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

NUREG-1921 Supplement 1 **EPRI 300200XXXX**

Draft Report
April 2016

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

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

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

EPRI Project Manager
A. Lindeman

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) 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 ORGANIZATION(S) 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, UNDER CONTRACT TO EPRI, 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

Scientech, a business unit of Curtiss-Wright Flow Control Company

THE TECHNICAL CONTENTS OF THIS DOCUMENT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI NUCLEAR QUALITY ASSURANCE PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B AND 10 CFR PART 21, ANSI N45.2-1977 AND/OR THE INTENT OF ISO-9001 (1994). USE OF THE CONTENTS OF THIS DOCUMENT IN NUCLEAR SAFETY OR NUCLEAR QUALITY APPLICATIONS REQUIRES ADDITIONAL ACTIONS BY USER PURSUANT TO THEIR INTERNAL PROCEDURES.

NOTE

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

CONTENTS

CONTENTS ..... **v**
LIST OF FIGURES ..... **xiii**
LIST OF TABLES ..... **xv**
CITATIONS ..... **xvii**
LIST OF ACRONYMS ..... **xxi**

1 **INTRODUCTION** **1-1**
1.1 Objectives and Scope 1-1
1.2 Intended Audience 1-2
1.3 Fire HRA Background 1-2
1.4 Technical Approach 1-3
1.5 Report Structure 1-4
1.6 References 1-5

2 **OVERVIEW OF MCRA QUALITATIVE HRA/PRA** **2-1**
2.1 Introduction 2-1
2.2 What's Unique about MCRA Context(s)? 2-1
2.3 Implications of MCRA Context(s) for HRA/PRA 2-2
2.4 NUREG-1921: What's the Same and What's Different for MCRA? 2-4
2.4.1 Fire HRA Process 2-5
2.4.2 Relationship with Other Fire PRA Tasks 2-6
2.4.3 General Assumptions 2-7
2.5 References 2-7

3 **MODELING MCR ABANDONMENT IN FIRE PRA** **3-1**
3.1 Introduction 3-1
3.2 Modeling Considerations for Crediting Abandonment 3-3
3.2.1 General Considerations for Detailed Fire Models (NUREG/CR-6850 Task 11) 3-4
3.2.2 Fire Scenario Development for Main Control Room Abandonment PRA (NUREG/CR-6850 Task 11) 3-5

3.2.3 Crediting MCRA for Loss of Habitability Scenarios....3-8
3.2.4 Crediting MCRA for Loss of Control Scenarios....3-9
3.3 Success Criteria Development....3-10
3.4 Incorporating the HFEs into the Model....3-10
3.4.1 Incorporating the Decision to Abandon the MCR....3-10
3.4.2 Incorporating Actions to Transfer Command and Control....3-11
3.4.3 Incorporating Actions After Abandonment....3-12
3.5 Incorporating Equipment Failures into the Model....3-12
3.5.1 Conditions Beyond the Capability of the RSD Equipment and Procedures....3-13
3.5.2 Random and Fire-induced Failure of RSD Panels and/or Local Stations....3-14
3.5.3 Random and Fire-induced Failure of Required Equipment....3-15
3.5.4 Modeling Dedicated Systems....3-16
3.5.5 Accounting for Intentionally Disabled Systems....3-16
3.6 An Example of a Detailed Integrated Logic Model....3-16
3.7 Alternate Approaches....3-21
3.7.1 Single Overall Probability for Alternate Shutdown....3-21
3.7.2 Modeling Alternate Shutdown with Scenario Bins....3-25
3.8 References....3-31

4 **ANALYSIS OF DECISION TO ABANDON....4-1**
4.1 Loss of Habitability....4-1
4.2 Loss of Control....4-1
4.3 Qualitative Analysis of Cognitive Decision to Abandon the MCR....4-2
4.3.1 Use of PRA Insights....4-3
4.3.2 Consideration of Timeline....4-4
4.3.3 Operator Interviews....4-5
4.3.3.1 Interview Questions....4-5
4.3.3.2 Post-interview Assessment....4-6
4.3.4 Key Feasibility Considerations....4-7
4.3.5 Other PSF Considerations....4-8
4.4 References....4-10

5 **IDENTIFICATION AND DEFINITION FOR MCR ABANDONMENT....5-1**
5.1 Introduction....5-1
5.2 Background....5-1

5.3 Understanding of Expected Plant Response for MCRA Scenarios 5-2
5.4 Information Gathering using Talk-Throughs and Walk-Throughs 5-3
5.5 Actions Required for MCRA Safe Shutdown 5-5
5.5.1 Actions Taken Before Command and Control Transfer Outside the Control Room 5-5
5.5.2 Actions Taken After Command and Control Transfer Outside the Control Room 5-6
5.5.3 Actions Taken While Command and Control Remains in the Control Room 5-7
5.5.4 Actions Taken That Use the Main Control Room as Local Station During Abandonment 5-7
5.6 Identification of MCRA Operator Actions 5-7
5.7 Definition of MCRA HFEs 5-9
5.8 Examples of HFE Definitions 5-17
5.9 References 5-21

6 FEASIBILITY ASSESSMENT FOR MCR ABANDONMENT 6-1
6.1 Introduction 6-1
6.2 Feasibility Assessment – Scenario Level versus Human Failure Event 6-2
6.2.1 Scenario Feasibility Assessment 6-2
6.2.2 Human Failure Event (HFE) Feasibility Assessment Criteria 6-4
6.3 MCRA Scenarios – What to do if “feasible” is the only acceptable answer 6-4
6.4 MCRA Feasibility Assessment Criteria 6-6
6.4.1 Human Failure Event (HFE) Feasibility Assessment Criteria 6-6
6.4.1.1 Command and Control 6-6
6.4.1.2 Sufficient Communications 6-7
6.4.2 MCRA Specific Issues in Existing Fire HRA Feasibility 6-8
6.4.2.1 Sufficient Time 6-8
6.4.2.2 Sufficient Staffing 6-8
6.4.2.3 Primary Cues Available / Sufficient 6-9
6.4.2.4 Proceduralized and Trained Actions 6-9
6.4.2.5 Accessible Location 6-10
6.4.2.6 Availability and Accessibility of Equipment and Tools 6-11
6.4.2.7 Operability of Relevant Components and Systems 6-11
6.5 Example Feasibility Assessment 6-11
6.6 References 6-15

7 TIMING AND TIMELINES FOR MCR ABANDONMENT 7-1
7.1 Introduction.....7-1
7.2 MCRA Timeline and Time Phases.....7-2
7.3 Timing Sources Used as Input to MCRA Timeline 7-5
7.3.1 Fire Progression Timeline 7-5
7.3.2 Accident Progression Timeline.....7-6
7.3.3 Phase II Timing Associated with the Decision to Abandon 7-7
7.3.3.1 Phase II Timing Parameters.....7-7
7.3.3.2 Example Approach for Phase II Decision to Abandon Time Estimation.....7-8
7.3.4 Procedure Progression Timeline (Operator Response).....7-10
7.4 Individual HFE Timeline.....7-13
7.5 Integrating All Timing Sources into MCRA Timeline.....7-19
7.6 Examples of MCRA Timeline and Individual HFE Timelines 7-21
7.7 Uncertainty Associated with Timing 7-29
7.8 References.....7-30

8 PERFORMANCE SHAPING FACTORS FOR MCRA SCENARIOS.....8-1
8.1 Introduction.....8-1
8.2 PSFs Relevant to MCRA 8-1
8.2.1 Complexity.....8-2
8.2.2 Crew Dynamics.....8-3
8.2.3 Crew Communications.....8-4
8.2.4 Cues and Indications 8-4
8.2.5 Procedures 8-6
8.2.6 Training.....8-7
8.2.7 Timing.....8-8
8.2.8 Time, Pressure, and Stress.....8-8
8.2.9 Human-Machine Interface.....8-9
8.2.10 Environment.....8-11
8.2.11 Staffing and Availability.....8-11
8.2.12 Special Equipment.....8-11
8.2.13 Special Fitness Needs 8-11
8.3 Special Considerations for Decision to Abandon on Loss of Control.....8-11
8.4 Guidance for Evaluating PSF Impacts 8-12
8.5 References.....8-23

9 RECOVERY, DEPENDENCY, AND UNCERTAINTY 9-1
9.1 Introduction 9-1
9.2 Recovery 9-1
9.3 Dependency Analysis 9-2
9.4 Uncertainty 9-5
9.4.1 Types of Uncertainty 9-6
9.4.2 Relationship of Uncertainty Types to MCRA Qualitative Analysis 9-7
9.4.3 Specific Uncertainty Issues in MCRA Qualitative Analysis 9-11
9.5 References 9-12

10 CONCLUSIONS AND DOCUMENTATION 10-1
10.1 Introduction 10-1
10.2 Properties of a Good Qualitative Analysis 10-1
10.3 MCRA Modeling and HRA Checklists 10-2
10.3.1 MCRA Modeling Checklist 10-2
10.3.2 MCRA HRA Checklist 10-3
10.4 Feedback to Operations 10-4
10.4.1 PRA Perspective 10-4
10.4.2 Plant Modifications 10-5
10.4.3 Procedure and Training Updates 10-7
10.5 MCRA Requirements from the PRA Standard 10-7
10.6 Documentation 10-8
10.7 Areas for Future Development 10-9
10.8 References 10-9

A MAIN CONTROL ROOM ABANDONMENT REGULATORY BACKGROUND AND HISTORICAL EVENTS A-1
A.1 Regulatory Background for Main Control Room Abandonment A-1
A.1.1 10 CFR Part 50, Appendix A and Related Guidance A-1
A.1.2 10 CFR Part 50, Appendix R and Related Guidance A-1
A.2 Historical Events Involving Main Control Room Abandonment A-2
A.2.1 Haddam Neck– Non-Fire Event with MCR Abandonment of Defueled US NPP [6] A-2
A.2.2 Narora Atomic Station – Fire with MCR Abandonment of non-US NPP [7] A-3
A.2.3 Challenging Fire Events That Did Not Result in MCR Abandonment A-3
A.3 References A-5

_B_ COMMAND AND CONTROL B-1
B.1 Introduction B-1
B.2 Human Performance, Macrocognition and Command and Control B-2
B.3 Plant Differences in Command and Control Structures B-5
B.4 Assessment of Command and Control Issues in MCRA B-6
B.4.1 Decision to Abandon the MCR B-7
B.4.1.1 Loss of Habitability Scenarios B-7
B.4.1.2 Loss of Control Scenarios B-7
B.4.2 Post Abandonment Operations B-8
B.4.2.1 Operations at the Remote Shutdown Panel B-8
B.4.2.2 Operations in Other Plant Areas B-9
B.5 Impact on PSFs B-10
B.5.1 Complexity and Stress B-10
B.5.2 Cues and Indications B-11
B.5.2.1 Pre-Abandonment B-11
B.5.2.2 Post-Abandonment B-11
B.5.3 Communications B-11
B.5.3.1 Pre-Abandonment B-11
B.5.3.2 Post-Abandonment B-11
B.5.4 Procedures B-12
B.5.4.1 Pre-Abandonment B-12
B.5.4.2 Post-Abandonment B-12
B.5.5 Training (Both pre- and post-abandonment) B-12
B.5.6 Time Pressure B-12
B.6 References B-19

_C_ GUIDANCE AND TIPS FOR MCR ABANDONMENT-RELATED INFORMATION COLLECTION C-1
C.1 Plant-Specific Information Collection for MCRA HRA / PRA C-1
C.1.1 MCRA Information Inputs C-2
C.2 Site Visit Preparation C-8
C.3 Talk-Throughs and Walk-Throughs C-9
C.3.1 Talk-Throughs C-9
C.3.2 Walk-Throughs C-16
C.4 Managing Resources C-18

C.4.1 MCRA PRA Scenario Binning.....C-18
C.4.2 Use of Previous MCRA HRAs C-19
C.5 References C-20

LIST OF FIGURES

Figure 2-1 NUREG-1921's fire HRA process step and sub-steps....2-5
Figure 3-1 Relationship between NUREG/CR-6850 Task 11 and Applicable MCRA Guidance....3-5
Figure 3-2 NUREG/CR-6850 Task 11 Flow Chart....3-6
Figure 3-3 Example logic for integrating main control room abandonment into the plant PRA model....3-18
Figure 3-4 Example logic for single value approach for main control room abandonment into the plant PRA model....3-24
Figure 3-5 Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 1 of 3)....3-28
Figure 3-6 Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 2 of 3)....3-29
Figure 3-7 Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 3 of 3)....3-30
Figure 7-1 Three time phases of MCRA....7-3
Figure 7-2 Time available for recovery of Phase III actions and time available for decision to abandon....7-8
Figure 7-3 Split between time available for recovery of Phase III actions and time available for decision to abandon....7-9
Figure 7-4 Time required and time available for recovery for the decision to abandon....7-9
Figure 7-5 Decision to abandon is not feasible....7-10
Figure 7-6 Illustration of Individual HFE Timing Concepts from NUREG-1921....7-14
Figure 7-7 MCRA timeline after the decision to abandon has been made....7-25
Figure 7-8 Timing of individual HFEs with respect to the same time origin....7-27
Figure 9-1 Dependency Rules for Post-Initiator HFEs....9-5
Figure B-1 A simplified model of macrocognition (based on Roth, Mosleh, et al. [5])....B-3
Figure B-2 Basic steps in post-event responses for non-abandonment scenarios....B-4
Figure B-3 Basic steps for post-event responses following MCRA....B-5

LIST OF TABLES

Table 2-1 Fire PRA/fire HRA task interfaces addressed in this report 2-6
Table 3-1 Binning for MCRA scenarios 3-26
Table 5-1 Example of HFE Identification for MCR Abandonment Scenarios 5-12
Table 5-2 Example of MCRA scenario functional relevance for identifying individual operator actions for MCRA Scenarios that involve PORV LOCAs when AC power recovery remains available 5-16
Table 6-1 Example MCRA Scenario Feasibility Assessment Summary 6-11
Table 7-1 Example 1: Actions credited and time required 7-15
Table 7-2 Example 2: Actions credited and time required 7-16
Table 7-3 Inputs to estimation of T_{delay} 7-17
Table 7-4 Example 1: Collection of timing information associated with locally starting EDG 7-18
Table 7-5 Example 2: Collection of timing information associated with establishing command and control at RSDP 7-18
Table 7-6 Integration of timing sources into MCRA timeline 7-19
Table 7-7 Example MCRA timeline for loss of habitability (format 1) 7-22
Table 7-8 MCRA timeline example (format 2) 7-23
Table 7-9 MCRA timeline example for LOC scenario (format 1) 7-28
Table 8-1 Potential PSF impacts given specific scenario characteristics 8-14
Table 8-2 PSF effects explained and potential offsetting factors 8-20
Table 9-1 Potential sources of uncertainty for MCRA HRA 9-8
Table 10-1 Example plant modifications for MCRA 10-6
Table 10-2 Example procedure changes for MCRA 10-7
Table B-1 List of situational factors identified in Roth, Mosleh, et al [5] B-13
Table B-2 List of situational factors associated with decision to abandon MCR (LOH) B-15
Table B-3 List of situational factors associated with decision to abandon (LOC) B-15
Table B-4 Hierarchical list of situational factors associated with post-abandonment responses at RSDP B-17
Table B-5 Hierarchical list of situational factors associated with post-abandonment responses at plant locations B-18
Table C-1 Input information used for MCRA C-3
Table C-2 MCRA HRA talk-through structure C-11
Table C-3 HRA interview form (from EPRI HRA Calculator v. 5.1 release notes) C-13

CITATIONS

This report was prepared by:

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

Principal Investigators:
A. Lindeman
M. Presley

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

Principal Investigators:
S. Cooper
K. Hill

Under contract to EPRI:

Jensen Hughes
3610 Commerce Drive, Suite 817
Baltimore, MD 21227

Principal Investigators:
E. Collins
P. Amico

Under contract to NRC-RES:

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

Principal Investigator:
S. Hendrickson

Scientech, a business unit of Curtiss-Wright Flow Control Company
16300 Christensen Road, Suite 300
Tukwila, WA 98188

Principal Investigators:
J. Julius
K. Kohlhepp

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: Qualitative Guidance for Main Control Room Abandonment Scenarios. EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C.: 2016. 300200XXXX/NUREG-1921 Supplement 1.

