INL/CON-23-71678-Revision-0



# Investigation of the Use of Dynamic Probabilistic Risk Assessment Methodologies for Identifying Digital I&C System Common Cause Failures

July 2023

Gulcin Sarici Turkmen, Tunc Aldemir, Han Bao

Changing the World's Energy Future

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

INL/CON-23-71678-Revision-0

# Investigation of the Use of Dynamic Probabilistic Risk Assessment Methodologies for Identifying Digital I&C System Common Cause Failures

**Gulcin Sarici Turkmen, Tunc Aldemir, Han Bao**

**July 2023**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

# Investigation of the Use of Dynamic Probabilistic Risk Assessment Methodologies for Analyzing Digital I&C System Common Cause Failures

Gulcin Sarici Turkmen[1], Han Bao[2], Tunc Aldemir[3]

[1] *The Ohio State University, Columbus, OH, sariciturkmen.1@osu.edu*
[2] *Idaho National Laboratory, Idaho Falls, ID, han.bao@inl.gov*
[3] *The Ohio State University, Columbus, OH, aldemir.1@osu.edu*

[Digital Object Identifier (DOI) placeholder]

## ABSTRACT

Digital instrumentation and control (I&C) systems play a key role in the upgrade of aging analog systems in nuclear power plants (NPPs). Digital systems improve plant safety and reliability through features such as increased hardware reliability and stability and improved failure detection capability. There is no consensus on which of the current probabilistic risk assessment methods are most suitable for use in the reliability analysis of digital I&C systems. While the traditional event tree/fault tree (ET/FT) approach is still used for their reliability modeling, there are concerns regarding this approach in properly accounting for dynamic interactions among system components since potentially significant dependencies among failure events may not be identified and/or their likelihood may not be properly quantified. Dynamic methodologies are expected to provide a much more accurate representation of probabilistic evolution on the I&C systems in time due to their capability to more properly account for complex interactions than the static approach.

The applicability of dynamic probabilistic risk assessment (PRA) methodologies for a digital I&C system is investigated using the criteria presented in the NUREG/CR-6901, and the comparisons made in NUREG/CR-6901 are updated in light of the latest studies. The dynamic event tree (DET) approach has been identified as one of the top dynamic methods when evaluated against the requirements for the reliability modeling of digital I&C systems. The DET method is a strong candidate for integration into existing PRA studies, as it bears many similarities to the traditional ET approach. In this study, the DET approach has been applied to a representative Plant Protection System, and the results are compared to results from its available traditional ET/FT analysis. Possible approaches to evaluate and quantify the effects of common cause failures (CCFs) on system safety using dynamic methods are also examined.

*Key Words*: dynamic event tree (DET), digital instrumentation and control (I&C), software reliability, common cause failure (CCF)

## 1 INTRODUCTION

Digital instrumentation and control (I&C) systems are replacing existing analog systems in being implemented in nuclear power plants (NPPs) due to their significant advantages. Digital systems offer improved plant safety and reliability in terms of increased hardware reliability, as well as improved failure detection capability, accuracy, and computational capability. Presently, no universally accepted methods for reliability analysis of digital systems are available in probabilistic risk assessment (PRA) methods [1] proposed to date. While the traditional event tree/fault tree (ET/FT) approach is still used for reliability modeling, concerns still exist with using this approach due to severe limitations in properly accounting for dynamic interactions among system components since potentially significant dependencies among failure events may not be identified and/or their likelihood may not be properly quantified [2].

Existing studies indicate that the traditional ET/FT approach does not satisfy all the requirements for ideal utilization in NPP reliability/safety assessments since the methodology is not capable of modeling time-dependent hardware/software/firmware/process interactions [1]. Other limitations with the traditional ET/FT approach include challenges in the modeling of changes in accident progression based on changes in the plant state, modeling of repair actions, and software aging [3].

