INL/CON-22-70268-Revision-0

Advanced Human-System Interface Risk Analysis Based on Redundancy-guided Systems-theoretic Hazard Analysis and Human Reliability Analysis

July 2023

Jooyoung Park

Changing the World's Energy Future

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

INL/CON-22-70268-Revision-0

Advanced Human-System Interface Risk Analysis Based on Redundancy-guided Systems-theoretic Hazard Analysis and Human Reliability Analysis

Jooyoung Park

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

Advanced Human-System Interface Risk Analysis Based on Redundancy-guided Systems-theoretic Hazard Analysis and Human Reliability Analysis

Jooyoung Park[1]*, Edward Chen[2], Han Bao[1], Tate Shorthill[3], Jisuk Kim[1], Sai Zhang[1], Ronald Boring[1]

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

[leave space for DOI, which will be inserted by ANS]

ABSTRACT

Human-system interfaces (HSIs) play an important role in enabling operators to communicate with the nuclear power plant (NPP) side. Getting the information required to understand a NPP's curren t status or perform necessary actions for responding to a given operational context are representati ve operator tasks performed using HSIs. To date, HSIs have been mainly evaluated in the context of human reliability analysis (HRA). However, the current HSI evaluation that occurs during HRA may be challengeable on two fronts: (1) reflecting the unique characteristics of HSI systems and (2) considering situations in which HSIs are poorly operated due to software/hardware malfunctions. Accordingly, this study proposes an approach for specifically evaluating HSIs for digital instrume ntation and controls (DI&C) systems, using Redundancy-guided Systems-theoretic Hazard Analys is (RESHA) and HRA. RESHA is a method for analyzing DI&C systems with redundancy feature s. In this study, we investigate how HSIs are evaluated in existing HRA methods, and what challen ges exist in the current approaches. To better evaluate HSIs for DI&C systems, this study modifies the existing HSI evaluation process by additionally modeling the HSI back- and front- ends. In thi s paper, a HSI fault tree for the APR1400 DI&C system is introduced through a piping and instru mentation diagram. It then touches upon what aspects of the suggested method must be further res earched.

Keywords: Human-System Interface, Digital I&C, Human Reliability Analysis, Risk Analysis

1. INTRODUCTION

In probabilistic risk assessment (PRA), the design of human system interfaces (HSIs) has been mainly considered and evaluated in terms of human reliability analysis (HRA) [1, 2]. HSIs play an important role in enabling operators to communicate with the nuclear power plant (NPP) side (e.g., getting the information required to understand a NPP's current status or perform necessary actions for responding to a given operational context). In HRA, it has been assumed that good/poor HSIs decrease/increase human error probabilities (HEPs). This notion is based on the performance-shaping factor (PSF) concept, which highlights error contributors and adjusts nominal HEPs in respect to PSFs such as stress, HSI, or task complexity.

Application of digital technology is a recent trend in the design of NPP main control rooms (MCRs) [3]. Newly constructed NPPs in various countries around the globe (e.g., the APR1400 in Korea [4], AP1000 in the United States [5], and EPR-1600 in France [6]) adopt fully digitalized and computerized MCRs. Digital MCRs possess characteristics that distinguish them from conventional (i.e., analog) MCRs. These traits include increased automation and the use of computer-based HSIs and/or intelligent operator aids. Many researchers believe these new features carry the potential to improve both human performance and nuclear safety. However, digital technologies have been known to increase the potential for common

* Jooyoung.Park@inl.gov

cause failure vulnerabilities due to redundancy within digital instrumentation and control (DI&C) systems, interactions between the system components and the controlled processes, or interactions among the various components themselves [7]. Accordingly, the current PSF-based HRA approach may be insufficient for specifically reflecting the risk carried by digital HSIs that present (or summarize) the information flow of DI&C systems.