LIST OF ACRONYMS

AC	Alternating Current
ADV	Atmospheric Dump Valve
AFW	Auxiliary Feedwater
ANS	American Nuclear Society
AOP	Abnormal Operating Procedures
ARP	Annunciator Response Procedures
ASD	Alternate Shutdown
ASME	American Society of Mechanical Engineers
ASP	Auxiliary Shutdown Panel
ATHEANA	A Technique for Human Event ANAlysis
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactor
C&C	Command and Control
CAFTA	Computer Aided Fault Tree Analysis System
CBDTM	Cause-Based Decision Tree Method
CCDP	Conditional Core Damage Probability
CDF	Core Damage Frequency
CFAST	Consolidated Model of Fire and Smoke Transport
CFR	Code of Federal Regulations
CLERP	Conditional Large Early Release Probability
CR	Control Room
CRE	Control Room Envelope
CRHS	Control Room Habitability Systems
CRS	Control Room Supervisor
CS	Core Spray
CSR	Cable Spreading Room
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
DC	Direct Current
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute

ERF	Emergency Response Facility
ERO	Emergency Response Organization
ERV	Electromatic Relief Valve
FAQ	Frequently Asked Question
FLEX	Diverse and Flexible Coping Strategies
FPRA	Fire Probabilistic Risk Assessment
FRANX	Fire Risk Analysis Tool
FSS	Fire Scenario Selection
FW	Feedwater
GDC	General Design Criterion
HCR/ORE	Human Cognitive Reliability/Operator Reliability Experiment
HEP	Human Error Probability
HFE	Human Failure Event
HMI	Human-Machine Interface
HPCI	High Pressure Coolant Injection
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation, and Air Conditioning
IEPRA	Internal Events Probabilistic Risk Assessment
IN	Information Notice
IPEEE	Individual Plant Examination of External Events
ISLOCA	Interfacing System Loss of Coolant Accident
JPM	Job Performance Measure
LAR	Licensee Amendment Request
LCS	Local Control Station
LCO	Limiting Condition for Operation
LERF	Large Early Release Frequency
LOC	Loss of Control
LOCA	Loss of Coolant Accident
LOH	Loss of Habitability
LOOP	Loss of Offsite Power
LPI	Low Pressure Injection
LWGR	Light Water Cooled Graphite Moderated Reactor
MAAP	Modular Accident Analysis Program
MCB	Main Control Board
MCR	Main Control Room
MCRA	Main Control Room Abandonment
MD AFW	Motor-Driven Auxiliary Feedwater
MFW	Main Feedwater
MOV	Motor Operated Valve
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break

MSO	Multiple Spurious Operation
NEI	Nuclear Energy Institute
NFPA	National Fire Protection Association
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSCA	Nuclear Safety Capability Assessment
OMA	Operator Manual Action
PHWR	Pressurized Heavy Water Reactor
PORV	Power Operated Relief Valve
PPE	Personal Protective Equipment
PRA	Probabilistic Risk Assessment
PRM	Plant Response Model
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
PZR	Pressurizer
RAI	Response for Additional Information
RCIC	Reactor Core Isolation Cooling
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RO	Reactor Operator
RPV	Reactor Pressure Vessel
RSD	Remote Shutdown
RSDP	Remote Shutdown Panel
RWST	Refueling Water Storage Tank
SAMG	Severe Accident Management Guidelines
SBO	Station Blackout
SCBA	Self-Contained Breathing Apparatus
SF	Situational Factors
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SORV	Stuck Open Relief Valve
SPDS	Safety Parameter Display System
SR	Supporting Requirements
SRM	Staff Requirements Memoranda
SRO	Senior Reactor Operator
SRV	Safety Relief Valve
SS	Shift Supervisor
SSC	Structures, Systems and Components
SSD	Safe Shutdown

STA	Shift Technical Advisor
TAF	Top of Active Fuel
TCOA	Time-Critical Operator Actions
T-H	Thermal Hydraulics
THERP	Technique for Human Error-Rate Prediction
TMI	Three Mile Island
TSC	Technical Support Center
US	United States

1 INTRODUCTION

This report provides human reliability analysis (HRA) and probabilistic risk assessment (PRA) guidance on treatment of scenarios that require main control room abandonment (MCRA) in response to a fire event, focusing particularly on qualitative analysis. Follow-on work is planned to address HRA quantification for MCRA scenarios.

This guidance is intended for practitioners of both fire human reliability analysis (HRA) and fire probabilistic risk assessment (PRA). Good practice for HRA/PRA always consists of close collaboration between HRA and PRA. As discussed in this report, proper treatment of MCRA scenarios requires an even closer cooperation of HRA and PRA analysts, as HRA must provide input ***before*** MCRA scenarios can be defined and developed for the overall PRA model.

Consequently, this guidance builds upon the fire HRA guidance provided in a previously published joint report, *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines* [1] **and** augments (and sometimes replaces) that given in the overall fire PRA methodology report, *Fire PRA Methodology for Nuclear Power Facilities,* (EPRI 1011989/NUREG/CR-6850) [2].

The fire HRA process steps identified in NUREG-1921 are unchanged for MCRA. Instead, this report expands upon the guidance and discussion given in NUREG-1921 on task interfaces and interactions between HRA and other disciplines in a fire PRA to address additional needs for performing HRA for MCRA. In addition, it focuses on the differences between MCRA scenarios and other fire scenarios and how such differences are treated in HRA/PRA.

1.1 Objectives and Scope

The overall objective of this most recent EPRI/NRC-RES collaboration is to provide additional guidance for both HRA and PRA involving MCRA scenarios. Main control room abandonment due to both loss of habitability (LOH) and loss of control (LOC) are addressed.

It is intended that this report supplement the fire HRA guidance provided in NUREG-1921, thus this report can be considered additional, rather than replacement, guidance (excepting certain specific NUREG-1921 guidance on MCRA quantification). NUREG-1921 remains the guiding document for the scope of fire HRA guidance, in general.

This updated guidance on MCRA scenarios has been developed with both NRC and industry needs for transition to National Fire Protection Association (NFPA) 805 [3] in mind. However, the authors also have tried to address the potential needs of the broader HRA/PRA community, including new fire HRA/PRA analysts.

Recognizing the breadth of such a project, EPRI and NRC-RES approached the development of guidance into two phases. This first Supplement to NUREG-1921 (i.e., this report) addresses qualitative HRA/PRA for MCRA, including:

- MCRA scenario development, including consideration of the decision to abandon
- Human failure event (HFE) definition and identification
- Qualitative HRA specific to MCRA scenarios, including consideration of performance shaping factors (PSFs) and other influences on operator performance

A second phase of guidance development will address HRA quantification for MCRA. Fire HRA tasks of recovery analysis, dependency evaluation, uncertainty analysis, and documentation will be addressed in both developmental phases, as appropriate. Guidance development in this second phase is expected to occur after the first report is issued.

However, as noted in NUREG-1921, fire HRA tasks are not typically performed in series or independently of one another. Consequently, Supplement 1 may include some discussion related to HRA quantification and vice versa.

Also, because MCRA guidance in this report also relates to fire PRA tasks, portions of this report are intended to supplement or replace portions of NUREG/CR-6850. This report addresses:

- Modeling considerations for MCRA
- MCRA-specific success criteria
- Incorporation of HFEs and equipment failures into the plant response model (PRM)

1.2 Intended Audience

This report provides guidance for:

- Fire HRA for MCRA scenarios, for which NUREG-1921 provides incomplete guidance
- Fire PRA tasks related to MCRA that NUREG/CR-6850 either does not address or does not clearly describe

In addition, proper treatment of MCRA scenarios requires a level of collaboration between HRA and PRA analysts that is not typical (and, therefore, may be unfamiliar to HRA/PRA analysts) of at-power, internal events Level 1 PRA or even of non-MCRA fire PRA. Consequently, while all of this report is intended for HRA analysts, portions of this report are more targeted to PRA analysts, with the HRA analyst providing key inputs to the MCRA fire PRA.

In a more general sense, this report is intended to serve the needs of the overall fire PRA team (or multidisciplinary team), as does NUREG-1921.

1.3 Fire HRA Background

Working jointly under a Memorandum of Understanding, the Electric Power Research Institute (EPRI) and the U.S. Nuclear Regulatory Commission's Office of Nuclear Regulatory Research (NRC-RES) published EPRI 1011989 / NUREG/CR-6850, *Fire PRA Methodology for Nuclear Power Facilities* [2]. While NUREG/CR-6850 developed methods, tools and data for performing

at-power fire probabilistic risk analysis, it did not identify or produce a method to develop best-estimate human error probabilities (HEPs) given the PSFs and the fire-related effects.

Following the publication of NUREG/CR-6850, another joint effort produced EPRI 1023001/NUREG-1921, *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines - Final Report* [1] to fulfill the need for explicit human reliability analysis (HRA) on performing both qualitative and detailed quantitative analysis to support best-estimate human error probabilities in fire PRAs. In particular, NUREG-1921 provided tools for performing fire HRA such as:

- Road maps for better understanding the relationship between fire HRA and other fire PRA tasks with respect to both information flow and treatment of fire-induced cable failures or electrical faults
- Search schemes and screening techniques for identifying human failure events (HFEs) to be included in fire PRAs, including operator responses to spurious operations of equipment and indications
- Criteria for assessing the feasibility of operator actions, especially those taken outside of the main control room
- Techniques for obtaining or developing more realistic timing inputs
- Identification of previously little (if at all) discussed factors that can influence ex-control room operator actions (e.g., security and keys for locked doors, communication equipment and its reliability)

As the above list illustrates, many of these tools provided in NUREG-1921 focused on operator actions taken outside of the control room. Explicit treatment of ex-control room actions is an advance in the current state-of-the-art in HRA. Both NRC and industry have taken advantage of this advance, expanding or extrapolating guidance from NUREG-1921 into other areas requiring additional HRA guidance. In particular, NRC-RES has used NUREG-1921 as the basis for its overall HRA approach in its site-wide, multi-hazard Level 3 probabilistic risk assessment (L3PRA) [4], as well as a new HRA approach for Level 2 HRA/PRA [5]. Also, EPRI based its preliminary approach for seismic HRA guidance [6] on NUREG-1921.

While NUREG-1921 represents an advance in HRA practice, NUREG-1921 (see Section 1.2 of Reference 1) does identify a few areas that would benefit from further research, especially treatment of main control room abandonment and associated shutdown strategies.

This report on qualitative MCRA HRA/PRA guidance is intended to partially address this research need. Future development of the quantitative aspects of MCRA HRA will be addressed in a future report. Since the development and publication of guidance for MCRA HRA qualitative and quantitative guidance will not be done in parallel, additional updates and improvements to this report (i.e., Supplement 1) are expected. Other improvements might be identified through separate HRA/PRA research projects (e.g., NRC's project to respond to SRM-M061020 [7] on HRA model differences).

1.4 Technical Approach

Following publication of NUREG-1921, industry proposed a Fire PRA Frequently Asked Question (FAQ) 13-0002 [8] to address a long-standing concern regarding the use of “screening”

human error probabilities (HEPs) for modeling failure to successfully abandon the MCR due to fire in the MCR and transfer functions necessary to maintain safe shutdown capability to ex-MCR location(s). After considerable effort by both industry and the NRC, ending with the recognition by both that more research was needed, the NRC documented some interim guidance in a memorandum to the Nuclear Energy Institute (NEI) [9].

As evident throughout the FAQ discussions and highlighted in this report, there are many variations between nuclear power plants (NPPs) with respect to main control room abandonment (MCRA) and associated shutdown strategies. This report represents a sampling of these variations but cannot achieve completeness. The authors of this report aim to provide appropriate HRA guidance that can be adjusted for plant-specific MCRA strategies. However, some gaps might be identified that warrant the development of more explicit guidance.

As stated above, this report provides expanded **qualitative** analysis for MCRA HRA. This guidance has been developed using the experience of the joint EPRI/NRC-RES fire HRA team, along with other industry and regulatory experience as needed.

A follow-on effort will offer **quantification** guidance for MCRA HRA. Insights and feedback from the development of both qualitative and quantitative guidance will be fed into publication of the final guidance for MCRA HRA.

1.5 Report Structure

This report is structured to address what additional guidance, beyond that in NUREG-1921 and NUREG/CR-6850, is needed for qualitative HRA/PRA involving MCRA scenarios. In some cases, this report structure coincides with that used in NUREG-1921. In other cases, new topics are addressed (e.g., modeling abandonment in PRA) or deferred to the next phase of guidance development (e.g., HRA quantification).

NUREG-1921 defines qualitative analysis as Step 2 in the overall fire HRA process (given in Section 2.2 of NUREG-1921. Most of the guidance for qualitative analysis is given in Section 4 of NUREG-1921. However, since qualitative analysis supports all HRA tasks, NUREG-1921 qualitative analysis guidance was sometimes repeated in discussion of other steps in the fire HRA process.

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

Section 1 (i.e., this section) identifies the objectives and scope of this report and provides background information on the project tasks conducted to develop this supplement to NUREG-1921 on qualitative HRA/PRA for MCRA.

Section 2 provides overview information for HRA analysts needed to adjust their thought process to the MCRA context, including what's unique about MCRA and analysis implications. Section 2 also provides MCRA interactions with other fire PRA tasks.

Section 3 discusses PRA modeling of MCRA, including important interactions and collaborations between HRA and PRA analysts.

Section 4 discusses the decision to abandon for both loss of habitability and loss of control.

Section 5 discusses the first step defined in NUREG-1921's fire HRA process, identification and definition of human failure events (HFEs), specifically for the MCRA context.

Section 6 discusses key changes to HRA feasibility assessment, as needed for MCRA HRA.

Section 7 provides guidance on the development of timing information needed for MCRA HRA, especially timelines.

Section 8 discusses performance shaping factors (PSFs) and the different features of PSF categories already identified in NUREG-1921 that must be addressed in MCRA HRA. The issue of "command-and-control", which is of key importance in MCRA, is introduced as a "meta-PSF" in this section, but is discussed further in Appendix B.

Section 9 discusses recovery analysis, sources of uncertainty, and dependencies for MCRA, paralleling Steps 4, 5 and 6 in the fire HRA process given in Section 2.2 of NUREG-1921.

Section 10 provides concluding remarks including a discussion of properties of a good qualitative analysis, MCRA modeling and HRA checklists, feedback to plant operations (including plant modifications, procedure modifications, and training updates), discussion of PRA standard requirements, documentation and areas for future development.

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

- Appendix A Main Control Room Abandonment Regulatory Background and Historical Events
- Appendix B Command and Control
- Appendix C Guidance and Tips for MCR Abandonment-Related Information Collection

1.6 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 PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

Note: When reference is made in this document to NUREG/CR-6850/EPRI 1011989, it is intended to incorporate the following as well:

Fire Probabilistic Risk Assessment Methods Enhancements: Supplement 1 to NUREG/CR-6850 and EPRI 1011989. EPRI, Palo Alto, CA and the NRC, Washington DC: September 2010. EPRI 1019259.

3. National Fire Protection Association (NFPA) Standard 805, *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants*, 2001 Edition.

4. Kuritzky, N. Siu, K. Coyne, D. Hudson, and M. Stutzke, *L3PRA:* "Updating NRC's Level 3 PRA Insights and Capabilities, "*Proceedings of IAEA Technical Meeting on Level 3 Probabilistic Safety Assessment*, Vienna, Austria, July 2-6, 2012. (Available through the NRC Agencywide Documents Access and Management System (ADAMS) Accession Number: ML12173A092.)

5. Cooper, S. Wreathall, J. Hendrickson, S, "How to Explain Post-Core Damage Operator Actions for Human Reliability Analysis (HRA): Insights from a Level 2 HRA/PRA Application, PSA 2015, Sun Valley Idaho, April 26-30, 2015. Available through ADAMS Accession Number: ML15113A940.

6. *A Preliminary Approach to Human Reliability Analysis for External Events with a Focus on Seismic*, Palo Alto, CA: December 2012. EPRI 1025294.

7. U.S. Nuclear Regulatory Commission, *Staff Requirements – Meeting with Advisory Committee on Reactor Safeguards, SRM M061020*, November 8, 2006.

8. Nuclear Energy Institute, Fire PRA Frequently Asked Question (FAQ) 13-0002, "Modeling of Main Control Room (MCR) Abandonment on Loss of Habitability," August 2013. Available through ADAMS Accession Number: ML13249A249.

9. Memorandum from U.S. Nuclear Regulatory Commission, Joseph G. Giitter, to Nuclear Energy Institute, Michael D. Tschiltz, dated July 23, 2013, with Supplemental Interim Technical Guidance, ADAMS Accession Number ML14156A522.

2
OVERVIEW OF MCRA QUALITATIVE HRA/PRA

2.1 Introduction

This section provides an overview of the qualitative HRA/PRA guidance for MCRA scenarios given in this report. As is the case throughout this report, this section builds upon the foundation in the Qualitative Analysis section of NUREG-1921 [1].

In particular, discussion is provided on why separate guidance is needed for MCRA, particularly what is unique about the MCRA context and the associated implications for HRA/PRA (in Section 2.2 and 2.3, respectively). Following this discussion, a high-level description is provided of what different HRA guidance is needed (as well as what is the same as for other fire scenarios), using the guidance in NUREG-1921 as the basis. The HRA/PRA steps or qualitative analysis tasks that require even more detailed discussion are identified, then addressed in later sections in this report.

It must be noted that, even more so than the fire HRA guidance provided in NUREG-1921, it is challenging to provide generic MCRA HRA/PRA guidance due to the very plant-specific nature of MCRA strategies.

2.2 What's Unique about MCRA Context(s)?

The contexts associated with MCRA are unique for many reasons, including:

- Being prepared to abandon the MCR is a regulatory requirement for not only fire events, but also other events (e.g., toxic gas intrusion) that make the control room uninhabitable. (See Appendix A, Section A.1, for a summary explanation of the regulatory requirements.)
- Events that require MCRA are extremely rare, even compared to other events modeled by HRA/PRA. (See Appendix A, Section A.2, for a summary of the very limited historical experience related to MCRA.)
- Unlike main control rooms (which have been almost standardized following post-Three Mile Island design upgrades), remote shutdown panel design varies greatly from one plant to another. In turn, these design differences can result in operational differences, such as:
    - Some plants have one remote shutdown panel (RSDP). A few plants have two RSDPs, although there can be differences between the two RSDPs so far as electrical independence from the MCR. Also, a few plants do not have a designated RSDP and, instead, perform many operator actions at local plant panels.
    - Remote shutdown panels vary in their capabilities with respect to what systems and associated equipment can be controlled, and what indications are provided. In essentially all cases, the capability is less than that found in the MCR.

