INL/CON-23-71687-Revision-0

Sensitivity and Importance Measure Analyses for Various Design Architectures for High Safety-Significant Safety-Related Digital Instrumentation and Control Systems of Nuclear Power Plants

Sai Zhang, Han Bao, Tate Shorthill, Jooyoung Park, Edward Chen

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-23-71687-Revision-0

Sensitivity and Importance Measure Analyses for Various Design Architectures for High Safety-Significant Safety-Related Digital Instrumentation and Control Systems of Nuclear Power Plants

Sai Zhang, Han Bao, Tate Shorthill, Jooyoung Park, Edward Chen

March 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

Sensitivity and Importance Measure Analyses for Various Design Architectures for High Safety-Significant Safety-Related Digital Instrumentation and Control Systems of Nuclear Power Plants

Sai Zhang[1*], Han Bao[2], Tate Shorthill[3], Jooyoung Park[4], Edward Chen[5]

[1]Idaho National Laboratory, Idaho Falls, ID
[2]Idaho National Laboratory, Idaho Falls, ID
[3]University of Pittsburgh, Pittsburgh, PA
[4]Idaho National Laboratory, Idaho Falls, ID
[5]North Carolina State University, Raleigh, NC

ABSTRACT

A transition from analog instrumentation and control (I&C) technologies to digital I&C technologies is taking place for license renewals of existing nuclear power plants and for operating licenses of new advanced reactors. This transition necessitates research on risk and economic assessments of digital I&C technologies to ensure the long-term safety and reliability of vital systems, reduce uncertainty in licensing costs in addition to timeline, support integration of digital I&C systems in the plant, and find the most efficient technology upgrades. Adding redundancy within systems or components is a common means of improving design safety; however, redundant designs are more prone to common-cause failures (CCFs). Introducing diversity into redundant systems or components is a way to mitigate and possibly eliminate CCFs, but it also increases plant complexity and may be costly. The balance between redundancy and diversity remains a challenge for digital I&C systems. This study performs sensitivity and importance measure analyses for four design architectures of two digital I&C systems—the reactor-trip system and the engineered safety features actuation system. For each system, two architectures are examined, including a redundant, non-diverse configuration and a redundant, diverse configuration. The sensitivity analysis will provide insights on the impact of introducing diversity to system reliability. The importance measure results will help identify risk-significant and risk-sensitive components and failure modes, which may be good candidates for future design improvement.

Keywords: Nuclear power plant; digital instrumentation and control; probabilistic risk assessment; sensitivity analysis; importance measure

1. INTRODUCTION

The instrumentation and control (I&C) systems at nuclear power plants serve a critical role in providing reactor operators with plant monitoring signals, allowing operators to perform control actions and automatically performing reactor protection functions during accidental scenarios. The I&C modernization from analog systems to digital systems holds a significant potential to transform the plant operations of existing reactor fleet and fit in advanced reactor designs at an early phase. Employing digital technologies in the I&C systems are expected to address obsolescence issues with analog components, enhance control and increase operational efficiency, and improve overall plant safety.

[*] Sai.Zhang@inl.gov

However, simultaneously, it poses new challenges such as increased reliance on software and higher vulnerability to cyber-attacks. It is important to evaluate digital I&C designs and determine how these pros and cons compare, and how a design can be optimized to improve safety and lower risk.

Adding redundancy within systems or components is a common means of improving design safety; however, redundant systems are more prone to common-cause failures (CCFs). Introducing diversity into redundant systems or components is a way to mitigate and possibly eliminate CCFs, but it also increases plant complexity and may be costly. The balance between redundancy and diversity remains a challenge for digital I&C systems. This study performs sensitivity and importance measure analyses for four design architectures of two digital I&C systems. For each system, two architectures are examined, including a redundant, non-diverse configuration and a redundant, diverse configuration. The sensitivity analysis will provide insights on the impact of introducing diversity to system reliability. The importance measure results will help identify risk-significant and risk-sensitive components and failure modes, which may be good candidates for future design improvement.

2. SYSTEM DESIGN ARCHITECTURES

This study analyzes two digital I&C systems—the reactor-trip system (RTS) and the engineered safety features actuation system (ESFAS). The reference designs are based on digital I&C systems of the Advanced Power Reactor 1400 MW electricity (APR 1400) designed by the Korea Electric Power Corporation. The referenced design documents are publicly available on the United States Nuclear Regulatory Commission website as part of the design certification application package [1].