Software aging could lead to important negative impact on NPP safety critical systems—such as digital I&C systems—and may lead to performance degradation rather than immediate failure [4]. Even though there is no physical failure in the software, it has been observed that software systems 'appear to age' due to error accumulation or depletion of operating system resources with increasing execution time. In addition, software failure rates significantly increase with increasing use [5]. The estimation of software failure rate due to aging is still an uncertain issue, and there is no consensus about any model since it depends on various reasons. The literature shows that the failure rates is being gradually increasing and can be assumed artificially increased failure rates for the parametric studies [6]. Software rejuvenation is one of the important methods to reduce performance degradation due to software aging [7]. Determination of the optimal schedule for software rejuvenation is crucial for software reliability analysis and should be addressed in detail in digital I&C reliability modeling. However, the traditional ET/FT approach cannot properly consider such a degradation due to the lack of explicit representation of time in the traditional ET/FT methodology.

Dynamic probabilistic risk assessment (DPRA) methods have been developed in order to overcome traditional PRA limitations and are expected to provide a much more accurate representation of the probabilistic evolution of the I&C systems in time due to their capability to account for complex interactions. In the literature, there is evidence that the traditional method overestimates the top event frequencies when the two methods are compared [8]. DPRA methods can also evaluate the safety impacts of spatial effects with higher resolution, as well as the timing and sequencing of events on the accident progression without the need to introduce overly conservative modeling assumptions or success criteria [9]. The timing of events has been included as a new degree of freedom in the issue space with DPRA methods; indeed, DPRA allows the evaluation of scenarios that could not have been considered before to investigate hidden risk insight.

The dynamic event tree (DET) approach is a DPRA method that is more compatible with the existing PRA structure and is similar to the traditional ET approach except that, unlike ETs, where the sequence of system responses following initiating events is predetermined by the analyst, both the timing and sequence of system responses with DETs are determined by a time-dependent model of system evolution and branching conditions selected by the analyst. DETs provide more comprehensive and systematic coverage of possible event scenarios than the traditional ET approach and allow consideration of hardware/process/software/ human interactions in a phenomenologically and stochastically consistent manner [9].

In the spirit of earlier work [1, 2, 3], this study further investigates the feasibility of using DPRA methodologies in digital I&C system reliability analysis. As a case study, the DET approach is used to determine the effect of software common cause failures (CCFs) and software aging in a representative engineered safety features actuation system (ESFAS) derived from the APR 1400 design.

Section 2 describes the ESFAS structure under consideration. Implementation details for the analysis are presented in Section 3. The results of the analysis are presented in Section 4, while Section 5 summarizes the results of the study.

## 2 ESFAS STRUCTURE

Figure 1 shows the functional logic of the example ESFAS. This four-division digital ESFAS includes the portion of plant protection system (PPS) that activates the engineered safety features (ESFs) and their component control system (CCS) [10]. The safety I&Cs of the ESF systems consist of the electrical and mechanical devices and sensor circuitry to actuation-device input terminals that are involved in generating signals that actuate the required ESF systems. The ESFAS portion of the PPS includes the following functions: (i) bistable logic (BL); (ii) local coincidence logic (LCL); (iii) ESFAS initiation; and (iv) the testing function. After receiving ESFAS initiation signals from the PPS, main control room (MCR) operator console, or remote shutdown room (RSR) shutdown console, the ESF-CCS generates ESF actuation signals to ESF component interface modules (CIMs), which transmit signals to the final actuated device [11].