        - For those plants with highly capable remote shutdown panels, relatively few local operator actions will be required to control needed equipment and obtain necessary information. However, the number of operators, the number of local actions, and the number of locations needed for safe shutdown will be greater than what would be performed in the MCR.
        - In contrast, those plants that have remote shutdown panels with limited capability are likely to require many field operator actions in multiple locations in order to perform equipment manipulations and monitor and/or check local indications. This case represents an even greater delta as compared to a plant shutdown from the MCR.
    - While many plant operators will need to abandon the MCR because certain equipment or information viewed can no longer be operated from the MCR, at other plants operators may not need to abandon because control of that specific equipment can be individually transferred to the remote shutdown panel.
- Typically, there is no indicator or explicitly defined cue that is used to determine when the MCR must be (or would be) abandoned. (Several sections address this topic, including Section 3 on PRA modeling, Section 4 on the decision to abandon, and Section 8 on performance shaping factors.)
- MCRA scenarios span three different contexts, involving different time frames (see Section 7 on timing) and locations:
    - In the MCR, before, during, and immediately after the decision to abandon
    - At the remote shutdown panel after abandonment
    - At local panels or equipment in the plant after abandonment

2.3 Implications of MCRA Context(s) for HRA/PRA

Although HRA/PRA guidance has recently evolved to include fire events (and some other external hazards, by extension), the guidance needed for MCRA scenarios is substantially different than that already developed. There have been HRA/PRA applications (especially for non-nuclear power PRAs) that have addressed some of the issues provided in this report. However, no formal guidance for those similar contexts has been developed prior to this document.

There are many reasons why MCRA HRA/PRA requires different guidance, and some of these are interconnected. High-level reasons for requiring additional guidance for MCRA include:

- MCRA is a special case of fire PRA that does not build directly from internal events HFEs (even though it may contain similar actions). The decision to abandon often is captured by a unique procedure that is likely to be separate from the fire response procedure set.[1] The potential for involvement of multiple operators performing distinct but correlated tasks outside the MCR makes the abandonment scenario a challenging analysis for both the fire

[1] See Appendix A for a background discussion on the regulatory requirements for MCR abandonment.

PRA and HRA. (More discussion on MCRA procedures and their implications is given below.)

- There are many implications for HRA when the control room crew leaves the MCR, going well beyond a simple location change for operator actions. Some of these implications are:
    - For US nuclear power plants (NPPs), response to the Three Mile Island 2 (TMI-2) event has resulted in standardized requirements for MCR design, emergency operating procedures (EOPs) (in format, content, etc.), and operator training. As a result, HRA analysts can assume (but should verify) that the MCR environment provides a high-level of support to MCR operator actions. However, that same level of support cannot be expected for MCRA scenarios. As a matter of fact, the HRA analyst should expect that every NPP's RSDP is unique in its design, capabilities, and limitations.
    - Almost all HRA methods have been based on assumptions related to the fact that decision-making, and most other operator actions, are taken in the MCR. However, one of these common HRA assumptions that cannot be used for MCRA scenarios, is that the MCR crew can be modeled as if it were a single operator. This assumption is justified for almost all other PRA scenarios (except Level 2 PRA) by the way the MCR operating crew works as a team and is supported by, for example:
        - MCR design
        - Frequent operator training
        - Real-time and face-to-face, 3-way communication
        - In many cases, all crew members working off same procedure and providing backup to other crew members
    - When "command-and-control" resides in the MCR, decision-making (and any operator actions taken) is supported by many alarms, indications, and other instrumentation. In addition, decision making by the Shift Supervisor (or Shift Manager) is supported by additional management or staff, either required to be present (e.g., the Shift Technical Advisor [STA]) or expected due to typical response to a serious plant upset. Such support and extra help (as well as probably multiple phones) also eases the burden of necessary communications, whether it be fire brigade updates, notifications to the NRC, or reports back from field operators or health physics. However, in MCR abandonment scenarios, command and control is likely to lose some of these supports. For example, staffing may change during MCRA due to fire brigade responsibilities (although plants are required to ensure that a basic level of staffing is maintained) and procedure assignments, perhaps even increasing for multi-unit sites where an “all hands on deck” approach to severe events is used. Consequently, command-and-control in MCRA scenarios typically must rely upon a different level and mode of information acquisition, staffing and communications. Appendix B provides background on the topic of “command-and-control.”

- Treatment of MCRA may not rely on the typical assumption that fire initiation, reactor trip, and the "start of the scenario" (from an operations perspective) are simultaneous. Instead, proper HRA treatment of MCRA needs to include explicit consideration of these scenario milestones since it is possible they may occur at different times.
- The definition of an MCRA scenario for LOC (if credit can be given) requires significant input from operators and operations personnel who would be making the abandonment decision rather than solely being based on plant conditions, associated engineering calculations, etc. HRA input is crucial for the proper definition of MCRA scenarios, rather than the typical situation in which the PRA analysts have the lead in scenario definition and development.
- The MCRA shutdown strategy almost certainly will involve a greater number of operator actions, with a correspondingly greater number of action locations and need for a greater number of operators to perform operator actions. In many cases, this means that assessment of the shutdown strategy requires consideration of the feasibility of the coordinated operator response, as well as the feasibility of individual operator actions. The resulting feasibility assessment requires consideration of multiple timelines that represent each operator/operator action, including important coordination points or other intersections.
- With the greater number of local (i.e., "in the field") operator actions, plant-specific differences with respect to shutdown strategy, overall design (including design of the alternate shutdown panel), plant layout, and equipment are even more important than for those fire scenarios involving principally in-control room operator actions.
- NPP operators are familiar with many "rare events" due to their frequent simulator training, but may consider MCRA scenarios even less credible. To-date, no MCRA events have occurred in the U.S, and realistic simulator training of MCRA scenarios (including representative communications with field operators) is very uncommon. Such limitations in operational experience are likely to change what input can be collected in interviews with operations personnel, how such input can be collected, and how to use such information. (Appendix A provides additional background information on MCR abandonment regulatory requirements and near miss events.)

2.4 NUREG-1921: What's the Same and What's Different for MCRA?

This supplement to NUREG-1921 is specially focused on HRA/PRA for MCRA scenarios. Consequently, NUREG-1921 remains the recommended HRA guidance for supporting non-MCRA scenarios in fire PRA. Also, the guidance in this report could be useful for other contexts and scenarios addressed by HRA/PRA.

In general, the reader can assume that, if this report does not address a certain topic or issue, then the guidance in NUREG-1921 still applies. Specific topics or issues that will be explicitly addressed for MCRA scenarios in the remaining sections include:

1. The fire HRA process,
2. Relationship with other fire PRA tasks, and

3. General assumptions.

In addition, Appendix C provides essential support material for qualitative analysis for MCRA scenarios, addresses plant-specific information collection, and discusses managing resources for performing MCRA HRA.

2.4.1 Fire HRA Process

Section 2.2 in NUREG-1921 provides a process for performing fire HRA that is comprised of the seven steps and associated sub-steps shown in Figure 2-1. All of these steps are relevant and applicable to performing HRA for MCRA scenarios.

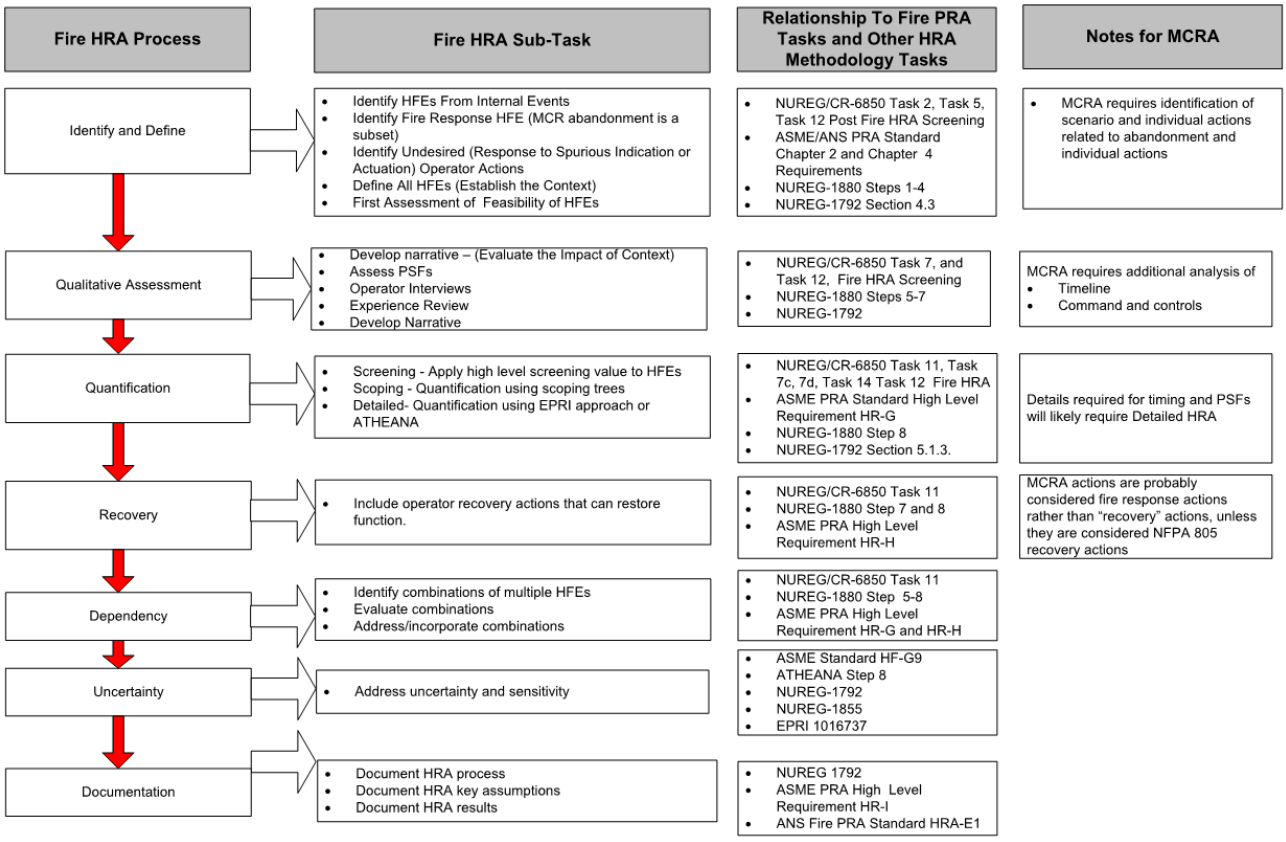

Figure 2-1
NUREG-1921's fire HRA process step and sub-steps

However, treatment of MCRA often requires that the HRA task provide input to the overall fire PRA for the appropriate development of MCRA scenarios. In other words, the HRA analyst may be tasked with performing tasks traditionally assigned to the accident sequence analyst, for example.

For simplicity[2], this supplement to NUREG-1921 treats the HRA process as unchanged, but recognizes that greater HRA input and interaction with the larger fire PRA is required (which also implies some alteration of the fire PRA guidance given in NUREG/CR-6850 [2]).

This report is particularly focused on supplementing NUREG-1921 with MCRA-specific guidance related to Steps 1 and 2 (and associated sub-steps), HFE Identification and Definition and Qualitative Analysis.

2.4.2 Relationship with Other Fire PRA Tasks

Section 2.3 in NUREG-1921 discusses the relationship between fire HRA and other fire PRA tasks. As part of this discussion, Figure 2-2 and Table 2-1 in NUREG-1921 illustrate where fire HRA fits into the overall fire PRA development and how information (e.g., inputs and outputs of various tasks) flows between fire HRA and fire PRA. Table 2-1 below is an abridged version of Table 2-1 in NUREG-1921, showing only the specific aspects of that table that have added guidance in this document. The discussion in NUREG-1921 remains relevant to MCRA HRA/PRA.

Internal events PRA accident sequence development is typically performed by PRA analysts because the information is needed to define success or failure of critical plant functions, systems, and components (with operators representing either alternate failure modes or opportunities for recovery). For fire PRA, and particularly for MCRA, accident sequence development requires input from HRA analysts, particularly the planned operator action times for performing the MCRA procedure. Section 3 provides additional discussion on the importance of the interface between the PRA modeling and HRA for MCRA. In summary, the modifications or refinements needed for appropriate HRA/PRA modeling of MCRA scenarios are summarized in Table 2-1:

Table 2-1
Fire PRA/fire HRA task interfaces addressed in this report

NUREG/CR-6850 [2] Fire PRA Task	Combined ASME/ANS Fire PRA Standard [5] Element (Category II)	MCRA HRA
3. Cable Selection	CS (general)	Ensure that the cables associated with the RSDP and any credited local instrumentation are included.
5. Fire-Induced Risk Model	PRM (general)	Integrate HFEs for MCRA-specific fire scenarios, depending upon binning strategy. Define the needs for thermal-hydraulic calculations to support the development of MCRA-specific timelines. Proper inclusion and integration of MCRA-specific equipment failures into the logic model.
12. Fire HRA	HRA	Substantial new guidance is addressed in this document.

[2] By making this choice, the fire HRA and fire PRA process diagrams remain the same, but guidance for how various tasks are performed is changed to address MCRA. However there are HRA methods (such as ATHEANA, specifically Step 3 that is titled 'describe the base case scenario') that include steps that overlap with PRA scenario development.

2.4.3 General Assumptions

Section 2.4 of NUREG-1921 provides five general assumptions applicable to performing fire HRA. All of these assumptions are also applicable to MCRA HRA/PRA.

One other important assumption used in NUREG-1921, carried over from NUREG/CR-6850 [2] and associated fire PRA modeling is that the start of the PRA scenario (i.e., t=0) occurs simultaneously with the start of the fire. This assumption is a common simplification in PRA (including for other initiating events that do not necessarily result in an immediate reactor trip).

For MCRA HRA/PRA, this assumption may not be applicable in all cases.

2.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
   Note: When reference is made in this document to NUREG/CR-6850/EPRI 1011989, it is intended to incorporate the following as well:

   Fire Probabilistic Risk Assessment Methods Enhancements: Supplement 1 to NUREG/CR-6850 and EPRI 1011989. EPRI, Palo Alto, CA and the U.S. NRC, Washington DC: September 2010. EPRI 1019259.
3. U.S. Nuclear Regulatory Commission. NUREG-1624, Revision 1. *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA),* Rockville, MD, May 2000.
4. U.S. Nuclear Regulatory Commission. NUREG-1880, *ATHEANA User's Guide,* Washington, D.C., June 2007.
5. 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
MODELING MCR ABANDONMENT IN FIRE PRA

3.1 Introduction

This section describes the modeling of MCRA scenarios in a fire PRA. The objective of this section is to provide a better understanding of how to address the aspects of the various MCRA requirements in the fire scenario selection (FSS, which covers the identification, definition, and fire modeling of fire scenarios) and plant response model (PRM, which covers the fire PRA logic model development and quantification) sections of the ASME/ANS Standard [1] that, by their very nature, apply to MCRA. This is accomplished by expanding on the MCRA procedure and guidance presented in NUREG/CR-6850 [2]. The need for this additional guidance results from experience gained through fire PRA peer reviews and requests for additional information (RAIs) from NRC to licensees on their NFPA 805 LARs. This experience has made clear that, although the HRA associated with MCRA is the single most significant issue, there are important PRA modeling issues that affect the results of the analysis that are often missed or modeled improperly. This section provides insights on the current state-of-practice for these PRA modeling issues.

Although the primary focus of the section is on the PRA modeling, there is important discussion about the interface between the PRA modeling and HRA. While this need exists in all aspects of PRA, it is perhaps much more acute for MCRA than other aspects. The need for the HRA analyst to understand the needs and limitations of the PRA models so that the HRA can be performed in such a way as to successfully support the model and quantification is very important. Therefore, the HRA analyst should become familiar with and understand the content of this section. Conversely, the PRM and FSS analysts should not assume that limiting themselves to this section will suffice to understanding all the needs and limitations faced by the HRA analysts. While it is not necessary to understand the details of all of the HRA modeling issues that are addressed in Sections 4 through 10, there are certain aspects that require the attention of the PRA and FSS analyst.

In order to develop the qualitative analysis for any given MCRA scenario, the modeling starts with the fire PRA. The fire PRA provides the inputs to the HRA such as the fire modeling and the subsequent impact on the plant, which is captured as a modeled scenario within the context of the PRA. Specifically, one must first understand how the HRA task for MCR abandonment fits within overall development of the fire PRA development and NUREG/CR-6850 fire PRA process before developing the qualitative and quantitative analyses. It should be noted that these considerations apply to fire areas that lead to MCR abandonment in addition to fires in the MCR. This section also describes how the MCRA HRA fits within the ASME/ANS PRA Standard [1] requirements.

For fires that progress to the point of requiring MCRA, the design basis plant response is to shut down at a Remote Shutdown Panel (RSDP) or Local Control Stations (LCS) outside of the main

control room. The procedure used to accomplish safe shutdown is designed to mitigate most, if not all, of the effects of fire including spurious component operations and to provide sustained decay heat removal. The overall process of abandoning the main control room and re-establishing decay heat removal provides a recovery from the fire and its effects. While fire-damaged components are not repaired, the fire-effects are mitigated.

The modeling guidance considerations that need to be addressed for MCRA are:

1. Define the plant conditions that would constitute a loss of control or loss of habitability for the plant based on the HRA operator interviews and procedure review, and then include appropriate logic in the model to capture when those conditions occur.
2. Based on the fire modeling for main control room fires, determine the scenarios that would result in a loss of habitability and generally only credit abandonment actions for those scenarios (i.e., do not credit actions in the control room that only appear in other procedures).
3. Include random failures of equipment required for remote shutdown (including the controls located at the remote shutdown panel) in the model.
4. Include mitigatable fire-induced failures of equipment required for remote shutdown (including the controls located at the remote shutdown panel) in the model. This requires performing circuit analysis of the remote shutdown panel and control circuits to determine if any abandonment scenarios can cause failure.
5. Include non-mitigatable fire-induced failures of equipment required for remote shutdown in the model. These would include spurious operations that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed, etc.).
6. For scenarios modeled with detailed fire modeling, account for detection and suppression to the extent that it is required to ensure realism in the dominant scenarios.

