U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

TECHNICAL LETTER REPORT
TLR-RES/DE-2022-006

HAZARD ANALYSIS: AN OUTLINE OF TECHNICAL BASES FOR THE EVALUATION OF CRITERIA, METHODOLOGY, AND RESULTS

DISCLAIMERS:

(1) This report 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 employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party complies with applicable law.

(2) This report does not contain or imply legally binding requirements. Nor does this report establish or modify any regulatory guidance or positions of the U.S. Nuclear Regulatory Commission and is not binding on the Commission.

Prepared by
Paul Rebstock, RES/DE/ICEEB

Date: June 17, 2022 (ML22172A099)

Office of Nuclear Regulatory Research

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research has prepared this report in response to Research Assistance Request (RAR) NRR-2021-012, "Outline of Technical Basis for Evaluating the Criteria, Methodology, and Results of Hazard Analyses" (ML21095A147), approved April 12, 2021 [1]. This report constitutes the sole deliverable in response to that request.

Staff anticipates that licensees and applicants will present hazard analyses in support of claims related to licensing or in support of actions taken independently of a need for explicit NRC approval (such as modifications under 10CFR50.59 [2]). The objective of the effort under the subject RAR has been to develop criteria for technical bases supporting the evaluation of the criteria and methodology for, and of the results from, such hazard analyses. Those criteria are the subject of this report. The RAR indicates that the technical bases themselves may then be developed more fully and presented in the form of a NUREG or some other type of technical document, and that those technical bases could then be used for the subsequent development of staff guidance for the evaluation of hazard analyses associated with both operating plants and advanced reactors. The particular focus of this effort is to address HA developed using new techniques that might complement or be used in place of traditional types of hazard analysis such as FMEA.

The course of this research, however, suggests an alternative and more aggressive approach. This research uncovered little published documentation of review criteria for hazard analyses, but ample guidance as to their development and use. Since the adequacy of any analysis is tied closely to the degree to which it has accomplished the intended goal, the development and use guidance can be used to infer review criteria. Current and recently-concluded research efforts concerning a particular type of hazard analysis, concerning the use of operating experience and risk considerations, and concerning the implications and mitigation of common-cause failures in redundant actuation channels that employ digital technology, also provide insights into the necessary scope and content of hazard analyses.

Furthermore, whereas this RAR and the HA RAR that preceded it are tied to the general concept of hazard analysis and avoid consideration of any particular type of HA, it is becoming increasingly clear that STPA and methodologies related to it or expanding upon it are becoming dominant in the industry for the analysis of complex digital systems.

It can be argued, then, that we already have enough background and technical basis information to enable development of appropriate guidance. We should proceed now to the development of a NUREG or RIL on HA, that describes and categorizes HA approaches, addresses objectives, pros, and cons, and provides guidance for assessment.

In addition, hazard analysis may well be the only available avenue for attaining adequate assurance of acceptable operation of digital systems of more than trivial complexity. So guidelines for the adequate assessment of a hazard analysis are of the utmost importance.

This report cites a technical basis document issued in 2015, along with additional reference materials for the expansion and refinement of the technical bases presented therein.

OUTLINE / TABLE OF CONTENTS

1. Background and Objectives 1
2. Scope 2
3. Introduction 3
3.1. What is a Hazard Analysis, and Why does it Matter? 3
3.2. Documents Cited in the RAR: 5
4. Key Considerations 6
5. Guiding Principles and High-Level Criteria 6
6. Epilogue 8
References 11

ACRONYMS AND INITIALISMS

CCF	Common-Cause Failure
CFR	Code of Federal Regulations
DEG	EPRI Digital Engineering Guide
DI&C	Digital Instrumentation and Controls
DICWG	DI&C Working Group
DRAM	Digital Reliability Analysis Methodology
DSRS	Design-Specific Review Standard
EPRI	Electric Power Research Institute
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HA	Hazard Analysis
HAZCADS	Hazards and Consequences Analysis for Digital Systems
HMI	Human Machine Interactions
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
MDEP	Multinational Design Evaluation Programme
NRC	Nuclear Regulatory Commission
NRR	NRC office of Nuclear Reactor Regulation
OUO	Official Use Only
RAR	Research Assistance Request
RES	NRC office of Nuclear Regulatory Research
RIDM	Risk-Informed Decision-Making
RIL	Research Information Letter
SAE	Society of Automotive Engineers
SSG	Specific Safety Guide
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis

1. BACKGROUND AND OBJECTIVES

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research has prepared this report in response to Research Assistance Request (RAR) NRR-2021-012, "Outline of Technical Basis for Evaluating the Criteria, Methodology, and Results of Hazard Analyses" (ML21095A147), approved April 12, 2021 [1]. This report constitutes the sole deliverable in response to that request.