This study proposes a method of specifically evaluating HSIs for DI&C systems, based on Redundancy-guided Systems-theoretic Hazard Analysis (RESHA) [7, 8] and HRA. RESHA, a method for analyzing DI&C systems with redundancy features, was technically developed based on the Systems-Theoretic Process Analysis method [9]. RESHA identifies the hazards and failure modes of digital systems and provides a foundation for quantification efforts such as reliability and consequences analyses. In this study, we investigate how HSIs are evaluated in existing HRA methods, and what challenges exist with the current approaches. To better evaluate HSIs for DI&C systems, we modified the existing HSI evaluation process by additionally modeling the HSI back- and front- ends. In this paper, a HSI fault tree for the APR1400 DI&C system is introduced through a piping and instrumentation diagram. We then touch upon what must be further researched in the suggested method.

2. HSI EVALUATION IN EXISTING HRA METHODS

As mentioned in Section 1, HSIs have been mainly evaluated in the context of HRA. Table I summarizes the various HSI-related PSFs, as well as the capabilities of four different HRA methods to properly evaluate these PSFs. These four methods are the Standardized Plant Analysis Risk HRA [2], Cause-based Decision Tree (CBDT) [11], Cognitive Reliability and Error Analysis Method [12], and Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA) [13]. In HRA, practitioners review the HSIs required for human actions, determine their PSF levels, then use them to estimate the final HEPs.

The current HSI evaluation process that occurs during HRA may be challengeable on two fronts. First, it rarely reflects the unique characteristics of HSI systems (e.g., analog or digital), but instead mainly focuses on the specific or overall qualities of the HSIs themselves. In other words, the current HRA methods are useful for ascertaining whether or not a HSI is good, but cannot determine whether an analog HSI is superior to a digital one, or which of two different digital HSIs is superior. This may lead to inconsistencies in HRA results generated from different HSIs. Second, the current HSI evaluation approach concentrates on the relationship between HSI designs and human performance (i.e., HEPs), but none of the software/hardware aspects of HSIs are considered when conducting HRA. In other words, hardware/software is essentially assumed to work perfectly when performing tasks that require HSIs. However, this may not in fact be the case. Furthermore, certain critical tasks may reflect higher error possibilities, or lead to guaranteed failure in situations involving hardware/software malfunctions. Nevertheless, this remains an area not specifically addressed in existing HRA.

Table I. Summary of How HSI-related PSFs Are Handled in Four Different HRA Methods

HRA Method	PSF	PSF Level
Standardized Plant Analysis Risk HRA [2]	Ergonomics/HSI	Missing/misleading
		Poor
		Nominal
		Good
		Insufficient information
CBDT [11]	Indicator available in control room	Yes
		No
	Accuracy of control room indicator	Yes
		No
	Front vs. back panel	Front
		Back
	Alarmed vs. not alarmed	Alarmed
		Not alarmed

	Indicator easy to locate	Easy
		Not easy
	Good/bad indicator	Good
		Bad
Cognitive Reliability and Error Analysis Method [12]	Adequacy of HSI and operational support	Supportive
		Adequate
		Tolerable
		Inappropriate
IHEAS-ECA [13]	HSI	No impact
		Indicator is similar to other nearby sources of information
		No sign or indication of any technical difference from adjacent sources (meters, indicators)
		Information regarding a given task is spatially distributed, unorganized, or cannot be accessed in simultaneous fashion
		Unintuitive or unconventional indications
		Poor salience of the target (indicators, alarms, alerts) out of the crowded background
		Inconsistent formats, units, symbols, or tables
		Inconsistent interpretation of displays
		Similarity in elements
		Poor functional localization
		Ergonomic deficits
		Labeling of the controls is confusing or does not agree with the document nomenclature
		Controls lack labels or indications
		Controls provide inadequate or ambiguous feedback
		Confusion in action maneuver states
		Unclear functional allocation

3. APPROACH TO HSI EVALUATION FOR DI&C SYSTEMS

To handle the two issues introduced in Section 2, and to specifically evaluate HSIs by reflecting the specific structures and characteristics of DI&C systems, this study enlarges the scope of the existing HSI evaluation process in the manner illustrated in Figure 1.