This section considers three approaches to accomplish this. The primary approach, which is addressed in most of the section, and is the preferred approach, is integration of the MCRA modeling into the plant logic model for the fire PRA. This approach is typically consistent with the other fire PRA scenarios and improves traceability and documentation. The two other approaches, discussed at the end of the section, use scenario bins or a single bounding MCRA failure probability for all recoverable MCRA scenarios.

This section is organized as follows:

- Section 3.2 - Modeling Application of Credit for Abandonment
    - Loss of Habitability (LOH)
        - Fire modeling to determine when LOH occurs
        - Applying LOH frequency by scenario
    - Loss of Control (LOC)
        - Discussion of the interface between logic model development and HRA to determine the conditions that the operators would consider to be LOC.
        - Discussion of how fire modeling interfaces with the logic model development to determine when LOC conditions occur.
        - Implementing the LOC logic into the model to determine when abandonment credit should be applied.

        - Implementing the abandonment actions and equipment into the logic model.
    - Screening for significance of MCRA scenarios
- Section 3.3 - Success Criteria Development for MCRA
- Section 3.4 - Integrating the HFEs into the model
    - Decision to Abandon
        - LOH
        - LOC
    - Actions to transfer command and control to the remote shutdown location(s)
    - After abandonment actions
        - Discussion of interface between the logic model development and HRA to determine HFEs
        - Identification of actions in procedures not required to meet success criteria, including risk-informed insights.
- Section 3.5 - Integrating Equipment Failures into the Model
    - Conditions beyond the capability of the RSD equipment and procedures.
    - Random and fire-induced failure of RSD panels and/or local stations
    - Random and fire-induced failure of required equipment
        - Recoverable (generally only fire-induced may be recoverable)
        - Non-recoverable (random failures or fire-induced permanent damage such as due to spurious operations)
- Section 3.6 - Example of an integrated model
- Section 3.7 - Alternative Approaches
    - Use of a single value for all abandonment scenarios
    - Use of scenario bins

3.2 Modeling Considerations for Crediting Abandonment

The first part of the modeling effort is to identify those scenarios that create conditions that may result in the need for control room abandonment. There are two types of scenarios where such credit may be applied – those that result in the main control room becoming environmentally uninhabitable due to heat or smoke (referred to loss of habitability, or LOH, scenarios) and those that result in a loss of ability to successfully prevent core damage from the main control room (referred to as loss of control, or LOC, scenarios).

Fires that occur in the main control room can lead to both types of scenarios, depending on the location and severity of the fire. Generally, fires that occur on electrical cabinets ancillary to the primary safety systems (e.g., "back panels") will only lead to LOH scenarios since, absent the LOH, the control room will remain functional. Fires on key panels containing circuits interfacing with important front line systems (e.g., main control board panels containing reactor systems or support system circuits) can lead to LOC or to LOH. In some cases, a fire causing LOC could get large enough to also result in LOH. In such case the scenario would be modeled as LOH, with the LOC failures being treated as consequential failures. This is because the LOH

would be the overriding reason for leaving the control room as there is no discretion about leaving, as there is with LOC (this difference is discussed later in this section).

Fires in other plant locations can usually only result in loss of control MCRA scenarios, and is usually only possible in relay rooms, cable spreading rooms, and cable tunnels/chases/corridors. It is unusual for a fire in one of these areas to result in loss of habitability in the MCR, but it should be confirmed that the plant does not have migration pathways for smoke or fire that could result in a LOH for fires that start in other areas. This assessment would be part of the fire modeling activities for MCRA, discussed in Section 3.2.1.

3.2.1 General Considerations for Detailed Fire Models (NUREG/CR-6850 Task 11)

Regardless of the type of MCRA scenario (LOH or LOC), detailed fire modeling plays a key role. Task 11 of NUREG/CR-6850 provides separate procedures for the detailed fire modeling within individual plant areas, for main control room fires, and for the multi-compartment analysis. The goal of Task 11 is to provide detailed PRA modeling of potentially risk significant scenarios including detailed analysis of fires, and those that can result in MCRA whether they occur in the MCR or in other plant areas. Task 11 provides final estimates for the frequency of occurrence of fire scenarios involving a specific fire ignition source failing a target set before fire protection succeeds in protecting the target set. This result is combined in the PRA quantification steps using the conditional core damage probability (CCDP) or conditional large early release probability (CLERP) given failure of the target set, in order to estimate the CDF/LERF contribution for each fire scenario.

In general, detailed PRA modeling requires detailed HRA for associated operator actions. The detailed fire modeling task has been divided into sub-categories in NUREG/CR-6850:

1) General single compartment fire scenarios (Section 11.5.1),
2) MCR fire scenarios (Section 11.5.2),
3) Subsets of 1 and 2 that result in LOC (Section 11.5.3) and
4) Multi-compartment fire scenarios (Section 11.5.4).

Of these, items 2 and 3 are the most relevant to the MCRA issue. As regards item 2 (fires in the MCR) the guidance for LOH (which will be discussed here) provides relatively good guidance that requires only a little clarification. Item 3 (fires that result in LOC) is treated very briefly in NUREG/CR-6850 and has a lack of clear guidance. Past experience has shown that this lack of guidance is the biggest problem leading to misrepresentation of LOC in MCRA analyses in PRA, and so that needed guidance is provided here.

Guidance for detailed HRA modeling for single and multiple compartment fires scenarios is addressed in NUREG-1921 [3]. That guidance is quite clear in the case of scenarios that do not result in MCRA. For those that do result in MCRA, the experience has been that the guidance is not as clear. Part of this is due to the fact that there is a very strong interaction required between the analysts performing the fire scenario selection (FSS) and preparing the MCRA plant response model (PRM), and those performing the MCRA HRA, much more so than might be considered typical and necessary for non-MCRA scenarios, and this is not made clear enough in either NUREG/CR-6850 or NUREG-1921. For fires that do not require abandonment, use of the FSS and PRM guidance in NUREG/CR-6850 and the HRA guidance in NUREG-1921 is applicable

and sufficient. For MCRA it is not, and hence the focus of this report. Figure 3-1 shows where the guidance for the MCRA FSS/PRM and HRA fits within NUREG/CR-6850 Task 11, NUREG-1921 and this report. Of particular note is that Section 11.5.3 of NUREG/CR-6850 provides no clear guidance on MCRA for loss of control from an FSS perspective, and that Task 5 of NUREG/CR-6850 provides no guidance at all for building the plant model for any abandonment scenarios, hence the need for this section.

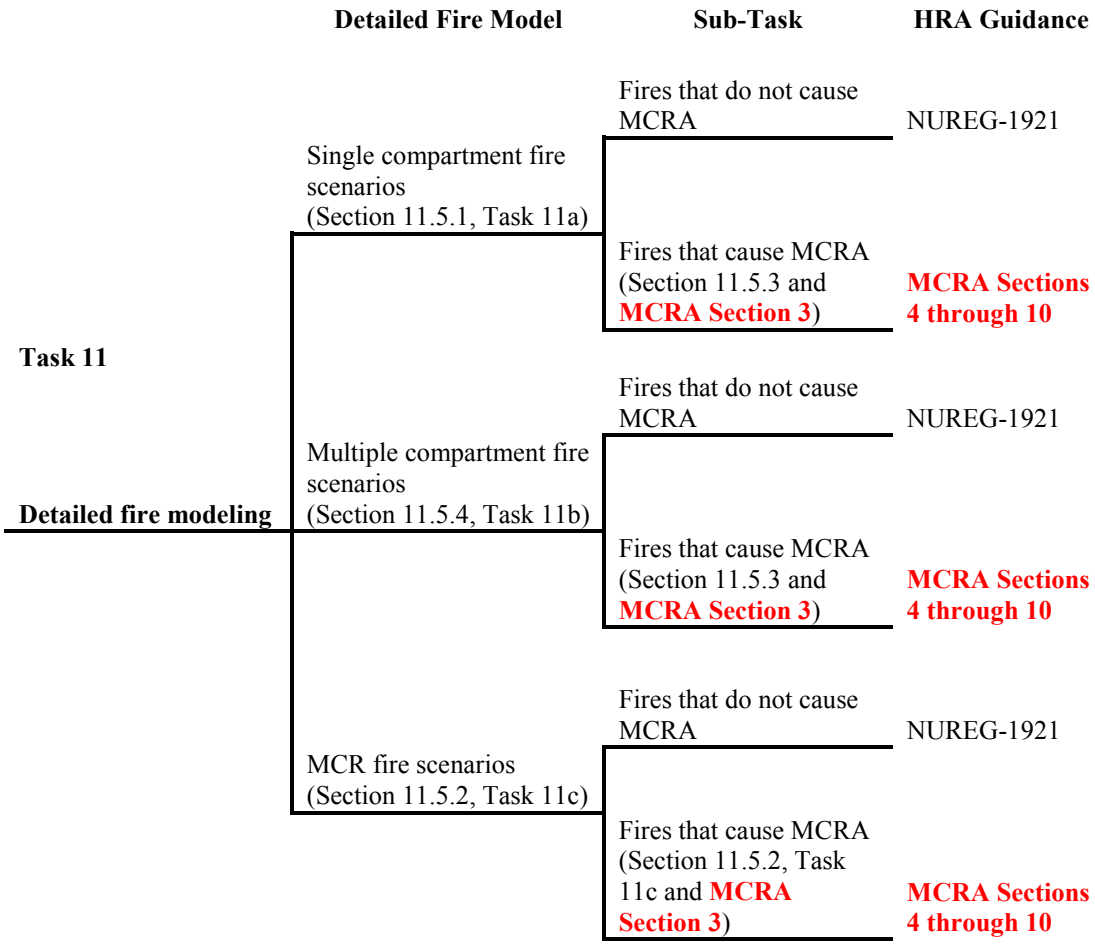

Figure 3-1
Relationship between NUREG/CR-6850 Task 11 and Applicable MCRA Guidance

3.2.2 Fire Scenario Development for Main Control Room Abandonment PRA (NUREG/CR-6850 Task 11)

For fires leading to MCRA conditions, NUREG/CR-6850 follows the same 11 step process used to perform the detailed fire modeling for individual areas. This process is depicted in Figure 3-2.

When following the 11 step process, compartment information is collected in Step 1, then detailed fire modeling occurs in Steps 2-9. The plant response model, specifically the failure probability for using alternate shutdown features is developed in Step 10. Step 11 concludes the process with documentation.

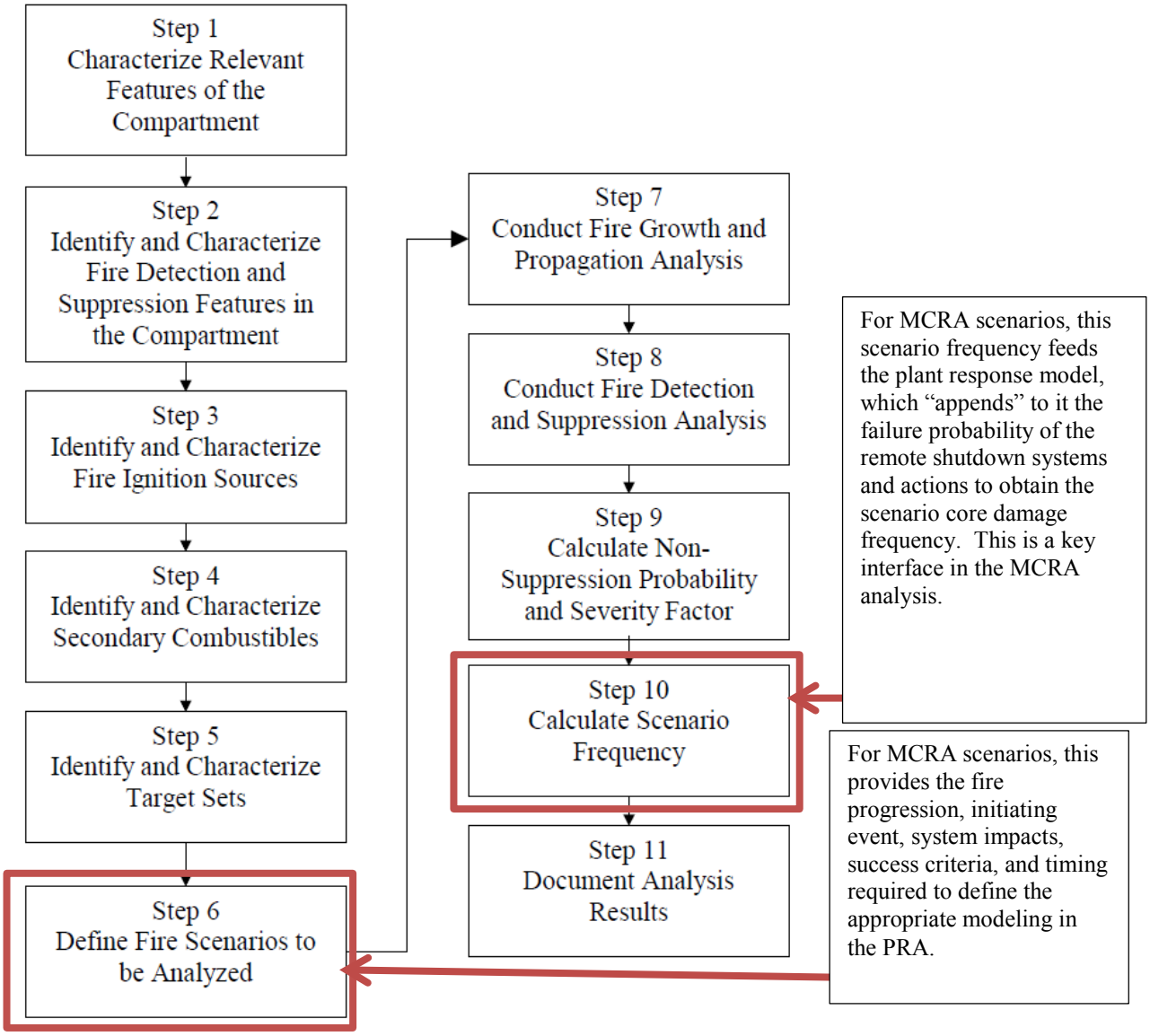

Figure 3-2
NUREG/CR-6850 Task 11 Flow Chart

Step 6 in Figure 3-2 is the point where the distinction is made between an abandonment and non-abandonment scenario. These scenarios all start with the same thing, a fire occurring at a specific ignition source. This distinction only applies to ignition sources that are in the MCR or in one of the designated plant areas where abandonment is an option in the plant procedures for responding to a fire. These fires can follow either the upper or lower branch in the third column of Figure 3-1. All other fires only follow the upper branch. Fire modeling will determine how long it takes for a fire that starts in one of the ignition sources to reach the point where a LOH or LOC condition exists. Fires that are suppressed before that time are non-abandonment scenarios (upper branch) and fires that are not suppressed are abandonment scenarios (lower branch).

As noted in Figure 3-2, Step 10 is the point at which the fire scenario development for MCRA interfaces with the plant response model, and also the MCRA HRA. The step is described in Section 11.5.2.10 of NUREG/CR-6850, and it provides a basic understanding of how MCRA fits within the overall fire PRA. The guidance in this Section is intended to expand on this discussion to aid in the process of implementation. Section 11.5.2.10 states:

> "Estimate Failure Probability of Using Alternate Shutdown Features
>
> *To eventually quantify main control room fire risk, the possibility of safe shutdown using the alternate shutdown means (i.e., safe shutdown from outside the; control room) should be included in the analysis. Two different approaches may be followed.*
>
> 1. *An overall failure probability is estimated representing the failure of the alternate shutdown means.*
> 2. *The alternate shutdown procedure is integrated in the plant response model (i.e., the fault - trees and event trees). The core damage sequences are adjusted to include failures associated with alternate shutdown means, and the human error probabilities are reevaluated based on the alternate shutdown procedures.*
>
> *The first approach (that is, the use of an overall probability value) can be used if the probability value is evaluated conservatively and a proper basis is provided. This approach was used in several IPEEE submittals. For example, in many cases, 0.1 was used as a point value estimate for the probability" from reference [11.3] Perspective Gained from the Individual Plant Examination of External Events (IPEEE), 2002.*
>
> *"For the second approach (i.e., integrating the alternate shutdown procedures in the plant response model), the following steps are suggested. The first step is to review the applicable procedures and associated documentation. This review should identify the preferred equipment for safe shutdown, and the operator actions necessary to actuate and control them. (If the procedure identifies backup equipment, the corresponding shutdown method should also be evaluated.) If a timeline is not provided in the procedure or other associated documents, a general timeline of key operator actions should be developed. The operator actions performed in the control room and automatic system actuations upon which the timeline is based should also be identified. This step, in effect, establishes the "design basis" or capability of alternate shutdown features.*
>
> *The second step is to verify that alternate shutdown capabilities satisfy the potential accident sequences associated with the postulated target set damage. Both the available equipment and the timeline for planned actuation should be evaluated.*
>
> *To evaluate the planned timeline, accident sequence timing modeled in the plant model (i.e., fault trees and event trees) should be compared with the alternate shutdown procedure timeline. The comparison should ensure that the planned operator action times upon which alternate shutdown procedures are based will be less than the operator actuation or recovery times postulated for the applicable fire-induced accident sequences.*
>
> *Consideration should also be given to how the timeline might change under various failure conditions. For example, if the procedure assumes that auxiliary feedwater is*

available and actuated from the control room, the analyst may need to consider the possibility of a stuck-open safety relief valve, thus significantly changing the time available to recover failed auxiliary feedwater system. As another example, a fire in a portion of the main control board may cause a RCP seal LOCA in excess of normal makeup capability. Complicated operator actions are generally necessary to safely shut down the plant under such conditions. This is further complicated if the alternate shutdown procedure has to be implemented.