Staff anticipates that licensees and applicants will present hazard analyses in support of claims related to licensing or in support of actions taken independently of a need for explicit NRC approval (such as modifications under 10CFR50.59 [2]). The objective of the effort under the subject RAR has been to develop criteria for technical bases supporting the evaluation of the criteria and methodology for, and of the results from, such hazard analyses. Those criteria are the subject of this report. The RAR indicates that the technical bases themselves may then be developed more fully and presented in the form of a NUREG or some other type of technical document, and that those technical bases could then be used for the subsequent development of staff guidance for the evaluation of hazard analyses associated with both operating plants and advanced reactors. The particular focus of this effort is to address HA developed using new techniques that might complement or be used in place of traditional types of hazard analysis such as FMEA.

The course of this research, however, suggests an alternative and more aggressive approach. This research uncovered little published documentation of review criteria for hazard analyses, but ample guidance as to their development and use. Since the adequacy of any analysis is tied closely to the degree to which it has accomplished the intended goal, the development and use guidance can be used to infer review criteria. Current and recently-concluded research efforts concerning a particular type of hazard analysis, concerning the use of operating experience and risk considerations, and concerning the implications and mitigation of common-cause failures in redundant actuation channels that employ digital technology, also provide insights into the necessary scope and content of hazard analyses.

Furthermore, whereas this RAR and the HA RAR that preceded it are tied to the general concept of hazard analysis and avoid consideration of any particular type of HA, it is becoming increasingly clear that STPA and methodologies related to it or expanding upon it are becoming dominant in the industry for the analysis of complex digital systems.

It can be argued, then, that we already have enough background and technical basis information to enable development of appropriate guidance. We should proceed now to the development of a NUREG or RIL on HA, that describes and categorizes HA approaches, addresses objectives, pros, and cons, and provides guidance for assessment.

In addition, hazard analysis may well be the only available avenue for attaining adequate assurance of acceptable operation of digital systems of more than trivial complexity. So guidelines for the adequate assessment of a hazard analysis are of the utmost importance.

Nevertheless, the present effort is limited by the scope of the initiating RAR to the development of criteria for the technical bases. The detailed development and documentation of the technical bases themselves, and the development of the evaluation guidance based upon those technical bases, are outside the scope of this RAR and of this report.

The RAR states that the information presented in this report "could be in the form, for example, of guiding principles and high-level criteria" that could later be used in the development of the detailed technical bases. [1, p. 3]

This effort is related to an earlier effort concerning an assessment of the suitability of HA-related provisions of IEEE 7-4.3.2-2010 [3] for NRC endorsement in an upcoming revision to regulatory guide 1.152 [4]. That earlier effort was initiated by RAR-NRR-2020-008 [5] and resulted in a non-public whitepaper [6]. The present effort is related in part to some of the recommendations and other provisions of that whitepaper.

Regulatory Considerations

IEEE 279-1971 [7] and IEEE 603-1991 [8] are incorporated by reference into the Code of Federal Regulations, and may be applicable to individual nuclear power plants on the basis of their date of license. Paragraph 3(8) of 279 and 4.8 of 603 are worded differently, but in essence require that plant design bases document conditions and types of events that could interfere with the performance of a safety function, and for which provisions are required to ensure retention of the safety function. Hazard analysis would support a determination that those provisions have been met and that the mitigation provisions would indeed be effective.

Later editions of 603 redesignate these provisions as 4h (rather than 4.8 as in the 1991 edition). The 1998 and 2009 editions retain the 1991 wording. The 2018 edition rewords the 1991 language slightly, and adds a provision requiring that an analysis be used to establish the system design basis. It includes a description of the required analysis that could easily be interpreted as a hazard analysis of the type addressed in this report.

THEREFORE: Hazard Analysis might be used in support of regulatory compliance.

