AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Public records include NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* (10 CFR) may also be purchased from one of these two sources:

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402-0001
   Internet: bookstore.gpo.gov
   Phone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161-0002
   Internet: www.ntis.gov
   Phone: 1-800-553-6847 or, locally, 703-605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, on written request to the following:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

E-mail: DISTRIBUTION@nrc.gov
Fax: 301-415-2289

Some of the NUREG-series publications posted under http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and might differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited might subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at:

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available for reference by the public. Codes and standards are usually copyrighted and may be purchased from their originating organization, or, if they are American National Standards, from:

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
Internet: www.ansi.org
Phone: 212-642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), (5) knowledge-management reports (NUREG/KM-XXXX), and (6) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under 10 CFR 2.206, "Requests for Action under This Subpart" (NUREG-0750).

EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Quantification Guidance for Main Control Room Abandonment Scenarios

EPRI 300201XXXX **NUREG-1921, Supplement 2**

Draft Report, March 2018

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304-1338

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research (RES)
Washington, D.C. 20555-0001

EPRI Project Manager
A. Lindeman

U.S. NRC-RES Project Manager
S. Cooper

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES (NO)

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATIONS NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATIONS BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATIONS PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research

JENSEN HUGHES

John Wreathall & Co., Inc.

Sandia National Laboratories

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ABSTRACT

While NUREG-1921 (EPRI 1023001) provided methods and guidance to estimate human error probabilities (HEPs) for fire probabilistic risk assessments (fire PRAs), the subject of main control room abandonment (MCRA) was reserved for future research. Supplement 1 of NUREG-1921 (EPRI 3002009215) addressed qualitative considerations for fire scenarios resulting in MCRA. Supplement 1 provided PRA modeling considerations and qualitative HRA guidance including: feasibility assessment, identification and definition, timing, performance shaping factors, and walk-through and talk-through guidance for MCRA scenarios.

This report provides detailed human reliability analysis (HRA) quantification guidance for fire PRA scenarios resulting in MCRA, building upon both NUREG-1921 and Supplement 1. The HRA process for MCRA scenarios remains unchanged from NUREG-1921, but supplemented by additional contextual factors unique to MCRA scenarios.

Guidance is provided based on the specific time phases of the MCRA timeline including; the time before abandonment, time for the decision to abandon, and the time once the decision to abandon has been made. A new decision tree was developed to analyze making the decision to abandon upon a loss of control (LOC) in time. Additional HRA guidance is also provided for accounting for command and control and communications once the main control room (MCR) is abandoned.

Keywords
Command and control
Fire human reliability analysis (Fire HRA)
Fire probabilistic risk analysis (Fire PRA)
Main control room abandonment (MCRA)
Quantitative analysis

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CITATIONS

This report was prepared by:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304

Principal Investigators:
M. Presley
A. Lindeman

Under contract to EPRI:

Jensen Hughes
111 Rockville Pike Suite 550
Rockville, MD 20850-5109

Principal Investigators:
E. Collins
P. Amico
J. Julius
K. Kohlhepp Gunter

U.S. Nuclear Regulatory Commission (NRC)
Office of Nuclear Regulatory Research (RES)
Washington, DC 20555

Principal Investigators:
S. Cooper
T. Rivera

Under contract to NRC-RES:

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Principal Investigator:
S. Hendrickson

John Wreathall & Co., Inc.
4157 MacDuff Way
Dublin, OH 43106

Principal Investigator:
J. Wreathall

This report describes research sponsored by EPRI and the NRC.

This publication is a corporate document that should be cited in the literature in the following manner:

EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Quantification Guidance for Main Control Room Abandonment Scenarios: Supplement 2 DRAFT, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2018. NUREG-1921 Supplement 2 and EPRI 300201XXXX.

LIST OF ACRONYMS

AFW	auxiliary feedwater
ANS	American Nuclear Society
AO	auxiliary operator
AOP	abnormal operating procedures
AOV	air operated valve
ARP	annunciator response procedures
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
BWR	boiling water reactor
C&C	command and control
CBDT	cause-based decision tree
CBDTM	cause-based decision tree method
CR	control room
CRS	control room supervisor
DHR	decay heat removal
ECCS	emergency core cooling system
EDG	emergency diesel generator
EDMG	extensive damage mitigation guidelines
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
FLEX	flexible and diverse mitigation strategies
HCR/ORE	human cognitive reliability/operator reliability experiment
HEP	human error probability
HFE	human failure event
HMI	human-machine interface
HRA	human reliability analysis

JHEP	joint human error probability
JPM	job performance measure
LOC	loss of control
LOCA	loss of coolant accident
LOH	loss of habitability
MCB	main control board
MCR	main control room
MCRA	main control room abandonment
MOU	Memorandum of Understanding
MOV	motor operated valve
MSIV	main steam isolation valve
NFPA	National Fire Protection Association
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSF	performance shaping factor
PWR	pressurized water reactor
PZR	pressurizer
RCP	reactor coolant pump
RCS	reactor coolant system
RES	NRC's Office of Nuclear Regulatory Research
RNO	response not obtained
RO	reactor operator
RSDP	remote shutdown panel
SAMG	severe accident management guidelines
SBO	station blackout
SCBA	self-contained breathing apparatus
SG	steam generator
SISBO	self-induced station blackout
SM	shift manager
SME	subject matter expert
SS	shift supervisor

SSC	structures, systems, and components
SSD	safe shutdown
STA	shift technical advisor
THERP	technique for human error-rate prediction
TSC	technical support center
U.S.	United States

1
INTRODUCTION

1.1 Background

This report provides quantitative human reliability analysis (HRA) guidance for human failure events (HFEs) resulting from fire scenarios that may require main control room abandonment (MCRA).

This guidance builds upon the fire HRA guidance provided in previously published reports,[1] presented as the most recent listed first.

- *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines: Qualitative Analysis for Main Control Room Abandonment Scenarios,* NUREG-1921 Supplement 1/ EPRI 3002009215 [1], which provides guidance for the probabilistic risk assessment (PRA) development of qualitative HRA for fire scenarios leading to MCRA and qualitative guidance for the associated HRA.

- *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines,* NUREG-1921/ EPRI 1023001 [2] which provides guidance for the development of HRA for fire scenarios that do not require MCRA. NUREG-1921 augments (and sometimes replaces) that given in the overall fire PRA methodology report (NUREG/CR-6850) [3].

- *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities Volume 2: Detailed Methodology,* EPRI 1011989/NUREG/CR-6850, [3] which primarily develops the fire model and associated plant response (PRA) models.

In particular, this report is a companion document to NUREG-1921, Supplement 1 and both supplements should be used with the original report, NUREG-1921.

1.2 Objectives and Scope

The overall objective of this most recent EPRI/NRC-RES collaboration is to provide guidance on the application of HRA quantification methods, including any adjustments needed to address the context of the fire scenarios leading to MCRA, in order to develop human error probabilities (HEPs) and uncertainty parameters.

While this report addresses all phases of MCRA scenarios, the primary improvements to the fire HRA were in the following areas:

[1] These joint reports were prepared under a Fire Risk Research Addendum to the Memorandum of Understanding (MOU) between NRC and EPRI. These reports are jointly published by both organizations. For simplicity, the NUREG number is used through this report.

- HRA quantification guidance for the decision to abandon (i.e. Phase II per definitions provided in Supplement 1) which is described in Section 3 (with background development provided in Appendix A)
- HRA quantification guidance for the actions to implement the MCRA procedure following the decision to abandon (i.e., Phase III per Supplement 1), including considerations for communications and command and control (C&C) which is described in Section 4 (with background development provided in Appendix B)

The guidance and examples presented in the report are derived from interviews and typical plant operating practices of the current fleet of nuclear power plants (NPPs) within the United States (U.S.). In general, this guidance may be applied internationally, but with the understanding that the strategies, remote shutdown panel (RSDP) capability, staffing, and procedure progression may differ from those found in the U.S.

1.2.1 Expected Usage

This report was developed based on methods described in NUREG/CR-6850 and NUREG-1921. These baseline documents provide general fire PRA and fire HRA modeling guidance and methods. For the MCRA analysis, additional, qualitative guidance is provided in Supplement 1. This report provides guidance for the quantification of HFEs (assessment of HEPs) and by extension, the MCRA scenarios in the fire PRA model.

The fire HRA section of the ASME/ANS PRA Standard [1] does not specifically discuss requirements for MCRA HRA. However, the requirements for fire HRA in the PRA Standard refer back to the internal events HRA standard requirements. The high level requirement for human reliability analysis post-initiator quantification is HLR-HR-G and the process developed for MCRA quantification is expected to meet HLR-HR-G.

1.3 Summary of Qualitative MCRA HRA

The guidance developed in NUREG-1921 Supplement 1 provides the elements to develop a qualitative foundation for the human response to fires resulting in MCRA. In addition to the HRA elements, Supplement 1 also provides guidance beyond that in NUREG/CR-6850 for modeling the MCRA scenario-specific success criteria and incorporation of HFEs and equipment failures into the plant response model.

The qualitative analysis process described in NUREG-1921 Supplement 1 serves as an input to the HRA quantification including the following:

- The development of fire PRA scenarios which establishes the PRA context for the HRA
- Collection and review of plant specific information for MCRA including procedures, models, success criteria, and operator action feasibility analyses
- Identification of the operator actions in the fire scenarios to be developed as human failure events as part of the plant response
- Definition of three phases for MCRA scenarios (see Section 1.3.1)
    - Phase I includes all operator actions prior the decision to abandon
    - Phase II includes the time from when cues indicate the need for abandonment to the time at which the decision to abandon is made
    - Phase III includes actions following the decision to abandon, including any actions required to transfer control from the main control room (MCR) to the RSDP before abandonment and actions taken to implement the MCRA safe shutdown strategy

- Definition of operator actions based on the relevant procedure steps associated with scenarios leading to MCRA, including:
    - Context of the fire scenarios from the fire progression timeline and the accident progression timeline
    - Time available and initial construct of the time required from the timeline development
    - Determination of the critical tasks (cognitive tasks and execution tasks) required to meet the fire PRA success criteria
- Feasibility assessment for MCRA scenarios as well as individual actions
- Timeline development for the MCRA progression, including:
    - Fire progression from fire modeling, consisting of ignition, detection, fire growth and propagation, and consideration of suppression effectiveness
    - Accident progression, consisting of the fire-induced initiating event and the associated plant and systems response; primarily thermal-hydraulic analyses, used to define the time available and provide timing information associated with cues
    - Procedure progression for operators to respond during MCRA based on procedure and training material reviews plus walk/talk-throughs or simulator exercises of MCRA that include the context of the fire and associated fire-induced initiating events
- Qualitative analysis of operator actions, including:
    - Evaluation of performance shaping factors (PSFs) based on the context of the fire scenarios for MCRA and other influences on operator performance observed during walk/talk-throughs and simulator exercises of the MCRA process
    - Initial data collection and assessment of C&C in terms of existing plans, training, and communication requirements
    - Dependency analysis considerations for multiple HFEs that occur in the same cutset
    - Identification of sources of uncertainty
- Documenting the analysis in sufficient detail to allow the basis for the qualitative analysis to be understood and the input parameters to quantification to be clearly identified

1.3.1 Time Phases of MCRA

NUREG-1921, Supplement 1 stressed the importance of developing a MCRA timeline that combined the fire progression, plant response, and operator response. The development of this timeline serves as a tool to visualize the interactions among operators and is valuable for both the qualitative and quantitative analysis. The timeline is divided into three time phases as represented in Figure 1-1. This information is replicated from Supplement 1 as the quantification approach is based on the three time phases. A brief description of the time phases is found below:

- Phase I – Time period before the operators recognize that abandonment may be required
- Phase II – Time period associated with the decision to abandon
- Phase III – Time period after abandonment during which the transitional and post-abandonment shutdown actions are performed

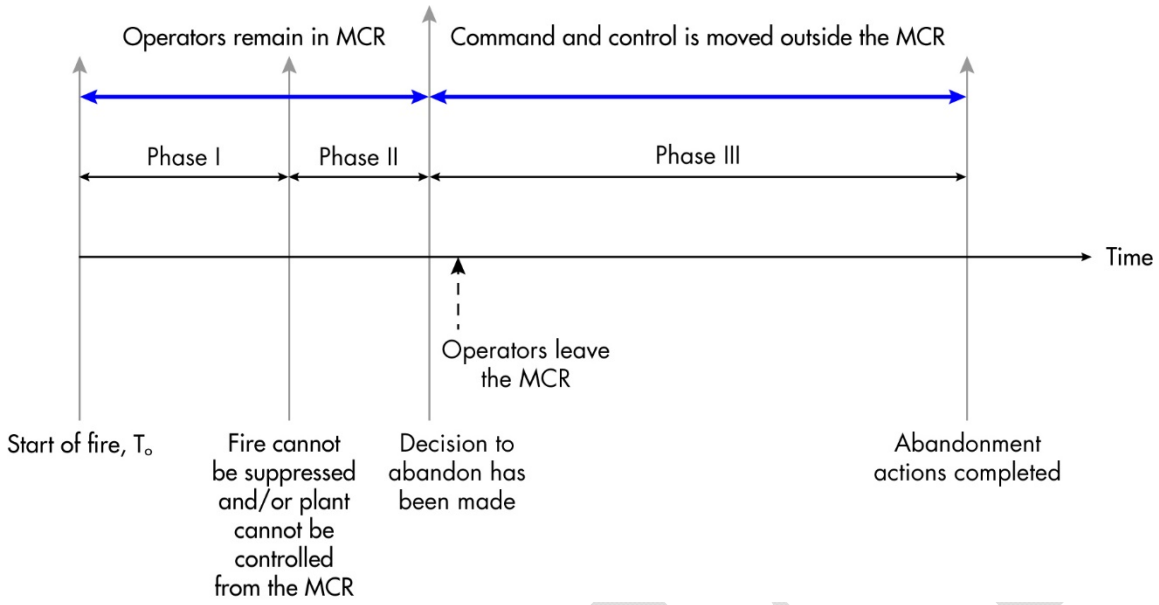


Figure 1-1
Three time phases of MCRA

For full details of how to construct the MCRA timeline, please refer to NUREG-1921, Supplement 1 Section 7.

1.4 Organization of Report

This report is structured to address what additional guidance is needed for the quantification of HFEs in fire scenarios leading to MCRA, beyond that provided in NUREG-1921 and NUREG-1921 Supplement 1. The general report is structured to provide the guidance to the analyst in the main report sections. The process used to develop the guidance, technical approach, and discussion with subject matter experts (SMEs) is documented in the appendices.

In particular, this report is arranged in the following sections and appendices:

- Section 1 (i.e., this section) identifies the objectives and scope of this report, summary of the qualitative MCRA report (NUREG-1921 Supplement 1), and provides an overview of the report.
- Section 2 provides guidance on how to treat pre-abandonment actions (Phase I actions).
- Section 3 provides guidance on how to quantify the decision to abandon (Phase II) using a newly developed decision tree.
- Section 4 provides guidance on how to quantify post-abandonment shutdown actions (Phase III actions) and address coordination between actions, associated with command and control.
- Section 5 discusses the recovery, dependency, and uncertainty.
- Section 6 provides a summary of lessons learned and concluding remarks.

The appendices are presented in order of expected usage. Specifically:

- Appendix A Technical approach and summary of discussion with SMEs for the decision to abandon (i.e., Phase II).

- Appendix B Background, technical approach, and summary of discussions on command and control in Phase III.

1.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1,* U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.
2. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
3. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology*, U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

2
PHASE I – PRE-ABANDONMENT ACTIONS

2.1 Introduction

During Phase I, operator actions are directed from the MCR, similar to other fire scenarios. In general, once the reactor is tripped, the operators are following a set of emergency operating procedures (EOPs) as well as fire response procedures. Typically, actions modeled for MCRA during Phase I include tripping the reactor, and possibly starting an emergency diesel generator (EDG) from the MCR or locally, or starting a system that failed to auto start. These actions are not necessarily unique to MCRA since the cognition and execution for these actions are very similar, if not identical, to fire scenarios where the fire is not inside the MCR or even internal events PRA actions following a reactor trip.

2.2 Quantification Guidance for Phase I HFEs

NUREG-1921 [1] provides guidance on the fire HRA for a variety of contexts and response strategies. Up until the point of the decision to abandon, the operating crew is responding to the fire from the MCR, so the guidance in NUREG-1921 is applicable and sufficient to evaluate and quantify Phase I actions. Existing HRA methods can address the timing associated with the actions, the ranges of cues and indications, training, and procedure guidance, the human-machine interface (HMI) and simple execution. Success and failures of Phase I actions can define the plant conditions following abandonment. For example, if operators recover the EDGs before abandonment, then alternating current (AC) power will be available following abandonment.

2.3 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.

3
PHASE II – DECISION TO ABANDON

This section describes the quantification of the HFE associated with decision to abandon for loss of control (LOC) MCRA scenarios, identified as Phase II of MCRA. The only HFE modeled in Phase II is failure to make the decision to abandon. During Phase II, the plant is typically following EOPs and/or AOPs and fire procedures, and accessing the MCRA procedure to decide whether or not MCRA is warranted.

NUREG 1921, Supplement 1 [1] provides the following guidance on the decision to abandon for LOC scenarios:

- Section 4 – Developing the definition and performing the qualitative assessment of the HFEs associated with the decision to abandon the MCR for both loss of habitability (LOH) and LOC
- Section 7.3.3 - Developing timing parameters for the Phase II decision to abandon HFE within the context of the combined MCRA scenario timeline
- Section 7.6.3 - Example of an MCRA timeline for a LOC scenario, including Phase II

3.1 Introduction

The fire PRA analyzes two types of scenarios where the operators would need to abandon the MCR:

1. Scenarios that result in the MCR becoming environmentally uninhabitable due to heat or smoke (referred to as LOH scenarios), and
2. Scenario that result in a loss of ability to successfully prevent core damage from the MCR (referred to as LOC scenarios).[2]

The only HFE modeled in Phase II is failure of the decision to abandon, therefore, this section discusses the quantification process for failure of the decision to abandon for only the LOC case. For LOH scenarios, the HEP associated with the decision to abandon is considered to be negligible because the effects of fire have created untenable environment conditions forcing abandonment.

The technical basis for the quantification approach is described in Appendix A. Existing HRA methods (CBDTM [2], HCR/ORE [2], SPAR-H [3], IDHEAS [4], NARA [5], and CREAM [6]) were reviewed for applicability with additional guidance. Several iterations occurred, and it was concluded that the existing HRA methods were not appropriate for modeling the decision to abandon. The resulting guidance is informed from the original cause-based decision tree method (CBDTM) trees as well as human cognitive reliability/operator reliability experiment

[2] The LOC may occur from fire-induced failures or from fire-induced failures plus one or more random failures. An example would be hot shorting of control cables during a fire in the cable spreading room. The operators would have no way to make the distinction – they only know that they have lost control and are unable to re-establish control from the MCR. Therefore, their decision to abandon the MCR is unaffected by why the LOC occurs. As a practical matter, however, the LOC scenarios that include additional random failures will tend to be lower frequency and thus not significantly impact the overall risk from MCRA scenarios.

(HCR/ORE), but specifically adapted toward operators making the decision to abandon the MCR in time.

3.2 Quantification Guidance

The quantification process for the decision to abandon consists of three steps:

1. Review and develop a timeline for the decision to abandon
2. Verification of feasibility
3. Assessment of decision to abandon decision tree

As part of the qualitative analysis, the analyst should have developed:

- A detailed MCRA scenario timeline
- A decision to abandon timeline as described in Section 7 of NUREG-1921 Supplement 1 and,
- A feasibility assessment as described in Section 6 of NUREG-1921 Supplement 1 [1].

These three pieces address steps 1 and 2 of the quantification process for the decision to abandon and additional discussion on each of these topics is provided on how they explicitly relate to quantification.

3.2.1 Decision to Abandon Timeline

It should be recognized at the outset that the timeline for the decision to abandon is highly coupled with the timeline for Phase III. This is because Phase II must end early enough such that all Phase III actions can be completed in time to meet the PRA defined success criteria (typically core damage). In other words, there is no specific criterion or definition for the endpoints of Phase II.

Also, unlike internal events operator actions, there is typically not a single parameter or procedure step that directs the operator(s) to abandon, instead the scenario must progress to the point where there is a set of cues and indications that the operators must observe before they would consider leaving the MCR. The required pieces of information can include confirmation of a fire, confirmation of fire damaged equipment, and reaching procedure steps that provide the abandonment criteria. The set of cues and indications needed for the decision to abandon will be plant-specific and is defined by existing procedure guidance, operator interviews, simulator observations and/or talk-throughs.