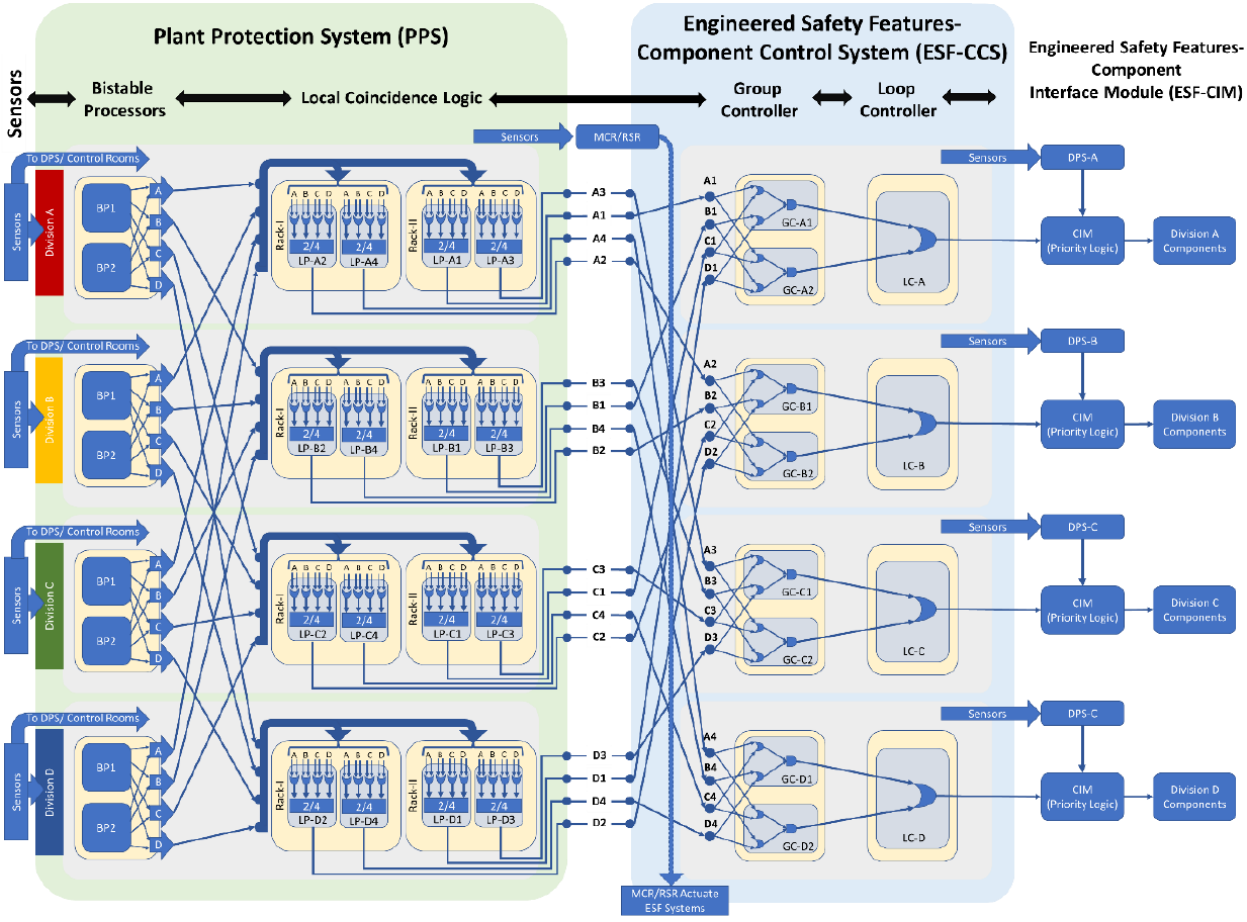


**Figure 1. ESFAS functional logic** *[10]*.

The ESFAS portion of PPS consists of four divisions, as indicated by Divisions A through D in Figure 1. Each PPS division is located in an I&C equipment room and contains both an input and output module, two bistable processors (BPs), two racks for the LCL functions, and other hardware for the interface with other PPS divisions. The redundant BPs generate ESF actuation signals to the LCL racks in the four redundant divisions if the process values exceed their respective setpoints. Each LCL rack contains two logic processors (LPs); the initiation signals are provided to the ESF-CCS, which consists of four divisions of group controller (GC) and loop controller (LC) cabinets. Each GC supports component control and provides ESF actuation signals to the LC. Each LC has component control logic and multiplexing function. Each ESF-CCS GC performs selective 2-out-of-4 coincidence logic. The output of the ESF-CCS GC is

transmitted to the component control logic in the LC. The logic produces digital output (DO) signals to control the component through the CIM, which performs signal prioritization [11] [12].