The RTS is a system that initiates reactor trips when required. The RTS initiates a reactor trip based on the signals from the sensors monitoring key plant operating parameters such as system temperature and pressure. When a pre-defined safety limit is reached, the RTS system will initiate a signal to open the reactor trip breakers. This action will remove power from the control rod drive mechanism so that the control rods can drop into the core by gravity, insert rapid negative reactivity, and shut down the reactor. A functional diagram of RTS is shown in Figure 1. The RTS in Figure 1 consists of four redundant divisions of components to monitor and ensure safety. Division-specific sensor signals are sent to the bistable processors (BPs), which determine whether a trip is needed. When required, trip signals from the BPs are sent to each division's local coincidence logic processors (LPs). The LPs vote on the incoming trip signals and send the output via digital output modules (DOMs) to selective relays, which again vote on the trip signals. The outputs of the selective relays pass through undervoltage trip devices (e.g., RTB-D1-UV in Figure 1) and activate the undervoltage reactor trip breakers (e.g., RTB-A1 in Figure 1). The success criteria for trip are given by the opening of a selected set of breakers.

The ESFAS is a system that activates a series of engineered safety features (ESFs) that perform critical protective actions (such as reactor coolant system inventory control and decay heat removal) given an accident. Examples of ESFs include safety injection system, auxiliary feedwater system, containment spray system, main steam isolation system, and containment isolation system. A functional diagram of ESFAS is shown in Figure 2. This four-division ESFAS in Figure 2 includes the portion of the plant protection system (PPS) that activates the ESFs and their component control system (CCS). ESF-CCS can generate ESF actuation signals and send them to ESF component interface modules (CIMs), which transmit signals to the final actuated device.

As one can imagine, a digital I&C system consists of numerous hardware and software components and could have a large number of failure paths. One failure path of many RTS-failure paths is shown as below ("←" means "caused by"): RTS system failure ← system actuation failure ← breaker failure ← undervoltage breaker trip failure ← logic cabinet rack failure ← digital output module failure ← local coincidence logic processor failure ← bistable processor failure. It can be seen from above that the RTS system failure can be traced down to as many as seven levels – very complicated. Processor failures can eventually lead to the RTS system failure.

Based on the APR1400 design, the RTS and ESFAS share the same set of bistable processors or BPs. In this study, design diversity is assumed as using different software for the BPs. For the baseline designs (i.e., Figures 1and 2), all BPs are assumed to use the same software. For the diverse designs, it is assumed that the BPs in four divisions use two different software, i.e., divisions A&C use software-1 and divisions B&D use software-2.