Section 7.3.3.2 in NUREG-1921 Supplement 1 describes the key timing aspects related to the decision to abandon for LOC scenarios. For quantification, the following key timing inputs, need to be explicitly defined (see the detailed timeline shown in Figure 3-1):

> $T_{SW\ Phase\ III}$ = The time window for Phase III is the time at which all Phase III actions must be completed, which typically comes from thermal hydraulic calculations given an assumed set component failures at T = 0.
>
> T_{delay} = the time from the reference time (generally T=0, the start of the fire and reactor trip) to the arrival of plant-specific cue(s) for the need to abandon.

T_{cog} = the time required for the making decision to abandon, consisting of the time for detection, diagnosis, and decision-making, including activities such as verification of the fire (especially if it is outside of the MCR) and evaluating the ability to control systems.

$T_{avail\ decision}$ = the time available for making the decision to abandon; determined by first identifying how much time is available in Phase III and then how much time is available to complete the required actions following abandonment to take the plant to a safe, stable condition.

The time available for the decision to abandon ($T_{avail\ decision}$) is the longest time during which the operators can remain in the MCR and still prevent the undesired end state, and can then be calculated as follows:

$$T_{avail\ decision} = T_{SW\ Phase\ III} - T_{delay} - T_{req,III}$$

Where:

T_{delay} = Time at which MCRA criteria are met

$T_{req,III}$ = Time required for Phase III

The timing parameters associated with Phase II are shown in blue in Figure 3-1 and the timing parameters associated with Phase III are shown in red.

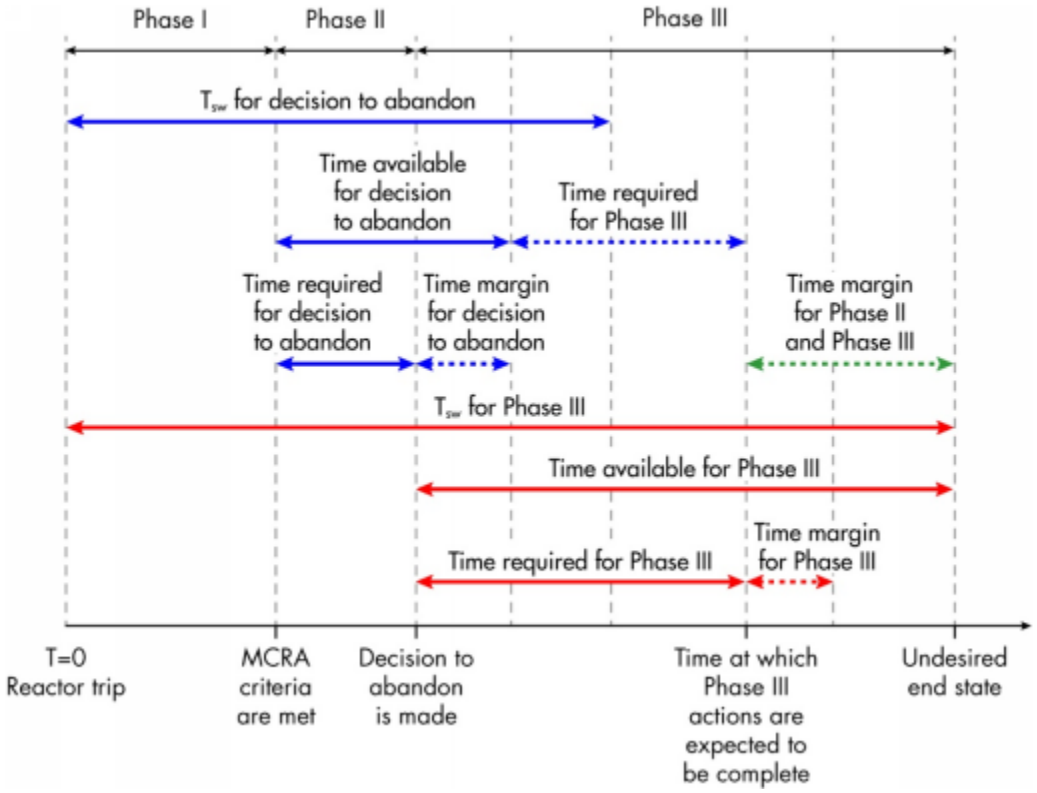


Figure 3-1
MCRA timeline for the decision to abandon

The time margin for the decision to abandon is the difference between the time required to make the decision and the time available. The time margin must be greater than or equal to zero in order for the MCRA scenario to be feasible.

In reality, however, it is recognized that there is significant uncertainty associated with each timing input related to the decision to abandon. For example, T_{cog} could be as short at 1 minute if the cues are unambiguous or many minutes if the decision requires consensus among operators or a crew brief. Generally, T_{cog} is not readily measureable by simulator observations, training, or walk through/talk throughs with operators. This is because operators prefer to remain in the MCR for as long as possible and there is generally a high reluctance to leave the MCR. T_{cog} must therefore be based on best estimate engineering judgments.
Based on a review of industry MCRA analyses completed to date at time of publication, T_{delay} for the decision to abandon can range from 1 minute to as long as 20 minutes. T_{delay} is highly dependent upon both fire impacts and the operators' expected procedure path. $T_{avail\ decision}$ can range from 5 minutes to 30 minutes since it is highly dependent upon the time required and time available to complete the Phase III actions.

Due to the uncertainties in the specific timing parameters, however, timing estimates might be better used as gauges of feasibility or factors for consideration in the Decision to Abandon Decision Tree, as discussed below, rather than as inputs to a time-based Phase II HEP.

3.2.2 Verification of Feasibility

NUREG-1921 Supplement 1 Section 6 describes the feasibility assessment for MCRA scenarios. In order for the decision to abandon action to be feasible, the following criteria must be met: (Note: this list is simplified from Supplement 1 Section 6 and is specific to the decision to abandon.)

1. The time available for the decision to abandon must be greater than T_{cog} the time required in order for the action to be feasible.
2. Cues and indications - There must be some indication available in the MCR that alerts the operators that they need to abandon. For example, the operators must have some indication, training or procedure guidance alerting them to the fact that: 1) there is a fire and 2) the fire could require abandonment. Additional cues such as component failures and procedure guidance could assist with the decision to abandon but are not required to establish feasibility.
3. Procedure guidance and/or training – There must be either procedure guidance about when to leave the MCR or classroom training or discussions on the decision to abandon and when to leave the MCR. The procedure guidance can be as simple as a statement that reads "for a fire in this area, consider abandoning the MCR".
4. Staffing – In order for the decision to abandon to be feasible, the staff required to make the decision must be present in the MCR at the time the decision is required. For example, if the Shift Technical Advisor (STA) is required to support the decision, then he must be in the MCR when the decision is needed. At some plants, the STA is not required to be in the MCR until 15 minutes after the start of the event and in these cases, if MCRA is required before 15 minutes and requires input from the STA, then the decision to abandon is not feasible.

3.2.3 Decision To Abandon Decision Tree

The final step in the quantification of the decision to abandon is the assessment of the decision to abandon decision tree. Figure 3-2 presents the decision tree logic and Table 3-1 provides the guidance associated with each branch.

There is a hesitancy for the operators leaving the MCR which contains the instrumentation and control for plant equipment. Operator reluctance to leave the MCR which is related to various factors including the capability, or perceived capability, of the RSDP, quality of training, quality of procedures, and/or operator confidence in the post-abandonment strategy.

The impact of reluctance, although not explicitly analyzed in the decision tree, is implicitly considered in the quantification of HEP estimates. Based on the semi-formal expert elicitation, the SMEs discussed the impact of reluctance on making the decision to abandon in time. The issue of reluctance is also addressed in the IDHEAS [4] decision tree on "Delay Implementation." The second branch point, *Assessment of Margin,* "questions whether the crew has an incorrect assessment of the operational margin (e.g., as measured or indicated by pressure, level, temperature) so that they think they can delay implementation longer than they actually can." While not directly applicable, the insights from the delay implementation tree allowed for the team to identify reluctance as a factor important to quantification. Based on the insights from the semi-formal expert elicitation, reluctance has been built into the HEP estimates.

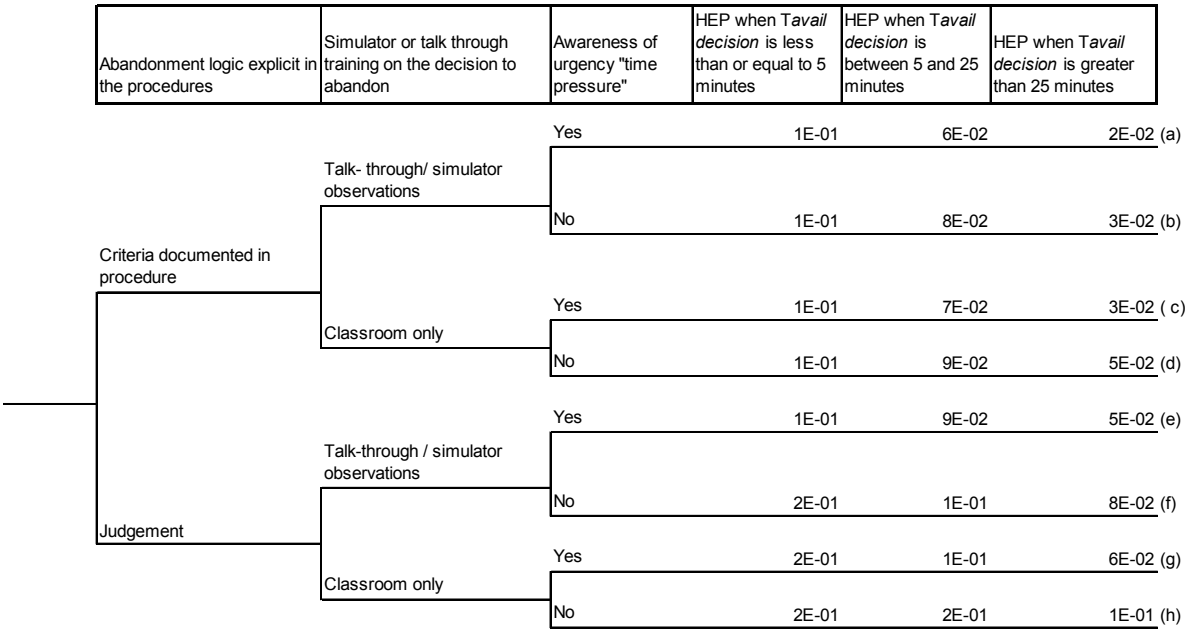


Figure 3-2
Decision to abandon decision tree

Table 3-1
Guidance for Decision to Abandon Tree

Heading	Guidance for HRA Analyst in Making Assessment
Abandonment logic explicit in procedure guidance	This branch point assesses the specificity of procedures for identifying the location and severity of the fire, equipment failures or other conditions where operators should abandon the MCR. The level of specificity of MCRA procedural guidance varies widely among plants; see Section 3.3 for examples. The up branch is selected when there is either explicit or qualitative guidance included in the procedures. In the best case, there is detailed guidance explicitly telling the operators under what equipment failures or operational conditions they should leave. The down branch is used when the procedure contains no guidance on the decision to abandon and the decision will be based purely on judgment. This is applied for cases where the operators have some general training on an abandonment criterion or set of criteria they would apply to make the judgment to leave. If no criteria are defined, then the abandonment action is not considered feasible and the HEP should be set to 1.0.
Simulator or talk through training on the decision to abandon	This branch point distinguishes between the different types of training provided for making the decision to abandon. The up branch on the decision tree is used when operators have either simulator or talk through training specifically on making the decision to abandon (Note that many plants conduct extensive training on what to do after the decision to abandon is made, but very few plants have detailed training on the actual decision to abandon). The down branch should be selected when operators have only classroom training. If there is no classroom or simulator training on the decision to abandon then the action is not feasible and the HEP is 1.0.

Heading	Guidance for HRA Analyst in Making Assessment
Awareness of Urgency	This branch point characterizes the operator's sense of time urgency. This heading questions whether the crew has an assessment of how long operator can remain in the MCR and still complete the Phase III actions and meet the PRA success criteria. Operator interviews can be used to establish the operator's sense of urgency by asking the following questions (taken and updated from Supplement 1, Table C-3): • Do you have any feeling for how long you can remain in the MCR and still reach a safe and stable state outside the MCR? • Would you wait as long as possible before going to the RSDP? Would you try to stay in the MCR in self-contained breathing apparatus (SCBAs)? • Is there any timing requirements covered in training related to the decision to abandon? The up branch on the decision tree is used when (1) the operators are aware of the time pressure to leave the MCR, or (2), operator training includes a timing requirement to leave the MCR by a specified time and this timing agrees with the modeled PRA scenario. If they are not aware of the time pressure, the down branch is used. The reasoning is that if they do not have this awareness of urgency, then they may delay making the decision so long such that Phase III would no longer be successful. The decision tree and the associated HEPs assume a general level of reluctance to leave the MCR for LOC scenarios. If the operators are aware of the timing requirements to leave the MCR, they would be more likely to leave and overcome this general reluctance.
Timing Bin	There are three different timing regimes for the time available for the decision to abandon (see equation in Section 3.2.1): • $T_{avail\ decision} \leq 5$ minutes • $T_{avail\ decision} > 5$ minutes and ≤ 25 minutes • $T_{avail\ decision} > 25$ minutes

3.3 Examples of Abandonment Decision Logic in Procedures

As discussed in Table 3-1, there is a range of procedure guidance throughout the U.S. industry on the decision to abandon logic, from vague to explicit. Three examples are provided to assist the analyst in determining how to select the first branch of the Figure 3-2 decision tree which asks whether abandonment criteria are provided in procedures explicitly.

3.3.1 Example 1

Example 1 provides the most explicit procedural guidance that has been identified in U.S. NPPs to date. This procedure clarifies the criteria for MCRA on LOC by establishing specific monitoring criteria and directing use of the disconnect switches or locally tripping the RCPs. While in this case, specific steps are identified for monitoring conditions, a plant might also

simply specify a list of components which, if affected by fire impacts, would identify a LOC. In this case, the up branch should be used.

Table 3-2
Example 1: Excerpt of procedure guidance – most explicit found to-date

Action/Expected Response	Alternative Action
Verify reactor coolant system (RCS) Pressure is Stable	Check all pressurizer (PZR) power operated relief valves (PORVs) are closed. If any are open, attempt to close them from the Main Control Board (MCB) If any cannot be closed from the MCB, attempt to isolate by closing the associated block valve If any cannot be closed or isolated, open MCB Disconnect Switches on Subpanel A & B.
Verify steam generator (SG) Pressure is Stable	Check all SG PORVs are closed. If any are open, attempt to close them from the MCB If any cannot be closed from the MCB, open MCB Disconnect Switches on Subpanel A & B.
Monitor reactor coolant pump (RCP) Seals for proper cooling RCP Lower Seal Water Temp < 225°F Controlled Seal Bleed-off (CBO) Temp < 250°F RCP Motor Bearing Temp < 195°F	If RCP Trip criteria are met, perform the following: Trip the Reactor and go to EOP-1.0 while continuing with this procedure Trip any affected RCP If any affected RCP will not remain secured, locally trip the associated breaker. If all RCPs must be tripped, place Steam Dumps in Steam Pressure Mode.
Verify Stable Reactor Operation Rx Power RCS Temperature PZR Level PZR Pressure	Stabilize the Primary, while continuing with this procedure. If necessary, trip the Reactor, then go to EOP-1.0 and continue with this procedure.
Verify Stable Secondary System Operation Turbine Load Feed Flow / Steam Flow SG Level Deaerator Storage Tank (DAST) Level Main Condenser Vacuum	Stabilize the Secondary while continuing with this procedure. If necessary perform one of the following: If Rx Power >30 %, Trip the Rx and go to EOP-1.0. If Rx Power is < 30%, Trip the Main Turbine and refer to the Turbine Trip AOP

Action/Expected Response	Alternative Action
Electrical Buses	
If in service, Verify EFW Flow is > 450 gpm	Attempt to Establish EFW from the MCB. If EFW cannot be established, implement Control Room Evacuation Due to Fire AOP.

3.3.2 Example 2

Example 2 provides some guidance, but there is still considerable decision-making required by the shift supervisor (SS). In this case, the Up branch for the decision tree should be used, especially because the fire procedure indicates that Critical Safety Function Status trees are also used to evaluate the plant functional state.

Note: IF the fire is in the Control Room/Relay Room, and evacuation is required, THEN go to the Control Room Evacuation (Fire) procedure.

Steps 1 and 2 of the Control Room Evacuation (Fire) procedure provide two symptoms that are expected to lead to MCR evacuation. These are:

1. A catastrophic fire as evidenced by flames or smoke in the Control Room and/or Relay Room that requires evacuation due to either of the following:

   - Environmental conditions (smoke/heat).

   OR

   - A loss of Control Room control of critical plant functions which cannot be adequately addressed by ARP, AOP, Instrument Failure Guide (IFG) or EOP response actions.

2. Actuation of fire detection and suppression in other fire areas which indicates conditions i.e., (smoke, fumes) that require Control Room evacuation

Figure 3-3
Excerpt from Fire Procedure: Impact of fire outside control/relay room

3.3.3 Example 3

Example 3 is a case where there is no guidance for making the decision to abandon and the decision would be based on judgment only. For this case, the Down branch of the decision tree would be selected.

For this example, the excerpt from the procedure is:

When a fire alarm is present in this fire area consider abandoning the MCR.

3.4 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1,* U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.

2. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment.* EPRI. Palo Alto, CA: 1992. TR-100259.
3. *The SPAR-H Human Reliability Analysis Method.* U.S. NRC, Washington, DC: 2005. NUREG/CR-6883.
4. *An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application: Volume 1.* U.S. NRC, Washington, DC: March 2017. NUREG-2199.
5. *B. Kirwan, H. Gibson, R. Kennedy, J. Edmunds, and G. Cooksley, "Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool," Probabilistic Safety Assessment and Management (PSAM) Proceedings, June 14-18, 2004, Berlin, Germany.*
6. Hollnagel, E., *Cognitive reliability and error analysis method (CREAM)*, Elsevier, 1998. ISBN 0-08-0428487.

4
PHASE III - ACTIONS FOLLOWING THE DECISION TO ABANDON

This section provides guidance for the quantification of HFEs which occur during Phase III of a MCRA HRA analysis (after the decision to abandon the MCR). The quantification guidance:

- Is built on the guidance given in NUREG-1921 (i.e., fire HRA guidelines)
- Expands upon the identification, definition, and qualitative analysis guidance given in NUREG-1921 Supplement 1 (i.e., qualitative analysis guidance for MCRA scenarios in fire events)
- Is based on research performed by the author team beyond that given in NUREG-1921 Supplement 1
- Is consistent with qualitative insights on operator performance in MCRA scenarios that were obtained from HRA/PRA and operations experts in a formal workshop

In addition to the quantification guidance for Phase III HFEs, this section also expands upon qualitative guidance associated with C&C given in NUREG-1921 Supplement 1 (i.e., qualitative analysis guidance for MCRA scenarios in fire events).

Appendix B documents the underlying details of this guidance, including the technical approach used for development and how issues and considerations identified from the development NUREG-1921 Supplement 1 (i.e., guidance for qualitative analysis for MCRA scenarios) were addressed. Appendix B also discusses aspects of C&C that may affect HFE quantification.

This section starts with a high-level summary of the HRA quantification guidance for Phase III operator actions, especially focused on differences from other HRA guidance (e.g., that provided in NUREG-1921). It should be noted that substantial portions of NUREG-1921, Supplement 1 are referenced in this section as the qualitative analysis guidance given in this report is crucial to the development of inputs needed for the Phase III HRA quantification. In some cases, guidance from NUREG-1921, Supplement 1 is repeated because of its importance. In a very few cases, qualitative analysis guidance from NUREG-1921, Supplement 1 is updated in this section.

4.1 High-Level Summary of Issues to Consider During Phase III HRA Quantification

For Phase III HFEs, the authors developed through their research a consensus perspective on the important issues that HRA quantification should address. This perspective also is specific to existing U.S. NPPs, the associated range of RSDP capabilities, associated MCRA procedures and training, and the manner in which that MCRA procedures are expected to be implemented.[3]

[3] Typically, the HRA analyst must consider a variety of factors with respect to operator actions, including who performs the action, what tasks are required for the action, where the actions take place, what procedures are used, what equipment and indications are used, and so on. In particular, most U.S. NPPs have a MCRA safe shutdown

If the HRA analyst is considering, for example, a new NPP design that uses a substantially different MCRA safe shutdown strategy, including re-constitution of the entire MCR operating crew at essentially a backup MCR, then HRA guidance for MCRA would be substantially different.