## 3 IMPLEMENTATION

The DET was quantified by sampling failures of all ESFAS divisions, as well as the activation time of each division on simplified case studies and injecting failures. An example DET is shown in Figure 2. Typically, failures were injected when ESFAS was needed during accident progression. In this study, two different cases were considered to investigate software CCFs and software aging. In Case Study I, the DET was used to determine the ESFAS failure probabilities with different sequences of failures and to identify worst-case scenarios. The impacts of increasing failure probabilities of ESFAS due to software aging were evaluated in Case Study II. It should be emphasized that all of the analyses performed for the DET methodology demonstration and numerical results that were obtained do not necessarily reflect actual ESFAS implementation.

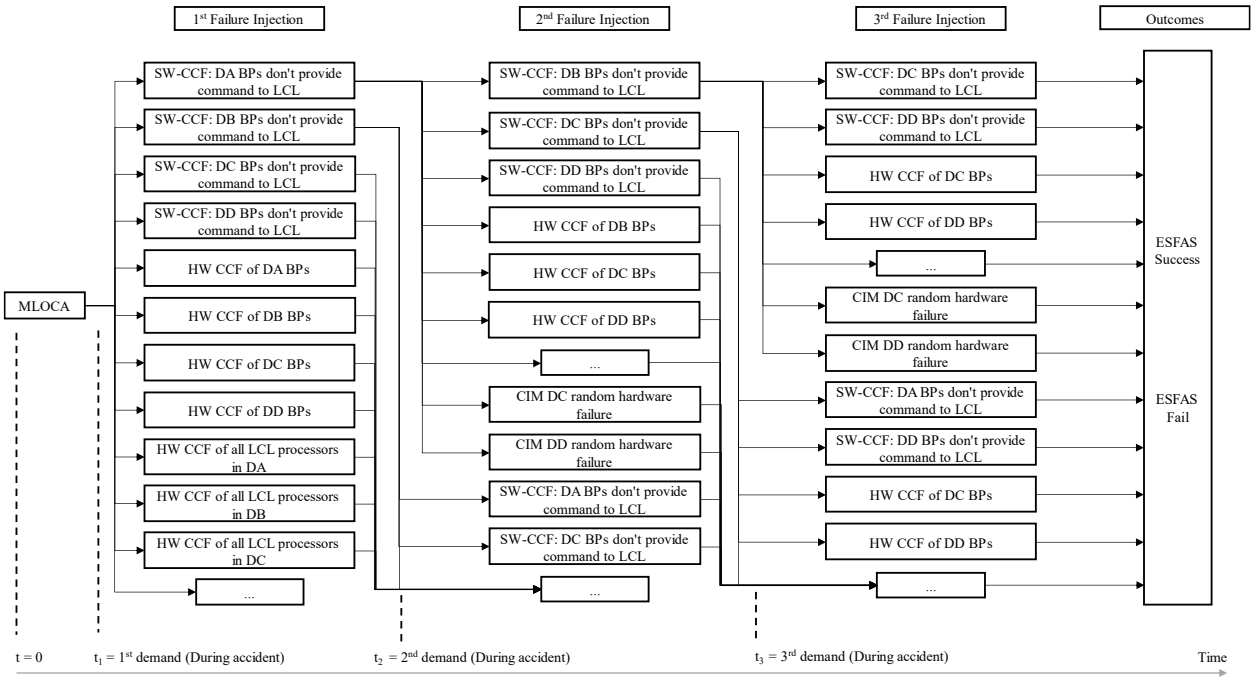


**Figure 2. Example DET.**

Some assumptions have been made to simplify case studies. The following assumptions are common for both Case Study I and II:

- Medium loss of coolant accident (MLOCA).
- Failures may occur only when ESFAS is needed during accident progression.
- All four ESFAS divisions are initially active and working before the accident.
- MCR/RSR and DPS failures are not included in the DET.
- No maintenance or replacement of failed components.
- After a software failure occurs in a division, there cannot be a hardware failure in the same division in the next time step, and vice versa.
- The branch probability cutoff value is 1, which allows running all possible accident scenarios.