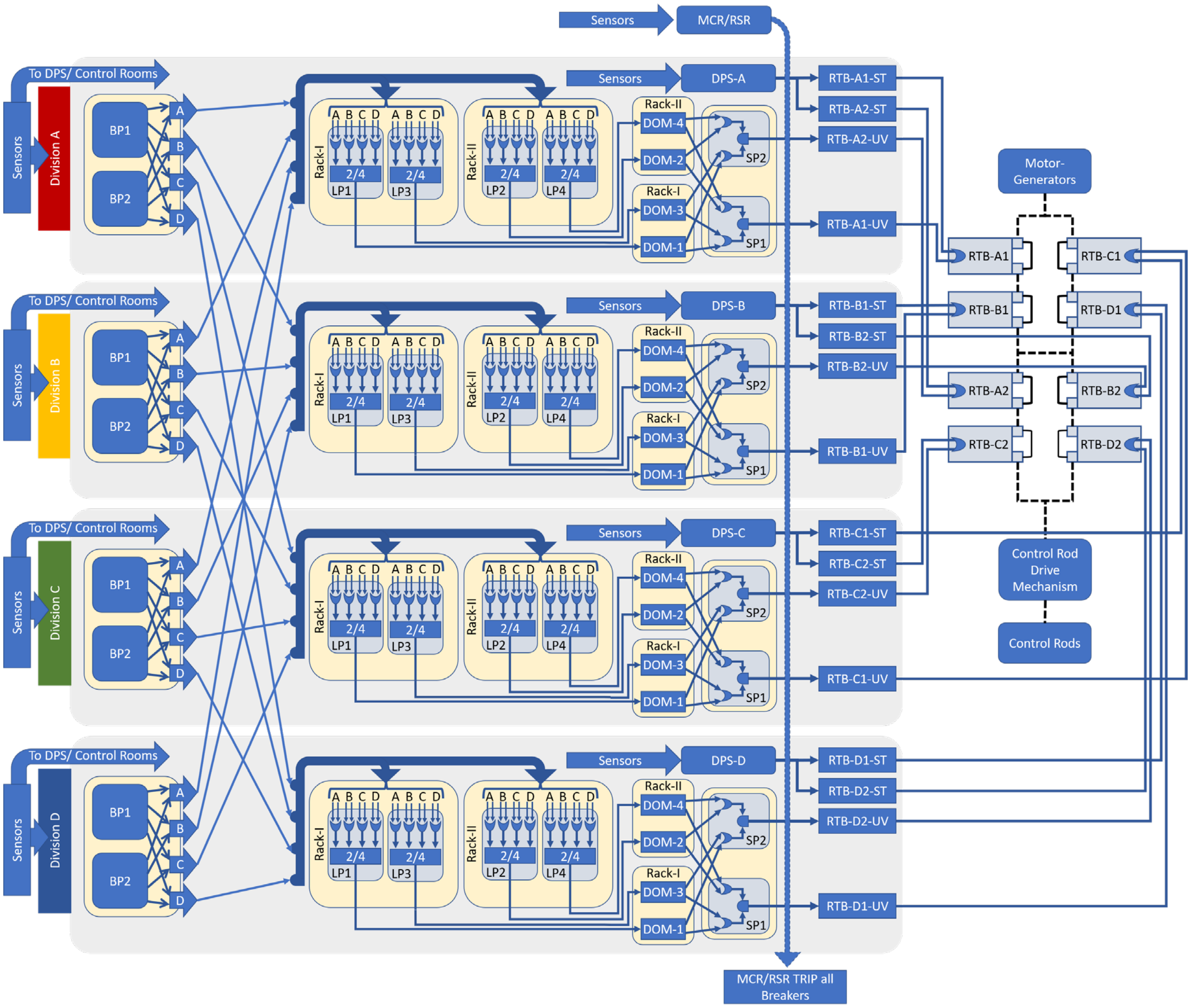

Figure 1. Functional diagram of a reactor trip system based on APR1400 design.

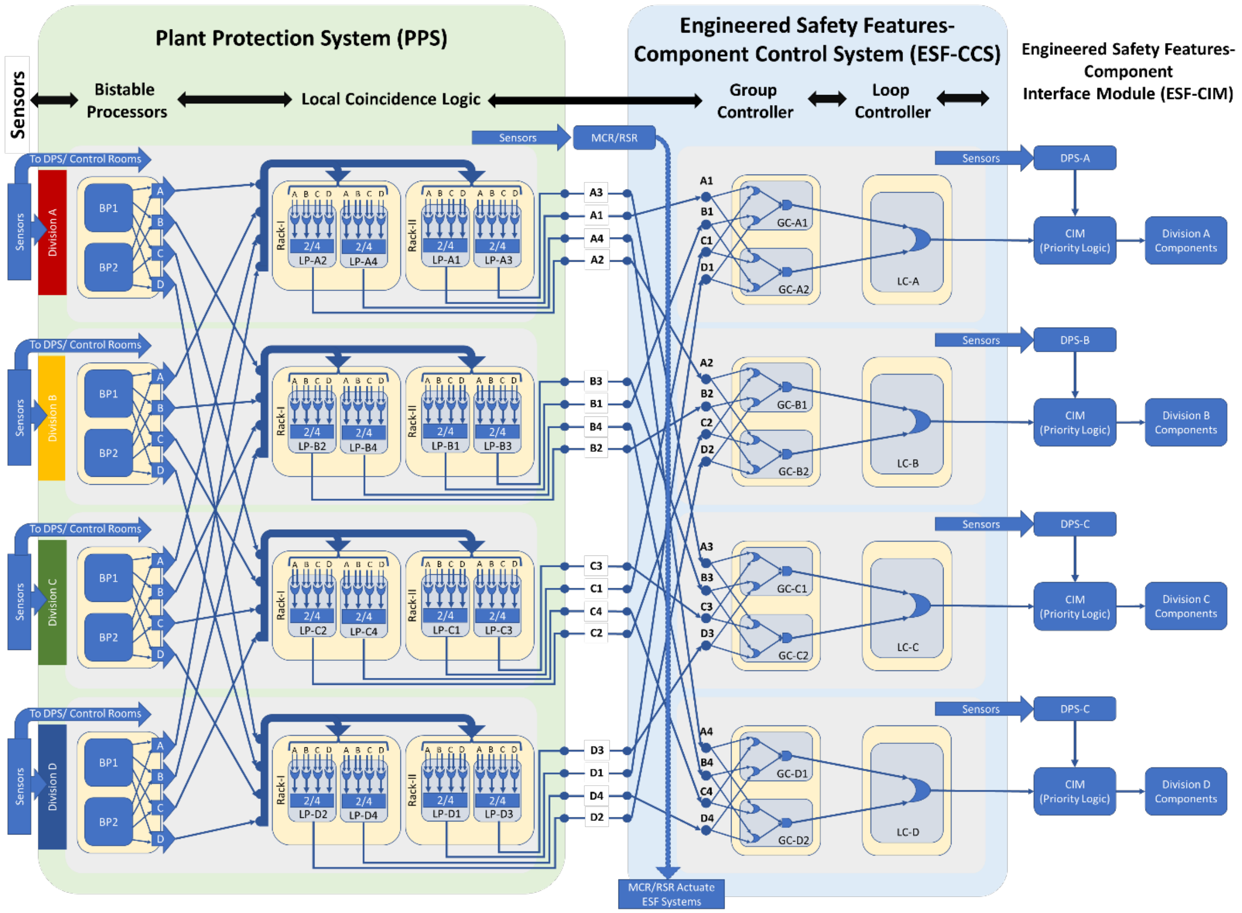

Figure 2. Functional diagram of an engineered safety feature activation system based on APR1400.