For the scope of this guidance, the following are the important issues for Phase III HRA quantification in MCRA scenarios:

1. General. To the extent possible, existing HRA guidance and quantification tools (from NUREG-1921) should be used.
2. Cognition. Because the MCRA safe shutdown strategies and procedures for existing U.S. NPPs address potential fire-induced initiating events and spurious operations, and because there are fewer options for trains of components that are available for safe shutdown, there typically is not a demand on the operator to "diagnose" what safe shutdown option to implement. Thus, the focus of HRA quantification in Phase III is on the execution of operator actions called out in MCRA procedures. However, there may be some NPPs that have some scenarios there may be options for recovery. For such cases, the cognitive modeling would follow NUREG-1921.
3. Execution. Regarding the execution aspects only, operator actions taken at the RSDP or local control panels in MCRA scenarios are similar to (or may be the same as) those local operator actions described in NUREG-1921. Consequently, HRA quantification guidance for the execution portion of these actions should be similar to that given in NUREG-1921.
4. Command and Control Impacts on Critical Tasks. An impact on the performance of critical operator actions from C&C should only be considered IF operator actions must be coordinated (e.g., one operator action is sequenced in a specific order after a previous action). If no coordination is required for implementation of the MCRA safe shutdown strategy, then the HRA quantification is based on the execution actions only. The time required to accomplish the actions should account for coordination, even if coordination is not modeled explicitly.

   In summary, based on research conducted, C&C potentially impacts the model in the following ways:

   a. Negative impact. C&C may add a critical task (or tasks) to an HFE if communication or coordination is needed for the correct sequencing of the critical tasks associated with an HFE. The time required to complete all critical tasks should account for the time to complete critical communications or coordination.

   b. Potential negative impact. C&C may add to the time required to accomplish a critical action if non-critical communications occur. For example, an operator may have multiple tasks and some of them may be non-critical for the fire scenario. The operator would complete these tasks and the associated communications following the procedure, and the non-critical tasks (including communication) would increase the time required for response. This type of modeling (establishing a realistic time required for response) is the same for all

strategy that involves a supervisor at the RSDP who uses the MCRA procedure and coordinates (as needed) the actions of multiple operators who are located at multiple local control panels, using radios (and maybe sound powered phones) to individually communicate with each local operator.

fire scenarios and non-fire scenarios, but is especially relevant to MCRA since the MCRA procedure is typically written for multiple fire impacts.

c. Positive impact. C&C may provide the potential for recovery of a critical task that is modeled within the HFE modeled, by either checking indications at the RSDP or by checking with another operator at a local control station.

5. Impact on Time Required. As described above in item #4 above for the critical tasks, the time required should address the following.

   a. Include critical communications and coordination in the time required to complete the HFE, and

   b. Also include non-critical communications in the time required to complete the HFE if it impacts the completion time, and

   c. Evaluate the time required for recovery. There are two types of recovery that may be applicable to MCRA: 1.) recovery within an HFE and 2.) recovery by adding an HFE (termed a recovery HFE) to the fire PRA model. Recovery within an HFE is addressed in Section 4.3 and recovery by adding an HFE, if possible, is addressed in Section 4.4.

4.2 Summary of Research Underlying C&C for Phase III

In NUREG-1921, Supplement 1, several factors were identified as being different and important for HRA treatment of MCRA scenarios. Two of those important factors were C&C and communications. In response to these factors, NUREG-1921 Supplement 1 added the following:

- Identified new feasibility assessment criteria for both communications and C&C (i.e., Section 6 of Supplement 1)
- Provided preliminary guidance on how to incorporate timing associated with communications and C&C into timelines (i.e., Section 7.3.4 of Supplement 1, extract copied below)

  "The timeline of the Phase III portion can be highly complex and requires the analyst to understand the expected procedure response. The timing should include any time for communication among operators in multiple locations as well as account for time delays due to feedback required by or from other operators before subsequent procedure steps can be taken."

- Discussed both communications and C&C in the context of performance shaping factors (i.e., Section 8 of Supplement 1)
- Provided preliminary research on C&C for both MCR and MCRA operations (i.e., Appendix B of Supplement 1).

The sections below briefly summarize the advances beyond that in NUREG-1921 Supplement 1 and that are important for HRA quantification for MCRA scenarios in Phase III.

4.2.1 Definition of Command and Control

NUREG-1921 Supplement 1 determined that C&C has not been previously considered explicitly for NPP operations. Consequently, Supplement 1 reviewed various cognitive models and

military definitions and, in Section B.3, defined the C&C functions applicable for NPPs, specifically:

- Maintaining a coherent understanding of the plant state (e.g., situational awareness)
- Making timely decisions
- Allocating resources as needed
- Coordinating actions
- Managing communications between team members such that they are timely and effective

In turn, the above definition is used in the next section to compare how C&C may change when moving from MCR operations to operations following MCRA.

4.2.2 Command and Control Differences Between MCR and MCRA

Having defined C&C for NPP operations, NUREG-1921 Supplement 1 went on to characterize in what ways MCR operations and MCRA operations may be different. In particular, Table B-2 in Section B.2 of Supplement 1 summarizes the differences between MCR and MCRA operations.

Following the publication of Supplement 1, the author team continued their research on C&C for MCRA operations. This research ended with a semi-formal elicitation of subject-matter experts (SMEs) on NPP MCRA operations. Appendix B of this report (Supplement 2) provides more details on this elicitation and its results.

One of the challenges in developing a list of differences between MCR and MCRA operations is that there are variations between U.S. NPPs regarding their RSDP capability and associated MCRA safe shutdown strategy.[4] In other words, distinguishing MCR versus MCRA differences is complicated by the fact that there are plant-to-plant differences in MCRA operations.

Input from SMEs was used to establish a consensus for the differences between in-MCR and MCRA:

1. Once the decision to abandon the MCR has been made, there are typically no procedure transfers, so there is no further decision-making (as is typically addressed when EOPs are used).
2. Because of how the MCRA safe shutdown strategy is implemented (including the content and format of MCRA procedures), C&C is different for MCRA operations because:
    a. For most U.S. NPPs, there are fewer controls and indications at the RSDP for supervisor to use in developing an understanding of plant conditions or to confirm completion of operator actions.
    b. For most U.S. NPPs, there are no alarms at the RSDP, requiring operators to closely monitor parameters. Such monitoring may be more susceptible to distractions.

[4] Section 2 and Appendix A of NUREG-1921 Supplement 1 discuss some of these variations between NPPs.

c. Although the supervisor is in charge of the overall MCRA procedures, he/she cannot directly observe implementation of MCRA procedure steps since most operator actions are performed at local plant stations (and not at the RSDP).

d. The allocation of operator resources is done mostly via the various MCRA procedure attachments (rather than by the supervisor) that are assigned to specific operators.

3. Communications within MCRA operations are different and impact the time required to operator actions to be completed. For example:

   a. Most communications are NOT face-to-face.

   b. There are different types of communications, including reports from operators who have completed MCRA actions.

   c. Communications equipment (e.g., radios) and associated problems (e.g., garbled communications, crosstalk on the same radio channel) are more of a concern.

4. C&C in MCRA operations may involve the coordination of operator actions which may be complicated by operators at different locations and by associated communications issues.

4.2.3 Most Important Concerns for Command and Control in MCRA Scenarios

As part of the research summarized in Appendix B of this report, input from SMEs regarding MCRA operations allowed the authors to establish that the most important concerns regarding C&C in MCRA scenarios is the need for coordination.

In particular, coordination of operator actions, as a C&C function:

- Is needed more in MCRA operations than for MCR operations
- May involve multiple operator teams, but this is not much different than for MCR operations
- May involve proper sequencing of operator actions
  - Implementation of the MCRA safe shutdown strategy can involve a significant amount of sequencing, especially before starting a pump
  - The MCRA procedure itself usually addresses this sequencing (e.g., typically, the procedure will include a Wait (or Hold) step if sequencing is needed)
  - Errors in sequencing may be due to confusion in using the MCRA procedure, communication problems, or a selection error
  - The likelihood of detecting errors in sequencing is reduced in MCRA due to fewer indications at the RSDP
- Depends on communications and an awareness of plant conditions for success
- Is strongly influenced by training for its success, ranging from:
  - Classroom only (i.e., more passive "receiving training")
  - Practicing coordination in the field (i.e., "active" and more realistic training is "best case")

4.2.4 Implications of C&C for HRA Quantification of Phase III Operator Actions

The HRA quantification implications of the updated research on C&C for Phase III operator actions are summarized below. Two additional topics are also addressed: communications and timing. However, the topic of communications is not considered separately; instead it is discussed along with either C&C or timing. Appendix B contains more details on these implications.

4.2.4.1 C&C for MCRA Operations

The HRA analyst should understand the important ways that command and control is different for MCRA operations, as opposed to MCR operations, in order to support HRA quantification. Identification of these differences and their implications was not finalized during the completion of Supplement 1, but is important to the modeling of command and control. Most aspects of command and control during the Phase III implementation of critical safety functions are incorporated into the MCRA procedures and timed walkthroughs as specific steps by (1) local operators reporting to the SS/SM at the RSDP on the status of their tasks and the enabled critical safety functions, such as “Inform control room supervisor (CRS) of source of power”, or (2) the SS/SM/CRS directing actions to be taken by local operators, such as “At the direction of the CRS, energize Safeguards Bus using an EDG”. However, while plants may have similar MCRA procedures and similar remote shutdown capabilities, the timing as well as the command and control aspects may vary since they are based on how the specific plant conducts its operations. Thus, careful review of the procedures and timing (from, for example, implementation plans, job performance measures (JPMs), etc.), operator interviews and simulator exercises are important to understanding the C&C policies and procedures at each plant.

The important aspects of C&C for MCRA operations are summarized under each element of the NPP definition of C&C:

- Maintaining a coherent understanding of the plant state (e.g., situational awareness):

  For MCRA operations, this means to establish and maintain a coherent understanding of the plant state following the establishment of a command post at the RSDP. This aspect of C&C is often addressed via task delegation or verification steps in the MCRA procedures (as discussed above) For MCRA, however, understanding the plant conditions may be hindered by the limited number of controls, indications, and alarms at the RSDP, in contrast to that available in the MCR. For MCRA operations, this element of C&C is important for the coordination of actions (see below[5]).

- Making timely decisions:

  There are two aspects to consider within this element of the definition of C&C: decision-making and timing. First, there are usually no "decisions," as typically considered in HRA for MCR operations, needed following the decision to abandon the MCR. This is because there are seldom procedure transfers or the like in the MCRA procedures for current U.S. NPPs (i.e., there is a single path to success) Secondly, timing for command and control is addressed in HRA through the development of timelines and the evaluation of feasibility by comparing the Time Required to accomplish an action with the Time Available. For MCRA it is important that the Time Required to accomplish the

[5] For current U.S. NPPs and how their MCRA safe shutdown procedures are written, recovery of a failed operator action is not credited. However, if a task fails and recovery is possible, then situational awareness is important to recognize the context associated with the failure in order to develop the appropriate response.

action includes time for communications (internal and external), and time for coordination. For example, if the communications plan uses runners, then the time required to complete the action is likely to be longer than when radios are use. See "coordinating actions" and "managing communications" below for more guidance.

- Allocating resources as needed:

  For MCRA, the allocation of operator resources is done mostly via the various MCRA procedure attachments (rather than by the supervisor) that are assigned to specific operators. In addition, the MCRA safe shutdown strategy is typically validated such that resources are available and are allocated by the MCRA procedure. If there are additional failures such that there are more actions to be accomplished than there are operators, then some of the actions would not be feasible.

- Coordinating actions:

  Coordination consists of two or more operators, and may be required for starting a train or system in order to restore a function, or for long term control of a parameter. Both types of coordination are considered during the conduct of each task. If failure of communications or coordination would fail a structures, systems, and components (SSC), then these are considered to be critical tasks and should be modeled explicitly.

- Managing communications between team members such that they are timely and effective:

  Because most communications during MCRA operations is not face-to-face, there is less clarity than for MCRA operations. Communications between team members accomplishing critical actions are included in the coordination discussion immediately above. For Phase III operator actions, communications with plant and utility staff, or external agencies, are addressed in the feasibility analysis and are not modeled explicitly. (Note that timing is addressed directly in the quantification of Phase II operator actions, i.e., the decision to abandon on loss of control.)

4.2.4.2 Timing Associated with C&C and Communications

Section 7 of NUREG-1921 Supplement 1 provided detailed guidance on the development of timing inputs and timelines for MCRA scenarios. As a result of additional research, this guidance is expanded here to include the following guidance for HRA analysts related to communications and coordination. This guidance also includes insights from the discussions with the SMEs as part of the semi-formal expert elicitation.

1. Determine the potential impact, if any, communications or coordination can have on the time required for response.

   a. Communications may be needed for critical tasks modeled in the HRA (such as for coordination needed for the proper sequencing of actions). The time required for operator actions may be impacted by time delays associated with communication needed to coordinate actions.

   b. Communications may also be conducted as part of non-critical tasks. For example, extra time may be needed for health physics surveys, if needed for operator action implementation (e.g., operation of valves inside containment for PWRs).

   c. The impact of all communications (critical and non-critical) should be included in the timeline if it impacts the total time required to complete critical actions.

d. Supplement 1, Section 7 discussed the development of an MCRA timeline where the major functions are plotted on the same timeline to understand the timing of individual HFEs with respect to the same time origin (see Supplement 1, Figure 7-7).

4.3 Detailed Phase III (After the Decision to Abandon) HRA Quantification Guidance

This section presents the steps for performing HRA quantification for Phase III HFEs. The quantification starts with understanding the qualitative analysis using the guidance given in NUREG-1921, Supplement 1. However, in addressing C&C, this report (Supplement 2) expanded the qualitative analysis (e.g. task analysis and timeline) before conducting quantification. Thus, this section includes steps from NUREG-1921 Supplement 1 and Supplement 2 (this report), both for completeness and to present new or modified guidance for these steps.

MCRA HRA quantification for Phase III HFEs is conducted using these steps:

1. Review the qualitative analysis from Supplement 1. This confirms that the starting point for quantification includes identification, definition, feasibility, timeline development, and PSF identification following NUREG-1921 Supplement 1.
    a. Re-check feasibility.
    b. Review individual HFE definitions to prepare for evaluation of for C&C impact
        i. Understand the MCRA procedure philosophy, staffing, roles and responsibilities.
        ii. Identify those steps in the procedure associated with the modeled HFEs
2. Develop qualitative analysis for C&C following Supplement 2 (new). This consists of review and update of the HFE definition and timeline development as part of evaluating the impact of C&C.
    a. Identify any operator actions that require C&C-related communication and coordination (e.g. adds a critical task related to C&C), and also identify where C&C-related tasks help with recovery within an HFE.
    b. Determine what potential impact, if any, communications or coordination can have on the timeline, especially the time required for response
    c. Review the collective set of HFEs qualitatively
3. Quantify Phase III HFEs given the updated HFE definitions and qualitative analysis from Supplement 2 (new) completed above. The guidance for the quantification of Phase III HFEs uses a mixture of existing NUREG-1921 guidance and new guidance from this report as summarized below:
    a. Diagnosis. The Phase III MCRA HRA focuses on execution using an appropriate tool such as technique for human error-rate prediction (THERP) [4], as described in Appendix B. However, if detection, diagnosis or decision-making is required, such as for a recovery HFE (see Section 4.4), then situational awareness is needed and an appropriate cognitive method should be used.
    b. For execution tasks other than C&C, the guidance provided in NUREG-1921 [1] for local manual actions, such as that given in Section B.7.5.3 and Appendix C.

c. For C&C execution tasks, see the quantification guidance provided in Section 4.3.3.

4. Review the HEPs for the collective set of HFEs

These steps are discussed in more detail below. Following quantification, the final steps are to incorporate the HRA into a PRA, and documenting the HRA results, but this report does not provide any new guidance for these steps.

4.3.1 Step 1: Prerequisite: Review the Qualitative Analysis

The technical approach has been written presuming the HRA analyst has completed the HRA process steps described in NUREG-1921 Supplement 1, consisting of identification, definition, feasibility assessment, timeline development, and qualitative analysis including PSF identification. Also, relevant plant data and PRA data have been collected.

1. Sub-step 1a: Re-check feasibility. If any Phase III HFEs appear to be infeasible based on the qualitative analysis (particularly the timeline), then review the existing data and analyses for potential conservatisms, and refine as appropriate.

   a) Start by using the feasibility criteria listed in Supplement 1, Section 6, including a check of the plan for C&C. C&C considerations may already be included in the HRA, but should be reviewed and confirmed following completion of Steps 3-5 below.

   b) Review the Communications Plan associated with MCRA and ensure it contains provisions or instructions for dealing with potential distractions and/or interruptions such as requests that are not associated with safe shutdown. These include internal requests such as health physics to take a survey or chemistry to take a sample; and external requests such as the arrival of the local, offsite fire department.

   c) Finally, as noted in the PRA modeling guidance provided in Section 3 of Supplement 1, the RSDP typically has limited capability and may not have the capability to mitigate some MCRA scenarios. Examples of such cases are some medium or large LOCAs in PWRs, or multiple relief valve openings in BWRs.

2. Sub-step 1b: Review individual HFE definitions

   a) Understand the MCRA procedure philosophy, staffing, roles and responsibilities. This includes identification of any personal protective equipment, tools, or other items needed for success. For example, for the operating crew implementing the set of actions during MCRA, identify “who does what’.

      i) Identify the key safety functions being accomplished by each operator.

      ii) Identify those key safety functions where multiple operators are required to accomplish the actions associated with an HFE.

         (1) Example: A single operator conducts all tasks needed to start electrical support systems, a second operator starts cooling water, and a third operator starts the front line systems during restoration of a function.

   b) Identify those steps in the procedure associated with the HFEs modeling the transfer of control from the MCR and with the critical safety functions listed below. Specifically, identify the list of critical tasks, meaning those tasks whose failure will fail the transfer to the RSDP or the key safety functions needed to respond to the MCRA scenario:

      i) Transfer of control from the MCR to the RSDP or local control stations (for this write-up the term RSDP will be used to apply to both, whichever is appropriate), e.g.,

(1) Electrical isolation of the MCR

(2) Start-up of the RSDP such as to energize the panel and ensure instrumentation is available

ii) Start-up and operation of systems used to fulfill modeled critical safety functions, e.g.,

(1) Decay heat removal front line and support systems

(2) Injection front line and support systems

(3) Reactivity control front line and support systems

(4) Primary integrity and secondary integrity (if applicable)

(5) Containment isolation and containment integrity

(6) In case of station blackout (SBO), EDG and support systems

iii) Actions taken to mitigate potential spurious operations such as:

(1) Spurious opening of primary or secondary relief valves

(2) Spurious (uncontrollable) feeding of SGs (PWR) or injection to the primary (PWR and BWR)

(3) Termination of spurious SI

4.3.2 Step 2: Develop Qualitative Analysis C&C Impact (and update if needed)

As the starting point, Step 1 helps the analyst by identifying the critical tasks related to safe shutdown after MCRA and the associated performance shaping factors (PSFs) consistent with NUREG-1921 Supplement 1, Sections 5 and 8, respectively. This is typically accomplished by reviewing the MCRA procedure, ideally in conjunction with a plant operator or an operations trainer, and considering the requirements of the MCRA context (LOH or LOC).

In order to address the potential for C&C-related failures, Step 2 identifies any tasks related to C&C that may lead to failure or may help with recovery, and also evaluates the impact on the timeline. This is accomplished in the sub-steps listed below:

4.3.2.1 Task 1: Identification of C&C Critical Tasks

The purpose of Task 1 is to identify C&C actions that are critical tasks or recovery tasks. Identify any operator actions that require C&C-related coordination and associated communication, specifically those whose failure would lead to failure of a SSC or key safety function. This sub-step, is new analysis (as part of this report) and it identifies C&C-related coordination of multiple operator actions involving communication via phones, radios, or another type of remote communication. A description of C&C-related coordination and communication is provided in Appendix B.