- ESFAS failure probability cutoff value is $10^{-18}$ per demand, which avoids unnecessary expansion of the DETs.

Case Study I demonstrated the DET method application and obtained the ESFAS failure probabilities as a result. For this purpose, all ESFAS divisions are assumed to be in the same condition, and failure rates are assumed to be constant. Case Study II assumes that all divisions are in different conditions with increased failure rates due to software aging with four divisions of the ESFAS replaced or maintained at different times. Increasing failure rates have been analyzed within the parametric study in Cases IIa, IIb, and IIc. Table 1 shows the percentage increase for each case.

**Table 1. Increasing percentages of failure rates of ESFAS.**

| # Division | Case IIa | Case IIb | Case IIc |
|---|---|---|---|
| Division A failure rates | 10% ↑ | 20% ↑ | 40% ↑ |
| Division B failure rates | 40% ↑ | 55% ↑ | 80% ↑ |
| Division C failure rates | 20% ↑ | 35% ↑ | 60% ↑ |
| Division D failure rates | 30% ↑ | 40% ↑ | 50% ↑ |

The branching conditions of the ESFAS and failure rates in Table 2 were artificial and only used for methodology development and demonstration. In the DET analysis, only three-fault scenarios were considered; scenarios with four or more faults were not considered due to their extremely low outcome likelihood values, which were on the order of $10^{-18}$ per demand or less. Table 2 summarizes all system-level failure modes and their rates.

**Table 2. Branching conditions and failure rates (per demand) of for Cases I and II.**

| ESFAS Modules | Branching Conditions | Failure Rate (per demand) | | | |
|---|---|---|---|---|---|
| | | Case I | Case IIa | Case IIb | Case IIc |
| BP | SW CCF: DA BPs do not provide command to LCL | 1.062E-04 | 1.168E-04 | 1.274E-04 | 1.487E-04 |
| | SW CCF: DB BPs do not provide command to LCL | 1.062E-04 | 1.487E-04 | 1.646E-04 | 1.912E-04 |
| | SW CCF: DC BPs do not provide command to LCL | 1.062E-04 | 1.274E-04 | 1.434E-04 | 1.699E-04 |
| | SW CCF: DD BPs do not provide command to LCL | 1.062E-04 | 1.381E-04 | 1.487E-04 | 1.593E-04 |
| | HW CCF of DA BPs | 5.943E-06 | 6.537E-06 | 7.132E-06 | 8.320E-06 |
| | HW CCF of DB BPs | 5.943E-06 | 8.320E-06 | 9.212E-06 | 1.070E-05 |
| | HW CCF of DC BPs | 5.943E-06 | 7.132E-06 | 8.023E-06 | 9.509E-06 |
| | HW CCF of DD BPs | 5.943E-06 | 7.726E-06 | 8.320E-06 | 8.915E-06 |
| LCL | HW CCF of all LCL processors in DA | 7.647E-06 | 8.412E-06 | 9.176E-06 | 1.071E-05 |
| | HW CCF of all LCL processors in DB | 7.647E-06 | 1.071E-05 | 1.185E-05 | 1.376E-05 |
| | HW CCF of all LCL processors in DC | 7.647E-06 | 9.176E-06 | 1.032E-05 | 1.224E-05 |