2. SCOPE

Hazard analyses typically address an entire system, including the mechanical and electrical equipment, the operator interface, the operator(s) themselves, the local environment, operating procedures, management context, and anything else that might impact the behavior of the system or the human operator use of it. Hazard analyses as addressed in this report may be limited to the provisions for the actuation and control of mechanical or electrical equipment, and might exclude consideration of the mechanical and electrical equipment itself. The objective of such a hazard analysis would be to demonstrate that the actuation and control system will ensure an adequate level of functional dependability in consideration of the role of the overall mechanical or electrical system in ensuring plant safety. In addition to operational context, such an analysis might also include consideration of the risk significance of the overall system function.

3. INTRODUCTION

3.1. What is a Hazard Analysis, and Why does it Matter?

But first of all, what is a hazard?

A hazard, in the context of this report, is anything that can go wrong. A spacecraft might crash into Mars rather than landing softly. An automated bakery might put too many chocolate chips in the cookies. A hazard might be life-threatening, expensive, or annoying. The consequences of a hazard might be bad from one point of view, and good from another. It is the consequences, rather than the hazard itself, that truly matter.

The STPA Handbook [9] provides a useful definition of "hazard:" "*A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.*" [9, p. 17] And: "*A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.*" [9, p. 16] This definition is in the context of a particular type of hazard analysis, STPA (System-Theoretic Process Analysis), but is generally useful regardless of the type of hazard analysis under consideration. Two observations to further generalize the definition of "hazard:"

- Whether the environmental conditions under consideration need to be "worst case" or not, and just what, exactly, "worst case" might actually mean, can be a matter for consideration within the context of a particular hazard analysis.
- The nature and acceptability of the "loss(es)" to which a particular hazard might lead is clearly a matter for consideration in each individual hazard analysis, regardless of the type of hazard analysis involved.

So….

A hazard analysis can be defined broadly as an analysis intended to identify hazards and their sources, and to determine appropriate design characteristics and constraints for the control or mitigation of those hazards. See, for example, Appendix A of *Engineering a Safer World*, by Nancy Leveson [10, p. 467], guidance for the design of digital systems in IEEE 7-4.3.2 [11, p. 12], and the EPRI *Digital Engineering Guide* (DEG) [12, p. 2.6]. RIL-1101 [13], produced by the NRC Office of Nuclear Regulatory Research to support NRC review of hazard analyses, provides a definition specifically attuned to NRC usage:

> *"Hazard analysis (HA) is the process of examining a system throughout its lifecycle to identify inherent hazards … and contributory hazards and to formulate requirements and constraints to eliminate, prevent, or otherwise control them." [13, p. 80]*

RIL-1101 then points out, in notes immediately following that definition, that the hazard identification includes identification of the "losses (harm) of concern," and that, while HA includes the formulation of constraints needed to avoid or mitigate the hazards, the implementation of those constraints and verification that they have been satisfied is outside the scope of HA.

Hazard analyses may be divided into two broad categories:

- Bottom-up analyses, such as Failure Modes and Effects Analysis (FMEA).
  These analyses look at each individual component of a module and assess the consequences of the failure of that component. This can be generalized to consideration of module failures and the effects of module failures on a system, or to consideration of external influences and the effects of those influences upon module or system behavior. The key is that these analyses attempt to enumerate everything that can go wrong and to assess the consequences of each of those things, but they consider each element independently. Interactions among elements, especially unplanned and unanticipated interactions, are not easily addressed or discovered in this type of analysis.
- Top-down analyses, such as the elements of Systems-Theoretic Accident Model and Processes (STAMP, see [10, p. 73]).
  These analyses look at the desired behavior of a system, and ask what could impede that behavior. Then they look at ways to mitigate those impediments, or at their own lower-level causes, digging deeper and deeper until the impediments have been mitigated or deemed to be sufficiently unlikely as to be acceptable from a Risk-Informed Decision-Making (RIDM) standpoint. The key here is the focus on system behavior and design, and the reduced focus on a need to enumerate every possible failure. The analytical process looks at what is necessary to support *success*, and then asks what could interfere with those supporting conditions or events.

This report deals primarily with “modern” hazard analyses, which fall into the “top-down” category.

And why do they matter?

