeling level of detail required are equally applicable to analog I&C systems. However, I

contend the last sentence in this paragraph completely mischaracterizes the objective of the modeling. The accuracy of the model is not intended to support a definitive evaluation of a safety metric (such as CDF or LERF). Rather, it is intended to ascertain the impact of the evaluated system (and possibly potential design / operational alternatives) in comparison to other attributes so that (from NRC perspective) an appropriate regulatory decision can be made with respect to the nuclear safety adequacy of the proposed system.

Response 6.19

This is a technical report and cannot comment on the role of PRA from a regulatory viewpoint.

Comment 6.20

Chapter 1 - Discussion of proposed categorization strategy (pp. 1-10 to 1-11): The proposed approach appears to be overly complex and it is not clear how this fits into the current regulatory framework. For example, if the system does not support or impact SSCs classified as safety significant (e.g. Maintenance Rule risk significant SSC or RISC-1 / RISC-2 classified SSC under Regulatory Guide 1.201), then only minimal modeling should be required regardless of the specific characteristics of the digital I&C system. Note that the example characterizations provided seem to support the viewpoint espoused in this comment.

Response 6.20

Disagree. A methodology to determine what modeling requirements need to be met for any particular system has not been established. It is the authors' intention to consider the current regulatory framework mentioned in the comment in finalizing the methodology.

Comment 6.21

Chapter 1 - Discussion of proposed categorization framework (p.1-12): I completely disagree with the authors statement that the "shape of these regions … would not even need to be able to be drawn". If the proposed concept would be adopted as a basis for regulatory decision-making, then it is essential that the specific criteria used to specify the depth and type of modeling required must be specified (with a basis provided), else it will not be possible to achieve regulatory consistency or predictability.

Response 6.21

Agree in part. It is the authors' intention that the criteria should be are attribute and not metric based.

Comment 6.22

Section 2.4.1 - Goal of Safety Quantification Methodology (p. 2-39): This paragraph essentially is a proposed statement of regulatory policy and it should be noted that these objectives represent the author's opinions and do not constitute objectives which must be met or methods which must be used by licensees. In particular, it should be explicitly stated that the intent is to provide one possible framework and method for ensuring applications of digital I&C systems

provide acceptable levels of nuclear safety from which the regulatory authority could evaluate proposed (safety related) applications of digital I&C technology.

Response 6.22

Agree in part. Section 2.4.1 has been revised in response to the comment.

Comment 6.23

Section 9 - Conclusion Second Paragraph (p. 9-1): Since no quantitative results were presented, in my opinion, the authors did not demonstrate that the results obtained from DFM and Markov modeling could be integrated into an existing PRA, In particular, the authors only discussed how the methods could be used to achieve this objective; however, since quantitative results were not produced, there was no actual integration of them into a realistic PRA model and thus it is not appropriate to state this was actually demonstrated.

The draft NUREG presents possible approaches for modeling digital systems in PRA but does not describe what industry problems the techniques are intended to address or the PRA applications for which these approaches are considered useful. In a telephone conversation with the authors of the draft NUREG on 12/7/06, it was stated that the expected application for which the proposed methodologies was to be used in the risk-informed licensing of new digital systems.

Response 6.23

Agree in part. The main objective of this research is to advance the state-of-the-art on digital system risk and reliability modeling to the point where the NRC can apply risk informed decision making to digital systems. Section 1.1 is revised to reflect these points. It is also the authors understanding that there are other NRC activities ongoing to support near-term future applications. Also, see *Responses 1.1.3, 1.1.6, 1.1.12, 1.1.18, 1.2.6, 1.3.6* and *6.7*.

Comment 6.24

The introduction to the report could use:

- A statement of the overall problem and how the proposed approach fits in to the solution of that problem.
- A statement regarding the application to which the proposed approaches are expected to be implemented as well as a discussion of the benefits over other approaches. In discussing potential applications, the proposed methods should be considered in context of the grades or capability categories provided in ASME Std RA-S-2002 or NEI 00-02.

Response 6.24

Agree in part. Section 1.1. has been revised to respond to the comment.