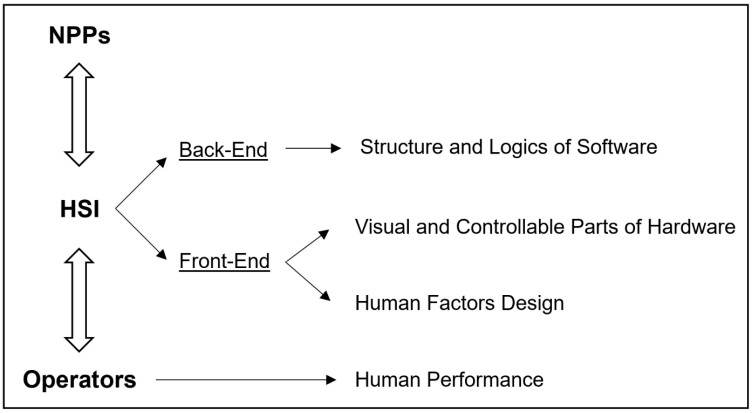


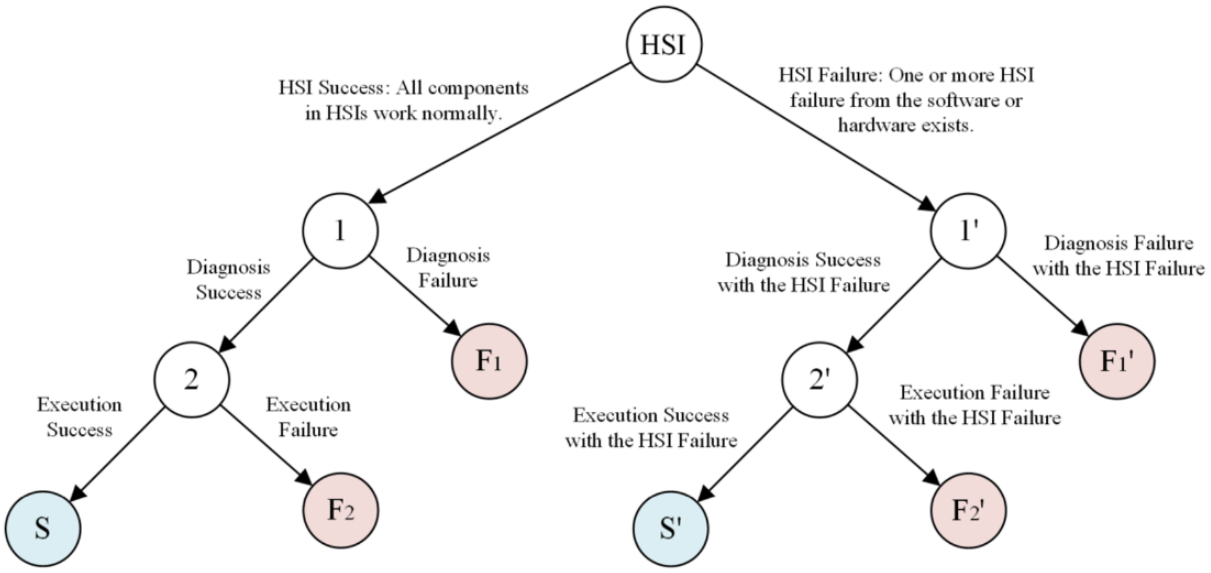
Figure 1. Extension of HSI Evaluation Process via the Suggested Approach

The approach suggested in the present study additionally considers the HSI back- and front- ends, whereas the current HSI evaluation process concentrates solely on HSI quality. The HSI front-end mainly focuses on visual and controllable aspects of the hardware, including human factors design. The back-end includes the software structure and logics. Thus, through detailed modeling of both the back- and the front- ends, this approach evaluates the potential risks carried by digital HSIs.

As this approach alters the manner in which HSIs are evaluated, the present study suggests that the existing quantification method be updated. In existing HRA, a human failure event can be divided into two portions: diagnosis and execution. The final HEP is calculated by summing together the HEPs for both.

The quantification method employed in the suggested approach (see Figure 2) distinguishes between two different types of situations: (1) situations in which HSIs operate successfully and (2) situations in which the HSIs are failed. The first is the same type of situation covered in the existing HRA approach. But in the second type of situation, a human failure event is evaluated whenever a HSI is failed, provides wrong information due to software failure, or is uncontrollable due to such things as hardware failure. In the suggested method, these detailed HSI conditions are specifically modeled via RESHA [7, 8], which offers a structured way of modeling hardware/software failure in DI&C systems. RESHA's outputted summaries of HSI conditions are generated as fault trees (i.e., HSI fault trees). The quantitative values in the fault trees come from [13], as well as from the unavailability equations suggested by the fault tree theory of PRA [13].