Systems are growing in complexity and in dependency upon software or upon software-like configuration provisions. There are trends toward interactions among diverse systems and even among elements of redundant systems that have traditionally been strictly isolated from one another. Centralization of functions into reduced numbers of independent electronic hardware modules is increasing. All these trends challenge the ability of traditional closed-form quantitative analyses to accurately predict system behavior under adverse or fault conditions, and also to fully assess the impact of interactions among system components and to reveal the presence and effects of unintended interactions — even under normal conditions with no faults present. Elements of these trends also challenge the feasibility and efficacy of traditional probabilistic analyses. As Dr. Nancy Leveson puts it in *Engineering a Safer World*:

> *“In the traditional causality models, accidents[1] are considered to be caused by chains of failure events, each failure directly causing the next one in the chain. … these simple models are no longer adequate for the more complex sociotechnical systems we are attempting to build today.” [10, p. 75]*

[1] In the paragraph following the one from which this quote is drawn, Dr. Leveson generalizes the meaning of the term “accident” to include any sort of “unplanned and undesired loss event.”

and later, on that same page:

> *"In systems theory, emergent properties, **such as safety**, arise from the interactions among the system components. The emergent properties are controlled by imposing constraints on the behavior of and interactions among the components. Safety then becomes a* control *problem where the goal of the control is to enforce the safety constraints. Accidents result from inadequate control or enforcement of safety-related*[2] *constraints on the development, design, and operation of the system."* [emphasis added]

It seems reasonable to infer from this latter statement that *un*safety is also an emergent property, wherein each individual component acts as intended and completely within its own safety constraints, and yet the behavior of the system as a whole is unsafe. Indeed, the *unsafe* behavior of the system as a whole may well be a direct consequence of the "*safe*" behavior of the individual components. The STPA Handbook [9, pp. 7–9] presents several examples of correct behavior that resulted in undesirable, sometimes disastrous, consequences.

A hazard analysis is a process for discovering the hazards that might affect a system, and for establishing the controls necessary to eliminate or mitigate those hazards. For a complex system, a hazard analysis may well be the most effective and efficient way to discover the hazards that might impact a system. A substantial increase in use of hazard analyses in support of claims related to nuclear power plant licensing may therefore be expected.

In the end, modern (top-down) hazard analysis is a formalized process for generating questions concerning the behavior of a system in consideration of system design but also in consideration of aspects of the way a system is to be used and of the environment in which it is to function. It is a qualitative tool. There can be no guarantee that the set of questions inspired by it is necessarily complete, or that the answers offered in response to those questions are correct or comprehensive. Nevertheless, it appears reasonable to expect that the formalized approach will yield insights that would otherwise remain hidden, and that the resulting design and implementation will be improved over what might be expected had HA not been employed.

3.2. Documents Cited in the RAR:

The RAR identifies five specific documents to be considered in connection with this effort. One of those documents, RIL-1101, gives high-level guidance concerning the review of hazard analyses. The remaining documents address the content and objectives of hazard analyses, but they do not provide specific review guidance. The specific documents cited in the RAR are:

1. Research Information Letter (RIL)-1101 [13]
   Technical basis to review hazard analysis of digital safety systems
2. *Design-Specific Review Standard for NuScale (DSRS)*, Chapter 7, "*Instrumentation and Controls*," Appendix A, "*Hazard Analysis*" [14]
3. Multinational Design Evaluation Program Generic Common Position DICWG-10 [15]
   Common Position on Hazard Identification and Control for Digital Instrumentation and Control Systems
4. IAEA SSG-39 [16]
   Design of Instrumentation and Control Systems for Nuclear Power Plants

[2] Dr. Leveson is using the term "safety-related" here in a general sense that includes but is not limited to the particular definition of that term in the context of nuclear power.

5. IEC 61508-1 [17]
   Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 1: General requirements

Points 3 and 4 of Section 5 of this report address the use of guidance for the review and development, respectively, of hazard analyses within the context of this report.

4. KEY CONSIDERATIONS

Hazard analyses are inherently qualitative and, to some extent, subjective. Individual statements within them might be subject to verification, but the overall content and construction of the analysis is not amenable to proof of accuracy or completeness. Misstatements can be shown to be wrong, but proof that nothing is missing can be elusive. Hazard analyses must be performed "correctly" but cannot be objectively proven to have been done so.

The training, skill, and commitment of the lead analyst and of each member of the HA development team are therefore of paramount importance. A hazard analysis should include or be supplemented with credible and convincing evidence that all persons involved in its development and verification have received appropriate training and are adequately qualified to perform the HA-related roles for which they are responsible.