The importance measure and sensitivity analyses in this study were performed based on a probabilistic risk assessment (PRA) model of a generic pressurized-water reactor plant. A PRA model consists of event trees representing accident scenarios and fault trees representing system designs. The detailed models and parameter estimates are provided in [2, 3], while this paper presents two sub trees only in Figure 3 to illustrate the differences in fault tree models for the baseline design (i.e., using the same software for BPs) and diverse design (i.e., using different software for BPs) of the digital I&C systems.

The fault trees of baseline and diverse systems are mostly the same but differ in the sub trees representing single BP failures as shown in Figure 3, left for the baseline design and right for the diverse design. It can be observed that there are more BP software CCFs in the diverse design sub fault tree. This is because a single BP is placed in more software-related common cause component groups (CCCGs). In the baseline case, a single BP is placed in two software-related CCCGs, including a single-division-level group and a four-division-level group. In the diverse case, a single BP is placed in one more software-related CCCG including two divisions using the same software. The corresponding basic event probabilities (both independent failures and software CCFs) change accordingly as well if comparing the baseline design to the diverse design.

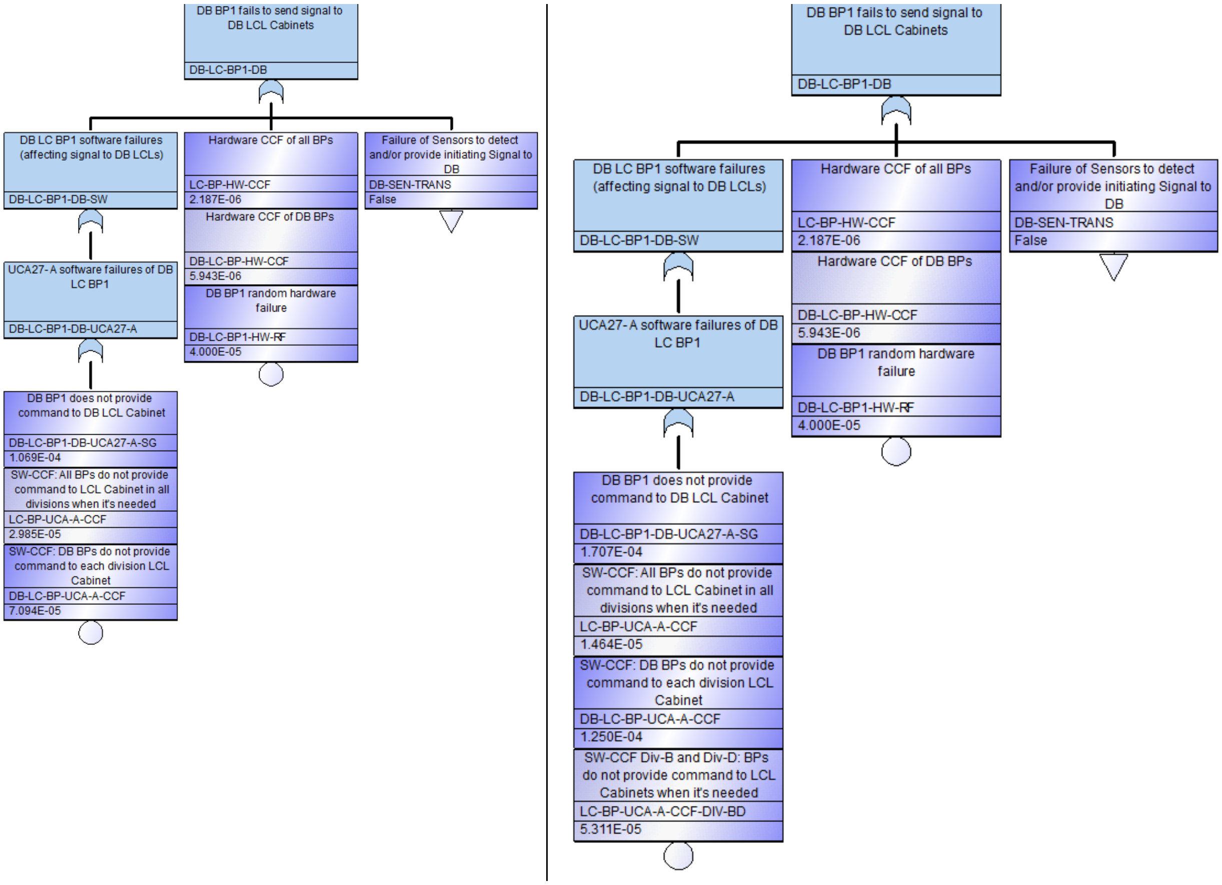
DB BP1 fails to send signal to DB LCL Cabinets
DB-LC-BP1-DB
DB LC BP1 software failures (affecting signal to DB LCLs)
DB-LC-BP1-DB-SW
Hardware CCF of all BPs
LC-BP-HW-CCF
2.187E-06
Hardware CCF of DB BPs
DB-LC-BP-HW-CCF
5.943E-06
DB BP1 random hardware failure
DB-LC-BP1-HW-RF
4.000E-05
Failure of Sensors to detect and/or provide initiating Signal to DB
DB-SEN-TRANS
False
UCA27-A software failures of DB LC BP1
DB-LC-BP1-DB-UCA27-A
DB BP1 does not provide command to DB LCL Cabinet
DB-LC-BP1-DB-UCA27-A-SG
1.069E-04
SW-CCF: All BPs do not provide command to LCL Cabinet in all divisions when it's needed
LC-BP-UCA-A-CCF
2.985E-05
SW-CCF: DB BPs do not provide command to each division LCL Cabinet
DB-LC-BP-UCA-A-CCF
7.094E-05
DB BP1 fails to send signal to DB LCL Cabinets
DB-LC-BP1-DB
DB LC BP1 software failures (affecting signal to DB LCLs)
DB-LC-BP1-DB-SW
Hardware CCF of all BPs
LC-BP-HW-CCF
2.187E-06
Hardware CCF of DB BPs
DB-LC-BP-HW-CCF
5.943E-06
DB BP1 random hardware failure
DB-LC-BP1-HW-RF
4.000E-05
Failure of Sensors to detect and/or provide initiating Signal to DB
DB-SEN-TRANS
False
UCA27-A software failures of DB LC BP1
DB-LC-BP1-DB-UCA27-A
DB BP1 does not provide command to DB LCL Cabinet
DB-LC-BP1-DB-UCA27-A-SG
1.707E-04
SW-CCF: All BPs do not provide command to LCL Cabinet in all divisions when it's needed
LC-BP-UCA-A-CCF
1.464E-05
SW-CCF: DB BPs do not provide command to each division LCL Cabinet
DB-LC-BP-UCA-A-CCF
1.250E-04
SW-CCF Div-B and Div-D: BPs do not provide command to LCL Cabinets when it's needed
LC-BP-UCA-A-CCF-DIV-BD
5.311E-05