HRA methods are used to quantify a human action in the two different HSI conditions. The suggested approach currently employs the CBDT and IDHEAS-ECA methods, since they provide relatively specific guidance for analyzing the quality of HSIs (see Table I).



$$HEP_{Final} = HEP_{HSI\_Success} + HEP_{HSI\_Failure}$$

$$HEP_{HSI\_Success} = HEP_{Diagnosis} + HEP_{Execution}$$

$$HEP_{HSI\_Failure} = P_{HSI\ Failure} \cdot (HEP_{Diagnosis\ with\ the\ HSI\ Failure} + HEP_{Execution\ with\ the\ HSI\ Failure})$$

Figure 2. Quantification via the Suggested Approach

4. DEVELOPMENT OF AN HSI FAULT TREE FOR THE APR1400 DI&C SYSTEM

This section mainly explores how we developed an HSI fault tree (a term introduced in Section 3). The HSI fault tree includes degraded HSI conditions and affects the human action of initiating a manual reactor trip. Upon completing review, the APR1400 DI&C system [15] was used to develop the HSI fault tree, in combination with RESHA. Within the APR1400 DI&C system, those subsystems of greatest relevance to the human action (i.e., QIAS-P, core protection calculator system [CPCS], IPS, and QIAS-N) were specifically modeled in the HSI fault tree.

Those particular subsystems provide all the necessary information for achieving safe plant shutdown and performing emergency operating procedures. First, as a safety-graded system, QIAS-P provides unambiguous indicators of inadequate core cooling, and affords advanced warning if such as state is being approached. It also acts as a continuous source of accident-monitoring information under both nominal and emergency scenarios. Second, the CPCS calculates important values related to core cooling and protection (e.g., departure from nucleate boiling and local power density) and provides them to other DI&C sub systems. Third, as a non-safety-related instrumentation and controls (I&C) system, QIAS-N receives analog and digital signals from both safety- and non-safety-related systems, analyzes the data, and presents the resulting information to the operator via the QIAS-N front panel displays, mini-large display panel, and shutdown overview display panel. Lastly, IPS—as a non-safety-related I&C system—collects relevant sensor information and determines plant states. IPS and QIAS-N are independent and diverse from each other. The IPS information is processed and then sent to the IPS information flat panel display, safety parameter display and evaluation system+, or computer-based procedure system (CPS).

Figure 3 shows the piping and instrumentation diagrams for QIAS-P, CPCS, IPS, and QIAS-N. The details of these diagrams were assumed based on the APR1400 DI&C system. First, in the figure, the QIAS-P is simplified into a diagram, having already been analyzed in our previous study [13]. The information from the QIAS-P is provided to the QIAS-N processor and the IPS server. Second, the CPCS, which has four divisions (i.e., A, B, C, and D), offers several modules for calculating core-related values such as departure from nucleate boiling and local power density, based on plant parameters (e.g., hot leg temperature). The CPCS then sends the values to the QIAS-N processor and the IPS server. Third, the QIAS-N system's processor, primary and backup controllers, server, and alarm processing function help gather plant information and analyze the data, while the QIAS-N front panel displays, mini-large display panel, and shutdown overview display panel present the information to operators in MCRs. Lastly, the IPS encompasses (1) the primary and dedicated backup servers for collecting information from the QIAS-P and CPCS, (2) the alarm processing system, and (3) applications such as the IPS information flat panel display, safety parameter display and evaluation system+, and CPS.

Figure 4 shows the top event of the HSI fault tree. The top event logic consists of fault tree gates that represent those cases in which QIAS-P, IPS, and QIAS-N fail to notify operators via an alarm, and fail to accurately reflect safety variables under a degraded reactor state. Figure 5 shows the fault tree logic for QIAS-N.