| ESFAS Modules | Branching Conditions | Failure Rate (per demand) | | | |
|---|---|---|---|---|---|
| | | Case I | Case IIa | Case IIb | Case IIc |
| | HW CCF of all LCL processors in DD | 7.647E-06 | 9.941E-06 | 1.071E-05 | 1.147E-05 |
| ESF-CCS | SW CCF: DA GC processors fail to provide signal | 1.062E-04 | 1.168E-04 | 1.274E-04 | 1.487E-04 |
| | SW CCF: DB GC processors fail to provide signal | 1.062E-04 | 1.487E-04 | 1.646E-04 | 1.912E-04 |
| | SW CCF: DC GC processors fail to provide signal | 1.062E-04 | 1.274E-04 | 1.434E-04 | 1.699E-04 |
| | SW CCF: DD GC processors fail to provide signal | 1.062E-04 | 1.381E-04 | 1.487E-04 | 1.593E-04 |
| | HW CCF on GC 1-2 in DA | 5.97E-06 | 6.57E-06 | 7.17E-06 | 8.36E-06 |
| | HW CCF on GC 1-2 in DB | 5.97E-06 | 8.36E-06 | 9.26E-06 | 1.08E-05 |
| | HW CCF on GC 1-2 in DC | 5.97E-06 | 7.17E-06 | 8.06E-06 | 9.56E-06 |
| | HW CCF on GC 1-2 in DD | 5.97E-06 | 7.76E-06 | 8.36E-06 | 8.96E-06 |
| CIM | CIM DA random hardware failure | 4.00E-05 | 4.40E-05 | 4.80E-05 | 5.60E-05 |
| | CIM DB random hardware failure | 4.00E-05 | 5.60E-05 | 6.20E-05 | 7.20E-05 |
| | CIM DC random hardware failure | 4.00E-05 | 4.80E-05 | 5.40E-05 | 6.40E-05 |
| | CIM DD random hardware failure | 4.00E-05 | 5.20E-05 | 5.60E-05 | 6.00E-05 |

**BP**: Bistable Processors, **LCL:** Local Coincidence Logic, **Dx**: Division X (A, B, C, D), **ESF-CCS**: Engineered Safety Features-Component Control System, **ESF-CIM**: Engineered Safety Features-Component Interface Module, **SW CCF**: Software Common Cause Failure, **HW CCF**: Hardware Common Cause Failure, **GC**: Group Controller

## 4 RESULTS

Table 3 and Table 4 show the best and worst DET results, respectively, of the Case Study I accident progression scenarios in terms of failure probability per demand along with sequences of failures and failure probabilities. A total of 11,088 different accident scenarios were evaluated; 432 scenarios ended with the ESFAS failing to transmit a signal to activate the emergency safety systems.

The results in Table 3 indicate that the system has better handling capability of hardware CCFs without transmitting signal failures. All of the best scenarios consist of hardware CCFs, as observed in Table 3 SN 1-5. On the contrary, software CCFs have significant importance for the system, as most of the worst-case scenarios in Table 4 include at least one software CCF. The top three worst cases consist of almost all software CCFs, as shown in Table 4 SN 1-3.

In Case Study II, a total of 33,264 different accident scenarios were evaluated; 1,296 scenarios ended with the ESFAS failing to transmit a signal to activate the emergency safety systems. Table 5 illustrates the results obtained from Case Study II with the top five worst-case scenarios and the change of the ESFAS failure probabilities with an increasing failure rate due to the software aging.

**Table 3. The best five accident progression scenarios of the ESFAS failure in Case Study I.**

| Scenario Number (SN) | 1st Failure Injection | 2nd Failure Injection | 3rd Failure Injection | Failure Probability (per demand) |
|---|---|---|---|---|
| **1** | HW CCF of DA BPs | HW CCF of DB BPs | HW CCF on GC 1-2 in DA | **2.109E-16** |
| **2** | HW CCF on GC 1-2 in DA | HW CCF on GC 1-2 in DB | HW CCF of DA BPs | **2.118E-16** |
| **3** | HW CCF of DC BPs | HW CCF of DD BPs | HW CCF of all LCL processors in DA | **2.701E-16** |
| **4** | HW CCF of DA BPs | HW CCF of all LCL processors in DB | HW CCF on GC 1-2 in DC | **2.713E-16** |
| **5** | HW CCF on GC 1-2 in DB | HW CCF on GC 1-2 in DC | HW CCF of all LCL processors in DD | **2.725E-16** |