Background: One of the unique aspects of MCRA HRA is that there are multiple operators and multiple operator actions that are needed for the plant to achieve a long term, safe and stable state using equipment outside of the MCR. Most MCRA studies model each critical safety function as an individual HFE (e.g., failure to start high pressure injection). However, since there may be actions conducted by one operator that may be required for success of the actions of a second operator, it is important to understand how all of the proceduralized operator actions are inter-related. A useful approach is to identify these interfaces on an integrated timeline

showing all operators who implement actions modeled during MCRA, such as that shown in Supplement 1, Figure 7-9 (which is related to dual units, but these interfaces can happen in single unit MCRA as well).

An impact on the performance of critical operator actions from C&C should be considered IF operator actions must be coordinated (e.g., one operator action is sequenced in a specific order after a previous action, or if the action relies on a critical communication). If no coordination is required for implementation of the MCRA safe shutdown strategy, then the HRA quantification is based on the execution actions only. The time required to accomplish the actions should account for coordination, even if coordination is not modeled explicitly as described below in the next sub-step.

In summary, based on research conducted, C&C potentially impacts the model in the following ways:

- Negative impact. C&C may add a critical task (or tasks) and an associated additional failure mode to an HFE if coordination, with associated communications, is needed for an operator to successfully accomplish an action. The time required to complete all actions should account for the time to complete critical coordination and associated communications.
- Potential negative impact. Communications associated with C&C may add to the time required to accomplish a critical action if non-critical communications occur. This sub-step identifies the potential impact and sub-step 2 captures that change in the timeline.
- For example, an operator may have multiple tasks and some of them may be non-critical for the fire scenario. The operator would complete these tasks and the associated communications following the procedure, and the non-critical tasks (including communication) would increase the time required for response. This type of modeling (establishing a realistic time required for response) is the same for all fire scenarios and non-fire scenarios, but is especially relevant to MCRA since the MCRA procedure is typically written for multiple fire impacts.
- Positive impact. C&C may add the potential for recovery within an HFE of a critical task, through the controlling station checking on a remote or local operator. This is usually modeled as a separate 'recovery task' in THERP.

4.3.2.2 Task 2: Identification C&C Actions That Impact Timeline

The purpose of Task 2 is to identify C&C actions that impact the timeline. Determine the potential impact, if any, communications or coordination can have on the time required for response. Review, and update if needed, the time required to accomplish individual HFEs once communications and coordination are taken into account. Supplement 1, Section 7 discussed the development of an MCRA timeline where the major functions are plotted on the same timeline to understand the timing of individual HFEs with respect to the same time origin (see Supplement 1, Figure 7-7).

Section 7 of NUREG-1921 Supplement 1 provided detailed guidance on the development of timing inputs and timelines for MCRA scenarios. As a result of additional research, this guidance is expanded here to include the following guidance for HRA analysts related to communications and coordination:

- Determine the potential impact, if any, communications or coordination can have on the time required for response.

  - Communications may be needed for critical tasks modeled in the HRA. Such as for coordination needed for the proper sequencing of actions. The time required for operator actions may be minimally impacted by time delays associated with communication needed to coordinate actions.
  - Communications may also be conducted as part of non-critical tasks. Extra time needed for health physics surveys, if needed for operator action implementation (e.g., operation of valves inside containment for PWRs)
  - The impact of all communications (critical and non-critical) should be included in the timeline if it impacts the total time required to complete critical actions.
  - Supplement 1, Section 7 discussed the development of an MCRA timeline where the major functions are plotted on the same timeline to understand the timing of individual HFEs with respect to the same time origin (see Supplement 1, Figure 7-7).

- The time required for operator actions should also account for the following:
  - Manipulation time for some SSCs (such as larger valves or valves with a differential pressure).
  - Manipulation time may be different in MCRA scenarios than for MCR scenarios (e.g., some MOVs and AOVs that are usually operated with electric power must now be operated manually).
  - Specific way field operators plan to implement procedure steps (e.g., for a set of 10 actions, does the operator follow the steps explicitly, or a prioritized approach such as changing the order of steps?)
  - Time required estimates should include some margin for uncertainty (e.g., develop a range of timing estimates, if possible, rather than a point value)
  - Extra time needed for health physics surveys, if needed for operator action implementation (e.g., operation of valves inside containment for PWRs)
- Time associated with recovery. In many cases, timed walk-throughs or simulations of time-critical actions such as the MCRA procedure already include steps where another operator is either checking equipment status, parameter status (e.g., flow through a valve that should have been opened), or the performance of a step as a requirement for their own next step. However, if these steps are not specifically timed, a starting assumption for this additional recovery time should be in the range of 1 to 3 minutes, but assignment of a recovery time should consider what indications of the initial failure are available (and where they are located), followed by the time needed to perform the recovery action(s). (Note that in some cases, even with consideration of additional time required for recovery, there may be a negligible contribution to the overall HEP. Also, it is possible that the operator actions might become infeasible due to the additional time required.)

Data Source. For the execution time associated with the critical tasks modeled in a given HFE, use the plant-specific timed walk-downs, simulator data of MCRA scenarios, and/or JPM data. Typically for MCRA, validated timing data exists. Given this data has been identified and collected, the new analysis needed as part of this sub-step is to consider whether or not C&C-related communication and coordination steps are included in this timing and if not, conduct operator interviews to assess the timing impacts and include in the execution time. Check to

ensure that any additional time for recovery does not make the HFE and the overall MCRA scenario infeasible ($T_{required}$ longer than $T_{available}$).

Background: Communications may be needed for critical tasks modeled in the HRA and also may be conducted as part of non-critical tasks. The impact of all communications (critical and non-critical) should be included in the timeline if it impacts the total time required to complete critical actions. Communications necessary for completion of critical tasks should be identified and accounted for as part of C&C.

4.3.2.3 Task 3: Review Qualitative Analysis

The purpose of Task 3 is to review the qualitative analysis for the collective set of HFEs. This review includes confirmation of the following.

- Time required to accomplish all HFEs includes communications and/or coordination
- Critical communication and coordination tasks are identified and associated with the appropriate HFEs
- Model logic for the HFEs captures the dependencies between operators and critical C&C tasks
- Feasibility check, given potential changes to the tasks and timeline

4.3.3 Step 3: Quantify Phase III HFEs

Modeling of Phase III HFEs is primarily conducted using 1) an evaluation of timing to ensure the operator action(s) to enable the critical safety functions can be done within the required timeframe (described above in the Step 2 qualitative analysis), and 2) assessment of the reliability of the actions taken (described below).

4.3.3.1 Overview of HFE Quantification for Phase III

The Phase III quantification is conducted using the updated HFE definitions and qualitative analysis from Supplement 2 (new) completed above in Step 2. The guidance for the quantification of Phase III HFEs uses a mixture of existing NUREG-1921 guidance and new guidance from this report as summarized below.

- Cognition. The Phase III MCRA HRA focuses on execution using an appropriate tool such as THERP, as described in Appendix B. For some scenarios there may be options for recovery, such as deciding among late containment venting options in a BWR, and in these cases the cognitive modeling would follow NUREG-1921. If the Cause-Based Decision Trees are used, for example when indications are at the RSDP; then detection, diagnosis or decision-making is required. This is typically used for recovery HFEs, then situational awareness is needed and an appropriate cognitive method should be used (see Section 4.4 for details).
- For execution tasks other than C&C, the guidance provided in NUREG-1921 for local manual actions, such as Section B.7.5.3 and Appendix C, applies as described in provided in Section 4.3.4.2.
- For C&C execution tasks, see the quantification guidance provided in Section 4.3.4.3.

4.3.3.2 Execution Failures Other than C&C for Phase III Operator Actions

The following tasks are generally involved in HFE quantification for Phase III operator actions in MCRA scenarios:

1. Cognition errors. Because the MCRA safe shutdown strategies and procedures for existing U.S. NPPs address potential fire-induced initiating events and spurious operations, and because there are fewer options for trains of components that are available for safe shutdown, there typically is not a demand on the operator to "diagnose" what recovery option to implement. Thus, the focus of HRA quantification in Phase III is on the execution of operator actions called out in MCRA procedures. For some scenarios there may be options for recovery, such as deciding among late containment venting options in a BWR, and in these cases the cognitive modeling would follow NUREG-1921. If the Cause-Based Decision Trees are used, for example when indications are at the RSDP, then see Section 4.4 below for considerations on recovery as a separate HFE.
2. Execution errors other than C&C. The modeling of execution actions taken at the RSDP, or local control panels, or locally within the plant, during MCRA scenarios are similar to (or may be the same as) those local operator actions described in NUREG-1921. Consequently, HRA quantification guidance for the execution portion of these actions should be similar to that given in NUREG-1921, such as provided in Section B.7.5.3 (for THERP) and Appendix C.
    a. The THERP HRA quantification method [4] is often used for the contribution of execution failures in HFEs. For the THERP modeling of each critical task, consider an error of omission and/or an error of commission as in typical THERP modeling of execution.
    b. Typically MCRA recovery is addressed via the C&C steps discussed earlier that involve communication to verify that a function has been enabled. These would be applied in THERP as an Execution Recovery step on the task performance procedure step, typically within an HFE. Section 4.4 has more guidance on recovery opportunities for MCRA scenarios as separate HFEs.

4.3.3.3 Execution Failures Modeling C&C for Phase III Operator Actions

This section describes the process for identifying, screening, and quantifying C&C-related failures due coordination failures or communication failures during C&C such as those associated with the incorrect sequencing of operations. Details describing the background on this approach, what the C&C error represents and what it does not represent, are provided in Appendix B. C&C errors are incorporated into the Phase III MCRA using the following tasks.

1. Identify significant C&C-related errors based on screening potential errors.
2. Assign an HEP

Identifying and Screening C&C-Related Failures

The first task is to identify significant C&C related failures based on the screening approach given below. An HEP contribution from C&C coordination failure should be included in the MCRA HRA only if all of the following conditions are met. In other words, a potential C&C-related failure does not need to be included in the MCRA HRA if any one of the ordered criteria in Table 4-1 is NOT satisfied (e.g., if any relevant compensatory measures are in place).

The screening tests for inclusion of a C&C-related due to C&C coordination failures are shown in Table 4-1:

Table 4-1
Screening test for inclusion of C&C-related coordination failures

Screening Step	Description of Screening Step	If 'No'	If 'Yes'
1.	C&C coordination is required for placing equipment into service, e.g., successful pump operation requires adequate suction head from supporting equipment/system.	Screened from consideration.	Go to screening step 2.
2.	Failure to properly sequence operator actions for placing equipment into service would result in an irreversible failure of the equipment, such as either condition below leading to SSC failure within 15 minutes or less.	Screened from consideration.	Go to screening step 3.
3.	Operators can not immediately detect improper functioning of equipment (in order to immediately shut down equipment), due to, for example, i. A lack of local indications (including a lack of equipment or flow noises that are recognizable from training or experience); or ii. The field operator moving to a different location without checking for proper functioning	Screened from consideration.	Go to screening step 4.
4.	Supervisor in C&C role has responsibility for all (or the bulk) of communications to/from field operators, e.g., i. No one else is providing significant help to take or make calls to field operators implementing MCRA safe shutdown strategy and call from other plant staff (e.g., fire brigade, health physics), or ii. C&C is NOT solely (or mostly) focused on the communications associated with the equipment of concern and its supporting equipment/systems such as due to lack of help from other staff in taking/making these communications. iii. Communications are "segregated" such that supervisor and multiple field operators whose actions must be coordinated are NOT on a common loop such that all parties hear all communications (e.g., operator controlling cooling water to a pump does not hear the command to start the front-line system pump and therefore cannot alert the supervisor that there is no cooling water in service).	Screened from consideration.	Go to screening step 5.
5.	There are NO compensatory measures to assist the supervisor with coordination. Example cases where compensatory measures are NOT present are: i. The MCRA procedure does NOT include a written step, or Hold Point, or Warning (Caution) that prerequisite SSC alignment is needed prior to operation. For example, if an MCRA procedure includes a caution about putting in supporting equipment/system into service before putting into service the equipment in question. ii. The MCRA procedure does NOT include place-keeping aids such that the supervisor can record when support systems are in service, allowing the start of front-line systems.	Screened from consideration.	Include C&C-related coordination failure.

Assigning an HEP for C&C-Related Failures

The second task is to assign an HEP. These tasks are only performed if the C&C-related failure does not screen based on the criteria specified in the preceding step.

To address C&C-related coordination failures, it is recommended that an HEP of 5E-2 be assigned. Because the opportunity for within an HFE recovery is addressed during the screening process, no additional recovery is applied to this.

4.3.4 Step 4: Review the Collective Set of Phase III HFEs

One of the unique aspects of MCRA HRA is that there are multiple operators and multiple HFEs needed to reach a long term, safe and stable state using equipment outside of the MCR. Most MCRA studies model the enablement of each critical safety function as an individual HFE (e.g., Failure to start high pressure injection). Supplement 1, Section 7 discussed the development of an MCRA timeline where the major functions are plotted on the same timeline to understand the timing of individual HFEs with respect to the same time origin (see Supplement 1, Figure 7-7). However, since there may be actions conducted by one operator that may be required for success of the actions of a second operator, it is important to understand how all of the proceduralized operator actions are inter-related. A useful approach is to identify these interfaces on an integrated timeline showing all operators who implement actions modeled during MCRA, such as that shown in Supplement 1, Figure 7-9 (which is related to dual units, but these interfaces can happen in single unit MCRA as well).

The HRA analyst should check for reasonableness, particularly the overall HEP of each HFE and the number of critical tasks. It is a well-known limitation of THERP that HFEs that require many individual tasks can result in excessively high HEPs. Grouping of tasks by functional, perceptual unit is allowed in THERP and is frequently used during MCRA to counter this limitation. Also compare the HEPs for all MCRA HFEs in a scenario to see whether the HEP matches the complexity of the actions modeled.

Finally, the analyst should re-check for feasibility and check that the dependencies between actions are captured appropriately in the model logic. See Section 5 for more discussion on dependencies.

4.4 Recovery within Phase III HFEs

The actions performed in Phase III are, for the most part, execution of steps in the post-abandonment procedural guidance. The opportunities for recovery in this phase are of the following types:

> Self-checking or peer checking for actions, where the person taking the action (or a co-located peer) realizes that they took a wrong action (e.g., operated a wrong switch or valve) and corrects the action before it has significant consequences. This recovery is typically applied within an HFE.
>
> In most MCRA cases involving actions taken in plant areas, it is likely that there will only be one person present so self-checking will be the predominant recovery opportunity at such locations. The potential benefit of self-checking is limited, though training can reinforce the behavior of operators to perform self-checking. However, the guidance in THERP (NUREG/CR-1278, Chapter 10, Ref. 4) for example, would suggest no more than a credit of 0.5 reduction in the overall probability of failure from self-checking. It is recommended that this credit only be permitted where the training and work practices

explicitly include self-checking as part of the tasks.

Unless information is collected in operator interviews that indicates more than one operator may be co-located in plant areas post-abandonment (and thus each be able to check the actions of the other), recovery by peer checking is possible when the results of the action are indicated at the RSDP such that the SS/CRS can observe the consequences of the action or its failure and relay the failure to the relevant operator. An example of such peer checking would be if the action is to open a valve to permit a flow that is indicated at the RSDP, the fact that no flow is indicated on the RSDP would allow the SS/CRS to inform the plant-located operator that the action has not been successfully completed. Given that in most cases the SS/CRS will be using the abandonment procedure steps as the basis for confirming parameters (e.g., the start of flow or changes in status indicators), the corresponding likelihood of the recovery for such steps is 0.05 based on the discussion of special one-of-a-kind checking discussed in NUREG/CR-1278, Chapter 19.

Recovery actions aimed at hardware failures and incorporated in the procedures that are taken if a normal step fails to accomplish the expected action (e.g., if a piece of hardware fails to start when selected to run). This recovery is may be applied within an HFE, or may be a separate HFE.

Many procedures contain instructions as to what actions are to be taken in the event that the operator actions in one step do not accomplish the intended outcome. These are often in the form of:

a. Start Pump "X"
    i. If pump X does not start, then:
        1. Start pump Y
        2. ….

Such sequences correspond to following the steps in any type of procedure and can therefore be modeled using the standard form of THERP.

Recovery if the abandonment procedure fails to accomplish its purpose, where the SS/CRS has to recognize the failure and decide on an alternative set of actions. This recovery is typically applied as a separate HFE.

Within the scope of this supplement, only the first two are considered explicitly in the guidance provided in this report since the likelihood of events leading to the need for the third, recovery following failure of the procedural actions to accomplish the safety mission, is considered to be low. However, it is recognized that conceptually it could be considered in some analyses of future NPP designs. In such a case, the analyst would need to model the probability of failure of the SS/CRS to recognize that the procedure is failing to accomplish its purpose and to make appropriate decisions about adopting an alternate strategy. This is consistent with the guidance in Supplement 1, Section 9.2, which acknowledges that recovery actions for the long term such as use of the extensive damage mitigation guidelines (EDMG) and severe accident management guidelines (SAMG) procedures could be considered. As observed there, "Recovery actions based on flexible and diverse mitigation strategies (FLEX) and SAMG procedures has been left to future evaluation and consideration."

4.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1*, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.
2. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
3. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology*, U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
4. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP),* A.D. Swain and H.E. Guttman, U.S. NRC, Washington, DC: 1983. NUREG/CR-1278.

5
RECOVERY, DEPENDENCY, AND UNCERTAINTY

This section provides quantification guidance on recovery, dependency, and uncertainty for MCRA scenarios. The fundamentals of each of these steps in the HRA process are not unique to fire HRA or MCRA HRA and NUREG-1921 Supplement 1 [1] Section 9 provides detailed guidance on what to consider qualitatively for MCRA.

5.1 Recovery

Section 9.2 of NUREG-1921 Supplement 1 discusses the definition of recovery and the modeling of recovery actions. There are two types of recovery that may be applicable to MCRA; 1) recovery within an HFE and 2) recovery by adding an HFE (termed a recovery HFE). Recovery HFEs may be added after the initial fire PRA model quantification in order to restore a function, reconfigure a system, or manually manipulate a component initially unavailable in the scenario. Crediting these types of actions is typically added to reduce the conservatism from the MCRA scenario, and is only implemented if the actions are feasible and plausible.

Quantification of recovery within an HFE is dependent on the phase where the action occurs. For Phase I HFEs, recovery credit is applied in the same manner as described in NUREG-1921, with the quantification guidance for detailed HFEs provided in Appendices B and C. For Phase II HFEs, no additional recovery credit can be applied to the decision to abandon decision tree due to the high reluctance of the operators to leave. See Section 3.2.3 and Appendix A of this report for additional details. During Phase III, recovery credit within a HFE is discussed in Section 4.4 of this report (which is consistent with the qualitative guidance in NUREG-1921 Supplement 1 Section 9.2).

During MCRA, the “initial, planned plant response” is the alternate shutdown procedure (the MCRA procedure). Typically, this procedure was developed assuming one train of equipment was failed by the fire. Since many of the U.S. plants only have two electrical trains, this means the alternate shutdown procedure is using the one remaining train - such that there are typically no options for recovery. However, some of the MCRA scenarios may have long time windows that could allow consideration of additional staff and additional recovery options that may be available for use during MCRA, such as actions in the Extensive Damage Mitigation Guidelines (EDMG) procedures. Although this report does not provide explicit guidance for such long-term cases, the quantification approach for newly identified recovery HFEs should follow the same approach as any other MCRA action. For example, any recovery action credited in a MCRA scenario should be accounted for the MCRA timeline, feasibility needs to be ensured, command and control needs to be addressed, and dependences between actions in the scenario should be considered.

5.2 Dependency

Section 9.3 of NUREG-1921, Supplement 1 discusses factors to consider for dependency analysis and stresses the importance of the scenario timeline. Generally, there are only a few

combinations of HFEs which need to be considered because in most cases a single failure will lead to core damage. However, there is the potential for the PRA model to generate combinations of HFEs which were not previous considered in the MCRA scenario development and these would need to be reviewed in detail associated timelines modified. Also, for some NPPs and associated MCRA safe shutdown strategies, additional recovery actions may have been added to the PRA since the MCRA timeline was developed. Consequently, the feasibility of these actions in combination with other actions will need to be addressed.

The dependency assessments among HFEs should follow the guidance in Supplement 1 Section 9.3 and NUREG-1921 Section 6.2 [2]. For Phase III HFEs command and control needs to be considered in the dependency assessment.