This study calculates failure probabilities and cutsets for three DI&C subsystem (i.e., QIAS-P, QIAS-N, and IPS), as well as for the top event. This fault tree is quantified by utilizing SAPHIRE 8, using truncation level 1E-12. Table II compares failure probabilities, numbers of cutsets, and cutset rankings for the top event, QIAS-P, QIAS-N, and IPS. The failure probability of the top event is 9.207E-4 with 394 cutsets. The failure probabilities for QIAS-N and IPS are 4.837e-4 and 5.337e-4, respectively, whereas that of QIAS-P is 9.663E-5. In other words, the safety-critical I&C system (i.e., QIAS-P) shows a lower failure probability than the non-safety-related I&C systems (i.e., QIAS-N and IPS). Note that the basic events from QIAS-N and IPS account for cutset rankings #1–5 in the failure probability of the top event.

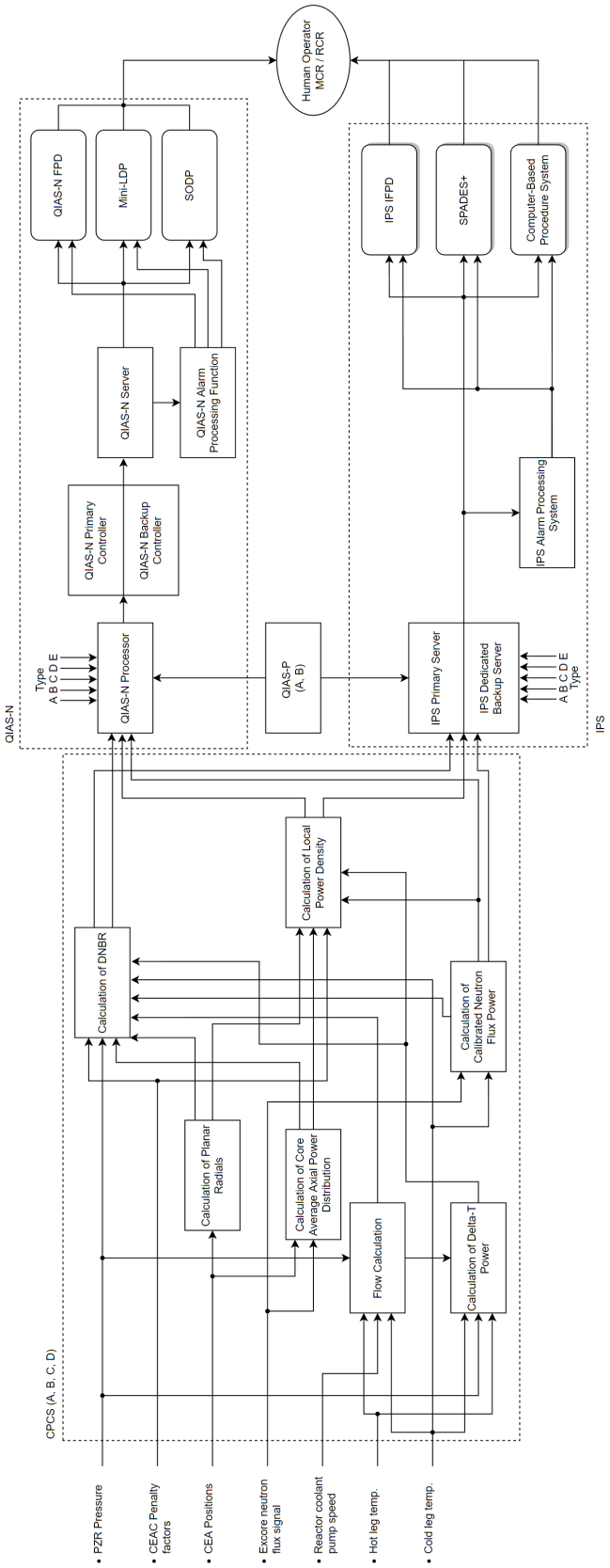


Figure 3. Piping and Instrumentation Diagram for QIAS-P, CPCS, IPS, and QIAS-N

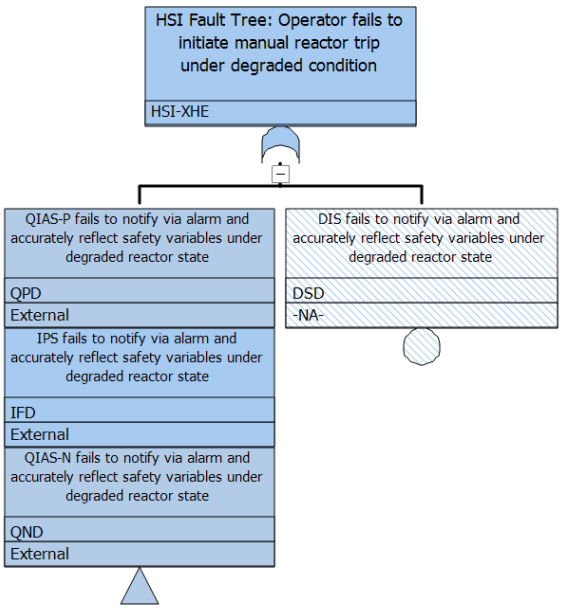


Figure 4. Top Event of the HSI Fault Tree

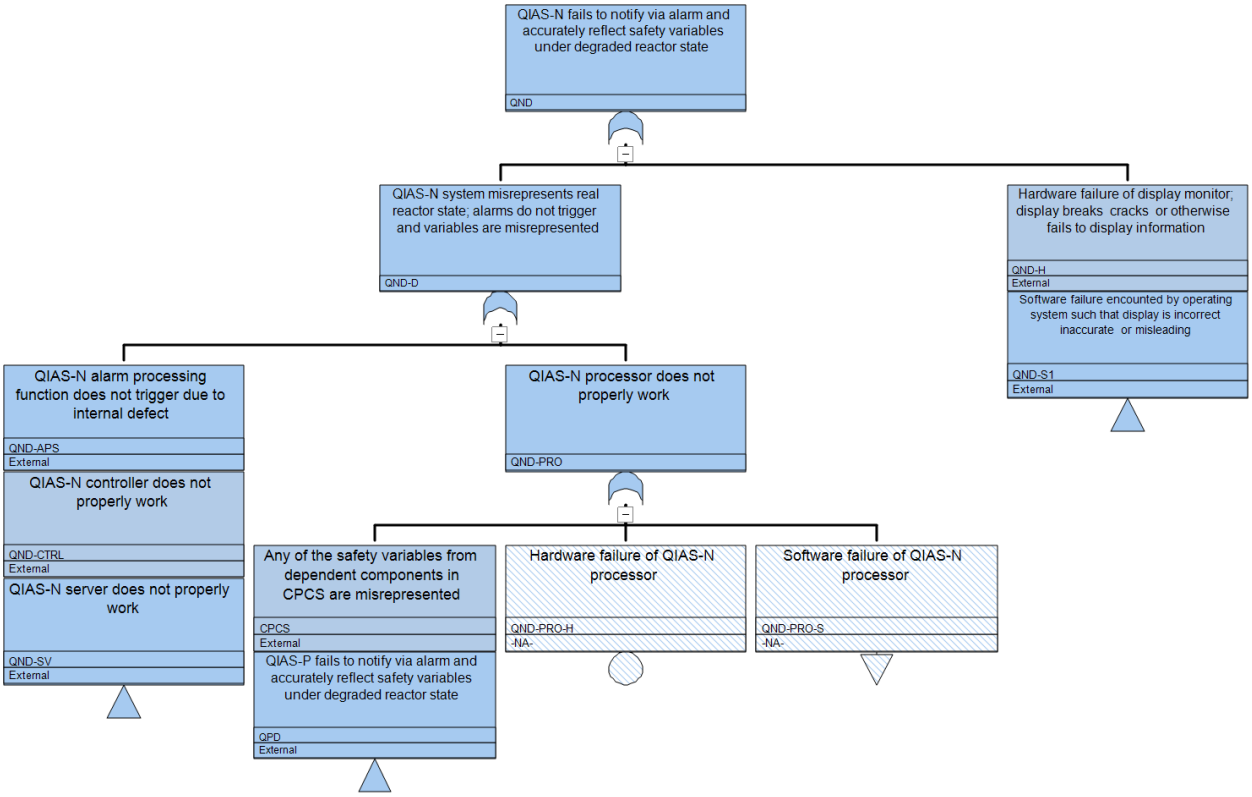


Figure 5. Fault Tree Logic for QIAS-N

Table II. Comparison of Failure Probabilities, Numbers of Cutsets, and Cutset Rankings