Comment 6.25

Regarding the problem statement, it is clear that there is industry and NRC consensus that digital systems can introduce new failure modes that impact the redundancy built into existing mitigating systems (See SRP BTP-19 and EPRI 1002835). Further, current deterministic evaluations of digital systems are limited in that they consider only design basis events. At the same time, it also is industry and NRC opinion that current digital systems are being designed conservatively (see transcripts of Commission briefing of 11/8). Whatever risk-informed methods are shown to be practical, they should be directed at addressing these issues.

Response 6.25

This is a technical report and cannot comment on regulatory policy and NRC research priorities.

Comment 6.26

For the purpose of this peer review, it is assumed that the objective of the proposed risk-informed methods in the draft NUREG is to assess the reliability of proposed digital systems in context with the integrated plant design (not just assess the reliability of the digital system itself), identify and remove unnecessary conservatisms in the design of digital systems (particularly those that increase risk) as well as to assure there are no unevaluated risks in potentially dominant accident sequences that are not currently considered in the current deterministic approach to evaluating digital systems.

Response 6.26

Agree in part. Section 1.1 has been modified to make the purpose of the report clearer.

Comment 6.27

Concur with the NRC staff position in the third paragraph of Section 1.3 that regulatory guidance should be performance based as opposed to prescriptive. Also concur with the concept that the modeling methods should be such that it is practical to analyze and make rational decisions regarding the non-digital portions of the plant as well as the digital systems. Suggest that the reference to 'importance measures' and 'risk achievement worth' be changed to 'evaluation of the risk impact using bounding assumptions' as it is not clear this application can be performed with importance measures.

Response 6.27

Agree in part. A methodology to determine what modeling requirements need to be met for any particular system has not been established. It is the authors' intention to consider the suggestions in finalizing the methodology.

Comment 6.28

Some modification to the report should be made before the NUREG is finalized and published. The executive summary and the report summary and conclusions should be modified to show that the report is intended as a proof of concept, and not as a recommenced licensing method. The limitations of this method, shown as challenges, should be more prominent and explicit.

Also, the fact that this is only a part of the overall research on reliability modeling of digital systems, and as such, is only a partial or interim report of the total research effort should be made clear.

Response 6.28

Agree. The Abstract, Executive Summary and Chapter 9 have been revised to respond to the comment.

Comment 6.29

It is also suggested that the title of the report be modified to reflect that this is only the report on one portion of the research effort, and is not a final and stand-alone report for use in risk informed licensing of digital systems for safety related use in nuclear power plants.

Response 6.29

Agree. Title has been changed to emphasize that the report is discussing one possible approach to the reliability modeling of digital systems.

Comment 6.30

References to a planned regulatory guide (or other RG) should not be referenced and deleted from the document.

Response 6.30

Agree. Abstract, Executive Summary, Chapter 1 have been revised in response to the comment.

Appendix A

Applicability of NUREG/CR-6901 examples to nuclear power plant PRAs

Example 1: CCW loss of a pump train

Problem description

Fault tree and Markov models are developed and compared of a CCW system for the length of an 80h outage.

Conclusions are

- Shorter mission time, more accurate Markov approach
- Fault tree approach is less accurate when CCF contribution is not dominant
- When random failure rate is high and mission time short, consideration of repair is important
- Different failure rates and repair characteristics for multiple components make Markov more appropriate

Applicability

The problem as stated is very similar to trip models or generation risk assessment models (GRA) currently in use at nuclear power plants for development of initiating event frequencies, configuration management and economic risk analysis purposes. In developing these models, the need to accommodate varying mission times and repair and recovery has been recognized and methods developed for use with current fault tree techniques (see references below). These fault tree techniques have been demonstrated to be sufficiently accurate that they are being used in Maintenance Rule (a)(4) assessments as well as economic cost benefit analyses to support maintenance and capital improvements. Software is available to perform the analysis and interpret the results (such as the CSRAM module of CAFTA).

It is not surprising that the fault tree developed in Figure 1.3 of the draft NUREG is not particularly accurate in its assessment of system reliability. As the example problem did not consider existing methods that reflect current approaches that would be used to assess the frequency of loss of systems such as that being modeled, the conclusions that Markov modeling is more accurate than fault tree modeling cannot be supported.

Example 2: HPCS operation during SB Loca

Problem description

Four top events:
- high pressure
- low pressure
- high level
- low level

The analysis results focus on the effects of the competition between these top events. A comparison of the probability of the above top events derived from dynamic models vs. fault trees is also provided.