5.3 Uncertainty

The 2009 version of the ASME/ANS PRA standard requirement HR-G8 says to *characterize the uncertainty in the estimates of the HEPs in a manner consistent with the quantification and PROVIDE mean values for use in the quantification of the PRA results* [3]. The same requirements apply to all three PRA capability categories. The quantification approaches described in this document are intended to produce mean HEP values. The quantification approaches for Phase I and Phase III are based on existing HRA methods and uncertainty distributions associated with these methods can be applied to MCRA HEPs. The data associated with Phase II quantification is based on semi-formal expert elicitation and each branch point probability is considered to be a point estimate mean. No distributions associated with these HEPs were developed. To address uncertainty associated with the decision to abandon, two sensitivity cases are recommended. For Case 1, set to the decision to abandon HEP to 1.0 and then characterize the impact on the overall results. For Case 2, set the HEP to 1E-3 and then characterize the impact on the overall results.

For MCRA scenarios, one of the key parameters is timing and for HRA quantification the timing parameters are considered to be point estimates. To characterize the uncertainty associated with the timing parameters the HRA analyst should consider sensitivity studies of various timing inputs. Table 9-1 of Supplement 1 lists potential sources of uncertainty to consider for MCRA**.**

EPRI 3002003150 [4] provides guidance on HRA dependency analysis and recommends a sensitivity studies be performed with and without a minimum JHEP. These sensitivity studies should also be performed for MCRA scenarios. Because the uncertainty for MCRA scenarios can be large it is recommended that a minimum JHEP value for MCRA scenarios be implemented into base line PRA model. The minimum value should not be lower than the value applied to non-abandonment scenarios (if applicable). Increasing it an order of magnitude greater than non-abandonment scenarios should also be considered.

5.4 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1,* U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, DC, and Electric Power Research Institute (EPRI), Palo Alto, CA: 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.

2. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
3. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008*, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,* The American Society of Mechanical Engineers, New York, NY, February 2009.
4. *A Process for HRA Dependency Analysis and Use of Minimum Values for Joint Human Error Probabilities*. EPRI, Palo Alto, CA: 2016. 3002003150.

6
CONCLUDING REMARKS

The conclusions of NUREG-1921 Supplement 1 [1] highlights lessons learned and experience gained from the development of qualitative analysis guidance to support fire scenarios that may result in MCRA, describes good practices for MCRA modeling and HRA, and the type of interface that should be conducted with plant operations personnel during the MCRA HRA qualitative analysis process.

The ASME/ANS PRA Standard [2] high level requirement (HLR) HR-G provides the quantification requirements for post-initiator HFEs, and the process developed for MCRA quantification is expected to meet HLR-HR-G.

The focus of this report (Supplement 2) is to provide guidance on the quantification model used in the MCRA HRA. Therefore, the concluding remarks here will focus on key insights on MCRA from the quantification model development.

6.1 Key Lessons Learned about MCRA

The NUREG-1921 guidance for quantifying HFEs in Fire PRA [3] is focused on actions that are directed from the MCR with both EOPs and fire response procedures being used. As discussed in Section 2.2 of Supplement 1 [1], there are some fundamental differences between the MCRA context and non-abandonment contexts. In HRA, the fundamental differences manifest themselves as changes to the quantification methods (e.g. for Phase II) or the guidance for implementing an existing method (e.g. for Phase III). The MCRA response can be broken down into three distinct phases, each with their own set of considerations and quantification methods. The key differences, and their impacts to quantification, are summarized here by phase.

6.1.1 Key Lessons Learned – Phase I

Phase I actions are those actions that are taken prior to the decision to abandon. These actions are similar to other typical human actions modeled in Fire PRA and follow the same EOP and fire response procedures as non-MCRA fire PRA, so no additional quantification guidance is provided in this report; the methods in NUREG-1921 are adequate for modeling human actions during this phase.

6.1.2 Key Lessons Learned – Phase II

Phase II is the time period associated with the decision to abandon. During Phase II, the decision to abandon the MCR is reached for two very different scenario types. For loss of habitability (LOH) scenarios, because the habitability criteria are based on physical parameters where it becomes untenable to remain in the MCR, there is no quantitative contribution associated with the cognitive decision to abandon the MCR.

For Phase II, the HRA is primarily concerned with LOC scenarios, specifically to quantify the HFE that the crew will fail to make the decision to abandon in sufficient time to execute the MCRA safe shutdown strategy. With respect to impacts on quantification, the decision to abandon for LOC scenarios is substantively different from typical EOP actions in three ways:

1) Cue response: Typically, there is no individual indicator or explicitly defined parameter-based cue that is used to determine when the MCR must be (or would be) abandoned for LOC scenarios. The "cue" for abandonment is in reality a progression of indications about the fire including fire-induced failures and fire suppression. Operators are integrating the information as it comes in until it reaches a "tipping point" severe enough to satisfy the abandonment criteria. In all cases, some level of judgment is required in the decision to abandon following LOC, and operators must rely on their training to think critically and integrate their overall understanding of the plant state and plant response.

2) Timing: Supplement 1 provided an in depth discussion about timing for MCRA; Section 3 of this report (Supplement 2) refines some of the timing definitions in Supplement 1 specific to Phase II. It should be recognized at the outset that the timing of MCRA Phase II actions are not as well defined as other actions in internal events or Fire PRA, meaning that:

    a. The traditional concept of system time window (T_{SW}) based on thermal-hydraulics calculations does not fit for Phase II, because the time available for the decision to abandon is derived value that depends on the time required for Phase III. Thermal Hydraulics calculations typically apply from the time of reactor trip until a damage state such as component damage, core damage, or large early release. During the MCRA, the system time window needs to be reduced due to the time spent implementing the MCRA Phase III actions, so the time available to make the decision in Phase II is impacted by how much margin there is in Phase III (i.e., the time difference between the time it takes to complete the Phase III actions and the total time until the safe shutdown actions are no longer effective, based on the thermal hydraulics calculations);

    b. For LOC scenarios, the cue is not a single parameter instead a collect set of cues and the exact time at which the minimum set of cues become available can be difficult to define.

    Based on a review of industry MCRA analyses for LOC scenarios, the time from reactor trip until operators must leave the MCR in order to complete Phase III actions typically range from 5-25 minutes, with the average being around 15 minutes.

3) Reluctance: Based on discussion with operators and the semi-formal expert elicitation, there is a high level of reluctance associated with abandoning the MCR, for both LOH and LOC scenarios. This natural reluctance to abandon the familiar environment of the MCR is compounded by the fact that abandonment scenarios are rare. NPP operators are familiar with many "rare events" due to their frequent simulator training, but they may consider MCRA scenarios even less credible. To date, no MCRA events have occurred in the U.S, and realistic simulator training of MCRA decision making is uncommon. The semi-formal expert elicitation identified this underlying reluctance as the primary driver in quantification, and its effect is built into the baseline HEPs in the new decision tree for Phase II. This judgment was based on the range of RSDP capabilities, MCRA strategies and training for the existing US NPP fleet.

NUREG-1921 stated that additional research was needed in order to address the cognitive challenges associated with the decision to abandon the MCR. These three aspects listed above for Phase II HRA were sufficiently different from typical cognitive actions that the HRA quantification guidance in this report and NUREG-1921 Supplement 1 should be used instead of NUREG-1921. Consequently, a new decision tree and timing discussion was developed in Section 3 of this report to quantify the timely decision to abandon on LOC.

6.1.3 Key Lessons Learned – Phase III

Phase III actions are those taken after the decision to abandon is made. These are typically local execution actions of the variety that are covered by the methods in NUREG-1921. However, the context of these actions differ from typical internal events or Fire PRA ex-CR actions in that there are typically more local actions, more remote coordination, and the command and control structure has shifted. Therefore, the quantification approach in this report for Phase III follows the existing methods with some additional considerations to account for the major differences in context.

Following MCRA, the C&C structure shifts from a co-located setting with multiple instruments, alarms and communications circuits that are provided in the MCR to a distributed setting with limited instrumentation, alarms and communications. As part of the development of this report, research beyond that given in Supplement 1 was conducted to define and address C&C-related failures. Key lessons learned from the research underlying Supplement 2 are:

- Despite research efforts for both Supplement 1 and Supplement 2, there is little relevant literature on C&C as part of human reliability
- For a "new" context such as MCRA operations, it was helpful to compare and contrast what little is known about C&C between MCR and MCRA operations
- Research for Supplement 2 identified a new failure mode applicable to Phase III operator actions that is caused by C&C coordination failures
- There are few SMEs for MCRA operations; with many plant-specific differences related to MCRA safe shutdown strategies and little realistic training of MCRA operations, there are few "experts" who have the breadth of experience and knowledge needed to address this area of research and HRA/PRA
- SMEs were helpful in identifying the most important issues for C&C in MCRA operations and the focus for HRA
- This report did not use SMEs to develop a specific quantification tool and associated HEPs. Although this may have been only due to lack of resources, there were indications during the semi-formal elicitation that the SMEs were pushed to the limit of their experience/knowledge in developing qualitative insights (and may not have been able to develop specific quantitative insights)

6.2 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1,* U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.
2. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008*, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant*

Applications, The American Society of Mechanical Engineers, New York, NY, February 2009.

3. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.

A
DEVELOPMENT OF THE TECHNICAL APPROACH FOR THE DECISION TO ABANDON

This appendix discusses how the technical approach for assigning an HEP for the decision to abandon the MCR upon a LOC was developed, including a summary of the discussions with SMEs who informed the final quantification approach.

In general, development of the quantification approach for the decision to abandon involved the following steps:

1. Initial efforts to review existing methods for applicability,
2. Development of a consensus list of key issues to address in quantification of the decision to abandon,
3. Testing of CBDT against the key issues,
4. Development of "strawman" decision trees for the decision to abandon, and
5. Adjustment of decision trees and assignment of HEPs using SMEs.

The final decision tree and associated guidance is given in Figure 3-2 and Table 3-1 in Section 3.

A.1 Initial Efforts to Develop a Quantification Tool for the Decision to Abandon

Initially, several HRA methods, including CBDT, HCR/ORE, SPAR-H, NARA, CREAM, and IDHEAS were reviewed for insights and applicability to the decision to abandon. These methods were also reviewed for potential quantification gaps, for instance, the “cues” for LOC are not as deliberate as other HRA cues. The softness of the LOC cue along with the general reluctance of operators to abandon the MCR were considered factors important to the quantification of the HEP for the decision to abandon.

A.2 Development of a Consensus List of Issues for the Decision to Abandon

Following the initial reviews of existing HRA methods, the team developed a consensus list of issues important to the decision to abandon. NUREG-1921 Supplement 1 was the key input to this list, especially Section 4 of Supplement 1 [1] that described the process to determine fire PRA scenarios that may result in abandoning the MCR upon a LOC. Additionally, Supplement 1 described some of the PSFs and other qualitative considerations. The list also represented follow-on research performed by the authors after Supplement 1 was published.

The team developed a list of issues that may be potentially important for the decision to abandon. This is documented in Table A-1.

Table A-1
Items important to the quantification of the decision to abandon HFE

Issue	Differentiation Points	Compensatory/Synergistic Issues
Procedures	- **Criteria available:** There is some level of qualitative or explicit criteria for loss of control. Explicit criteria for identifying/confirming fire location and associated systems/components (consistent with fire PRA modeling) whose failure due to fire requires abandonment or Procedure provides fire locations that, when identified and confirmed, indicate likelihood of needing to abandon, but still leave it up to SS/SM decision - **Judgment only:** There are no specific criteria, and the decision is purely at the discretion of the commander.	More detailed or realistic MCRA training may be able to partially compensate for lack of content
Training	- Best case: "Realistic" training in simulator with RSDP mockup or detailed talk-throughs - Worst case: Classroom only training at minimum level	Training can help when procedural guidance is less explicit, but the reverse impact unlikely to be true (i.e., better procedural guidance does not mean that operators need less training)
Time available (versus time required)	- Best case: Long (~20-25 mins) - Worst case: Short (~5 mins) - Intermediate case: Moderate (15 mins) [The Phase II timing is based on the detailed timeline development discussed in Section 7 of NUREG-1921, Supplement 1 and will depend on the remainder from Phase III action timing.]	Traditionally, HRA would represent the impact of more explicit procedural guidance on the decision to abandon & more realistic training as a faster (& more reliable) action
Reluctance	Reluctance includes consideration of: a) capability of the RSDP, b) operator comfort & familiarity with MCR, c) inability of operators to conceive of such a desperate situation. - Best case: Capable RSDP, explicit MCRA criteria & "realistic" training - Worst case: Very limited capability RSDP, no explicit MCRA criteria, & minimum classroom training - Intermediate case: Most major systems on RSDP, some MCRA criteria; some training	None

Issue	Differentiation Points	Compensatory/Synergistic Issues
Staffing & communications	-Best case: SS/SM aided in decision-making by STA or other crew who are monitoring clear abandonment criteria as would be done with Critical Safety Function Trees -Worst case: SS/SM discretion only -Intermediate case: SS/SM receives timely input from ex-MCR operator on severity of fire OR from other in-MCR crew on status of MCR boards and key equipment	None

A.3 Efforts to Map Existing HRA Methods to the Issues List

Following the development of the issues list, the team returned to review of existing HRA methods with the intention of identifying how the method can address each of the issues. This effort started with the review of the CBDT decision trees.

Early on in the project, some of the CBDT trees were re-interpreted specifically for the decision to abandon. It became clear, however, that the re-interpreted trees still contained elements that were not specific to the decision to abandon and it was also felt that using the same set of CBDT trees would lead analysts to interpret them as they had conventionally done, rather than with the new guidance for the decision to abandon. This led to a subsequent review of the revised CBDT trees was performed to understand: a.) Is the failure mode of the tree still applicable? b.) Are the PSFs in the tree appropriate for the new context? and c.) Are there dominant failure modes or mechanisms missing from the set that should be accounted for? This second review of the CBDT trees yielded the following insights:

- The CBDTs trees were intended to be applied for one main cue (e.g., a procedure step, parameter or set of parameters) – for LOC, the “cue” is more vague and encompasses the fire alarm, plus verification of fire, and verification of LOC.
- Both the actual abandonment procedural step and the transfer to the abandonment procedure were supposed to be covered and this presented some confusion in the re-interpretation of the trees.
- Revised trees also added an extra level of differentiation where CBDT did not have that resolutions (e.g., trees were binary decisions, but the procedure quality range was too large to fit well in a binary structure).

Table A-2 provides the results of the initial guidance for using the revised CBDT trees and the discussion that preceded the stress test.

Table A-2
Comparison of Revised CBDT Trees

Tree Branch	Guidance for Evaluating CBDT Trees	Discussion
Pca, Availability of information	The path selected for this cause-based decision tree method (CBDTM) tree is usually either [c] or [d], with the following rationales for each branch selection in the tree: *Indication Available in Control Room - The primary cue of the fire alarm will be available in the MCR and the unavailability of key instrumentation in the MCR due to fire will be noticed by the crew.* *Control Room Indication Accurate - One of the reasons for the decision to evacuate the MCR is the lack of reliable instrumentation due to the severe fire either in the MCR, cable spreading room or other similar location.* *Warning / Alternate in Procedure - The plant fire procedure identifies the possibility of potential indication differences and directs the operators to monitor unit/plant parameters and to notify the Shift Manager (SM) of any unusual or abnormal indications which occur. For fire areas in which indications could be impacted, the fire area guidance lists of protected instruments by safe shutdown path.* *[The down branch should be selected if warnings are not provided in the procedure.]* *Training on Indication-The extent of training on the systems and instrumentation loss that would mandate MCR evacuation is not clear and is therefore not credited.* *[The down branch should be selected if interviews and observations determine that training is not provided or adequate for the instrumentation losses.]* Another example discussion of the rationale for path [c] is the following: *It is assumed that MCR indications are not reliable due to the fire; however, based on operator interviews, it was discussed that it is one of the responsibilities of the STA to identify and notify the operations crew on which indications are reliable. This is considered equivalent to Warning/Alternates in a procedure. It was stated that this is also covered in training.*	This tree provided the basis for the new operator/information interface failure tree that represents the possibility that cues for abandonment in LOC events are not clear and available such that the operators do not decide that abandonment is necessary. For the LOC case, it was considered that the "CR Indications Accurate" branch would always be "no" for LOC because the large amount of "noise" in the cues is expected to obfuscate the decision to abandon versus a non-MCRA fire - this is the essence of an LOC fire, that indication failure modes cannot be predicted. The other two branches – asking about procedures and training – were directly incorporated into the new tree.

Tree Branch	Guidance for Evaluating CBDT Trees	Discussion
Pcb, Data not attended to	The path selected for this CBDTM tree is usually [j], with the following rationales for each branch selection in the tree: *Low vs. High Workload - High workload is assumed due to fire conditions.* *Check vs. Monitor - The fire alarm would be checked to see what areas are impacted; this draws the crew's attention to the fire and the need to control the plant.* *Front vs. Back Panel - Alarm is located on the back panel.* *[The fire alarm location is plant-specific and needs to be identified during walkdowns or interviews.]* *Alarmed vs. Not Alarmed - The fire alarm is very loud, according to the operator interview.*	This tree was omitted as it was considered a negligible contributor – the combination of the fire alarm and the other instrumentation readings are unlikely to be missed, which is the intent of this tree.
Pcc, Misread/miscommunicated data	The path selected for this CBDTM tree is usually [a], with the following rationales for each selection in the tree: *Indication Easy to Locate - Fire alarms and system functionality indications are expected to be easy to locate when crew are confirming that the indicators are failed or do not respond.* *Good/Bad Indicator - The fire alarm provides room location of fire and description.* *Formal Communication - Formal communication is used by operators.*	This tree was omitted because the indications are multiple and because this was a low-level contributor to the total HEP (e.g., highest HEP still in the E-3 range)
Pcd, Information misleading	The path selected for this CBDTM tree is usually [b], with the following rationales for each selection in the tree: *All Cues as Stated - Secondary cues and indications not directly applicable to the operator action under consideration could be inaccurate as a result of fire impacts. Therefore, it is possible that not all cues present in the control room are as stated.* *Warning of Differences - The plant fire procedure identifies the possibility of potential indication differences and directs the operators to monitor unit/plant parameters and to notify the Shift Manager of any unusual or abnormal indications which occur. For fire areas in which indications could be impacted, the fire area guidance within the lists of protected instruments by safe shutdown path. Consistent with Pc-a, it is also expected that cues may be impacted by fire and warnings are provided by the STA during the fire event.* *Specific Training – N/A* *General Training – N/A*	Because of the nature of the indications during LOC, it was difficult to see how this tree was substantively different than Pca when applied to LOC scenarios. Therefore, this tree was absorbed into the new operator/information interface failure tree along with Pca. Similar discussion to Pca to what is actually the cue (e.g., fire alarm, system failures)?

Tree Branch	Guidance for Evaluating CBDT Trees	Discussion
Pce, Skip a step in procedure	The path selected for this CBDTM tree is usually [e], with the following rationales for each selection in the tree: *Obvious vs. Hidden - The steps for this action are not hidden but the direction from the fire procedure to the MCRA procedure is not clear and compelling.* *Single vs. Multiple - The operators would likely be in multiple procedures (Fire, EOPs, AOPs).* *Graphically Distinct - The steps are considered to be graphically distinct as there is a bolded caution statement concerning this action.* *Placekeeping Aids - There are placekeeping aids in the procedures.*	This tree was omitted as it was considered a negligible contributor. While the crew will likely be in multiple procedures during the time, the MCRA step is not unlikely to be simply "skipped" (e.g., E-3 or lower contribution).
Pcf, Misinterpret instruction	The path selected for this CBDTM tree is usually [f] or [g], with the following rationales for each selection in the tree: *Standard or Ambiguous Wording - The step from the Fire procedure to the MCRA procedure is ambiguous.* *All Required Information - The step does not contain all the information needed for making the abandonment decision.* *Training on Step –* *For [f] - The procedure step itself is ambiguous and does not contain all the information needed for making the abandonment decision, but training is provided.* *For [g] - Training is not provided; it is considered a judgment call on the part of the Shift Manager.*	This tree was used as the basis of the new operator/procedure interface failure tree. The new tree was created to include both the clarity of the procedural path to transition to the MCRA procedure as well as the instruction within the MCRA procedure. The branches were altered to focus less on the "standardness" of the wording and more on the content and level of explicitness of the procedural step(s).
Pcg, Misinterpret decision logic	The path selected for this CBDTM tree is usually [k], with the following rationales for each selection in the tree: *NOT & AND or OR Statement -The procedure does not provide specific wording* *Practiced Scenario -The scenario is practiced in training.*	Similar to Pcf, for LOC, the important feature of the decision to abandon is if the step explicitly provides a decision logic or leaves the decision to judgment. The intent of this tree, along with Pcf was absorbed into the new operator/procedure interface failure tree.