Figure 3. Sub fault trees showing the failures of a single bistable processor in the baseline design (left) and diverse design (right).

3. SENSITIVITY ANALYSES FOR REACTOR TRIP SYSTEMS AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEMS

3.1. Reactor Trip Systems

This section calculates system-level failure probabilities of the baseline and diverse designs for RTS.

It can be observed from Table 1 that by introducing BP software diversity, the RTS failure probability is reduced by 5%. The reduction becomes more significant if focusing on the automatic actuation failure only, which decreases by 9% (Table 2). This is because the RTS function can be either achieved by automatic actuation or by manual actuation, and the software is involved in automatic actuation only.

Table 3 presents the dominant cut sets of RTS failure for baseline design and diverse design. For both designs, hardware CCF of rod cluster control assembly (RCCAs) to drop is the most dominant cut set. Each of the other dominant cut sets require the concurrence of an operator/human system interface (HSI) failure and a hardware or software CCF. By introducing BP software diversity, the cut set with concurrent operator/HSI failure and BP software CCF is reduced by 51% from 2.985E-07 to 1.464E-07.

The above results suggest that the introduction of BP software diversity can improve RTS reliability. It can reduce BP software CCF probability, reduce RTS automatic actuation failure probability, and thus reduce the failure probability of the entire RTS. The extent of failure probability reduction is expected to be larger when expanding the scope of diversity such as by adopting different software for each division, introducing diversity to BP hardware, introducing diversity to LP hardware and/or software.

Table 1. Failure probabilities of different RTS designs.

FT Name	RTS System Failure Probability	Δ / Non-Diverse	# of Cut Sets
RTS w/ software diversity	2.920E-06	−5%	123
RTS w/o software diversity	3.086E-06	0%	114

Table 2. Failure probabilities of automatic actuation in different RTS designs.

FT Name	RTS Automatic Actuation Failure Probability	Δ / Non-Diverse	# of Cut Sets
RTS w/ software diversity	1.566E-04	−9%	55
RTS w/o software diversity	1.718E-04	0%	44

Table 3. Dominant top cut sets with greater than-1% contribution of different RTS designs.