Applicability

The description of the success criteria for this system is inconsistent with how HPCS is modeled in a BWR PRA.

Reactor pressure has no effect on HPCS success, nor does high level. Only low level (which is acknowledged in the example). So there is only one top event, that for low level, which would be incorporated in a PRA. Therefore, there is no competition between the four top events. Even if a system does have multiple top events, existing software is capable of handling that by producing condition specific cut sets and integrating them appropriately into the accident sequences containing those conditions. The basis for the conclusion that these four top events are somehow competing with one another is not clear.

In comparing the final results, the Markov and fault tree results are within a factor or 2 to 3. In PRA space this is a bulls eye and, therefore, the conclusion that the fault tree results are not sufficiently accurate does not appear to be supported.

HPCS is a single train system with active components (a pump and valves) and the I&C is likely multidivisional with redundancy. That dynamic modeling of the system results in a factor of two to three change in the system failure probability is remarkable. The only way it appears that this could occur is if the I&C (the only repairable part of the system) dominates system availability. This is unusual in power plant systems and deserves some additional explanation.

Finally, the statement in the draft NUREG that event tree fault tree methods may not produce satisfactory results for a problem of this nature appears to suggest current BWR PRAs may not be appropriately quantifying sequences in which high pressure systems are credited. It is assumed that this was not the intent of the statement and that this conclusion cannot be supported by the material presented in the draft NUREG.

Example 3: Reactor level setpoint drift

Problem description

The example evaluates the effects of setpoint drift on a level control system for a BWR.

Applicability

Setpoint drift is not modeled in nuclear power plant PRAs.

- Level related setpoints for successful actuation of mitigating systems in US PRAs are SG dryout for PWRs and below TAF for BWRs.
- The instrumentation failure rate is dominated by calibration, power dependencies, functional failure.

These success criteria and failure modes have a much more significant effect than any failures that would be expected as a result of setpoint drift.

Were there to be an issue regarding setpoint drift, it is acknowledged that there may be better tools than fault trees for quantification of its effects.

Example 4: FW control system (this example is a benchmark in a draft NUREG that references NUREG/CR-6901)

Problem description

The feedwater control system modeled in this example has the following characteristics:

- Success criteria is controlling level between +30" and -24"
- Uses steam generator level, feedwater flow, feedwater temperature and neutron flux to determine FW bypass valve position
- Includes two division main computer and backup computer for each steam generator receiving signals from above sensors and providing analog signal to FW bypass valve.
- Bypass valves are modeled as failing in their current position.

FMEAs are performed for the main computer, backup computer and controllers for the FW bypass valves and pressure differential indicators.

Markov and DFM models are developed for the system.

The fault injection methods are used to assess the dependability of the system.

It is proposed that the prime implicants from the model results be imported to fault tree software in cut set form to integrate the results with existing feedwater system models.

Applicability

What do we know from operating experience about FW control systems?

By themselves, they are not dominant contributors to loss of the feedwater system

- 70-80% of loss of FW initiating events are due to non-I&C related causes (this appears to be the case for analog FW I&C, digital FW I&C is expected to contribute even less)
- Post non-loss of FW initiator, the reliability of the feedwater system is dominated by
    - Physical plant response to a turbine trip (e.g., the likelihood of a subsequent high level trip in BWRs or spurious SI signal in PWRs
    - Guidance provided by the EOPs with respect to operation of the system
    - Whether the pumps are turbine or motor driven

Post-trip FW control I&C typically often is not dependent on the normal FW control system, but on manual action or alternate control systems that override normal FW controls (e.g., steam flow, feed flow play no role). See summary in Appendix B for seven plants.

Where do the risks lay with respect to feedwater control systems?

Even though it does not dominate the reliability of the feedwater system, FW control has been a relatively significant contributor to risk from an economic standpoint. Economics is one of the drivers toward replacement of analog systems with digital FW controls.

Consistent with industry and NRC consensus regarding the potential risks of digital I&C, the only way to make FW control systems dominate safety is if they have something in common with a redundant system within the accident sequence.

- Initiator - is there a common failure mode with turbine controls?
- Post-initiator - is there a common failure mode with mitigating systems?