**BP**: Bistable Processors, **LCL:** Local Coincidence Logic, **Dx**: Division X (A, B, C, D), **ESF-CCS**: Engineered Safety Features-Component Control System, **ESF-CIM**: Engineered Safety Features-Component Interface Module, **SW CCF**: Software Common Cause Failure, **HW CCF**: Hardware Common Cause Failure, **GC**: Group Controller

**Table 4. The worst five accident progression scenarios of the ESFAS failure in Case Study I**

| Scenario Number (SN) | 1st Failure Injection | 2nd Failure Injection | 3rd Failure Injection | Failure Probability (per demand) |
|---|---|---|---|---|
| **1** | SW CCF: DB BPs do not provide command to LCL | SW CCF: DC BPs do not provide command to LCL | SW CCF: DD BPs do not provide command to LCL | **1.198E-12** |
| **2** | SW CCF: DB GC processors fail to provide signal | SW CCF: DC GC processors fail to provide signal | SW CCF: DD GC processors fail to provide signal | **1.191E-12** |
| **3** | SW CCF: DB GC processors fail to provide signal | SW CCF: DD GC processors fail to provide signal | HW CCF on GC 1-2 in DC | **6.708E-14** |
| **4** | HW CCF of DC BPs | HW CCF of DD BPs | SW CCF: DB BPs do not provide command to LCL | **6.703E-14** |
| **5** | CIM DB random hardware failure | CIM DC random hardware failure | CIM DD random hardware failure | **6.400E-14** |

**BP**: Bistable Processors, **LCL:** Local Coincidence Logic, **Dx**: Division X (A, B, C, D), **ESF-CCS**: Engineered Safety Features-Component Control System, **ESF-CIM**: Engineered Safety Features-Component Interface Module, **SW CCF**: Software Common Cause Failure, **HW CCF**: Hardware Common Cause Failure, **GC**: Group Controller

Table 5 shows the effect of the software aging on the ESFAS failure probabilities over the worst five scenarios and indicates that software aging causes a significant increase in the ESFAS failure probabilities. When the Case IIa, IIb, and IIc (see Table 1 for case definitions) results were compared to the results obtained from Case I, it was observed that the probability of error increased by 118.9%, 193.7%, and 333.2%, respectively.

**Table 5. The worst five accident progression scenarios of the ESFAS failure in Case Study II.**

| Failure Injection Order | Branching Conditions | Failure Probability (per demand) | | | |
|---|---|---|---|---|---|
| | | Case I | Case IIa | Case IIb | Case IIc |
| 1st | SW CCF: DB BPs do not provide command to LCL | **1.198E-12** | **2.616E-12** | **3.510E-12** | **5.175E-12** |
| 2nd | SW CCF: DC BPs do not provide command to LCL | | | | |
| 3rd | SW CCF: DD BPs do not provide command to LCL | | | | |
| 1st | SW CCF: DB GC processors fail to provide signal | **1.191E-12** | **2.616E-12** | **3.510E-12** | **5.175E-12** |
| 2nd | SW CCF: DC GC processors fail to provide signal | | | | |
| 3rd | SW CCF: DD GC processors fail to provide signal | | | | |
| 1st | SW CCF: DB GC processors fail to provide signal | **6.708E-14** | **1.472E-13** | **1.973E-13** | **2.912E-13** |
| 2nd | SW CCF: DD GC processors fail to provide signal | | | | |
| 3rd | HW CCF on GC 1-2 in DC | | | | |
| 1st | HW CCF of DC BPs | **6.703E-14** | **8.194E-15** | **1.099E-14** | **1.621E-14** |
| 2nd | HW CCF of DD BPs | | | | |
| 3rd | SW CCF: DB BPs do not provide command to LCL | | | | |
| 1st | CIM DB random hardware failure | **6.400E-14** | **1.398E-13** | **1.875E-13** | **2.765E-13** |
| 2nd | CIM DC random hardware failure | | | | |
| 3rd | CIM DD random hardware failure | | | | |