Clearly, the timelines and especially comparison of the timelines between those in the fault tree and event tree models and the alternate shutdown procedures should be used to establish the human error probabilities. Furthermore, if needed, those times can be used to quantify dynamic human actions or evaluate the feasibility of recovery actions, should random equipment failures occur."

The second approach mentioned above is the preferred approach and is thus the primary focus of this section. The first approach is less desirable, but it may be used in situations where MCRA scenarios are not dominant risk contributors since it is conservative for most scenarios (it is likely to be realistic for the most severe MCRA scenarios, if applied correctly).

3.2.3 Crediting MCRA for Loss of Habitability Scenarios

The determination of which scenarios to credit MCRA for LOH situations is a direct result of fire modeling calculations. There are very clear criteria in NUREG/CR-6850 related to concentration of smoke or room temperature that would result in an inability for the operators to effectively remain in the main control room. The FSS process discussed in Section 3.2.1 is followed to determine how long a fire would need to burn in order to reach those conditions. This is done for each ignition source in the MCR[3]. The scenario frequency is then determined by applying the non-suppression probability associated with that amount of time (i.e., if the fire is suppressed before that time is reached, then the LOH condition is not postulated to occur). In some cases it may be seen that that a given ignition source cannot result in LOH conditions, in which case there is no LOH scenario associated with the ignition source.

The PRA logic model needs to be set up so that the failure of LOH MCRA to mitigate the scenario is applied to the scenarios that are determined by the fire modeling to result in exceeding the LOH criteria, and only to those scenarios. The time of abandonment (as previously calculated by the FSS process) for each scenario is a key input to the HRA. This time is scenario-specific based on the specific characteristics of the ignition source, available combustibles, and location within the MCR. This time will impact the HRA because it changes the amount of time operations can be performed in the MCR as well as the remaining time to affect a successful remote shutdown after the control room is abandoned. How this information is used in the development to the HRA timeline is discussed in Section 7.

[3] In rare cases, it may be possible for a fire that is not in the MCR to result in a loss of habitability in the MCR. Following the detailed fire modeling for those fires can also be used to determine the time until those conditions are reached.

3.2.4 Crediting MCRA for Loss of Control Scenarios

The plant model logic needs to determine for which scenarios the loss of control situation has occurred, and to then allow consideration of the actions and equipment required to successfully accomplish a remote shutdown only under these conditions. This is a typical modeling requirement in PRA. For example, for a PWR that has a once-through cooling (i.e., bleed-and-feed) procedure, the model is structured such that this cooling procedure is only credited when there is a non-recovered total loss of secondary cooling resulting in certain parameters being exceeded. The fire-induced loss of control scenario needs to follow a similar approach, but the situations are less clear since loss of control is not a consistently defined scenario from plant-to-plant in the way that loss of secondary cooling is. These considerations are discussed in detail in other sections of this report. What is important from the modeling perspective is that the conditions that are considered to be a loss of control for the specific plant need to be determined, and model logic implemented that only credits MCRA for LOC when the cues associated with those conditions are present. Because standard fire PRA modeling assumes that all fire-induced failures for any given scenario occur concurrently, and that this also includes the fire-induced plant trip, the time of abandonment does not change by scenario – it is the time it takes the operators to confirm the loss of control and make the decision to abandon. This will come from the HRA, not from the fire modeling.

These cues do not come directly from the abandonment procedure in the same way as they come from other AOPs and EOPs. The abandonment procedure does not generally provide unambiguous cues for abandonment – the "when parameter x reaches value y and alarm z occurs" that we are used to for most accident conditions. Some guidance along these lines may appear in the procedure, but in the end there is always a certain amount of discretion allowed to the final decision maker (e.g., shift manager) to declare when "it is no longer possible to successfully reach a safe-and-stable condition from the MCR". For this reason, the determination of the cues for LOC requires significant interaction between the plant logic modelers, fire modelers and HRA analysts, since (as noted above) the MCRA procedures generally do not contain the same specificity of cue-response as other AOPs and EOPs. It will be necessary for the logic modeling and fire modeling analysts to provide insights into the expected fire-induced failures that will dominate the LOC scenarios. LOC scenarios are those that will lead directly to core damage if the operators remain in the MCR (i.e., in the absence of abandonment actions). For each LOC scenario (or group of scenarios that share the same characteristics) that will lead to core damage in the absence of abandonment actions, the HRA analysts will need to conduct operator interviews to determine if the abandonment procedures and equipment cover these situations and also whether the operators would interpret the conditions as a loss of control. The HRA team would then define the specific cues/conditions that the operators would interpret as loss of control, and the PRM analysts would implement logic in the model that would allow MCRA credit when (and only when) those cues/conditions exist. The details of the interview process and how it is used to determine the cues that are required to open up the abandonment option to the operators are contained in Section 4.

3.3 Success Criteria Development

There are two aspects to the success criteria. The first is determining if there is a relationship between the internal event PRA (IEPRA) initiating event success criteria and the characteristics of the MCRA scenarios. In general, the following three guidelines apply.

1) If the characteristics of the MCRA fire scenario maps to an IEPRA initiating event, use the success criteria from the IEPRA.

2) If the characteristics of the MCRA fire scenario maps to multiple IEPRA initiating events, either use the limiting success criteria from the IEPRA or split the fire into multiple scenarios and apply the appropriate criteria to each.

3) If the characteristics of the MCRA fire scenario do not map to the IEPRA, for example spurious operation leads to an initiating event not explicitly modeled, then either develop success criteria for that particular scenario or choose bounding success criteria from the IEPRA.

This needs to be done such that each scenario is appropriately addressed, so it may be that all three of these options will be used, depending on the set of MCRA fires in the FPRA.
The second aspect is that even MCRA scenarios that map to success criteria from the IEPRA may need special consideration when it comes to the success criteria for achieving successful remote shutdown because the impacts of the fire may be unique and also because of the limited equipment available. This may result in situations where the success criteria used for the IEPRA (or even specifically for the fire PRA) may be too conservative with regard to timing. In many cases the success criteria timing for a scenario may, for the sake of simplicity, be taken for a bounding case. For example, time to recover feedwater may have been based on plant trip at low water level and used for all cases of loss of feedwater because the additional time available given trip at nominal water level has no significant impact on the HEP for recovering feedwater in the MCR. However, MCRA actions take longer than control room actions and having additional time could have a significant impact, even in some cases making the difference between the action being feasible versus unfeasible. Therefore, it is important when evaluating the use of previously calculated success criteria for MCRA scenarios to determine whether they are overly conservative with respect to the specifics of the MCRA scenarios being evaluated. This information is fed into the development of the overall timeline, which is addressed in detail in Section 7.

3.4 Incorporating the HFEs into the Model

A key aspect of developing the model is to incorporate the HFEs into the model logic. This, of course, requires defining the appropriate HFEs to include, which requires significant interaction between the PRA and HRA analysts. There are two different types of HFEs that need to be addressed – the decision to abandon the MCR and the performance of the necessary actions to avoid core damage under an abandonment scenario.

3.4.1 Incorporating the Decision to Abandon the MCR

Section 3.2 discussed the modeling associated with assuring that the model correctly identifies the scenarios for which abandonment credit should be applied. Once the operators have

determined that an abandonment option applies, the model needs to account for whether the decision to abandon is made in time for the actions required to avoid core damage to be successful. The cases of loss of habitability and loss of control are fundamentally different, and so will be discussed separately.

Abandonment for Loss of Habitability. The PRA model does not need to incorporate a HFE basic event for the failure to abandon the MCR in the case of loss of habitability. As discussed in Section 3.2.3, the occurrence of the conditions associated with a loss of control room habitability are specified in NUREG/CR-6850 and their onset for any given fire scenario is a direct result of a fire modeling calculation. This criterion is one most frequently encountered, where a fire in a panel, cable bundle, or transient source burns sufficiently to generate smoke and heat that would necessitate evacuation. For MCRA on loss of habitability, it is not necessary to consider the possibility that the main control room will not be abandoned. The conditions established in Step 11c of NUREG/CR-6850 will result in scenarios where it is physically very difficult for the operators to remain in the MCR without risking serious physical harm. In general, plant procedures and training provide specific cues to indicate an abandonment condition. The fire PRA and MCRA HRA assume that it is not credible that the operators will remain in the MCR under these conditions. Therefore, the probability of abandonment due to loss of habitability is not based on the HRA, but rather developed by establishing and justifying the fire conditions that would force abandonment (e.g., smoke, heat) and using probabilistic fire modeling techniques to assess the conditional probability that MCR fire scenarios would lead to abandonment due to loss of habitability. This is the probability that the fire grows to the point of requiring evacuation, and is performed with a zone model or computational fluid dynamics calculation. Therefore, the model need not include an HFE for failure to abandon in time on a loss of habitability.

Abandonment for Loss of Control. Abandoning for a loss of control situation is, like most other decisions, a matter of the operators interpreting the available cues correctly and making the correct decision to transition to the plant emergency procedure for abandonment. The modeling for this was discussed in Section 3.2.4, which would allow credit for the MCRA on loss of control only when the appropriate cues exist. The model would then require that an HFE for the failure of decision to abandon be included in the model and that the failure of this decision would result in the failure of all actions associated with the abandonment procedure. The development of that HFE would be performed by the HRA analyst (see Sections 4 and 5).

3.4.2 Incorporating Actions to Transfer Command and Control

Regardless of the type of abandonment (LOH or LOC) or the extent of fire-induced damage, there is always a base set of actions that are required in order to transfer command and control to the remote shutdown location(s). Some will be in the control room before it is physically evacuated and some will be at the local location(s). In some cases, there will be actions taken while going to the local location(s). These actions typically include isolating MCR control circuits, de-energizing control circuits to prevent spurious operations, energizing the remote panels, and similar actions. From the perspective of the logic modeling, all of these actions are assumed to be required in order for the abandonment scenario to be mitigated. Therefore, the model simply needs to include a single HFE to represent these actions, applied to both LOH and LOC scenarios. The HEP for this will be provided by the HRA analyst.

3.4.3 Incorporating Actions After Abandonment

There are a number of execution actions that are required for implementing the MCRA procedures. In order for them to be fully integrated into the model, they should be organized in terms of recovery of each required system/function. This is similar to the way non-MCRA actions are generally organized in a PRA. The reason for this is so the MCRA actions can be treated appropriately as "back-up" actions for the systems/functions under consideration. The MCRA scenarios do not always fail all of the systems that the MCRA procedures include as part of the shutdown process. In those scenarios, the systems that operate properly despite the fire can be credited as functional without success of the MCRA actions associated with those systems. Therefore, the MCRA execution actions associated with each system/function should be incorporated into the model in an AND relationship with the failure of the system/function to operate automatically.

Defining the execution HFEs requires significant interaction between the PRM and HRA analysts in order to address both the needs of the model and the structure of the procedures. This is relatively straightforward for those aspects of the procedures that are written functionally. For example, if the procedure has an attachment where the sole purpose of the attachment is to establish power to one or both emergency AC busses, all the execution actions in that attachment would be associated with that recovery and would fit into the associated HFE.

The situation gets more complex where an attachment is structured around location (performing all the actions in the same area of the plant, which may involve multiple systems/functions). For example, there may be two attachments, one each for a plant operator, where they work in tandem to first restore AC power and then start the charging system. It would be natural from an HRA perspective to put the entire set of actions in a single HFE, where occurrence of that HFE would fail MCRA. However, this would not serve the purposes of the plant model, because in some MCRA scenarios AC power will not fail, but charging will. For those scenarios, the performance of the actions associated with the AC power recovery would not be required, and their failure would not impact MCRA success. Combining them into an HFE with failures associated with recovery of charging would incorrectly represent the response to the scenario in the model.

There is also a set of actions associated with the transfer of control from the MCR to the remote shutdown panel(s) or station(s). These are commonly referred to as the "enabling" actions: they isolate the control circuits in the MCR and activate (or permit) the local control circuits to allow operation of the required equipment locally at the panels/stations. These common actions can be assumed to all be required in order for the MCRA to be successful, and so should be incorporated into the model as failing all system/function recoveries. For that reason, they can be incorporated into a single HFE in the model. For the LOC case, they could be considered as the execution part of the cognitive failure to abandon, but would need to be a separate HFE for the LOH case since there is no cognitive failure to abandon.

3.5 Incorporating Equipment Failures into the Model

In evaluating the failure probability for remote shutdown following MCRA, some have assumed that the human failure events will dominate the failure and that the human error probability is an

adequate surrogate for the overall failure. This has been observed for some plant models, but other plants that have performed more detailed assessments have shown that this is not always (or even not often) the case for various scenarios. For example, if offsite power is failed and the alternate shutdown relies on the emergency diesel generator (EDG) and the analysts uses a 24 hour mission time, then the EDG fail to run can be comparable to the HEP for MCR abandonment.

This section addresses the incorporation of equipment failures into the model to correctly capture their impact on the MCRA failure probability.

- Conditions beyond the capability of the RSD equipment and procedures cannot be modeled other than to reflect these conditions lead to core damage.
- Random and fire-induced failure of RSD panels and/or local stations
- Random and fire-induced failure of required equipment
  - Mitigatable (generally only fire-induced may be mitigatable, such as a fire-induced failure of control circuit could be mitigated by using an alternate control circuit or manually operating the affected component)
  - Non-mitigatable (random equipment failures and fire-induced permanent damage, such as might be cause by MSOs)
- Dedicated systems used only under MCRA situations
- Systems intentionally disabled under MCRA situations

3.5.1 Conditions Beyond the Capability of the RSD Equipment and Procedures

The remote shutdown capability of the plant is usually designed to allow a shutdown under specific initial conditions that are defined using deterministic rules, for example using the single failure criterion, assuming the absence (or mitigation) of spurious operations, assuming turbine trip/MSIV closure, or other such conditions. In PRA, there may be scenarios with significant frequency of occurrence where the initial conditions assumed in the design of the remote shutdown capability are exceeded. That is, there will be scenarios where failures occur such that, even if every action and piece of equipment called for in the MCRA procedure is successful, there will still be core damage. It is essential that an assessment be performed to identify scenarios where such conditions would exist and that the model assure that MCRA credit is not applied in those cases. Most remote shutdown capabilities are designed to achieve successful shutdown only under general transient conditions and may not have considered the impact of multiple spurious operations. In such situations, no credit for remote shutdown should be applied for conditions such as ATWS, LOCA, interfacing systems LOCA, or main steamline break conditions (e.g., unisolated stuck open atmospheric relief valves for PWRs). However, this is not always the case, so the assessment must be conducted on a plant-specific basis, so it is not possible to provide a comprehensive list of situations to consider, but the following list should always be considered when performing the remote shutdown capability assessment:

- ***Loss of coolant accidents***. Fire-induced or random LOCAs (spurious PORV opening or failure to re-close, RCP seal LOCAs, spurious opening of RCS interface valves, etc.) are often situations that cannot be mitigated in an MCRA situation. The RSDP or procedures may not provide for RCS make-up. Even if they do, they may not provide for recirculation or for containment cooling.

- ***ATWS.*** Some plants have identified fire-induced failures that can prevent RCS trip long enough that the limited functionality provided under MCRA conditions will not mitigate it.
- ***MSLB***. Spurious valve opening or failure to close MSIVs on the non-credited train will have minimal effect on safe shutdown. The non-credited steam generator will blow dry and then the credited SG will be used for cooldown. Spurious opening of MSIV or atmospheric steam dump valve on the credited SG must often be isolated locally in order to provide an intact SG for decay heat removal. In the case where no MSIVs close, all SGs will blow down through the common steam supply to the turbine, which typically is an unanalyzed condition that cannot be mitigated using remote shutdown procedures.
- ***Interfacing Systems LOCA.*** Spurious valve operations may result in ISLOCA. Most plant MCRA procedures and equipment will be unable to mitigate them.

The equipment failures that can lead to these conditions should be incorporated in the model as a direct failure of successful shutdown when MCRA would otherwise be credited. Since some of these failures can result from fire-induced failures, circuit analysis must be conducted and the circuits mapped to the MCRA scenarios where credit is intended to be taken.

3.5.2 Random and Fire-induced Failure of RSD Panels and/or Local Stations

Implementation of MCRA requires the isolation of the primary control circuits that go to the main control room and enabling controls at the RSDP or local control stations, or some combination of the two. One of the pitfalls in modeling MCRA in the PRA is to take this process for granted. There are two aspects that need to be considered.

The first is the potential for fire damage to defeat either the MCR isolation or the enabling of the RSDP/local station functions. It could seem that, since the purpose of the entire MCRA design capability is to allow a controlled shutdown of the plant when the control room must be abandoned, one could assume that if a fire occurred in an area where MCRA is intended to be utilized then obviously these functions would be free from fire damage. However, it has been found in some plants that this is not always the case – that the design is not always free from fire damage for scenarios where it is needed. Therefore, a complete circuit analysis of the local functions at the RSDP/local stations is needed, including adverse impacts to the MCR isolation function, and the cables that could cause these functions to fail mapped to the MCRA scenarios where credit is intended to be taken.