A hazard analysis can include detailed consideration of system design and of the design of system modules and components. Each member of the HA development and verification team therefore should be adequately knowledgeable of those details, while also maintaining sufficient independence from the design team to support an appropriate level of objectivity.

Similarly, NRC personnel responsible for evaluating and dispositioning a hazard analysis provided in support of a licensing claim should be adequately trained in hazard analysis and adequately familiar with the relevant details of the analyzed system.

RIL-1101 [13] presents a detailed discussion of technical bases for the review of hazard analyses, including consideration of the role of HA in regulatory activities. RIL-1101 also presents a list of considerations that should be addressed in a hazard analysis, and addresses a potential nexus between HA and risk-informed decision-making. It should be noted, however, that Section 1.6, "Purpose and intended audience," of RIL-1101 points out that the RIL "*…presents a learning opportunity from which NRC expects to identify needs for future improvements in its review guidance, regulatory guidance, and the underlying technical basis…*" The information presented in the RIL should therefore be tempered by the accumulated experience achieved subsequent to its publication in 2015.

5. GUIDING PRINCIPLES AND HIGH-LEVEL CRITERIA

These principles and criteria should be taken into consideration in the development of specific technical bases for the evaluation of hazard analyses used to support activities or claims related to the licensing of NRC-regulated facilities. As described in the opening section of this report, the development of the detailed bases themselves is not included in the scope of this effort. The detailed bases are to be developed separately from the current effort, and will be presented in the form of a NUREG or other technical document.

1. ***Describe what is meant by "hazard analysis" in this context.***
   HA of interest are those used in support of some licensing consideration. Therefore, it is important that the HA be shown to adequately support the associated claims. The technical bases must support that objective.

2. ***Define the scope and purpose of the types of hazard analyses to be covered by these bases.***

3. ***References addressing the review of hazard analyses:***
   A search for guidance concerning technical bases for the review of hazard analyses yielded very few resources other than RIL-1101.

   a. RIL-1101 [13] *Technical Basis to Review Hazard Analysis of Digital Safety Systems*
      This is a peer-reviewed presentation of technical bases for the review of hazard analyses, and should be used as a primary source. Appendix E is a checklist for hazard recognition

   b. INL/LTD-20-59984[3] [18] *Technical Approaches to Address Hazards from Common Causes in Digital Instrumentation and Control Systems* (OUO)
      Revision 0 Section 1.1 states that the objective of that project was to “develop a technical basis… for addressing hazards from common causes…[from DI&C]."

   c. INL/LTD-20-60088[3] [19] *Protecting Against Hazards from Common Causes in Digital Instrumentation and Control Systems* (OUO)
      Revision 0 Section 1.1 identifies the project objective: "The objective of this project is to develop a technical basis for identifying and analyzing hazards that could prevent a safety system from performing its function, esp., by degrading its means of fault tolerance such as defense in depth (commonly called common cause failures or CCF). …"

4. ***References addressing the development of hazard analyses:***
   Most available documentation addresses the development and use of hazard analyses, rather than the evaluation of hazard analyses. Nevertheless, insight into the bases for evaluation can be gleaned from insights into the bases for creation and application. The following documents, in addition to those cited in Section 3.2 of this report, may provide helpful information:

   a. IEEE 7-4.3.2 [11], *IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations*
      Annex D, “*Identification and control of hazards*,” provides some general guidelines for the development of hazard analyses.
      (i) *An Assessment of IEEE 7-4.3.2-2016 Provisions Concerning Hazard Analysis* [6] addresses the suitability of Annex D for NRC endorsement in an update to regulatory guide 1.152 [4].

   b. *STPA Handbook* [9]
      This is a fundamental resource for the development of a particular type of hazard analysis, System-Theoretic Process Analysis (STPA)

[3] These documents have not been accepted by the NRC as of the time of this writing, and they might be modified and converted into NRC-issued NUREG. These documents should be taken into consideration in the development of detailed technical bases, but the form and designation of the documents at that time is not presently known.

c. EPRI *Digital Engineering Guide* (EPRI DEG) [12]
The EPRI DEG presents a general approach to the development of a digital system, and includes references to the use of hazard analysis in support of various phases of the system design.