**BP**: Bistable Processors, **LCL:** Local Coincidence Logic, **Dx**: Division X (A, B, C, D), **ESF-CCS**: Engineered Safety Features-Component Control System, **ESF CIM**: Engineered Safety Features-Component Interface Module, **SW CCF**: Software Common Cause Failure, **HW CCF**: Hardware Common Cause Failure, **GC**: Group Controller

## 5 CONCLUSION

This study illustrates how DETs can be used to estimate failure likelihoods for digital I&C system reliability assessment and the effect of software aging with two simplified case studies. In Case Study I, it was assumed that the failure probabilities used in the DET analysis did not change over time and that all of the subsystem components were new. In addition, it was also assumed that there is no replacement or maintenance for the failed components. MLOCA was chosen as an initiating event for analysis and failure injection times were determined according to when ESFAS was needed during accident progression. In Case Study II, the failure probabilities were assumed to increase over time due to software aging. All four ESFAS divisions were assumed to be in different conditions. The results show that software aging impacts

with the assumed sensitivity modeling can impact digital I&C system reliability significantly without proper software rejuvenation.

The DET approach represents reality closer than the traditional PRA and can be integrated into the traditional ET/FT analysis of NPPs [7]. The results of this study point out that the DET approach can be useful to understand the hidden risks of the systems with existing PRA structures.

## 6 REFERENCES


[1] T. Aldemir, D. Miller, M. Stovsky, J. Kirschenbaum, P. Bucci, A. Fentiman and L. Mangan, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," NRC, 2006.

[2] T. Aldemir, M. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. Mangan, D. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks and a. S. Arndt, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NRC, 2007.

[3] T. Aldemir, S. Guarro, D. Mandelli, J. Kirschenbaum, L. Mangan, P. Bucci, M. Yau, E. Ekici, D. Miller, X. Sun and a. S. Arndt, "Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies," *Reliability Engineering and System Safety*, vol. 95, pp. 1011-1039, 2010.

[4] J. Zhao, K. Trivedi, Y. Wang and X. Chen, "Evaluation of software performance affected by aging," in *IEEE*, 2011.

[5] Y. Bao, X. Sun and K. S. Trivedi, "A Workload-Based Analysis of Software Aging, and Rejuvenation," in *IEEE*, 2005.

[6] S. Ballerini, L. Carnevalli, M. Paolieri, K. Tadano and F. Machida, "Software Rejuvenation Impacts on a Phased-Mission System for Mars Exploration," *IEEE,* 2013.

[7] T. Dohi, A. Avritzer and K. S. Trivedi, Handbook Of Software Aging And Rejuvenation: Fundamentals, Methods, Applications, And Future Directions, Singapore: World Scientific, 2020.

[8] D. Mandelli, A. Alfonsi, C. Wang, Z. Ma, C. Parisi, T. Aldemir, C. Smith and R. Youngblood, "Mutual Integration of Classical and Dynamic PRA," *Nuclear Technology,* vol. 207, pp. 363-375, 2020.

[9] T. Aldemir, "A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants," *Annals of Nuclear Energy,* vol. 52, pp. 113-124, 2013.

[10] H. Bao, T. Shorthill, E. Chen and H. Zhang, "Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology," INL, 2021.

[11] H. Bao, T. Shorthill and H. Zhang, "Hazard analysis for identifying common cause failures of digital safety systems using a redundancy-guided systems-theoretic approach," *Annals of Nuclear Energy,* vol. 148, 2020.

[12] "APR1400 Desing Control Document Tier 2. Chapter 7: Instrumentation and Controls," Korea Electric Power Corporation; Korea Hydro & Nuclear Power Co., Ltd, 2018.