In addition to addressing the fire-induced failures, the second area that needs to be considered is that these circuits could fail randomly. The primary issue here is the failure of the switches themselves (that is, the isolation, enabling, and activation switches). While individual switches are generally reliable, the sum of the failure probability of all the required switches could be a meaningful contributor, especially for those plants where only a single train is used in the MCRA design (so all the switches must work) and for the scenarios where there is not much fire damage (which tend to have the highest frequency). Therefore, in addition to mapping the cables to the basic events for failures of the RSDP/local stations, a random failure probability should also be assigned. Some have made an argument that the switches are a small fraction of the equipment

failures and do not need to be counted, but these models have been challenged during reviews. Depending on the number of switches required for operation, these may or may not be important.

Because these circuits are fundamental to MCRA, their failure is considered fatal to the success of the MCRA shutdown as the procedures will not provide for "work-arounds" to recover from these failures in time.

3.5.3 Random and Fire-induced Failure of Required Equipment

The final piece of the equipment puzzle for MCRA is the front line and support system components that need to operate in order to reach a safe-and-stable state. Even if the scenario is one within the capabilities of the MCRA equipment and procedures, the operators perform all the correct actions, and all of the control circuits are free from fire damage and operate successfully, it is still possible that the equipment will fail. For example, if the turbine-driven AFW pump is needed to provide flow to the steam generators, and if it has suffered a random mechanical failure of the shaft, it does not miraculously start because the RSDP control circuit tells it to. On the other hand, if it only failed because of fire damage to the control circuit from the MCR, and that is now isolated and the RSDP control circuit is enabled, it may now start if commanded to. So, there are two types of failures that need to be considered – mitigatable and non-mitigatable.

Non-mitigatable failures can either be fire-induced or random. Random failures, as with internal events PRAs, are always considered non-mitigatable. These failures would appear both in the non-MCRA part of the model and in the MCRA part of the model (that is, they fail the component whether or not an MCRA has occurred). In integrating them into the model, it is important that the same basic event name be used in both parts of the model in order for the Boolean reduction to work properly. Fire-induced failures become non-mitigatable only when the affected component is directly damaged by the effects of the fire. In general this does not mean the case where the fire is in the same area as the component. MCRA usually applies to fires in the control complex (e.g., MCR, cable spreading room, relay room) where there is a potential for a fire to do substantial damage to the circuits required to supply both control and indication to the MCR or render the MCR uninhabitable. These areas do not contain the front line and support systems components used in the MCRA process. The fire-induced non-mitigatable failures of concern are those that result from control system faults that cause a needed component to damage itself. Examples include:

- Causing a diesel to start and overload while disabling the protective trips.
- Causing components to run without cooling.
- Causing valves to over torque so they cannot be operated.

These failures are typically modeled as part of the multiple spurious operation (MSO) evaluation process. Where such MSOs could cause failure of a component credited in the MCRA, the same MSO logic should appear in both the non-MCRA and MCRA parts of the model.

Mitigatable failures of the required equipment are a subset of the fire-induced failures.

3.5.4 Modeling Dedicated Systems

Some plants have dedicated shutdown equipment – those items that can only be controlled at either the RSDP or a local control station (equipment that is solely installed for either station blackout or fires) that should not have any portion of the required equipment/circuits impacted by the fire in the MCR or other fire area when it is credited. These systems will not have been modeled in the PRA prior to the consideration of MCRA, and so would need to be added to the model. Even though they should, by definition, be free from fire damage (unaffected by any fire in a remote shutdown area), this should be confirmed by cable selection and circuit analysis. The model would need to include all other equipment failures specified above as well as relevant HFEs that could lead to failure of the systems.

3.5.5 Accounting for Intentionally Disabled Systems

The fire model will account for systems that are disabled by the fire, but there is the additional issue of systems that may be disabled as part of the abandonment process, and so even if not damaged by the fire they should not be credited as potential mitigating systems when abandonment has occurred. This is generally associated with actions that disable systems in order to prevent spurious operations, but there is no provision in the procedures to utilize the system after abandonment. The model needs to account for this by failing the system whenever an abandonment scenario has occurred. In some cases it may only be a specific train of a system that needs to be disabled, such as when the procedure calls for disabling all but the "credited" train. The logic should account for this by placing an OR gate above the existing gate for failure of the system or train, with the second input being either a house event or other logic that will be set to 1.0 for any scenario where the MCR is abandoned.

3.6 An Example of a Detailed Integrated Logic Model

Putting all the above discussed modeling aspects together, this section provides an example of integrated model logic for MCRA. The logical construct for developing the integrated model is shown in Figure 3-1. This figure is intended to illustrate required the Boolean logic to account for all of the issues previously discussed. This logic is a very key aspect of the process and is intended to be implemented individually for each system/function that is involved in the abandonment process. Note that this section only applies to systems that can be credited under MCRA conditions. For systems that are intentionally disabled as part of the abandonment process, see the discussion in Section 3.5.5.

It should be noted that this logic may not always be implemented in the model in the form of such a fault tree. The capabilities of various codes that are used for PRA are such that some aspects of the logic could better be implemented as boundary conditions, rules files, flag files, exchange sets, or other post-processing techniques. There is no reason why this cannot be done, as long as the Boolean logic represented by the figure propagates properly throughout the model. The following is the description of the key gates/events in the structure shown in Figure 3-1.

- SYS-X-FAIL-ALL: This gate is added at the system level for each system that can be restored (if it fails) during the abandonment process. It assures that a system will only

fail if it fails automatically (due to fire or random events) and if it also fails to be restored when the control room is abandoned.

- SYS-X-FAIL: This gate represents the system event tree as it is used for all fire and internal events scenarios. It is the internal events system fault tree with the fire PRA impacts added, in accordance with the individual fire PRA modeling requirements. This part of the tree will include the mapping of the fire-induced circuit failures to the component failures, and would also include any operator actions that are credited for non-abandonment scenarios. Note that this gate would not exist in the case of dedicated shutdown systems, discussed in Section 3.5.4, since these systems are not credited in the internal events PRA or in non-abandonment scenarios in the fire PRA.
- SYS-X-FAIL-MCRA. This sub-tree represents the credit for the system restoration actions called for the in the abandonment procedure. It is set up such that it will automatically fail in a non-abandonment scenario, and thus is only actuated if the scenario being evaluated can take credit for abandonment.
- NOT-MCRA. This flag event is what controls whether an abandonment scenario is taking place, and so is set to allow credit for abandonment restoration when warranted. The default value for this flag is TRUE, which means that gate SYS-X-FAIL-MCRA will be failed and no abandonment credit will be added.
    - When using CAFTA, the general approach would be that FRANX is used to set the flag to FALSE for abandonment cases. These will be MCR fire scenarios that are determined to be a loss of habitability and scenarios that cause failures that would result in meeting the cues for loss of control (e.g., fire in control complex and failure to be able to start any injection from the MCR).
    - It is also possible to build a fault tree structure that models the loss of control conditions (i.e., system failures) that provides the cues for loss of control and that also include the logic of the loss of habitability scenarios.
- SYS-X-NONMIT-MCRA. This is the main logic for the abandonment credit. This side of the tree, when activated by the loss of control or loss of habitability conditions, determines the probability that System X does not perform its required function for shutdown from outside the control room given that it failed to perform its function automatically.
- SYS-X-NONMITFAIL. As discussed previously, it is necessary to take into account failures of equipment that cannot be mitigated by shutdown outside of the MCR. This logic will fail abandonment credit for System X if failures have occurred that would not allow successful restoration of the system even if the operator actions are performed successfully.
- SYS-X-NONMIT-FIRES. This gate simply gathers together failures that are non-mitigatable, which can be either random or fire-induced.

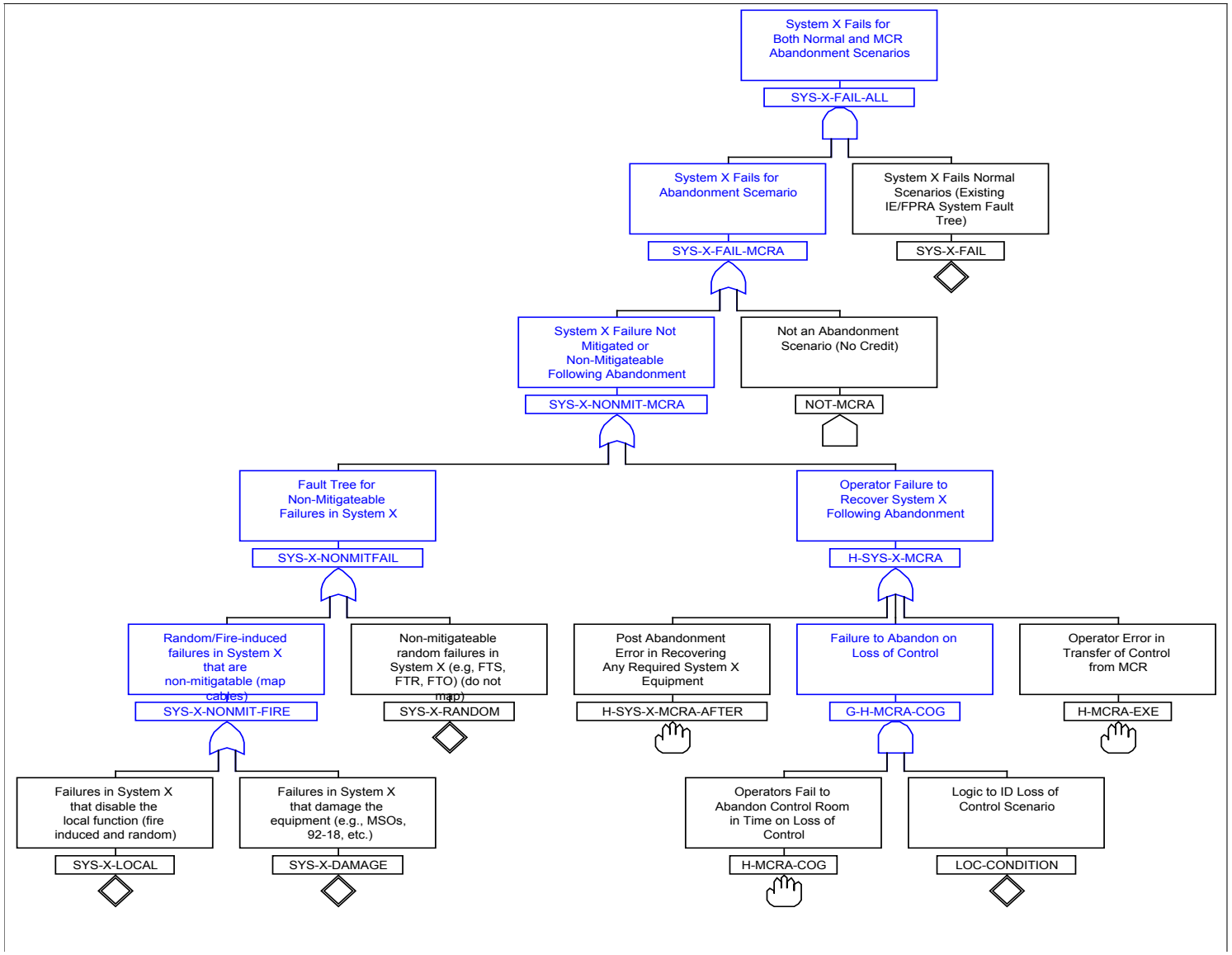

Figure 3-3
Example logic for integrating main control room abandonment into the plant PRA model

- SYS-X-LOCAL. This will be a gate that contains failures associated with the operability of the alternate shutdown panel for the specific system being modeled (System X). This would include faults that would fail the transfer of control to the panel or failure of the panel functions themselves. They would include both random and fire-induced failures, so they would need to have random failure probabilities assigned and also be mapped to cables. These would include the transfer switches that activate the remote panel, any isolation switches that clear hot shorts essential to shutdown, and any controlled located on local panels not at the remote shutdown panel.

- SYS-X-DAMAGE. This will be a gate that contains failures that would cause fatal damage to needed equipment for the specific system being modeled. This is mostly related to MSO induced failures, such as fire-induced faults that would overload diesels, cause 92-18 valves to jam, etc. Note that this logic would likely also appear under gate SYS-X-FAIL, since it would also fail the system in non-abandonment scenarios. It would be repeated here to assure that its recovery is not credited during abandonment. Note that this gate would include logic for any conditions that cannot be successfully mitigated by the capabilities of the remote shutdown panel or that are not covered by the remote shutdown procedures. For example, the remote shutdown capabilities of many PWRs are such that they cannot successfully respond to a LOCA condition. In this case, this logic would include the occurrence of an RCP seal LOCA as being a fatal condition that would defeat the remote shutdown function following abandonment.

- SYS-X-RANDOM. This will be a gate that contains random failure of required equipment representing mechanical failures that cannot be overcome by the panel actions, even if they work properly. This is to assure that random failures to start, run, etc. that represent mechanical failures are not restored, while still allowing restoration for those cases where a fire-induced failure would be bypassed by the function at the panel. Again, this will be logic that would also appear under gate SYS-X-FAIL, but in this case fire-induced effects would not be mapped to these events because it has been determined that the fire-induced failures are not fatal (i.e., the equipment can be recovered by following the abandonment procedure). The modeling here can be a little tricky, because these basic events need to be properly linked to the equivalent failures under SYS-X-FAIL, but without the fire-induced impacts. It is clearly important to carefully review all the basic events and failure mechanisms to make sure they are properly apportioned to SYS-X-LOCAL, SYS-X-DAMAGE, and SYS-X-RANDOM.

- H-SYS-X-MCRA. The structure under gate SYS-X-NONMITFAIL addressed the equipment failures that will fail the abandonment shutdown. This gate addresses the human failures that will fail abandonment shutdown, and so gathers the HFEs that will fail system restoration. There are three such errors considered; (1) failure to properly execute the actions to transfer command and control, which will appear for every system and fails MCRA for all LOH or LOC scenarios; (2) failure to abandon the MCR, which applies only to LOC, will appear for every system, and fails MCRA for all LOC scenarios; and (3) failure to properly execute the after abandonment actions for the

specific system, which will appear only under that system and fails MCRA for all LOH and LOC scenarios where the fire impacts that system.

- H-SYS-X-MCRA-AFTER. This gate includes the actions that take place after abandonment that will always fail the restoration of the specific system under abandonment conditions, regardless of the cause of the abandonment. The approach shown, provides a structure that allows for variations on this HFE to address different failure conditions. Although this could significantly complicate the modeling, the distinction between certain actions based on relevance to the scenario (e.g., diesel start and load shedding actions for AC power recovery cases) may be functionally warranted, in particular if the risk associated with abandonment scenarios is significant. Note that an alternative approach would be that all individual actions required could be represented by a single HFE that represents the bounding case for failing to successfully reach a safe and stable condition (i.e., it would include all actions required to recover all systems). This alternative and other variations are discussed in Section 3.7.
- G-H-MCRA-COG. It is generally accepted that the operators will abandon the control room if the conditions are such that they cannot function and that their safety is threatened, so there is no cognitive decision about whether to abandon or not for the case of loss of habitability. However, the decision as to whether there is a loss of control is always somewhat at the discretion of the shift manager, and so for the loss of control case, there is a decision process involved and so a cognitive HFE is required to be considered. This is the gate that decides if the cognitive HFE for failure to abandon should be applied.
- H-MCRA-COG. This basic event is the cognitive HFE that will always fail abandonment for loss of control. This same basic event appears under every abandonment tree for all the systems modeled, so is a common failure mechanism that will fail all functional recoveries covered by the abandonment procedure.
- LOC-CONDITION. This will be a gate that determines whether the loss of control condition exists. It will be a model of the conditions that result in a loss of control from the control room, as defined in the plant procedures or through operator interviews and/or simulator training.
- H-MCRA-EXE. This basic event is the execution HFE for the actions that take place after the decision is made to abandon and the time at which command and control has been transferred from the MCR. These actions are common to all abandonment scenarios, and generally include such things as isolating the MCR circuits, depowering circuits to prevent spurious operations, powering up the remote shutdown locations, etcetera. These actions are common to all MCRA scenarios, and so this BE will appear under every abandonment tree for all systems modeled.

3.7 Alternate Approaches

While the approach discussed above will provide the most realistic assessment of MCRA, there are simplified approaches that may provide a sufficient answer, in particular for those plants where the use of a simplified approach results in the MCRA scenarios where it is used not being significant risk contributors.

One alternative approach comes directly from NUREG/CR-6850, which is to use a single overall value for the probability of failure to achieve a successful alternate shutdown. However, it does not really provide sufficient guidance on how to implement this approach, what the considerations are, and what constituent pieces of this single value need to include. To address this gap, the guidance for using this approach is therefore discussed in Section 3.7.1. The key problem with the single value approach is that the value must be bounding for all abandonment scenarios. Because the most severe scenarios also tend to be the ones with the lowest frequency, the use of a bounding value based on the most severe scenarios will be quite conservative for the more frequent, less severe scenarios. If the use of a single value results in MCRA scenarios being eliminated as dominant contributors, it would be an acceptable modeling choice.

Many plants cannot live with this conservatism, but also did not wish to perform the more detailed approach illustrated in Section 3.6. This resulted in the development of a "middle ground" approach that was not mentioned at all in NUREG/CR-6850 and that removes some, but not all, of the conservatism from the use of a single value. This approach uses severity bins for the MCRA scenarios, with a value for the probability of failure to achieve a successful alternate shutdown tailored to each bin. Again, there has been no sufficient guidance provided for the use of such an approach, and so the necessary guidance is provided in Section 3.7.2. If using this approach can eliminate MCRA as a dominant contributor, then the remaining conservatism would be considered acceptable.