#	Cut Set Probability	Total %	Cut Set	Description
RTS design using different software to control bistable processors				
1	1.210E-06	41.44	RPS-ROD-CF-RCCAS	Hardware CCF of 10 or more rod cluster control assembly (RCCAs) to drop
2	1.179E-06	40.37	LC-LP-SF-CCF-TA	Software CCF of all LPs to provide trip commands to DOMs
			RPS-XHE-XE-SIGNL	Operator/human system interface (HSI) fails to respond with reactor protection system (RPS) signal present
3	1.763E-07	6.04	RTB-UV-HD-CCF	Hardware CCF of undervoltage trip mechanisms of all reactor trip breakers (RTBs)
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present
4	1.464E-07	5.01	LC-BP-UCA-A-CCF	Software CCF of all BPs to provide a trip command to each division's local coincidence logic (LCL) cabinet when needed
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present
5	3.961E-08	1.36	LP-HW-CCF	Hardware CCF of all LPs
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present
RTS design using the same software to control bistable processors				
1	1.210E-06	39.21	RPS-ROD-CF-RCCAS	Hardware CCF of 10 or more RCCAs to drop
2	1.179E-06	38.20	LC-LP-SF-CCF-TA	Software CCF of all LPs to provide trip commands to DOMs
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present
3	2.985E-07	9.67	LC-BP-UCA-A-CCF	Software CCF of all BPs to provide a trip command to each division's LCL cabinet when needed
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present
4	1.763E-07	5.71	RTB-UV-HD-CCF	Hardware CCF of undervoltage trip mechanisms of all RTBs
			RPS-XHE-XE-SIGNAL	Operator/HSI fails to respond with RPS signal present
5	3.961E-08	1.28	LP-HW-CCF	Hardware CCF of all LPs
			RPS-XHE-XE-SIGNL	Operator/HSI fails to respond with RPS signal present

3.2. Engineered Safety Features Actuation Systems

This section calculates system-level failure probabilities of improved non-diverse design and improved diverse design for ESFAS. It needs to be re-emphasized here that the BPs used in ESFAS are the same as those used in RTS. The LPs used in ESFAS in RTS are dedicated to one system only and are modeled as distinct basic events in the PRA model, although the same basic event values are used.

It can be observed from Table 4 that by introducing BP software diversity, the ESFAS failure probability is reduced by 5%. In the current PRA model, only automatic action of ESFAS failure is modeled. The 5% reduction represents the reduction of ESFAS automatic actuation failure probability, which is smaller than the 9% reduction of the corresponding RTS automatic actuation failure probability. Table 5 presents the dominant cut sets of ESFAS failure for baseline design and diverse design. For both designs, each of the dominant cut sets is a hardware or software CCF. By introducing BP software diversity, the cut set BP software CCF is reduced by 51% from 2.985E-05 to 1.464E-05.

The above results suggest that the introduction of BP software diversity can improve ESFAS reliability. It can reduce BP software CCF probability and thus reduce ESFAS failure probability. Based on the results from this section and Section 3.1, it can be concluded that introducing BP software diversity can simultaneously reduce RTS failure probability and ESFAS failure probability, each by 5%.

Table 4. Failure probabilities of different ESFAS designs.

FT Name	ESFAS System Failure Probability	Δ/Non-Diverse	# of Cut Sets
ESFAS w/ software diversity	3.028E-04	−5%	22
ESFAS w/o software diversity	3.180E-04	0%	11

Table 5. Dominant top cut sets with greater than-1% contribution of different ESFAS designs.

#	Cut Set Probability	Total %	Cut Set	Description
ESFAS design using different software to control bistable processors				
1	1.179E-04	38.93	LP-UCA-A-CCF	Software CCF of all LCL processors in all divisions to provide command when it is needed
2	8.914E-05	29.44	ESF-CCS-GC-UCA-A-CCF	Software CCF of all divisions of ESF-CCS GC processors to provide actuation signal when it is needed
3	6.842E-05	22.59	ESF-CCS-LC-UCA-A-CCF	Software CCF of all divisions of ESF-CCS LC processors to provide actuation signal
4	1.464E-05	4.83	LC-BP-UCA-A-CCF	Software CCF of all BPs to provide a trip command to each division’s LCL cabinet when needed
5	3.961E-06	1.31	LP-HW-CCF	Hardware CCF of all LCL processors
ESFAS design using the same software to control bistable processors				
1	1.179E-04	37.07	LP-UCA-A-CCF	Software CCF of all LCL processors in all divisions to provide command when it is needed
2	8.914E-05	28.03	ESF-CCS-GC-UCA-A-CCF	Software CCF of all divisions of ESF-CCS GC processors to provide actuation signal when it is needed
3	6.842E-05	21.51	ESF-CCS-LC-UCA-A-CCF	Software CCF of all divisions of ESF-CCS LC processors to provide actuation signal
4	2.985E-05	9.39	LC-BP-UCA-A-CCF	Software CCF of all BPs to provide a trip command to each division’s LCL cabinet when needed
5	3.961E-06	1.25	LP-HW-CCF	Hardware CCF of all LCL processors

4. IMPORTANCE MEASURE ANALYSES FOR REACTOR TRIP SYSTEMS AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEMS

This section calculates system-level importance measures of improved non-diverse designs and improved diverse designs for the RTS and the ESFAS. In this section, the importance measure analysis refers to an analysis that utilizes a PRA model to measure impact of model inputs on total risk and quantifies the impacts from separated factors on total risk; in other words, the importance measure analysis examines the impacts of individual factors one at a time. The components with relatively high importance measures are suggested as worth-watching candidates for different purposes such as prioritizing investments to make design changes and increase system reliability.