d. *Hazard Analysis Methods for Digital Instrumentation and Control Systems* (EPRI) [20]
From "Product Description" (page v): "*This report documents an investigation of the use of various hazard and failure analysis methods to reveal potential vulnerabilities in digital instrumentation and control (I&C) systems before they are put into operation.*"
Table 9-1, on page 9-4, presents a summary of the comparative strengths and limitations of the various HA methods investigated.

e. *Hazards and Consequences Analysis for Digital Systems* (EPRI HAZCADS) [21]
HAZCADS builds on the information in the EPRI study of HA methods (item d, above), developing an analytical approach that employs both STPA and Fault Tree Analysis (FTA).

f. *Digital Reliability Analysis Methodology* (EPRI DRAM) [22])
DRAM combines information developed through the use of the DEG (item c, above) and of HAZCADS (item e, above) with information developed through reliability analysis. This can provide insights concerning the relative effectiveness of various methods for mitigating vulnerabilities.

g. *System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems* [23]

"*Scope of this effort intends to provide both educational materials and recommended practices regarding how system theoretic process analysis (STPA) may be applied within a safety assessment process focusing on safety-critical content.*

Purpose of this task force is to align industry (starting with, but not limited to, automotive/aerospace) best practices and translate them across industry regarding the implementation and use of STPA across human- and software-intensive systems (controls, human machine interactions (HMI), autonomous, etc.), and to explore focus areas suited for STPA use, or for supplementing other safety tools." [23, p. 1]

6. EPILOGUE

RIL-1101 [13] presents technical bases for NRC staff review of hazard analyses used in support of NRC-regulated activities. Section 1.6 of RIL-1101 acknowledges that that document is a first effort at the production of such technical bases, and that it is likely to be superseded by later efforts. It should be noted that RIL-1101 was produced in 2015, about seven years prior to this present writing. The review of RIL-1101 conducted in connection with the efforts reported here indicates that it provides an adequate initial set of technical bases for staff review of hazard analyses, but also that accumulated wisdom and insights gained in the time since its publication should also be taken into consideration through future research efforts, such as the recently-approved RAR on STPA [24]. Nonetheless, RES does not consider that there is a need to develop a new technical basis document (e.g., NUREG) for complimenting future staff guidance required for evaluating the HA criteria, methodology, and results from licensees and applicants that may use new HA techniques as an additional means of demonstrating safety that compliments traditional HA types such as FMEAs. Instead, RES considers that the information in RIL-1101 provides an adequate initial technical basis for the development of future guidance that would allow staff to provide more granularity to address specific needs in

licensing activities for both operating plants and advanced reactors regarding the use of HA in support of applications of digital technology.

The STPA efforts described above, and defined in reference [24] are independent of this present RAR [1]. Neither effort is contingent upon the other. But the STPA work might benefit from this report and from the efforts associated with the development of the anticipated staff review guidance document, and the guidance document may benefit from elements of the STPA RAR efforts.

It is important to remember that, in the context of this report, a hazard analysis may be limited in scope to the provisions for actuation, monitoring, and control of a plant system. Such an analysis may exclude the associated mechanical equipment and the provisions for the supply of electrical power. The actuation, monitoring, and control functions are presumed in this report to be provided by means of digital technology, and are therefore aggregated under a general moniker of “digital system,” but whether they are actually digital or analog is irrelevant to the HA considerations presented herein.

Finally, as noted in the opening section of this report, it is recommended that, rather than development of an explicit generic technical basis document to support development of generic review guidance for hazard analyses, the next step in this process be the development of a document that focuses on the nature, content, and review of the types of hazard analysis most likely to be used in support of regulatory considerations. The guidance might be specific to a particular type of HA, or it might be slightly generalized to address a family of related types of HA. The degree of specificity or generality should be established by the authors when the guidance is developed. The technical basis for each provision of the guidance document should be presented in the guidance document itself. It is possible that the guidance, and some of the technical bases behind it, will exceed the provisions of RIL-1101. It is also possible that the bases and the associated guidance provisions may in some cases be developed iteratively.

REFERENCES

[1] "Outline of Technical Basis for Evaluating the Criteria, Methodology, and Results of Hazard Analyses (ML21095A147)," NRC, Research Assistance Request (RAR) NRR-2021-012, Apr. 2021.