Tree Branch	Guidance for Evaluating CBDT Trees	Discussion
Pch, Deliberate violation	The path selected for this CBDTM tree is usually [a], with the following rationale: *Not Applicable. The decision to evacuate the MCR is left to the discretion of the Shift Manager; therefore, the question of whether the operator will follow the guidance is not relevant to this HFE (i.e., the procedure is simply providing the operator with a choice to perform the action or not).*	This tree was traditionally included as a catch-all place holder for unusual scenarios where the operators were skeptical about the success of the procedural path and that the procedural path had negative consequences (e.g., irreversible plant damage). For LOC, this tree was replaced by a new Reluctance tree, which specifies under what conditions operators are most likely to delay the decision to abandon beyond the time it would be useful.

A stress test of the revised trees was performed against a range of strategies and conditions defined in the "issues" table and concluded that the trees could be consolidated by looking at 1) operator-information interface, 2) operator-procedure interface and 3) reluctance (new factor). In some cases, the revision of the trees was substantial enough that the developers were worried that users would not adequately consider the new guidance and therefore miss the significance of the revision in the quantification.

A.4 Development of New Decision Trees for the Decision to Abandon

From the insights and consideration of the "issues" table, three new trees were developed:

- Failure to transfer to MCRA procedure
- Failure of understand the MCRA criteria have been met
- Reluctance/delay

These three trees are shown in Figures A-1 through A-3 (in Section A.5.2).

A.5 Use of Subject Matter Experts to Modify and Provide HEPs for the Decision to Abandon Quantification Tool

The next step in the process for developing a quantification tool for the decision to abandon was to perform a semi-formal expert elicitation in order to: 1) verify (or modify) the three decision trees for applicability to the decision to abandon, and 2) develop HEPs for the end points on the decision tree(s).

The three trees and the issues table formed the skeleton for discussions with knowledgeable SMEs. The results of this exercise are documented in Section A.5.2. As a result of the SME feedback, the trees continued to evolve. A summary of the revisions included:

- The *Failure to transfer to MCRA procedure* was removed from further consideration. This was determined to not be a significant contributor for failure.
- The *Failure of understand the MCRA criteria* tree remains. This tree will be further expanded to incorporate reluctance and incorporate timing.
- The *Reluctance/delay* tree was eliminated. The reluctance will be built into the HEP estimates for the *Failure to understand the MCRA criteria* tree.

The re-structured tree were presented to the SMEs, who were asked to assign probabilities for a range of scenarios. A pairwise comparison between the different end states was also conducted. The final event trees, probabilities, and guidance are provided in Figure 3-2 and Table 3-1 in Section 3.2.3

The sub-sections below summarize aspects of the semi-formal expert elicitation.

A.5.1 Soliciting Feedback and Confirmation of Issues

On December 19, 2017 the team solicited feedback on the issues and technical approach. Two experts were from the NRC and two experts were supported by EPRI. The SMEs include:

- **Harry Barrett** (U.S. NRC) received a BS degree in Marine Nuclear Science from SUNY Maritime College (Fort Schuyler) in 1975. Early in his career, he worked in the U. S. merchant marine as a Coast Guard licensed marine engineer and as a nuclear engineer at several shipyards refueling and testing naval reactors. He has extensive experience in the commercial nuclear industry in the areas of nuclear plant operations (Senior Reactor Operator), maintenance, engineering (PE), and project management. Prior to joining the NRC, he was responsible for the first National Fire Protection Association (NFPA) 805 Pilot Plant (Duke Energy's Oconee). Mr. Barrett came to the NRC in May 2007 as a fire protection engineer in NRR. Since that time, he has developed guidance and resolved technical issues related to risk-informed fire protection programs while performing numerous technical and regulatory reviews of NFPA 805 license amendment requests. He provided technical oversight of the first NFPA 805 Pilot safety evaluation (Shearon Harris) and assisted at the triennial fire protection inspections at both NFPA 805 pilot plants and most non-pilot plant NFPA 805 inspections.
- **Erin Collins** is a Senior Engineer at JENSEN HUGHES with 32 years of experience in safety, reliability, and risk assessment, specializing in data analysis and human reliability analysis for nuclear, chemical, and aerospace applications. She was a key technical participant in the Fire HRA Task of the Fire PRAs for ANO-1, ANO-2, Kewaunee, Monticello, Nine Mile Point 1 and Prairie Island plants and provided review and input to the HRAs for the Browns Ferry, Ginna and Palo Verde Fire PRAs. She was also a primary analyst for the Main Control Room abandonment HRAs for the Diablo Canyon and V.C. Summer Fire PRAs. Ms. Collins was a reviewer of the EPRI Seismic HRA methodology and is a key participant on the JENSEN HUGHES' Seismic HRAs for the Duke Energy fleet Seismic PRAs. Ms. Collins is on the team developing EPRI-NRC RES Guidelines for Main Control Room Abandonment HRA and was the Principal Investigator for the EPRI Guidelines for PRA Data Analysis. She performed PRA equipment reliability database updates for ANO-1, Hatch and Palisades, as well as the FAA regional air route traffic control centers (ARTCCs), the U.S. Army Chemical Weapons Destruction facilities, the Titan IV/Cassini RTG Safety Study for NASA and its contractors, and the

U.S. Department of Energy's (DOE) License Application for the Yucca Mountain Project for nuclear plant waste disposal.

- **Jeff Julius** is a Director of Risk and Safety with JENSEN HUGHES. He has 37 years of experience in the operation, maintenance, and probabilistic risk assessments (PRA) of nuclear reactors. These analyses supported risk-informed decision-making such as plant licensing and start-up, satisfied regulatory requirements including periodic safety reviews and transition of the plant's fire protection program to NFPA 805, evaluated potential plant modifications, and maintained safety while remaining on-line at power. He has researched and developed new Risk Assessment methods and PRA techniques in the areas of Shutdown PRA and Human Reliability Analyses. Mr. Julius has been the senior technical advisor or project manager for several fire and flood PRAs, and Peer Reviews. Additionally, Mr. Julius was a co-author on reports for Fire HRA (NUREG-1921 and NUREG-1921 Supplement 1).
- **Jim Kellum** (U.S. NRC) is a Senior Engineer in the Office of New Reactors with over 35 years of experience in the nuclear power industry. During his 11.5 years at the NRC he has contributed to the Knowledge and Abilities (K/A) catalog develop for the AP-1000, ABWR, and NuScale designs. Mr. Kellum has extensive experience with main control room simulators; participating in the development of IP-41502 (simulator inspection), and a committee member of ANSI 3-5. He is also an Operator Licensing Examiner for the Westinghouse, Combustion Engineering, and AP-1000 designs. Prior to joining the NRC, Mr. Kellum spent 24 years in operations and training in the commercial nuclear power industry. Mr. Kellum held SRO licenses at Beaver Valley and Calvert Cliffs. Mr. Kellum's commercial nuclear experience also includes EOP development, SAMG development, simulator instructor, training supervisor, exam writer, and requalification supervisor. Mr. Kellum has a BS from the University of Toledo and spent 8.5 years in the nuclear Navy.

A.5.2 Discussion of Factors Important to Decision to Abandon on LOC

The following high level "issues" were discussed relative to the decision to abandon:

- Transfer to MCRA procedure
- Procedure guidance
- Cues and indications
- Training
- Timing
- Reluctance to leave MCR
- Staffing and Communications

Transfer to MCRA Procedure: Do the operators have sufficient pointers or guidance to review the entry criteria for MCRA in order to make the decision to abandon in time? A summary of the discussion about this topic included:

- This issue is less important than the other issues presented.
- Entry into the procedure is based on what the operators observe on the main control boards / annunciators.
- Operators will not leave the MCR unless there are significant control and instrumentation failures from the fire. This would likely include observation of multiple fire alarms and loss of significant control functions.

- Operators may mentally be running through criteria along with severity of fire. Operators are familiar with the specific locations that may require abandonment and are familiar with the entry criteria.

Changes to tree structure: Removed "Failure to transfer" tree from further consideration.

Specificity of procedure guidance: How much specificity in the entry criteria is helpful in making the decision to abandon? The relevant discussion included:

- More detail may help, but in reality, there is an infinite number of scenarios / things that can go wrong. More detail helps with the decision and training will compensate.
- Training and experience will help the operators recognize a potential LOC scenario. This may be more of a factor than the specificity of the criteria.
- Some procedures may be explicit: if fire is in switchgear room; trip reactor, trip turbine, close main steam isolation valves (MSIVs), and abandon. Even with this specificity, crews may hesitate. There are criteria, but they know there is margin/leeway in them.

Changes to guidance: Qualitative and/or explicit guidance is helpful, but training and experience are more relevant in deciding whether or not to abandon the MCR.

Cues and Indications: What type of information needs to happen for the operators to consider abandoning? The relevant discussion included:

- Operators are integrating the information as it comes in. Operators would need to observe cues related to the fire and observe system impact to consider abandoning.
    - If a sprinkler alarm indicator comes in, you have a pretty good idea that it is a real fire.
    - Sometimes you may see electrical impacts prior to fire alarm
    - More likely to trust water flow alarm versus just a single smoke alarm
- Based on what operators see, they may abandon immediately (e.g., loss of electrical distribution). For slower progressing fires, operators will likely want visual confirmation of severe fire (reports of operators not being able to see anything, heavy smoke, etc.) or observation of spurious equipment operations (PORVs, ADVs, emergency core cooling system (ECCS) pumps).

Training: How does training specific to the decision to abandon assist the operators? The relevant discussion included:

- The training for control room abandonment may exclude "the decision", in other words, the operators are told by operator trainers that the conditions for abandonment have been met.
- Based on plant training philosophies, shift managers can make decisions based on knowledge and observation of what is occurring (this/that/the other thing go away and the SM makes the decision independent of procedures just based on understanding of plant).
    - Reliability isn't always based on procedural guidance.
    - "Prudent actions" category in training that gives them leeway away from verbatim compliance.
    - Even with good procedures and very good RSDP, wrong decisions can be made – it comes down to judgment and understanding.

Timing: Will the decision be made in time, such that there is enough time for remote shutdown? The relevant discussion included:

- There is a sense of urgency needed when making the decision to abandon. The definition of urgency has two components:
  - 1.) The fire progression is rapid/large/obvious; for example: electrical cabinets on fire and seeing the electrical distribution system going away
  - 2.) Time critical actions linked with fires in certain areas (e.g., need to start auxiliary feedwater (AFW) locally within 30 minutes).

Reluctance: What is the impact of reluctance? The relevant discussion included:

- The capability of the RSDP may play a role. If a plant's RSDP is limited there may be higher reluctance.
- At the same time, many operators will only be familiar with their plant's strategy and will have some level of comfort in the strategy. (In other words, the operators will be reluctant to abandon the MCR regardless of the RSDP capability and increasing the RSDP capability may not reduce reluctance significantly.)
- There will always be reluctance. The MCR is a familiar place, with lots of capabilities and options.
- Plants with a self-induced station blackout (SISBO) strategy may be reluctant to leave MCR.
- There is a time pressure component to reluctance. *Will they make the decision in time?*
- Factors that may play into reluctance include; capability of RSDP, communications, complexity of plant, training using simulator mockup, leaving a familiar place with lots of capability and options, scenario (SISBO, etc.).

Examples:

- Reluctance similar to BWRs injecting liquid poison.

A.5.3 Discussion of Decision Trees

Tree 1: Failure to transfer to abandonment procedure. Will operators be able to reach the procedure step to view the MCRA criteria in time? The tree included the following branch points:

- *Multiple procedure transfers required?* Is there a clear path in the fire procedures to the step that provides the MCRA criteria?
- *Status assessment supported by STA OR practiced scenario?* Has the crew practiced this scenario or a scenario similar to this one in a simulator? Unless the training has covered the actual decision-making process, this will most likely be "No." OR STA is available AND trained on LOC abandonment criteria.

The SMEs provided the following feedback:

- Fire has to be of a significant nature to review criteria.
  - If fire is small, operators wouldn't necessarily open the procedure even though there may be explicit transfer criteria. If a fire causes a reactor trip, you would still be in the procedure for post-trip actions / EOPs while verifying the severity of fire.
- There are typically only a handful of plant locations where abandonment may be required. If a fire is in that area, they will be evaluating *when will it get so bad that I*

need to abandon? Operators may open the procedure to review the criteria as the scenario progresses.

- The tree is less important than the other factors discussed. Operators are not leaving unless there is a real fire impact (seeing functions that are lost). Once impact is observed, operators will be thinking abandonment automatically.
- Is local confirmation of a fire needed? If multiple fire alarms come in and see plant impacts, may not wait for confirmation of fire (even if there isn't a procedure step or procedure is circuitous), particularly if the fire location is known.

Conclusions: The SMEs concluded this tree was <u>not</u> a driving factor in quantification. Tree 1 is removed from further consideration.

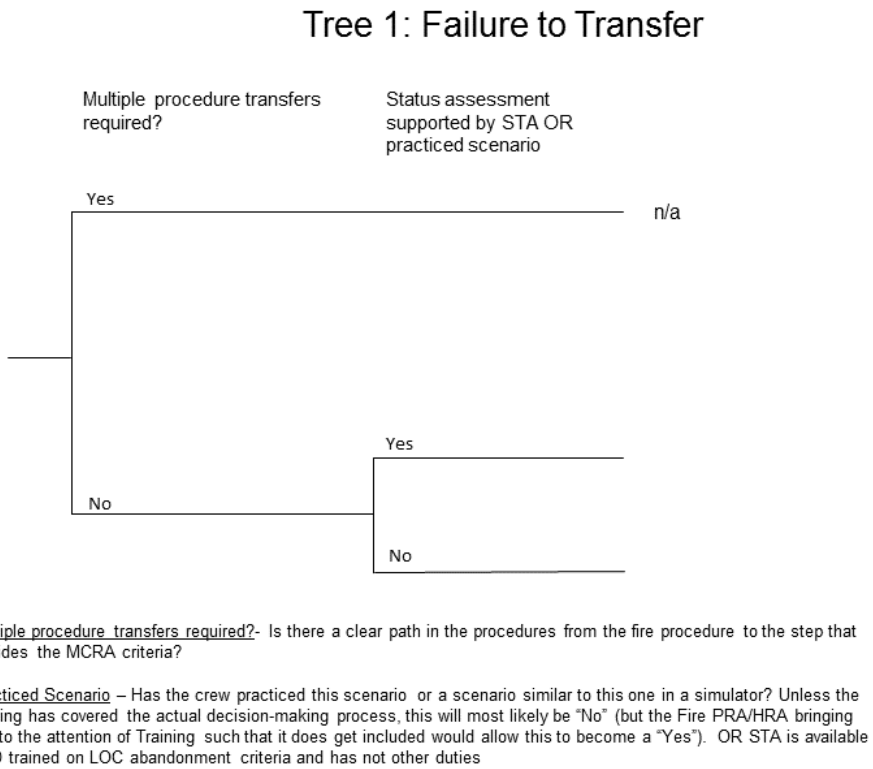


Figure A-1
Tree 1: Failure to transfer

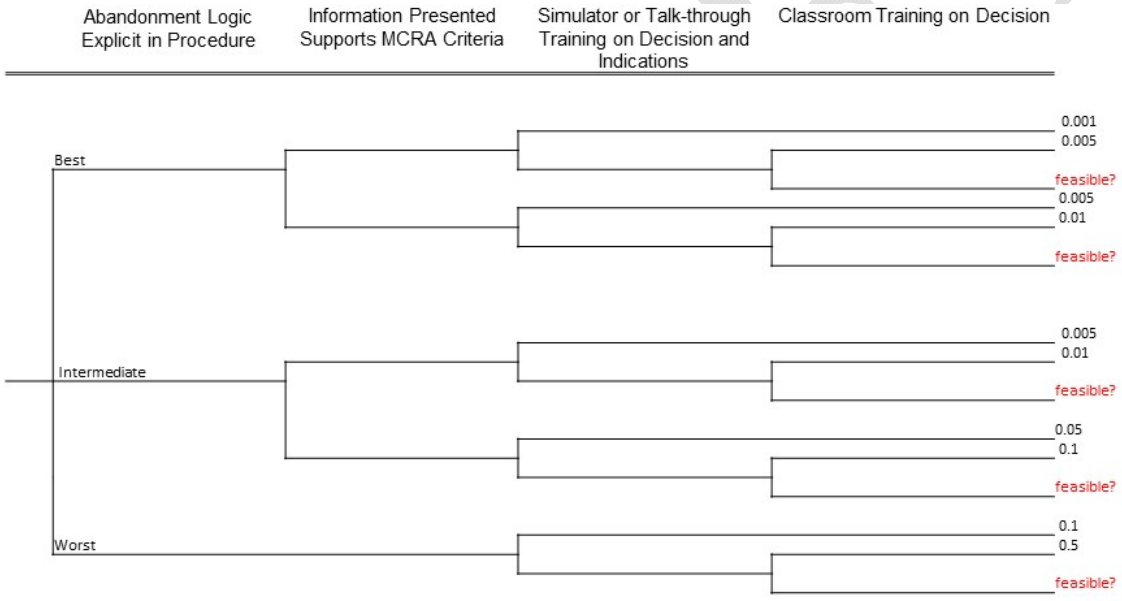
Tree 2: Failure to understand abandonment criteria has been met. Do the procedures help operators map between what they are seeing in the MCR and the definition of a LOC scenario? The tree included the following branch points:

- *Abandonment logic explicit in procedure?* This included a best case (explicit criteria), intermediate (qualitative description, but with some decision-making), and worst case (no criteria / pure judgment).
- *Simulator or talk-through training on decision and indications?* Has the crew practiced this scenario or a scenario similar to this one in a simulator or talk-through? Unless the training has covered the actual decision-making process, this will most likely be "No."

The SMEs provided the following feedback:

- There are an infinite number of potential scenarios, so while more detail in criteria is good, this may not be consequential because there will be consistent checking of systems as the fire progresses. Training and experience are more important than procedures in this case.
- In the abandonment criteria, there is a balance between the amount of guidance and the ability to think agilely, especially for less experienced operators that may be more reliant on procedures.
- More specificity may be needed for time constrained scenarios.
- Is there a need to have three levels of differentiation between procedure criteria specificity? There will always be judgment involved, so more criteria are not necessarily better. The prescriptiveness of the criteria may not be the same for each plant, and a lot of that depends on the management philosophy (more procedurally reliant).
- Operational experience is key. SROs should have an understanding of priorities. Less experienced SROs will be more reliant on procedures.

Conclusions: Condensed first branch point (explicitness of abandonment logic) to criteria available or judgment.



Abandonment Logic Explicit in Procedure
Best - Explicit criteria
Intermediate - Qualitative description but requires some decision-making.
Worst - Pure judgement + basis feasibility criteria (at discretion of SS….nothing else…)

Information Presented Supports MCRA Criteria
Do the operators have an immediate way of knowing whether or not the MCRA criteria are satisfied based on the information they have?
Is it obvious or not (e.g., running vs. standby).
For example, for standby systems (RHR, LPI) -> how do the operators know if they've failed until they try to actuate them?

Simulator training on LOC decision

Classroom training on LOC decision
Consolidate training into one "Practiced Scenario" branch? Has the crew practiced this scenario or a scenario similar to this one in a simulator? Unless the training has covered the actual decision-making process, this will most likely be "No" (but the Fire PRA/HRA bringing this to the attention of Training such that it does get included would allow this to become a "Yes"). OR STA is available AND trained on LOC abandonment criteria and has not other duties

Figure A-2
Tree 2: Failure to understand abandonment criteria has been met

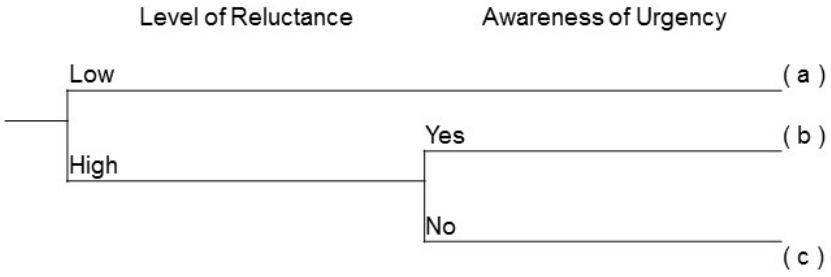
Tree 3: Reluctance/Delay Tree. The branch points include:

- *Level of reluctance.* Is there trust in the strategy? This includes the procedures following abandonment and capability of the RSDP.
- *Awareness of urgency.* Have the operators had training on the need for decision-making in a timely basis before it is too late? Do they understand that, beyond a certain time, abandonment will no longer be a successful option?