3.7.1 Single Overall Probability for Alternate Shutdown

NUREG/CR-6850 Section 11.5.2.10 clearly identifies that the failure probability for MCRA should be identified and addressed as part of the analysis and provides two suggestions for how to incorporate in the fire PRA model. As discussed in Section 3.2.2, one of those approaches is a simplified model consisting of estimation of a single probability. The applicable text from that section of NUREG/CR-6850 states:

> *The first approach (that is, the use of an overall probability value) can be used if the probability value is evaluated conservatively and a proper basis is provided. This approach was used in several IPEEE submittals. For example, in many cases, 0.1 was used as a point value estimate for the probability" from reference [11.3] Perspective Gained from the Individual Plant Examination of External Events (IPEEE), 2002.*

So, it can be seen that there are only two requirements to this approach in NUREG/CR-6850:

1. That the overall probability for shutdown be evaluated conservatively, and
2. That the basis be provided.

The benefits of this approach from a modeling perspective is that it is not necessary to add a number of different HFEs and equipment failures into the model structure at various locations –

it becomes a single basic event appended to cutsets where MCRA can be credited. It is effectively a CCDP given the frequency of a recoverable MCRA scenario. This allows the abandonment model structure to be placed very high up in the model and triggered when needed. It is even possible, depending on the software used, to treat this as a recovery rule, although it would be a rather complex one.

However, NUREG/CR-6850 does not state what should, or should not, be included in this overall probability, which has led to analyst inconsistency. For example, should this overall probability include both operator actions and hardware probabilities or does it represent only operator actions?

As a result of this open question, the fire PRAs performed to date have modeled main control room (MCR) abandonment scenarios using different quantification approaches and different levels of detail. For example, some fire PRA models consist of a single, overall human error probability (HEP), which in many cases has been based on judgment rather than actual HRA, to represent the collective set of operator actions needed to safely shutdown the plant following a fire in the MCR or a fire in the cable spreading room requiring MCRA. This single HEP may have been applied to all MCR fire scenarios that led to evacuation due to loss of habitability (LOH). Several reviews have questioned the validity of applying a single representative HEP (or CCDP) to the range of scenarios modeled in the PRA based on the principle value may not be bounding, such as when time-critical actions are involved, if hardware failures are not included, or if the HEP is applied to scenarios where recovery actions are not feasible.

Because the guidance in NUREG/CR-6850 is ambiguous, this report recommends that if the fire PRA follows this approach it should not be applied to the following scenarios:

1. If the scenarios modeled include operator actions that are not feasible, then those scenarios should not be credited with mitigation.

2. If the scenarios modeled include operator actions that are time-critical (defined as Time Required within 5 minutes of Time Available) then a detailed analysis is needed.

If this approach is followed, first the consideration of situations where success is not possible need to be taken into account. That is, the CCDP is only applied to cases where success of MCRA is possible.[4] So, the assessment discussed in Section 3.5.1 still needs to be performed and the model developed such that no credit is given for MCRA for those scenarios. In addition, some of the cutsets in otherwise recoverable scenarios may include failures of equipment required for MCRA that themselves are not recoverable. These are discussed in Section 3.5.3, and the model must be constructed such that the occurrence of *any* non-recoverable failure of a piece of equipment utilized in the MCRA process should preclude credit for MCRA for that cutset. Finally, any fire-induced failures of required equipment at the RSDP and/or local stations should also be assumed to preclude credit for MCRA (random failures of this equipment is addressed in the single value; see below). When using the single basic event approach to MCRA, this is best done "up front" in the model as part of the logic that excludes credit for MCRA.

[4] So, while we refer to a single CCDP for MCRA, there are in fact in reality two – 1.0 for cases where MCRA cannot succeed and the single value where it can.

For the scenarios that can be credited, the following are various elements that need to be incorporated into the single probability:

1. All of the execution actions required for safe shutdown can be analyzed separately and integrated into a single, overall HFE.[5] This means that the HEP for this HFE is the failure of *any* required action, regardless of the status of the systems in the scenario (e.g., it is assumed that AC power *always* has to be recovered for MCRA). So, a single overall HEP is acceptable since it would be developed from detailed human reliability analysis that assumes that all the actions required for shutdown are always needed for all scenarios.
2. If credit is to be taken for loss of control situations, the decision to abandon must be taken into account as described previously and that HEP added to the probability.[6]
3. All of the *random* failures discussed in Section 3.5.2 covering failure of required equipment for the RSDP and/or local stations are added to the single probability.
4. All of the *random* failures of required equipment discussed in Section 3.5.3 covering failure of required equipment are added to the single failure probability. It is understood that this may result in some double counting, since any cutsets that already include random failure of this equipment will be excluded from MCRA credit. However, this is necessary in order to assure that the single probability is bounding in all cases where it is applied.

An example of the logic that would need to be implemented is shown in Figure 3-2. While shown in fault tree structure, this logic could be implemented in any number of ways, such as using recovery rules.

What will immediately be noticed is the similarity between this logic structure and the logic structure for the integrated modeling approach discussed previously. This should not be particularly surprising, since it is expected that the "one value" approach still needs to consider all of the same effects on MCRA as discussed above. The key difference is where this appears in the overall logic of the model and how it is applied. Note that the logic shown is not input at the

[5] Note that this is unlikely to be all actions taken during abandonment. It is expected that some actions that are taken are to protect equipment, and failure to perform those actions would not result in core damage. Therefore, these would not need to be considered in the analysis.

[6] One approach would be to give no credit for LOC, in which case these scenarios would be assigned to a CCDP of 1.0. If LOC is credited, either the LOC decision to abandon HEP could be incorporated into the single probability of two probabilities could be used; one for LOC and one for LOH. The model would become a little more complicated, as the logic would need to differentiate between the two.

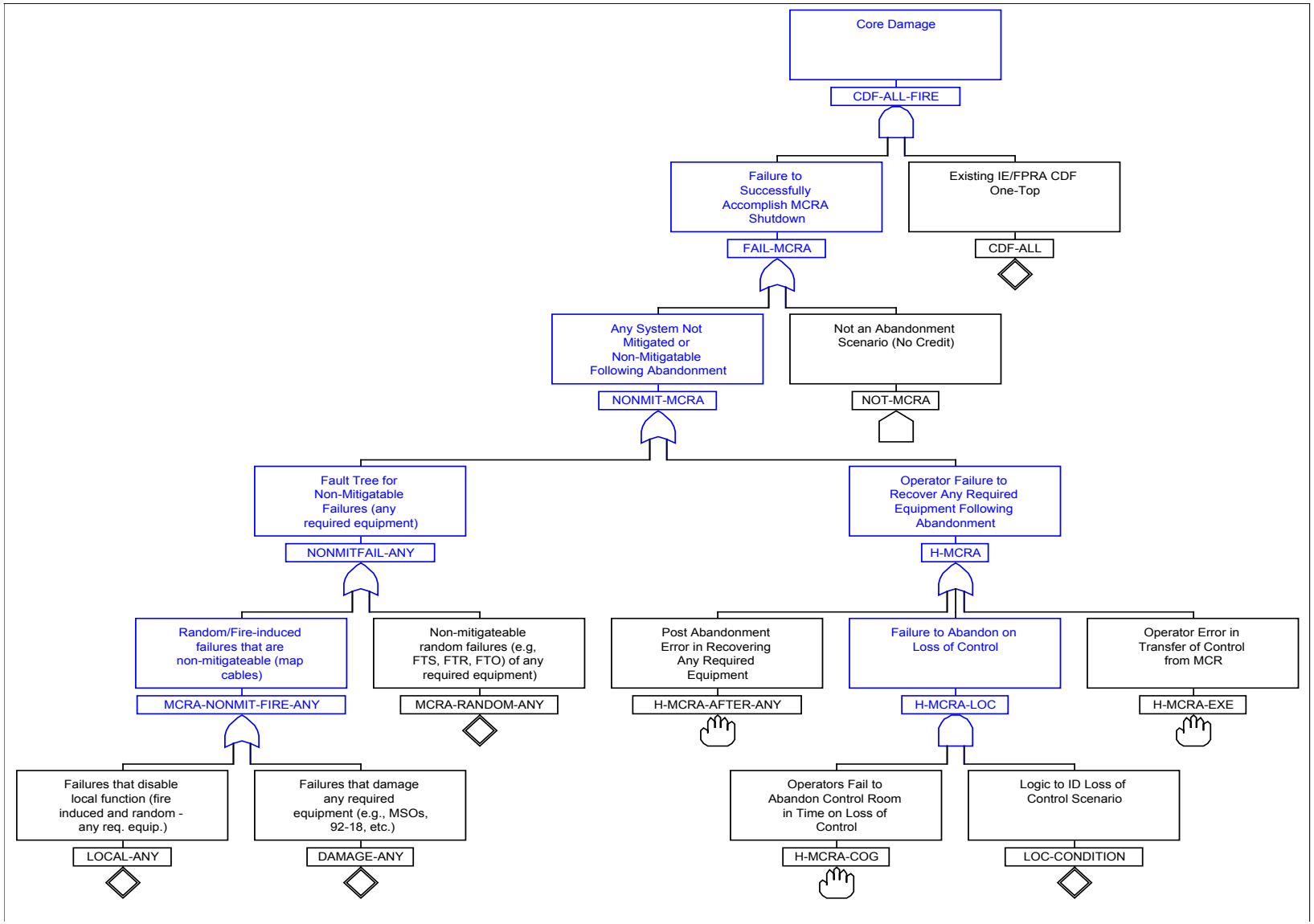

Figure 3-4
Example logic for single value approach for main control room abandonment into the plant PRA model

system level, but rather at the highest level as an adjustment to core damage frequency (or LERF). Therefore, whereas for the integrated approach the tree structure is developed for each system required for MCRA and thus appears at a number of places in the tree with many of the basic events being system oriented, the "one-value" approach applies the logic rules only once to post-process the core damage cutsets by crediting MCRA actions and equipment.

The common elements of each both models are NOT-MCRA, H-MCRA-COG, LOC-CONDITION, and H-MCRA-EXE. These are the elements that were the same in every one of the system failure trees in the preferred approach, and so failed all systems for the MCRA scenarios. Thus, they still appear in the one-value logic.

The remaining elements are redefined to be at the overall MCRA function level as opposed to at the system level. For example, LOCAL-ANY replaces SYS-X-LOCAL in the logic. LOCAL-ANY will consist of all of the local control functions that are used during the MCRA process, meaning that the failure of any local function will fail MCRA even if the automatic function for a particular was not affected by the fire. In other words, no credit is taken for any system other than would result from taking the local actions in the abandonment procedure. It is as if every MCRA system in the plant was completely shut down (even if it was working) and then restored after transition of command and control to the remote shutdown stations.

3.7.2 Modeling Alternate Shutdown with Scenario Bins

An alternative fire PRA approach is to divide the ignition sources into scenario bins. This can be accomplished within a fault tree, such as grouping all decay heat removal scenarios under one gate, or outside of a PRA tool such as in a spreadsheet. This approach can be easier to defend, since this approach can better capture the range of fire scenarios from those with no SSC impact to those that may be beyond the capability of the alternate shutdown procedure. The drawback to this approach is in defending the grouping.

The idea of using scenario bins is to remove some of the conservatism implicit in the single probability approach without adding the complexity of the full model integration. In establishing the bins, it is useful to think in terms of categories of actions and equipment required for the MCRA scenarios.

Action and Equipment Categories. The operator actions and equipment for each scenario can generally be grouped into three categories:

- *Category 1 – Actions and Equipment Needed for All Scenarios*. This category of actions and equipment consists of those required to restore decay heat removal (such as AFW in a PWR, torus cooling in a BWR), injection (such as CVCS in a PWR, RCIC in a BWR) and associated support systems; which are the minimum set of systems necessary to provide safe shutdown. Failure of any of these actions or equipment is modeled in the PRA as leading to core damage. These actions and equipment are assumed to be required for all MCRA scenarios.
- *Category 2 – Actions and Equipment Needed for Some Scenarios*. This category of actions consists of those that may be required in order to support the Category 1 actions, but in certain scenarios may not be initially failed and so not need to be

recovered. For example, there may be a need to restore power to a bus in order to restore AFW. It would be expected in this case that once the power had been restored to the bus, the AFW actions would still be required (that is, AFW would not simply automatically start when power was restored). However, some scenarios may not be accompanied by failure of the bus power, and so failing to perform those actions would not result in failure to restore AFW.

- *Category 3 – Additional Actions and Equipment Needed to Mitigate Spurious Operations*. This category of actions is modeled in addition to the actions taken for all scenarios (Category 1). This category consists of actions required to mitigate spurious equipment operation and restore the RCS and SG boundaries to a state where the AFW and CVCS systems can provide for safe shutdown. This category of actions for PWRs includes reactor coolant pump trip, isolation of RCS boundary valves (pressurizer PORV, RCS head vent, pressurizer vent, and RCS letdown), isolation of the SG's (closure of open MSIVs, closure of open SG ADVs, and closure of open SG blowdown valves), and termination of spurious safety injection. An example action for BWRs would be isolation of spurious SRVs. These actions are required only when fire damage causes a spurious event that must be terminated.

Using these categories, simple bins can be constructed with combinations of these and scenarios assigned to them. A typical set of bins could be:

Table 3-1
Binning for MCRA scenarios

Bin	Category 1 Failures	Category 2 Failures	Category 3 Failures
1	X	X	X
2	X	X	
3	X		X
4	X		
5			

A single value (CCDP) would be defined for each bin.[7] Bin 1 is essentially the bounding bin described in Section 3.7.1. This would be the starting point for the other bins. For Bin 2, the equipment and actions associated with recovery from fire-induced spurious operation (e.g., isolating the PORV control circuits) would be removed from the total Bin 1 CCDP. For Bin 3, the equipment and actions associated with recovery of fire induced failure of support systems (e.g., recovery of AC power to a vital bus) would be removed from the total Bin 1 CCDP. For Bin 4, both of these sets of equipment and actions would be removed from the Bin 1 CCDP. For Bin 5 (which would only be applicable to LOH scenarios) all actions associated with recovering from fire-induced failure of equipment would be removed from the CCDP, leaving only those

[7] Or two values, one for LOC and one for LOH, with the only difference being the addition of the HEP for the decision to abandon.

actions and equipment required to establish control at the remote shutdown panels/stations and complete the plant shutdown. These are just examples, and other bins could be defined and/or fewer bins used. It is only necessary to assure that the CCDP applied to each bin bounded the most restrictive scenario in the bin.

This approach does not take full credit for the lack of fire damage to each system in each scenario, but it does take credit for some extent of equipment free from fire damage in the MCRA scenarios in the model. Effectively, all of the requirements of the single value approach discussed in Section 3.7.1 still apply, but they apply to the characteristics of the worst-case example of a recoverable MCRA scenario in each bin rather than the characteristics of the worst-case example of a recoverable MCRA scenario.

For the purpose of illustration, we will use an example where two bins are defined – one where everything is assumed to initially fail except AC power (i.e., the failure of all systems except AC needs to be mitigated by the abandonment actions) and one where everything including AC initially fail (i.e., station blackout - the failure of all systems needs to be mitigated by the abandonment actions.) An example of the logic that would need to be implemented for this case is shown in Figure 3-3. While shown in fault tree structure, this logic could be implemented in any number of ways, such as using recovery rules.

The structure here closely resembles the single-value case, but there are two different "single-value" cases in the logic – single value for all abandonment scenarios that involve station blackout and single value for all abandonment scenarios that do not involve station blackout. The station blackout case would be the "Bin 1" case from the table above. The Bin 1 case is the same as the bounding single value case from Section 3.7.1. This bin, which represents the most severe abandonment scenarios, would always be required to be one of the bins used. The non-blackout case would be Bin 3 in the table above. The use of only two bins in this example would be a simplification that would mean that Bin 2 would be represented by Bin 1 and Bins 4 and 5 would be represented by Bin 3. The entire right side of the logic shown is the same as the single value approach, since it represents Bin 1. The left side represents Bin 3. The key difference is the need to implement logic that differentiates between SBO and non-SBO and to make sure the other logic under NONMIT-MCRA-xxx (where xxx is either SBO or NOSBO) include the correct set of equipment and actions.