In practice, the importance measures are usually calculated at the core damage frequency (CDF) level. However, as informed by the sensitivity analysis results in [2], the impacts of introducing BP software diversity on CDF values from different scenarios are not significant. Hence, the importance measures in this section are calculated at a system level.

The importance measures are calculated using a PRA software, SAPHIRE (The Systems Analysis Programs for Hands-on Integrated Reliability Evaluations). SAPHIRE provides seven different basic event importance measures, which can be categorized in three types: (1) ratio importance measures, including Fussell-Vesely Importance (FV), Risk Reduction Ratio, and Risk Increase Ratio; (2) interval importance measures, including Birnbaum Importance (Birnbaum), Risk Reduction Interval, and Risk Increase Interval; (3) uncertainty importance [4]. The current PRA model for the DI&C systems for this study hasn't included uncertainty analysis yet, so uncertainty importance measure is not applicable at this moment. Two common measures, FV and Birnbaum are selected for this study to represent ratio-type measures and interval-type measures, respectively.

The mathematical equations of these two measures are not provided in this section and can be found in [4]. Conceptually, FV measures the overall percent contribution of cut sets containing a basic event of interest to the total risk, which is the RTS or ESFAS failure probability here; Birnbaum measures the rate of change in total risk (again, the RTS or ESFAS failure probability here) as a result of changes to the probability of an individual basic event. A high FV indicates a higher importance, so does a higher Birnbaum. Two commonly used cutoff values, i.e., FV > 0.005 and Birnbaum > 0.0001, are selected for the analyses in this study.

Table 6 and Table 7 present importance measures of basic events with regard to failure probabilities of different RTS and ESFAS designs. From the results in these tables, it can be observed that the FV rankings and the Birnbaum rankings do not necessarily agree. In other words, a basic event with a high FV does not necessarily have a high Birnbaum. Taking the results in Table 6 as an example, among all the basic events in the non-diverse RTS FT, the basic event RPS-XHE-XE-SIGNL (operator/HSI fails to respond with RPS signal present) has the highest FV and the CCF event RPS-ROD-CF-RCCAS (CCF of 10 or more RCCAs fail to drop) has the highest Birnbaum. This can be interpreted as that RPS-XHE-XE-SIGNL has a high marginal probability and thus poses high impact on system failure probability. However, RPS-ROD-CF-RCCAS has a high risk (i.e., system failure) sensitivity; this suggests that it can be a good candidate for future investment, since just a little improvement of design and a little reduction of this CCF potential can significantly reduce system failure probability.

By comparing the results for different RTS designs in Table 6, it can be observed that the importance measures and basic event rankings for non-diverse RTS and diverse RTS mostly remain the same, with slight changes in FV values and Birnbaum values, as well as the ranking swap of the events RTB-UV-HD-CCF (hardware CCF of undervoltage trip mechanism of all RTBs) and LC-BP-UCA-A-CCF (software CCF of all BPs to provide command to LCL cabinet in all divisions when it is needed). In both RTS designs, RPS-XHE-XE-SIGNL has the highest FV and RPS-ROD-CF-RCCAS has the highest Birnbaum. Four events, including LC-LP-SF-CCF-TA, RTB-UV-HD-CCF, LC-BP-UCA-A-CCF, and LP-HW-CCF, have the same second highest Birnbaum as well as high FV rankings, which can be taken as good candidates for future investment priorities of design improvements.

By comparing the results for different ESFAS designs in Table 7, it can be observed that the importance measures and basic event rankings for non-diverse ESFAS and diverse ESFAS mostly remain the same, only with slight changes in FV values. As a result of introducing BP software diversity, the FV value of LC-BP-UCA-A-CCF (software CCF of all BPs to provide command to LCL cabinet in all divisions when needed) is reduced by 49% from 0.0939 to 0.0483. Another observation is that all the basic events with a non-truncated importance measure have the same Birnbaum value, so the suggestion for future prioritization could be based on FV values only. It should be noted that for both non-diverse ESFAS and diverse ESFAS, the FVs of software CCF events are higher than the FVs of hardware CCF events, suggesting that future investment might be prioritized to reduce software CCF potentials.

Table 6. Importance measures (top five) of basic events within fault tree of RTS designs.