The SMEs provided the following feedback:

- There is always some reluctance that will surround the decision to leave the MCR.
- Like liquid injection post anticipated transient without scram (ATWS) – operators really do not want to do it, but understand when it is necessary and will do it.
- Scenario really boils down to what is lost due to the fire. The operators are worried about random failures and if you get one at the RSDP, it may be fatal to the strategy. There is also a reluctance due to lack of familiarity with the panels – there may be training only once every two years.
- *Is communication important to reluctance?* Depends on the plant and how important the communication plan is to success. If there is no RSDP, communication becomes a big deal, if you have one panel and send people to configure equipment but all of the control happens at the panel, then it is not as big of a deal.
    - This would also depend on complexity of plant (few actions may not challenge your teamwork and command and control)
- SISBO situations would have an extra layer of reluctance.

Conclusions: Reluctance is a general influence in the decision to abandon. Merge the awareness of urgency with Tree 2.



Level of Reluctance -
Do operators trust the strategy (procedures following abandonment and capability of the RSDP)?

Awareness of Urgency - Have the operators had **training** on the need for decision-making on a **timely basis before it is "too late**"? Do they understand that, beyond a certain time, abandonment will no longer be a successful option?

Figure A-3
Tree 3: Reluctance/delay tree

A.5.4 Expert Elicitation Results

Upon finalizing the event tree, the next objective was to obtain probability estimates. The following calibration points were provided to the experts:

- Not possible = 1.0
- Very likely to fail = 0.5
- Infrequently failed = 0.1 (9/10 are successful)
- Unlikely to fail = 0.01 (99/100 are successful)
- Very unlikely to fail = 0.001 (999/1000 are successful)

The experts were then asked about a range of different LOC scenario contexts. The worst case scenario was discussed first, followed by the best case. Pairwise comparisons surrounding the intermediate end states were conducted to determine the ranking and probabilities for the remaining end states.

Worst case (End State 8)

The first scenario discussed was the least optimal LOC case. The scenario included a short timeframe, judgment only (no qualitative or quantitative criteria), classroom training, and no awareness of time urgency (end state 8).

Consensus value: 0.2 (Individual values: 0.1, 0.1, 0.1, and 0.3)

Discussion: Time, awareness of urgency, and reluctance are drivers. Experience can offset the lack of awareness, but a less experienced crew may not correctly interpret the signals to abandon in time. The short timeframe was also a concern; with minimal time, reluctance will drive and operators may take alternate actions (like trying to start another charging pump) and not be focused on abandoning in time.

The second scenario was identical to the worst scenario except for a longer timeframe was available.

Consensus value: 0.1 (Individual values 0.05, 0.08, 0.1, and 0.1)

Discussion: With additional time, there is reduced reluctance and time for additional checking.

Best case (End State 1)

This scenario describes the most optimal LOC case. Scenario characteristics include criteria for abandonment, simulator or talk-through training on the decision to abandon, an awareness of the time urgency, and a long timeframe.

Consensus value: 0.02 (Individual values 0.01, 0.01, 0.02, 0.05)

Discussion: General reluctance still the overriding factor in quantification. Training helps offset, but still, there is a tendency for incorrect actions to be taken (or not taken in time). On the other hand 25 minutes is quite a long time and if there are clear criteria, then the action should be reliable.

For the same scenario characteristics, but with a short timeframe.

Consensus value: 0.1 (Individual values 0.1, 0.1, 0.05, 0.15)

A.5.5 Calculation of Probabilities

Table A-3 lists the pairwise comparison raw data. Since all experts agreed that Branch 1 is the best and Branch 8 is the worst, the pairwise comparison determines the ranking of Branch 2 through Branch 7.

Table A-3
Pairwise Comparison of Raw Data

Branch comparison	Better (e.g., Branch 7 is better than Branch 8)	Worse (e.g., Branch 7 is worse than Branch 8)	The braches are equivalent in terms of HEP
8-7	4		
8-4	4		
7-6		4 – but if simulator scenario is the same then it is close	
7-5	4		
7-4			4
7-3	4		
7-2	4		
6-5	4		
6-4	1	1	2
6-3	4		
6-2	4		
5-4			4
5-3	3		1
5-2	3		1
4-3	4		
4-2	4		
3-2		4	

The pairwise comparison scores of Branches 2 through 7 are summarized in Table A-4 in a matrix format. If an expert thought that the branch in a particular row was better than the branch in a particular column, the branch in the row gets 1 point. Similarly the branch gets half a point for a tie, and loses 1 point for being worse than the branch in a particular column.
From Table A-4, we can conclude the following (A > B means A is better than B):

1. B1 > B3 > B2> B4 > B8
2. B7 > B6
3. B5 > B6

4. B4 = B5, B4 = B7 (**bolded font)**
5. B5 > B7 (*italicized font*)

Bullet 5 contradicts Bullet 4. Considering the structure of the decision tree and the PSFs associated with Branch 7 and Branch 5, it is logical to reconcile the inconsistency by assuming B4 = B5 >= B7 (A >= B means A is not worse than B).

To summarize, the ranking is determined to be B1 > B3 > B2> B4 = B5 >= B7> B6 > B8
To assign probability to each branch, the ranked branches are assumed to be a geometric series with a constant ratio of $(\frac{0.1}{0.02})^{1/6}$ for the "long time" case and $(\frac{0.2}{0.1})^{1/6}$ for the "short time" case.

Table A-4
Pairwise Comparison Score Summary

	B3	**B4**	**B5**	**B6**	**B7**
B2	4*(-1)	4*1	3*1+0.5	4*1	4*1
B3		4*1	3*1+0.5	4*1	4*1
B4			**4*0.5**	1-1+2*0.5	**4*0.5**
B5				4*1	*4*1*
B6					4*(-1)

The probabilities for each branch are listed in Table A-5 for each case. The constant ratio, to some extent, implies a multiplicative impact of the PSF "Simulator or Talk-Through Training".

Table A-5
Branch Probabilities

Branch	Long time Case	Short time case
1	0.02	0.1
2	0.034	0.13
3	0.026	0.11
4	0.045	0.14
5	0.045	0.14
6	0.076	0.18
7	0.058	0.16
8	0.1	0.2

A.6 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios*, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.

B
DEVELOPMENT OF THE TECHNICAL APPROACH FOR PHASE III MCRA, INCLUDING COMMAND AND CONTROL

B.1 Overview of Phase III (After the Decision to Abandon) Quantification

This appendix documents the basis for the quantification guidance for the HRA of a MCRA analysis. Phase III represents the time period after the decision to abandon the MCR, and includes the collective set of actions needed to isolate the MCR electrically, start up the RSDP or local control stations, and to achieve a safe, stable end state. Specifically, this appendix provides the background on how the technical approach was developed and resulted in the guidance provided in Section 4 of this report.

This appendix section starts with a summary of how the Phase III technical approach was developed, including the tasks conducted and the research developed during the production of the HRA technical approach and guidance. This appendix then describes the resulting technical approach, and indicates those portions that would benefit from additional research.

The guidance developed in this report is based on existing U.S. NPPs, a range of RSDP capabilities, associated MCRA procedures and training, and the manner in which that MCRA procedures are expected to be implemented. In particular, most U.S. NPPs have a MCRA safe shutdown strategy that involves a supervisor at the RSDP who uses the MCRA procedure and coordinates (as needed) the actions of multiple operators who are located at multiple local control panels, using radios (and maybe phones) to individually communicate with each local operator. If the HRA analyst is considering, for example, a new NPP design that uses a substantially different MCRA safe shutdown strategy, including re-constitution of the entire MCR operating crew at essentially a backup MCR, then HRA guidance for MCRA would be substantially different.

B.2 How the Phase III Technical Approach was Developed

During the development of NUREG-1921 Supplement 1 [2], guidance was provided on the identification and definition of HFEs associated with implementing MCRA. Supplement 1 also provided guidance for a qualitative HRA analysis and considerations for feasibility. The development in this report (NUREG-1921 Supplement 2) started with the identification of factors or considerations that may impact the HFE but may not be addressed in current HRA methods. These factors are listed in Table B-1 and include communications and command and control. These factors were then discussed with an expert panel of MCRA SMEs. Feedback obtained during the discussion on command and control helped define those factors that would be addressed qualitatively and those that would be included in the quantification.

B.2.1 Technical Issues Associated with Phase III

The authors addressed the following in the development of an HRA quantification tool for Phase III in MCRA scenarios.

- Command and control, including communications (Appendix B.2.2)
- Integrated Phase III timeline (Appendix B.2.3)
- Cognitive errors during Phase III (Appendix B.2.4)
- Recovery during Phase III (Appendix B.2.5)
- Reasonableness check during Phase III (Appendix B.2.6)
- Quantification of Command and Control Coordination (Appendix B.3)

The technical issues associated with the HRA for Phase III MCRA operator actions come from experience in developing fire PRA and from concern regarding the issues of communications and command and control. The research done to address these issues is described in this appendix. Communications are considered and discussed as part of command and control.

B.2.2 Research Underlying Command and Control for Phase III

NUREG-1921 Supplement 1 [2] presents the initial research conducted to develop the concepts of C&C related to NPP operations. In NUREG-1921 Supplement 1, several factors were identified as being different and important for HRA treatment of MCRA scenarios. Two of those important factors were command and control and communications. In response to these factors, NUREG-1921 Supplement 1 added the following tasks for the HRA**:**

- Identified new feasibility assessment criteria for both communications and command and control (i.e., Section 6 of Supplement 1).
- Provided preliminary guidance on how to incorporate timing associated with communications and command and control into timelines (i.e., Section 7.3.4 of Supplement 1, extract copied below):

  > The timeline of the Phase III portion can be highly complex and requires the analyst to understand the expected procedure response. The timing should include any time for communication among operators in multiple locations as well as account for time delays due to feedback required by or from other operators before subsequent procedure steps can be taken.

- Discussed both communications and command and control in the context of performance shaping factors (i.e., Section 8 of Supplement 1).
- Provided preliminary research on command and control for both MCR and MCRA operations (i.e., Appendix B of Supplement 1).

Following the publication of Supplement 1, the author team continued their research on C&C for MCRA operations. This research ended with a semi-formal elicitation of SMEs on NPP MCRA operations. The elicitation for Phase III was conducted in conjunction with Phase II. The SME team qualifications are described in Section A.2. Discussions with the SME team confirmed that the definition of command and control presented in Appendix B.2.2.1 applies to NPP plant operations, including MCRA. Insights from the SME elicitation are included in the sub-sections

below, specifically the advances beyond that in NUREG-1921 Supplement 1 and that are important for HRA quantification for MCRA scenarios in Phase III.

B.2.2.1 Definition of Command and Control

Since the treatment of C&C is a new topic for HRA, much discussion was conducted on where/how command and control fits into the HRA quantification process. As part of the discussions on Phase III, Table B-3 of Supplement 1 [2] helped identify those aspects of command and control, and communications that potentially impact Phase III quantification. This led to the development of a table of factors to consider in developing a quantification approach for MCRA Phase III (Table B-1). The PSF table along with discussions of scenario best-case and worst-case contexts supported a discussion with SMEs to obtain feedback on those factors and situations that may require explicit treatment during quantification.

NUREG-1921 Supplement 1 determined that C&C has not been previously considered explicitly for NPP operations. Consequently, Supplement 1 reviewed various cognitive models and military definitions, and in Section B.3 defined the C&C functions applicable tor NPPs, specifically:

- Maintaining a coherent understanding of the plant state (e.g., situational awareness)
- Making timely decisions
- Allocating resources as needed
- Coordinating actions
- Managing communications between team members such that they are timely and effective

In turn, the above definition is used in the next section to compare how C&C may change when moving from MCR operations to operations following MCRA.

B.2.2.2 Command and Control Differences Between MCR and MCRA

The guidance developed in this appendix focuses on addressing differences from previous HRA guidance, specifically those differences associated with the challenges and context during MCRA. The reason C&C was identified as potentially important to the reliability of MCRA HRA was because the MCRA strategies involve a collective set of actions, and these actions may be implemented a variety of ways such that they may require more communication and coordination than during operations in the MCR. This section describes the differences between MCR and MCRA.

Having defined C&C for NPP operations, NUREG-1921 Supplement 1 went on to characterize in what ways MCR operations and MCRA operations may be different. In particular, Table B-2 in Section B.2 of Supplement 1 summarizes the differences between MCR and MCRA operations.

One of the challenges in developing a list of differences between MCR and MCRA operations is that there are variations between U.S. NPPs regarding their RSDP capability and associated MCRA safe shutdown strategy.[6] In other words, distinguishing MCR versus MCRA differences is complicated by the fact that there are plant-to-plant differences in MCRA operations. However, input from SMEs allowed the following to be established as consensus:

[6] Section 2 and Appendix A of NUREG-1921 Supplement 1 discuss some of these variations between NPPs.

1. Confirmed the definition of command and control presented in Appendix B.2.2.1 applies to NPP plant operations, including MCRA.
2. Once the decision to abandon the MCR has been made, there are typically no procedure transfers, so there is no further decision-making (as is typically addressed when EOPs are used).
3. Because of how the MCRA safe shutdown strategy is implemented (including the content and format of MCRA procedures), C&C is different for MCRA operations because:
    a. For most U.S. NPPs, there are fewer controls and indications at the RSDP for supervisor to use in developing an understanding of plant conditions or to confirm completion of operator actions.
    b. For most U.S. NPPs, there are no alarms at the RSDP, requiring operators to closely monitor parameters. Such monitoring may be more susceptible to distractions.
    c. Although the supervisor is in charge of the overall MCRA procedures, he/she cannot directly observe implementation of MCRA procedure steps since most operator actions are performed at local plant stations (and not at the RSDP).
    d. The allocation of operator resources is done mostly via the various MCRA procedure attachments (rather than by the supervisor) that are assigned to specific operators.
4. Communications within MCRA operations are different and impact the time required to operator actions to be completed. For example:
    a. Most communications are NOT face-to-face.
    b. There are different types of communications, including reports from operators who have completed MCRA actions as well as communications that are not associated with safe shutdown (e.g. radiation surveys).
    c. Communications equipment (e.g., radios) and associated problems (e.g., garbled communications, crosstalk on the same radio channel) are more of a concern during MCRA.
5. C&C in MCRA operations may involve the coordination of operator actions which may be complicated by operators at different locations and by associated communications issues.

B.2.2.3 Most Important Concerns for Command and Control in MCRA Scenarios

As part of the discussions with the SMEs regarding MCRA operations, this report established that the most important concern regarding C&C in MCRA scenarios is the need for coordination. Coordination consists of several factors and considerations. In particular, coordination of operator actions, as a C&C function can be summarized as follows:

- Coordination is needed more during MCRA operations than for MCR operations involving EOPs.
- Coordination may involve multiple operator teams, but this is not much different than for MCR operations during plant evolutions, maintenance and testing.

- While communications may be needed for successfully starting SSCs needed to achieve safe shutdown, it is failures related to the proper sequencing of steps that are important to the HRA associated with starting SSCs.
- Sequencing of operator actions can be characterized as follows:
    - Implementation of the MCRA safe shutdown strategy can involve a significant amount of sequencing, especially before starting a pump. For example, a pump's suction and discharge valves must be opened before starting a pump.
    - The MCRA procedure itself usually addresses this sequencing (e.g., typically, the procedure will include a written procedure step to "Wait" or "Hold", or to provide a written Caution, if sequencing is important.
    - Errors in sequencing may be due to confusion in using the MCRA procedure, communication problems, or a place-keeping error such as if written "Wait" or "Hold", or Cautions are not provided.
    - The likelihood of detecting errors in sequencing is reduced in MCRA due to fewer indications at the RSDP.
    - Some sequencing errors such as failure to align motive power, are easily detected and corrected.
- Successful coordination depends on communications, controlling potential distractions, and an awareness of plant conditions for success.
- Successful coordination is strongly influenced by training for its success, ranging from:
    - Classroom only (i.e., more passive "receiving training")
    - Practicing coordination in the field (i.e., "active" and more realistic training is "best case")
- While C&C may be a modeling concern for Phase III, the SMEs with plant experience indicated that conduct of plant evolutions and alignments during normal plant operations provide similar communications and control challenges such that C&C during MCRA does not add a new or dominant failure mode.

B.2.2.4 Implications of C&C for HRA Quantification of Phase III Operator Actions

The HRA quantification implications resulting from the updated research on C&C for Phase III operator actions are presented below, and includes communications and coordination. The impact of C&C on timing is discussed in Section B.2.3.

The HRA analyst should understand the important ways that command and control is different for MCRA operations, as opposed to MCR operations, in order to support HRA quantification. Identification of these differences and their implications was not finalized during the completion of Supplement 1, but is important to the modeling of command and control. Most aspects of C&C during the Phase III implementation of critical safety functions are incorporated into the MCRA procedures and timed walkthroughs as specific steps by: (1) local operators reporting to the SS/SM at the RSDP on the status of their tasks and the enabled critical safety functions, such as "Inform CRS of source of power", or (2) the SS/SM/CRS directing actions to be taken by local operators, such as "At the direction of the CRS, energize safeguards bus using an EDG". However, while plants may have similar MCRA procedures and similar remote shutdown capabilities, the timing as well as the command and control aspects may vary since they are based on how the specific plant conducts its operations. Thus, careful review of the procedures

and timing (e.g., implementation plans, JPMs, etc.), operator interviews and simulator exercises are important to understanding the command and control policies and procedures at each plant.

The important aspects of C&C for MCRA operations are summarized under each element of the NPP definition of C&C:

- Maintaining a coherent understanding of the plant state (e.g., situational awareness):

  For MCRA operations, this means to establish and maintain a coherent understanding of the plant state following the establishment of a command post at the RSDP. This aspect of C&C is often addressed via task delegation or verification steps in the MCRA procedures (as discussed above). For MCRA, however, understanding the plant conditions may be hindered by the limited number of controls, indications, and alarms at the RSDP, in contrast to that available in the MCR. For MCRA operations, this element of C&C is important for the coordination of actions (see below[7]).

- Making timely decisions:

  There are two aspects to consider within this element of the definition of C&C: decision-making and timing. First, there are usually no "decisions," as typically considered in HRA for MCR operations, needed following the decision to abandon the MCR. This is because there are seldom procedure transfers or the like in the MCRA procedures for current U.S. NPPs (i.e., there is a single path to success) Secondly, timing for C&C is addressed in HRA through the development of timelines and the evaluation of feasibility by comparing the time required to accomplish an action with the time available. For MCRA it is important that the time required to accomplish the action includes time for communications (internal and external), and time for coordination. For example, if the communications plan uses runners, then the time required to complete the action is likely to be longer than when radios are use. See "coordinating actions" and "managing communications" below for more guidance.

- Allocating resources as needed:

  For MCRA, the allocation of operator resources is done mostly via the various MCRA procedure attachments (rather than by the supervisor) that are assigned to specific operators. In addition, the MCRA safe shutdown strategy is typically validated such that resources are available and are allocated by the MCRA procedure. If there are additional failures such that there are more actions to be accomplished than there are operators, then some of the actions would not be feasible.

- Coordinating actions:

  Coordination consists of two or more operators, and may be required for starting a train or system in order to restore a function, or for long term control of a parameter. Both types of coordination are considered during the conduct of each task. If failure of communications or coordination would fail an SSC, then these are considered to be critical tasks and should be modeled explicitly.

- Managing communications between team members such that they are timely and effective:

[7] For current U.S. NPPs and how their MCRA safe shutdown procedures are written, recovery of a failed operator action is not credited. However, if a task fails and recovery is possible, then situational awareness is important to recognize the context associated with the failure in order to develop the appropriate response.

Because most communications during MCRA operations are not face-to-face, there is less clarity than for MCRA operations. Communications between team members accomplishing critical actions are included in the coordination discussion immediately above. For Phase III operator actions, communications with plant and utility staff, or external agencies, are addressed in the feasibility assessment and are not modeled explicitly. (Note that timing is addressed directly in the quantification of Phase II operator actions, i.e., the decision to abandon on LOC.)