		Top Event	QIAS-P	QIAS-N	IPS
Failure Probability		9.207e-4	9.663e-5	4.837e-4	5.337e-4
# of Cutsets		394	383	388	389
Cutset Ranking	**#1**	QND-APS-UIFA	QPD-H	QND-APS-UIFA	IFD-APS-UIFA
	#2	IFD-APS-UIFA	QPD-PA-CTC-S-CFD	QND-APS-H	IFD-SPA-H
	#3	QND-APS-H	QPD-PA-RCS-S-CFD	QND-SV-H	QPD-H
	#4	IFD-SPA-H	QPD-PA-HJC-S-CFD	QPD-H	IFD-APS-H
	#5	QND-SV-H	QPD-PA-RLC-S-CFD	QND-PRO-H	IFD-CPS-H

5. CONCLUSIONS

This study is part of ongoing research to specifically evaluate—via RESHA and HRA—DI&C system HSIs. However, the information covered herein is not exhaustive, as the approach remains under development. The areas of further research, summarized below, account for the missing contents in the approach suggested in Section 3. Further details on these areas will be presented at the conference.

- Which HRA method is adequate for quantifying HEPs under degraded HSI conditions?
- How are degraded HSI conditions handled in the HRA method?
- In terms of risk assessment, how meaningful are HEPs calculated via the suggested method, and to what extent do they contribute to the risk matrix of PRA (e.g., core damage frequencies)?
- How can we quantify hardware failure probabilities to which the data do not apply?

ACKNOWLEDGMENTS

The research activities and achievements documented in this paper were funded by the U.S. Department of Energy (DOE)'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] J. Park, A. Arigi and J. Kim, "A comparison of the quantification aspects of human reliability analysis methods in nuclear power plants," *Annals of Nuclear Energy,* vol. 133, pp. 297-312, 2019.

[2] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H human reliability analysis method, NUREG/CR-6883," US Nuclear Regulatory Commission, 2005.

[3] J. Park, D. Lee, W. Jung and K. Jonghyun, "An experimental investigation on relationship

between PSFs and operator performances in the digital main control room," *Annals of Nuclear Energy,* vol. 101, pp. 58-68, 2017.

[4] "Development of human performance measures for human factors validation in the advanced MCR of APR-1400," *IEEE transactions on nuclear science,* vol. 54(6), pp. 2687-2700, 2007.

[5] W. E. Cummins, M. M. Corletti and T. L. Schulz, "Westinghouse AP1000 advanced passive plant," in *Proceedings of ICAPP*, 2003.

[6] R. C. Twilley, "EPR development-an evolutionary design process," *Nuclear News,* vol. 47(4), pp. 26-30, 2004.

[7] 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, p. 107686, 2020.

[8] T. Shorthill, H. Bao, H. Zhang and H. Ban, "A Redundancy-Guided Approach for the Hazard Analysis of Digital Instrumentation and Control Systems in Advanced Nuclear Power Plants," *Nuclear Technology,* vol. 208, pp. 892-911, 2022.

[9] N. G. Leveson and J. P. Thomas, STPA Handbook, 2018.

[10] G. Parry, A. Beare, A. Spurgin and P. Moieni, "An approach to the analysis of operator actions in probabilistic risk assessment, EPRI Report TR-100259," 1992.

[11] E. Hollnagel, Cognitive reliability and error analysis method (CREAM), Elsevier, 1998.

[12] J. Xing, J. Chang and J. DeJesus, "Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA), RIL-2020-02," US Nuclear Regulatory Commission, 2020.

[13] H. Bao, T. Shorthill, E. Chen, J. Park, S. Zhang, A. V. Jayakumar, C. Elks, H. Ban, H. Zhang, E. Quinn and S. Lawrence, "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, 2022.

[14] W. Vesely, F. Goldberg, N. Roberts and D. Haasl, "Fault tree handbook," US Nuclear Regulatory Commission, 1981.

[15] KHNP, "Chapter 7: Instrumentation and Controls. Rev 3," US Nuclear Regulatory Comission, 2018.