[2] "Title 10 'Energy' of the Code of Federal Regulations, Part 50 'Domestic Licensing of Production and Utilization Facilities' Section 59 'Changes, tests, and experiments.'" NRC. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html

[3] IEEE Power Engineering Society, Nuclear Power Engineering Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, "IEEE standard criteria for digital computers in safety systems of nuclear power generating stations," Institute of Electrical and Electronics Engineers, New York, IEEE-7-4.3.2-2010, 2010. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=5542300

[4] "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (ML102870022)," NRC, Regulatory Guide 1.152, Revision 3, Jul. 2011. [Online]. Available: https://www.nrc.gov/docs/ML1028/ML102870022.pdf

[5] "An Assessment of IEEE 7-4.3.2-2016 Provisions Concerning Hazard Analysis (ML20107F478)," NRC, Research Assistance Request (RAR) NRR-2020-008, Apr. 2020.

[6] P. Rebstock, "An Assessment of IEEE 7-4.3.2-2016 Provisions Concerning Hazard Analysis (ML21019A421)," NRC Office of Nuclear Regulatory Research, Internal Whitepaper, Jan. 2021.

[7] "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE, Standard 279, Jun. 1971. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=6125205

[8] "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE, Standard 603–1991, Dec. 1991. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=2933

[9] Nancy G. Leveson and John P. Thomas, *STPA Handbook*. 2018. [Online]. Available: http://psas.scripts.mit.edu/home/

[10] Nancy G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, Mass.: MIT Press, 2011.

[11] "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," IEEE, Standard 7-4.3.2-2016, Aug. 2016. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=7552417

[12] "Digital Engineering Guide: Decision Making Using Systems Engineering," EPRI, Technical Report 3002011816, Jan. 2021. [Online]. Available: https://www.epri.com/research/products/000000003002011816

[13] "Technical Basis to Review Hazard Analysis of Digital Safety Systems (ML14237a359)," NRC, Research Information Letter RIL-1101, 2015. [Online]. Available: https://www.nrc.gov/docs/ML1423/ML14237A359.pdf

[14] "Design Specific Review Standard for NuScale SMR Design: Instrumentation and Controls -- Hazard Analysis (Chapter 7, Appendix A, Revision 0, ML15355A316)," NRC, Jun. 2016. [Online]. Available: https://www.nrc.gov/docs/ML1535/ML15355A316.pdf

[15] “Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems,” Multinational Design Evaluation Programme (MDEP), MDEP Generic Common Position DICWG-10, Version 7, 21March2016.

[16] “Design of Instrumentation and Control Systems for Nuclear Power Plants,” International Atomic Energy Agency (IAEA), Vienna, Austria, Specific Safety Guide SSG-39, May 2016. [Online]. Available: https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4853343

[17] “Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 1: General Requirements,” International Electrotechnical Commission, Geneva, Switzerland, Basic Safety Publication IEC 61508-1, Edition 2.0, Apr. 2010.

[18] Kurt Vedros, Ahmad Al-Rashdan, and Robert England, “Technical Approaches to Address Hazards from Common Causes in Digital Instrumentation and Control Systems (ML20297A312, OUO),” Idaho National Laboratory (INL), Technical Report INL/LTD-20-59984, revision 0, Oct. 2020.

[19] Kurt Vedros, Ahmad Al-Rashdan, and Robert England, “Protecting Against Hazards from Common Causes in Digital Instrumentation and Control Systems (ML20297A313, OUO),” Idaho National Laboratory (INL), INL/LTD-20-60088, revision 0, Oct. 2020.

[20] “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” EPRI, Technical Report 3002000509, Jun. 2013. [Online]. Available: https://www.epri.com/research/products/000000003002000509

[21] “HAZCADS: Hazards and Consequences Analysis for Digital Systems - Revision 1,” EPRI, Technical Report 3002016698, Jul. 2021. [Online]. Available: https://www.epri.com/research/products/000000003002016698

[22] “DRAM: Digital Reliability Analysis Methodology,” EPRI, Palo Alto, CA, Technical Report 3002018387, Jun. 2021. [Online]. Available: https://www.epri.com/research/products/000000003002018387

[23] SAE Functional Safety Committee, “System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems,” SAE International, Industry Standard J3187-2022, Feb. 2022. doi: 10.4271/J3187_202202.

[24] “Evaluate adequacy of Systems Theoretic Process Analysis (STPA) for identifying common causes of systematic failures for digital I&C (DI&C) systems,” NRC, Research Assistance Request (RAR) NRR-2022-013, Apr. 2022.