B.2.3 Integrated Phase III Timeline

Section 7 of NUREG-1921 Supplement 1 provided detailed guidance on the development of timing inputs and timelines for MCRA scenarios. As a result of additional research, this guidance is expanded here to include the following guidance for HRA analysts related to communications and coordination. This guidance also includes insights from the discussions with the SMEs as part of the semi-formal expert elicitation.

1. Determine the potential impact, if any, communications or coordination can have on the time required for response.
    a. Communications may be needed for critical tasks modeled in the HRA. Such as for coordination needed for the proper sequencing of actions. The time required for operator actions may be minimally impacted by time delays associated with communication needed to coordinate actions.
    b. Communications may also be conducted as part of non-critical tasks. Extra time may be needed for health physics surveys, if needed for operator action implementation (e.g., operation of valves inside containment for PWRs).
    c. The impact of all communications (critical and non-critical) should be included in the timeline if it impacts the total time required to complete critical actions.
    d. Supplement 1, Section 7 discussed the development of an MCRA timeline where the major functions are plotted on the same timeline to understand the timing of individual HFEs with respect to the same time origin (see Supplement 1, Figure 7-7).
2. The time required for operator actions should also account for the following:
    a. Manipulation time for some SSCs (such as larger valves or valves with a differential pressure) may be longer than might be expected.
    b. Manipulation time may be different in MCRA scenarios than for MCR scenarios (e.g., some MOVs and AOVs almost never are operated without power).
    c. Specific way field operators plan to implement procedure steps (e.g., for a set of 10 actions, does the operator follow the steps explicitly, or a prioritized approach such as changing the order of steps?)
    d. Time required estimates should include some margin for uncertainty (e.g., develop a range of timing estimates, if possible, rather than a point value)
    e. Extra time needed for health physics surveys, if needed for operator action implementation (e.g., operation of valves inside containment for PWRs)
3. Time associated with recovery. In many cases, timed walk-throughs or simulations of time-critical actions such as the MCRA procedure already include steps where another

operator is either checking equipment status, parameter status (e.g., flow through a valve that should have been opened), or the performance of a step as a requirement for their own next step. However, if these steps are not specifically timed, a starting assumption for this additional recovery time should be in the range of 1 to 3 minutes, but assignment of a recovery time should consider what indications of the initial failure are available (and where they are located), followed by the time needed to perform the recovery action(s). (Note that in some cases, even with consideration of additional time required for recovery, there may be a negligible contribution to the overall HEP. Also, it is possible that the operator actions might become infeasible due to the additional time required.)

4. Once the integrated timeline is established for Phase III.

B.2.4 Cognitive Errors during Phase III

Because in MCRA procedures there are fewer options for trains of components that are available for safe shutdown, there typically is not a demand on the operator to "diagnose" what recovery option to implement. Discussions with the SMEs indicate that once the decision to abandon the MCR has been made, there are typically no procedure transfers, so there is no further decision-making (as is typically addressed when EOPs are used).

Thus, the focus of HRA quantification in Phase III is on the execution of operator actions called out in MCRA procedures. However, there may be some NPPs that have some scenarios there may be options for recovery. For such cases, the cognitive modeling would follow NUREG-1921.

The Phase III MCRA HRA focuses on execution using an appropriate tool such as THERP, as described in Appendix B. However, if detection, diagnosis or decision-making is required such as for a recovery HFE (see Section 4.4), then situational awareness is needed and an appropriate cognitive method should be used.

B.2.5 Recovery during Phase III

During MCRA the plant typically has fewer opportunities for response if there are problems with implementing the MCRA procedure. Thus, the addition of recovery HFEs should be considered on an exception basis, primarily when there is a long $T_{available}$. In these cases the recovery must be plausible and feasible. However, command and control protocols such as status checking provide the opportunity for recovery within an HFE.

Within the scope of this supplement, only recovery within an HFE is considered explicitly in the guidance provided in this report since the likelihood of events leading to the need for the third, recovery following failure of the procedural actions to accomplish the safety mission, is considered so low as not to be needed in any foreseeable plant analyses. However, it is recognized that conceptually, it could be considered in analyses, for example, of future NPP designs. In such a case, the analyst would need to model the probability of failure of the SS/CRS to recognize that the procedure is failing to accomplish its purpose and to make appropriate decisions about adopting an alternate strategy. This is consistent with the guidance in Supplement 1, Section 9.2, which acknowledges that recovery actions for the long term such as use of the EDMG and SAMG procedures could be considered. As observed there, "Recovery actions based on FLEX and SAMG procedures has been left to future evaluation and consideration."

B.2.6 Reasonableness Check

The HRA analyst should check for reasonableness, particularly the overall HEP of each HFE and the number of critical tasks. It is a well-known limitation of THERP that HFEs that require many individual tasks can result in excessively high HEPs. Grouping of tasks by functional, perceptual unit is allowed in THERP and is frequently used during MCRA to counter this limitation. Also compare the HEPs for all MCRA HFEs in a scenario to see whether the HEP matches the complexity of the actions modeled.

Finally, the analyst should re-check for feasibility and check that the dependencies between actions are captured appropriately in the model logic. (See Section 5 for more discussion on dependencies.)

Table B-1
Factors Associated with MCRA Phase III HRA

Factors	Considerations Applicable to All Plants and Crews	Worst Case Plant/Crew Characteristics	Best Case Plant/Crew Characteristics	Potential Treatment in Quantification
Communications	Interactions with plant staff conducting MCRA tasks. If the communication is associated with starting a modeled SSC it is considered to be included with Coordination below.	Slowest, limited communications such as a single, shared circuit or a circuit with noise. Multiple simultaneous communications	Training and procedures supplement good hardware	A Communications Plan (and associated hardware) exists and is trained upon; addresses receiving reports from watch standers (ASD staff) as well as external staff. Procedure (plan) and training is sufficient to demonstrate feasibility, such that during quantification communications (by itself) will be treated as negligible compared to other C&C sub-tasks and compared to THERP HEPs associated with critical tasks (so not explicitly quantified).
	Interactions with plant staff other than those conducting MCRA tasks, such as the local fire department			Impact related of communications should be captured in the Time required.
Coordination	Requires communications between 2 or more individuals	Three people - where a supervisor coordinates the activities of two other operators, and can become a bottleneck; or misdirect start-up tasks (sequencing errors).	Peer to peer coordination; with a separate person to track (or check) if completion is not reported or seen in local indications.	Communication and coordination failures that lead to sequencing errors may lead to irreversible SSC failure. Impact coordination should be captured in the Time required.
Situational Awareness	Function of the indication and alarms available at RSDP	Challenging when a component in the success path (SSD path) is failed,	All information available at the RSDP	Subsumed by Communications and Coordination. When communications and coordination is successful, and RSDP

Factors	Considerations Applicable to All Plants and Crews	Worst Case Plant/Crew Characteristics	Best Case Plant/Crew Characteristics	Potential Treatment in Quantification
		requiring recognition and recovery.		indications are successful, then situational awareness is successful. More important if Recovery (options to the SSD train) are needed.
Timely Decision Making	Procedure written to assume worst case, with typically no decisions.	Procedures do not address failures in the safe shutdown train.	Training on the procedures ensures timely response.	Includes failure to establish situational awareness in time. If situational awareness is successful, then timely decision-making is facilitated. More important if Recovery (options to the SSD train) are needed.
Resources allocated	MCRA procedures are well scripted such that resources are allocated and available	Resources diverted or unavailable (then modeled as not feasible)	MCRA procedures are well scripted such that resources are allocated and available	More important if Recovery (options to the SSD train) are needed.
Tools & equipment	Equipment not co-located with	Equipment needed at RSDP is a mixture of items located in the MCR & items at the RSDP with little control over potential "pirating."	All necessary equipment (except keys that are trained to be taken from MCR to RSDP) is located at RSDP & verified to be available on a regular basis (e.g., no "pirating").	Demonstrated during feasibility Impact related of RSDP capability is captured in the Time required
Recovery	Most operating NPPs in the USA consist of 2 trains of safety	Lack of procedures, lack of training on recovery and staffing	Procedures, training (e.g. trust but verify steps taken) and	Consider application of recovery within an HFE.

Factors	Considerations Applicable to All Plants and Crews	Worst Case Plant/Crew Characteristics	Best Case Plant/Crew Characteristics	Potential Treatment in Quantification
	equipment, and the MCRA procedure might be based on a single train (with the other train being fire damaged).	limitations may not address equipment unavailability or failure of SSCs needed to achieve a safe stable end state.	C&C protocols provide opportunity for recovery.	Limit the addition of recovery HFEs to those that are plausible and feasible.
Many critical tasks	Successful isolation of the MCR and start-up of the RSDP, including start of critical safety functions such as decay heat removal; and isolation of spurious operations involve many procedure steps and tasks.	N/A (modeling issue not a plant issue)	N/A (modeling issue not a plant issue)	Task grouping is likely needed because too many steps for THERP. Conduct a reasonableness check to ensure the overall HEP is consistent with the number of critical tasks, and the context associated with the MCRA scenario.

B.3 Basis for HEPs Recommended for Phase III C&C Coordination Failures

This section describes the background on how the authors developed their recommendation for an HEP associated with a C&C sequencing failure in coordination. Section 4.3 provides the quantification guidance for HFEs modeled in Phase III and Section 4.3.3.3 provides the specific recommendation for assigning an HEP of 5E-2 to any contributions to Phase III execution failures from C&C sequencing failures in coordination. This recommendation is consistent with HEPs provided by existing HRA methods.

B.3.1 Focus of HRA Modeling for C&C Coordination Failures

Unlike for Phase II, the authors had not developed a candidate HRA quantification tool before meeting with subject matter experts (SMEs). Instead, the SMEs were presented with a set of candidate issues and were asked to confirm the relevance of these issues for C&C following MCRA. As a result of discussions with SMEs, a consensus on the important concerns for MCRA operations and C&C, specifically, was developed and is documented in Appendix B.2 and summarized in Section 4.2. The SMEs recommended that HRA quantification focus on failures in C&C coordination, especially C&C failures to properly sequence two or more operator actions (e.g., the supervisor directs that operator action B be performed before operator action A, when the normal order is A then B) such that equipment key to the MCRA safe shutdown strategy is irreversibly damaged. Section 4.3.3.3 also describes the process for identifying such C&C failures.

B.3.2 How Can C&C Coordination Result in Sequencing Failures?

Appendix B.2.2 and Sections 4.2.2 and 4.2.3 highlight the key differences between MCR and MCRA operations and why C&C is different when implementing MCRA procedures. Combining some of the key facts from both sections, C&C coordination:

- Is needed more in MCRA operations than for MCR operations involving EOPs and may involve proper sequencing of operator actions
    - Implementation of the MCRA safe shutdown strategy can involve a significant amount of sequencing, especially before starting a pump
- Depends on the MCRA procedure which usually addresses this sequencing (e.g., typically, the procedure will include a Wait (or Hold) step or a written Caution if sequencing is needed)
    - Errors in sequencing may be due to confusion in using the MCRA procedure, communication problems, or a place-keeping error such as if written “Wait” or “Hold”, or Cautions are not provided.
- Depends on communications for success
    - Most communications during MCRA are NOT face-to-face.
    - There are different types of communications, including reports from operators who have completed MCRA actions that are needed for subsequent component startup.
    - Communications equipment (e.g., radios) and associated problems (e.g., garbled communications, crosstalk on the same radio channel) are more of a concern during MCRA.

- Depends on an awareness of plant conditions for success
    - For most U.S. NPPs, there are fewer controls and indications at the RSDP for the supervisor to use in developing an understanding of plant conditions or to confirm completion of operator actions.
    - For most U.S. NPPs, there are no alarms at the RSDP, requiring operators to closely monitor parameters. Such monitoring may be more susceptible to distractions.
    - Although the supervisor is in charge of the overall MCRA procedures, he/she cannot directly observe implementation of MCRA procedure steps since most operator actions are performed at local plant stations (and not at the RSDP).
    - The likelihood of detecting errors in sequencing is reduced in MCRA due to fewer indications at the RSDP
- Is strongly influenced by training for its success during MCRA, ranging from:
    - Classroom only (i.e., more passive "receiving training")
    - Practicing coordination in the field (i.e., "active" and more realistic training is "best case")
- May be easily detected and recovered or may lead to irreversible SSC failure if not recovered.

B.3.3 Causes of Coordination Failures in C&C from Literature

The major causes of coordination failures related to C&C are distractions and interruptions.[8]

An interruption (e.g., something [like a new cue] that stops something from happening) or a distraction (e.g., something that turns your attention away from something you want to concentrate on), in almost all instances, are disruptive to performance and can induce errors. For example, in the 1940s, Fitts and Jones (as described in Reference 5) reported that interruptions were the cause of pilot errors and flying accidents, and made recommendations on reducing these disruptive effects. To this end, the Federal Aviation Administration (FAA) implemented a “sterile cockpit” rule in 1981 requiring pilots to refrain from non-essential activities during critical phases of flight to limit distractions [6]. Similarly, healthcare research has shown the perils of distractions during urgent care settings [7].

With respect to HRA, interruptions or distractions can:

- cause errors
  take time to deal with (e.g., if no cues to guide operator back to interrupted step in procedure (e.g., place markers), this can take 1-2 minutes)
- take time to recover

The authors determined, based on the literature review, that "interruption" (i.e., field operator calls regarding systems or equipment that do not require coordination) is the term that best fits the MCRA context.

[8] Differentiating distraction from interruptions can be difficult. In this report a distraction is an external cue that draws your attention away from what you are supposed to be focused on. An interruption is when someone tells you about an external cue that takes your attention away from what you are supposed to be focused on.

B.3.4 Search for Similar Issues in Existing HRA Methods

Using the insights from above, the authors reviewed existing HRA methods that addressed distractions and interruptions. Overall, there were no methods that exactly matched the contexts and concerns that have been identified for C&C sequencing failures due to coordination in MCRA scenarios. However, there were elements in existing HRA methods that matched some of the MCRA C&C coordination concerns (e.g., interruptions/distractions, communications). The following are the results of this review:

- NUREG-2114 (pages 5-72 through 5-74) [8] considers "workload" as multi-tasking and a "distraction" as "a simultaneous demand for attention from other sources, which could result in the crew looking or stepping away from a procedure and picking back up in the wrong place OR could result in the crew misreading the procedure because of interference.
- NUREG-2199 (i.e. IDHEAS At-Power HRA method), Figure 5-14 [9], shows a decision tree that addresses "workload," including distractions/and interruptions (per the definitions in NUREG-2114)
- The NARA *(*Nuclear Action Reliability Assessment) HRA method (see for example, Reference 10) addresses some of the relevant issues, such as:
    - a generic task type (GTT) for verbal communications of safety-critical data (GTT D1)
    - error producing conditions (EPCs) such as:
        - time pressure (EPC 3)
        - difficulties caused by poor shift hand-over practices and/or team coordination problems or friction between team members (EPC 6)
        - information over-load, particularly, one caused by simultaneous presentation of non-redundant information (EPC 10)
- THERP, Table 20-8 [4] provides estimated HEPs of errors in recalling oral instructions that are not written down, as a function of the number of items communicated and the number of items that need to be recalled

The range of HEPs that are associated with these methods are:

- NUREG-2199 [9] (see Figure B-1):
    - Workload high, complex procedure, with compensating factors (e.g., work practices, place-keeping aids):1.9E-2
    - Workload high, complex procedure, NO compensating factors: 9.4E-2
- NARA [10] (HEPs are to be considered maximums; analyst can make changes by adjusting the “strength” of the EPC’s affect [influence of EPC]):
    - GTT D1: 6E-3
    - GTT D1 plus EPC 10: 3.6E-2
    - GTT D1 plus EPC 6: 6E-2
- THERP [4]:
    - recall one item out of 3 items: 1E-2
    - recall one item out of 5 items: 0.1

From the above, the range of HEPs from the HRA methods above is 1E-2 to 0.1. The authors decided to use an HEP of 5E-2 for C&C sequencing failures in coordination for MCRA operations.

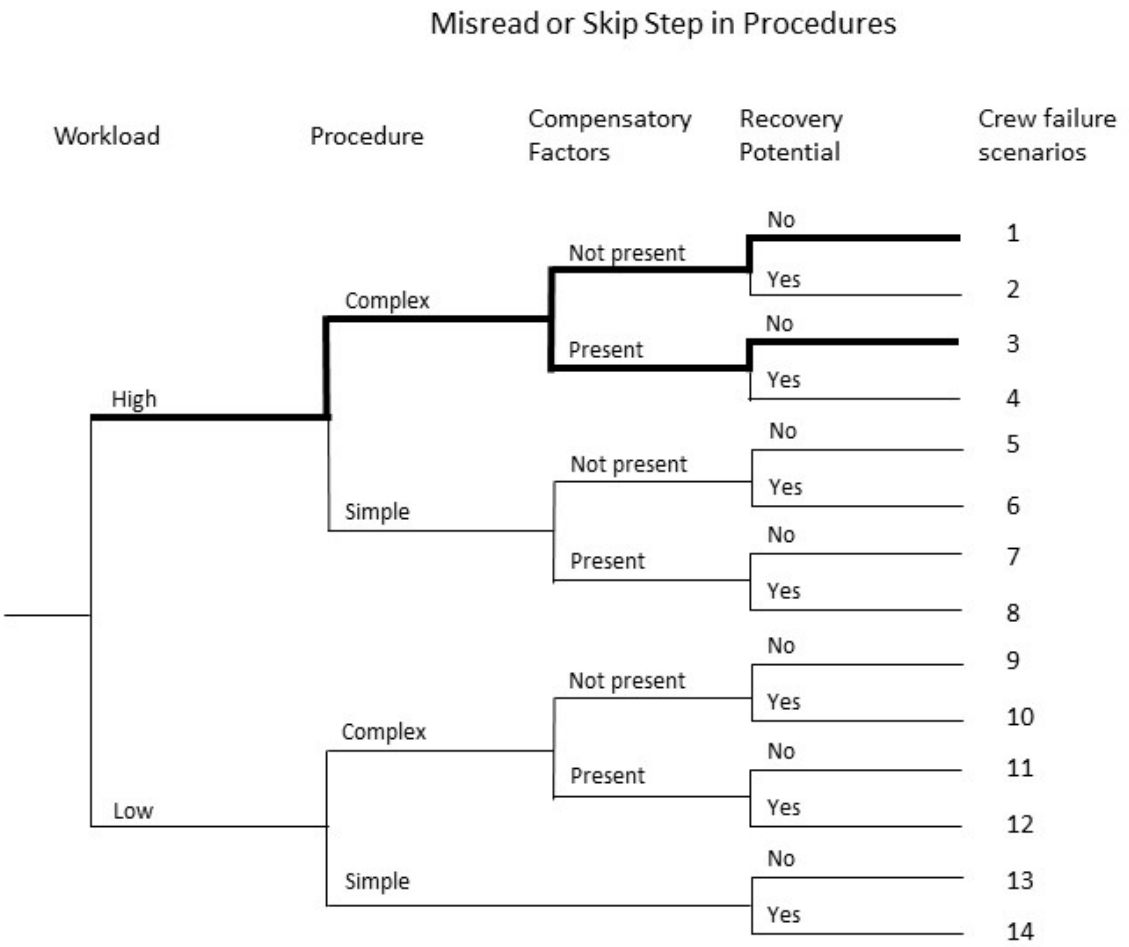


Figure B-1
IDHEAS At-Power Decision Tree for "Misread or Skip Step in Procedure"

B.4 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
2. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1*, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215.
3. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology*, U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
4. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP),* A.D. Swain and H.E. Guttman, U.S. NRC, Washington, DC: 1983. NUREG/CR-1278.

5. *Gillie, Tony; Broadbent, Donald* (April 1989). "What makes interruptions disruptive? A study of length, similarity, and complexity". *Psychological Research*. **50** (4): 243–250.

6. U.S. FAR 121.542/135.100, "Flight Crewmember Duties"

7. *Anthony, K.; Wiencek, C.; Bauer, C.; Daly, B.; Anthony, M.K*. (June 2010) "No interruptions please: impact of a No Interruption Zone on medication safety in intensive care units". *Crit Care Nurse*. **30** (3): 21-9.

8. *Cognitive Basis for Human Reliability Analysis.* U.S. NRC, Washington, DC: January 2016. NUREG-2114.

9. *An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application: Volume 1.* U.S. NRC, Washington, DC: March 2017. NUREG-2199.

10. *B. Kirwan, H. Gibson, R. Kennedy, J. Edmunds, and G. Cooksley, "Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool," Probabilistic Safety Assessment and Management (PSAM) Proceedings, June 14-18, 2004, Berlin, Germany.*