Treatment of these type of dependencies would be the principal purpose of modeling FW controls in any detail. If these dependencies are not present, then the FW controls can be treated as a module independent of the rest of the model (regardless of the dynamics).

The example problem does not model the success criteria of the feedwater system as it would be in a nuclear power plant PRA.

- The range +30" to -24" is very narrow as compared to what is used in the PRA (overfill to the steam lines to steam generator dryout). Exceeding the levels assumed in the example analysis is not failure for the feedwater system until these extremes are reached.
- Differentiation between high level and low level as a failure mode in the steam generators is not relevant to accident sequence quantification. If a high level occurs, then feedwater is tripped and it becomes unavailable for heat removal. If a low level occurs then feedwater is unavailable for heat removal. The consequences of these two failure modes as modeled in most PRAs is the same.
- Steam generator level, neutron flux, feedwater flow and feedwater temperature would not be the likely inputs to FW bypass valve position as the system would be taken into manual by the operators or preferentially overridden by alternate post-trip controls (either single element control on level or control by an alternate I&C system).

Appendix B
Feedwater flow control post trip at seven plants

3 BWRs
4 PWRs (one an advanced reactor)
All have digital feedwater control systems

FW control is not used to initiate or control AFW (PWRs) or high pressure injection systems (BWR) in any of the plants investigated. AFW and high pressure injection systems are actuated by I&C (usually safety-related) that is independent of the FW control system.

Control of the FW system itself manual In all but two of the plants post reactor trip. Investigating the reasons for this:

- BWRs - Following closure of the stop valves, a momentary pressure spike is expected in the primary system resulting in a level drop due to void collapse. On opening of the turbine bypass valves, a subsequent pressure reduction occurs. This results in void expansion and a level rise. At many BWRs, this level rise results in a relatively high likelihood of FW pump trip (designed to prevent overfilling the primary system, a demand on SRVs and carry over of water into the secondary system). To recover from this feedwater pump trip, plants having motor driven feedwaterpumps will restart them manually (or if there is a motor driven startup pump, initiate operation that pump). Plants without motor driven feedwater pumps will rely on standby high pressure injection systems (RCIC, HPCi, HPCS) which can be automatic or manual. In any case, reactor level is manually controlled by the operators following initiation of a high pressure makeup system.
- PWRs - On turbine trip and closure of the turbine stop valves, initial feedwater flow is greater than that needed to makeup for steam flow. As feedwater heaters are no longer in service following the turbine trip, the water being injected to the steam generators is also colder than during normal operation. This can result in a relatively high amount heat removal from the primary system as compared to decay heat levels and a subsequent drop in reactor pressure. To avoid a spurious safety injection signal, PWR EOPs often instruct the operator to take feedwater control to manual as one of the first few actions following a reactor trip. In some PWRs, an automatic isolation of FW valves occurs with manual action to reopen these valves only if AFW becomes unavailable.

Both of the plants that did not have this dependency on operator action to control feedwater flow were PWRs.

- The first PWR has turbine driven feedwater pumps (no motor driven startup pump). To keep feedwater in service following a plant trip, normal feedwater flow control is are bypassed automatically by design in favor of ramping back feedwater pumps to 5% normal operating speed. As a result, the feedwater control system does not play a role following plant trip. Further investigation of

the EOPs at this plant also revealed that one of the first steps following reactor trip is to switch feedwater control to manual. So, even with this automatic feedwater pump speed ramp down, the operator takes manual control over feedwater flow as is the case for the PWRs previously discussed.

- The last PWR was an advanced reactor and has motor driven feedwater pumps. (Note that EOPs are not yet available for this plant and might also require the operators to take manual control of feedwater flow after a reactor trip). The PRA for this plant assumes that feedwater flow control continues to maintain steam generator level post reactor trip. However, should steam generator level exceed a prescribed range (either high or low), the feedwater flow control system is bypassed in favor of FW valve position control from the plant protection system (FW bypass valves close on high level and open on low level). The setpoints for this plant protection feature are not known at this time but are expected to be well within that required for success criteria for the PRA. Regardless, it appears the advanced reactor has a feature which overrides normal feedwater control similar to the plant with the turbine driven feedwater pumps noted above.