#	Name	Prob	FV	Birnbaum
RTS design using different software to control bistable processors				
1	RPS-XHE-XE-SIGNL	1.00E-02	5.36E-01	1.57E-04
2	LC-LP-SF-CCF-TA	1.18E-04	4.41E-01	1.09E-02
3	RPS-ROD-CF-RCCAS	1.21E-06	4.14E-01	1.00E+00
4	RTB-UV-HD-CCF	1.76E-05	6.59E-02	1.09E-02
5	LC-BP-UCA-A-CCF	1.46E-05	5.48E-02	1.09E-02
RTS design using the same software to control bistable processors				
1	RPS-XHE-XE-SIGNL	1.00E-02	5.57E-01	1.72E-04
2	LC-LP-SF-CCF-TA	1.18E-04	4.17E-01	1.09E-02
3	RPS-ROD-CF-RCCAS	1.21E-06	3.92E-01	1.00E+00
4	LC-BP-UCA-A-CCF	2.99E-05	1.06E-01	1.09E-02
5	RTB-UV-HD-CCF	1.76E-05	6.24E-02	1.09E-02

Table 7. Importance measures (top five) of basic events within fault tree of ESFAS designs.

#	Name	Prob	FV	Birnbaum
ESFAS design using different software to control bistable processors				
1	LP-UCA-A-CCF	1.18E-04	3.89E-01	1.00E+00
2	ESF-CCS-GC-UCA-A-CCF	8.91E-05	2.94E-01	1.00E+00
3	ESF-CCS-LC-UCA-A-CCF	6.84E-05	2.26E-01	1.00E+00
4	LC-BP-UCA-A-CCF	1.46E-05	4.83E-02	1.00E+00
5	LP-HW-CCF	3.96E-06	1.31E-02	1.00E+00
ESFAS design using the same software to control bistable processors				
1	LP-UCA-A-CCF	1.18E-04	3.71E-01	1.00E+00
2	ESF-CCS-GC-UCA-A-CCF	8.91E-05	2.80E-01	1.00E+00
3	ESF-CCS-LC-UCA-A-CCF	6.84E-05	2.15E-01	1.00E+00
4	LC-BP-UCA-A-CCF	2.99E-05	9.39E-02	1.00E+00
5	LP-HW-CCF	3.96E-06	1.25E-02	1.00E+00

5. CONCLUSIONS

This study performs sensitivity and importance measure analyses for four design architectures of two digital I&C systems—the RTS and the ESFAS. For each system, two architectures are examined, including a redundant, non-diverse configuration and a redundant, diverse configuration. The findings from the results are summarized: (1) By introducing BP software diversity, notable reductions in system-level risks are observed (i.e., RTS failure probability and ESFAS failure probability are both reduced by 5%). However, the reductions in dominant cut sets are found to be substantial (i.e., the probability of cut set with concurrent operator/HSI failure and BP software CCF is reduced by 51%). (2) By introducing BP software diversity, it can be observed that for both RTS and ESFAS, the importance measures and basic event rankings mostly remain the same, except for the FV value of LC-BP-UCA-A-CCF (software CCF of all BPs to provide command to LCL cabinet in all divisions when needed) is reduced by 49%.

ACKNOWLEDGMENTS

The research activities and achievements documented in this paper were funded by the United States Department of Energy's Light Water Reactor Sustainability Program, Risk Informed Systems Analysis (RISA) Pathway. This submitted manuscript was authored by a contractor of the U.S. Government under DOE Contract No. DE-AC07–05ID14517. Accordingly, the U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

REFERENCES

1. Korea Hydro-Nuclear Power Co., Ltd. (2018). APR1400 design control document. Tier 2. Chapter 7. Instrumentation and Controls. Revision 3. United States Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML1822/ML18228A654.pdf
2. Bao, H., Zhang, S., Youngblood, R., Shorthill, T., Pandit, P., Chen, E., Park J., Ban, H., Diaconeasa, M., Dinh, N., & Lawrence, S. (2022). Risk analysis of various design architectures for high safety-significant safety-related digital instrumentation and control systems of nuclear power plants during accident scenarios. INL/RPT-22-70056. Idaho National Laboratory. https://lwrs.inl.gov/RiskInformed%20Safety%20Margin%20Characterization/DIC_Technologoies.pdf
3. Bao, H., Lawrence, S., Park, J., Ban, H., Chen, E., Dinh, N., Jayakumar, A., Elks, C., Zhang, H., Quinn, E., Zhang, S., & Shorthill, T. (2022). An Integrated Framework for Risk Assessment of High Safety Significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants: Methodology and Demonstration. INL/RPT-22-68656. Idaho National Laboratory. https://doi.org/10.2172/1924498
4. C. Smith, J. Knudsen, K. Vedros, M. Calley, K. Kvarfordt and T. Wood. (2016). SAPHIRE 8 Basics An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software. Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_1039.pdf