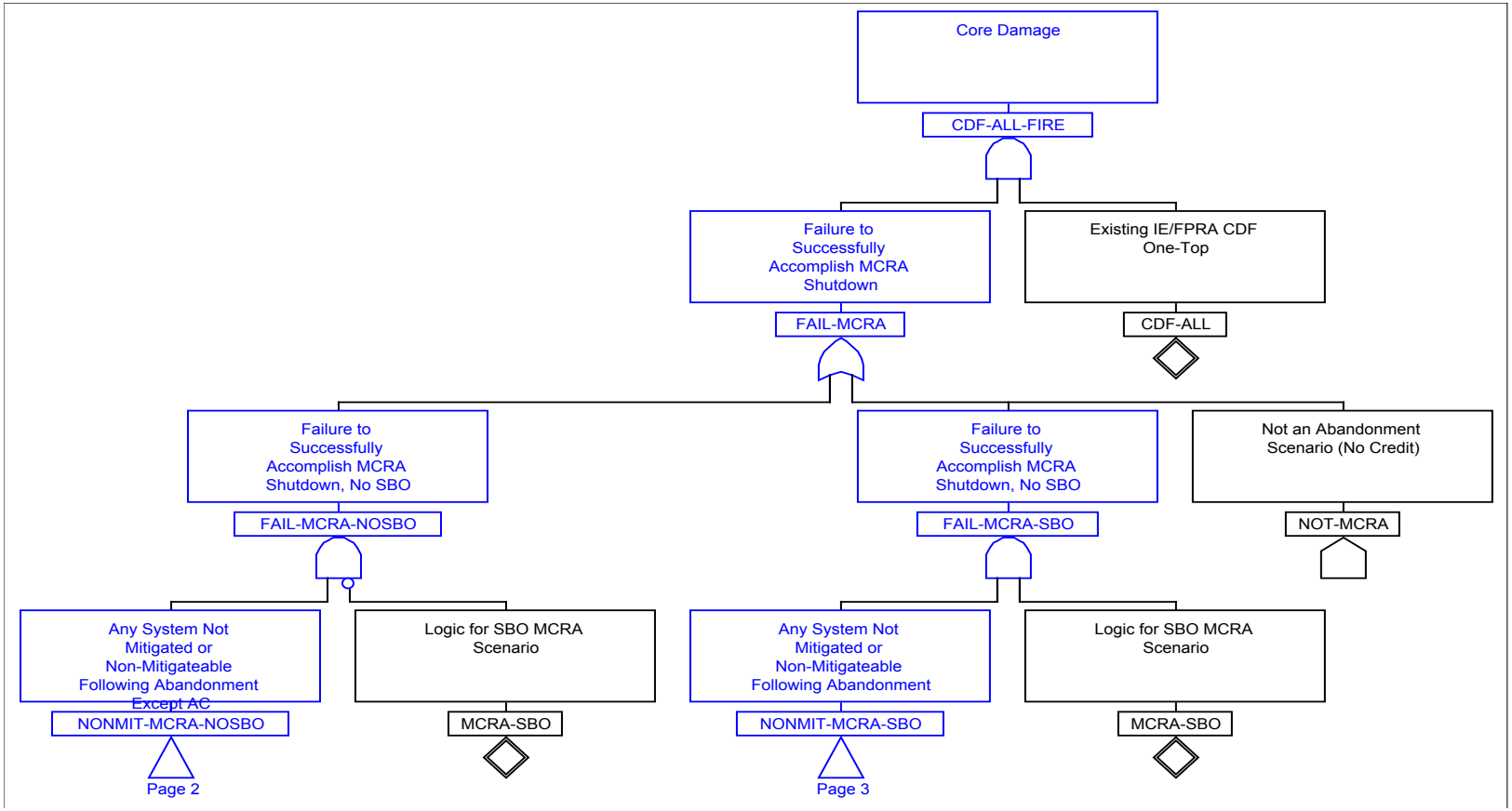

Figure 3-5
Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 1 of 3)

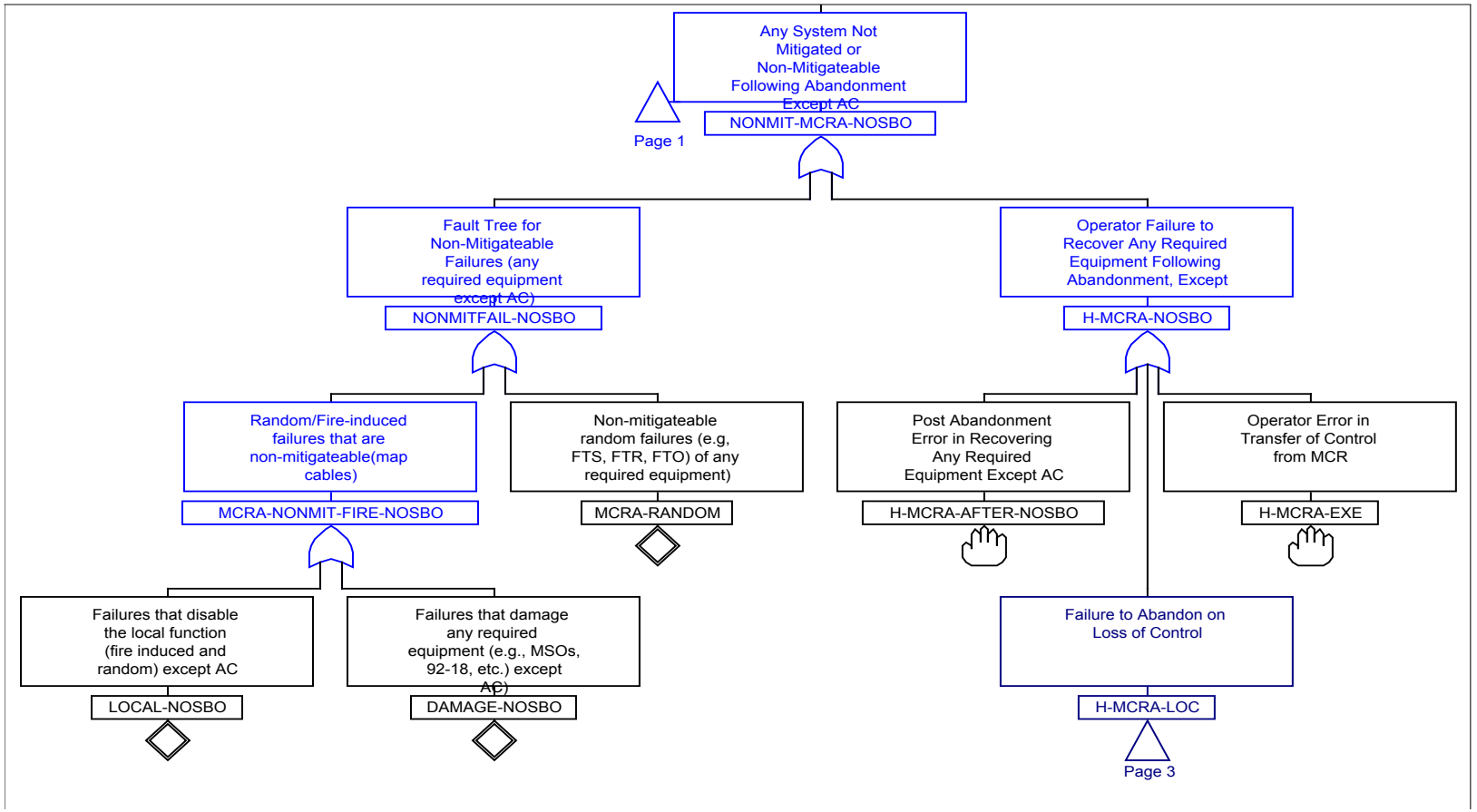

Figure 3-6
Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 2 of 3)

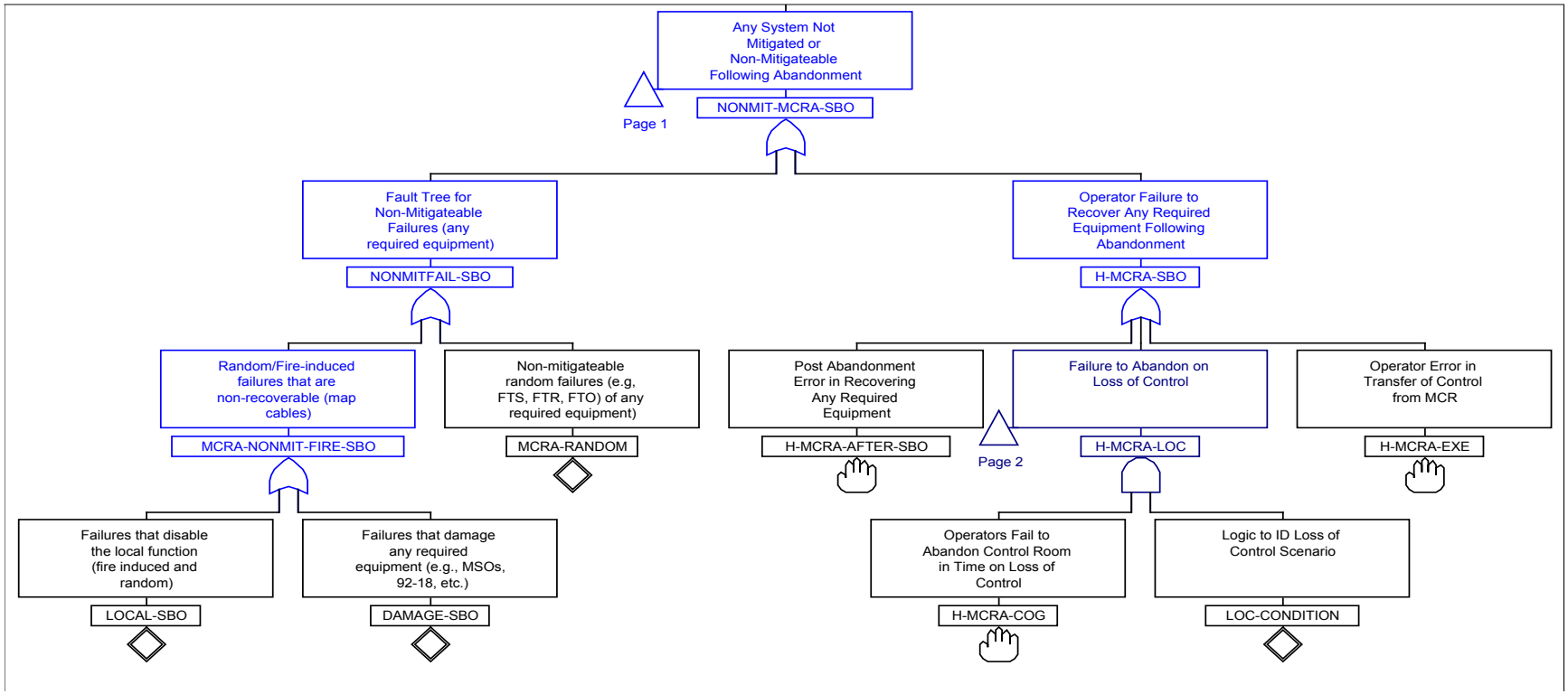

Figure 3-7
Example logic for scenario bin approach for main control room abandonment into the plant PRA model (Sheet 3 of 3)

3.8 References

1. 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.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD: 2005. EPRI 1011989 and NUREG/CR-6850.
3. *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.

4
ANALYSIS OF DECISION TO ABANDON

This section provides guidance for developing the definition and performing the qualitative assessment of the HFEs associated with the cognitive decision to abandon the MCR. When fire-induced conditions in the MCR lead to uninhabitable conditions, due to flames, smoke, or toxic gases, the MCR is abandoned due to Loss of Habitability (LOH). In other instances, plant monitoring and control may not be achievable due to fire-induced damage. These scenarios may occur from fires either in the MCR or in other key plant areas such as the cable spreading room. In this case, the MCR is abandoned due to Loss of Control (LOC).

4.1 Loss of Habitability

A loss of habitability in the MCR can result due to a fire in the MCR or due to a fire in a nearby compartment wherein smoke may enter the MCR rendering it uninhabitable. The decision to abandon the MCR is assumed to be forced due to untenable environmental conditions within the MCR. Therefore, it is assumed that there is no contribution from the failure to diagnose and decide to abandon the control room in time to execute a successful shutdown (i.e., the decision to abandon is considered to always be successful). Thus, for LOH, only the failure to shut down after abandonment is modeled in the PRA.

Fire modeling is used to determine when LOH conditions will occur. This is discussed in detail in Section 3. Since there is no "decision process" per se, there is no need to define an HFE for the decision, and so no qualitative assessment is necessary.

4.2 Loss of Control

In addition to the LOH scenarios, there may be additional scenarios (possibly involving fires in the MCR and other locations within the plant), that contain a sufficient set of cables for redundant components to cause significant loss of function, rendering the MCR ineffective in reaching and maintaining the plant in a safe condition. Fires in these locations also can result in the need for ex-control room plant shutdown (i.e., reliance on alternative shutdown features). In most plants, such locations are known in advance based on the plant's post-fire safe shutdown analysis. Typical examples of such locations include the cable spreading room, auxiliary equipment room and cable tunnels. These locations should be determined on a plant-to-plant basis.

Unlike LOH, where environmental cues like smoke and fire within the MCR are obvious, the cues for LOC in the MCR may not be as clear. Furthermore, entry criteria and/or procedural guidance to abandon the control room given loss of control may be vague or may not exist in the current procedures.

Because of both plant-to-plant variations and the likely lack of explicit cues for the decision to abandon, HRA modeling of the decision to abandon for LOC is typically more challenging than other fire HRA tasks. Consequently, additional guidance is needed to address this context.

It is recommended that the cognitive decision to abandon the MCR on loss of control be developed as a separate HFE. However, modeling such an HFE must be based on a well-understood set of "cues" that the operators use to determine that a LOC condition has occurred. There are two cases for establishing this basis:

- The less common case is that the abandonment procedure contains explicit guidance on the "cues" for abandonment, as is typical in other EOPs. In this case, the cues can be assumed to be well-understood.
- The prevalent case is that such explicit guidance does not exist, and thus a substantial amount of judgment is required, as is typical in the Severe Accident Management Guidelines (SAMGs). In this case, the development of a set of well-understood cues is performed through interviews of operators and trainers, and requires that they provide a consistent message on "this is what we understand to be loss of control."

Execution actions that follow MCR abandonment will not include cognitive evaluations unless the procedure indicates that some diagnosis is involved (e.g., if/then statements are used in the procedures). Additional HRA modeling recommendations and qualitative analysis tips for the decision to abandon for LOC are given below.

4.3 Qualitative Analysis of Cognitive Decision to Abandon the MCR

There is rarely any specific guidance on what constitutes a LOC and definition of LOC is likely to be highly plant-specific. Even when MCR abandonment is trained through simulator exercises and Job Performance Measures (JPMs), the conditions for abandonment are generally presented to the operators as the entry to the training scenario rather than the decision-making process for abandonment being part of the training session. In addition, there is often a credibility issue for operators in recognizing that fire related damage could actually reach the point where the MCR is no longer the preferred center for plant command and control. Since the conditions that lead to a LOC situation involve significant uncertainty, including fire damaged cables and equipment, timing of those fire-induced effects further "complicates" the plant and operator response.

It, therefore, becomes the responsibility of the HRA analyst to evaluate the fire PRA inputs, plant fire and MCRA procedures, and timing information to identify and define credible scenarios in which operators would truly leave the MCR. The HRA must also evaluate whether there are scenarios for which the operator MCRA response is simply not feasible, given the timing, level of damage, and/or lack of cues.

The objective is to define a human failure event that assesses the diagnosis and decision making process for abandoning the MCR in time to permit the plant to be taken to a safe and stable condition by the subsequent actions at the RSDP and locally in the plant (modeled as separate HFEs). This process is likely to require several iterations as the HRA analyst develops a better understanding of the fire PRA modeling, procedural direction versus training, time constraints and performance shaping factors.

In order to evaluate the cognitive decision to abandon, the analyst needs to understand the:

- entry criteria for the MCRA procedures
- impact of fire damage (specifically, the scenarios that could result in the inability or very high likelihood of such inability) to achieve successful shutdown if the operators remain in the MCR)

While some such procedures explicitly identify, given a fire, specific cues (e.g., loss of identified instrumentation or equipment) that direct control room operators to transfer into an abandonment procedure (i.e. relocate command and control outside of the MCR), this is the exception rather than the rule. Most control room abandonment procedures leave the decision to abandon "up to the discretion of the operations staff," which could lead the operations staff to abandon too late. Where such specific cues exist in the procedures, the evaluation of the cognitive HFE is relatively straightforward and can be performed in the same manner as for other cognitive HFEs used in the fire PRA model and additional guidance is not required. Where such cues do not exist in the procedures, the process is more challenging. Regardless of whether the procedures are vague or prescriptive, the HRA analyst must still evaluate the effectiveness of the cues in providing the decision-making criteria for abandonment to the operator. The additional guidance in this section is intended to support the analysis for the more common case where the MCRA cues are not explicitly stated in the procedures.

There are a number of topics addressed that play a role in the process of the qualitative analysis of the decision, which are all discussed in this section.

- Insights from the PRA, which will identify the specific scenarios for which the plant can only be successfully shut down if the operators abandon the MCR. The plant conditions (e.g., plant response, equipment impacts) associated with these scenarios form the situational context under which the decision will be made.
- The scenario timeline, which will define the timeframe within which the decision must be made in order to prevent the scenario from progressing to core damage.
- The operator interviews, which will provide the necessary understanding of how the operators will interpret the context as it regards the decision (i.e., what will they consider as loss of control, and how does it apply to the scenarios of concern).
- The feasibility assessment, which determines whether the three items above, when taken together, indicate that making the necessary decision within the available timeframe is possible.

4.3.1 Use of PRA Insights

Prior to incorporating credit for MCRA in the model, the fire PRA will be constructed with no credit for MCRA. This will allow for identification of scenarios where abandonment credit would be beneficial to incorporate. The focus would be on scenarios with conditional core damage probability (CCDP) or conditional large early release probability (CLERP) that are 1.0 or very close to 1.0 and that also are significant risk contributors. Therefore, the PRA outputs will be a good source of example scenarios to start conversations with the operations staff. Note that high CCDP and CLERP scenarios may end up being excluded if their overall risk contribution is low enough. That is, the model may indicate that the only way to damage all equipment/instrumentation such that operators would consider abandoning the MCR would

occur in rare event scenarios such as multi-compartment scenarios. Based on the frequency of such an event occurring this scenario may end up being screened or truncated from the model. The results or PRA output may also be a potential iteration point to bring in fire modelers if conservative assumptions were made in the creation of the fire scenario, which may be influencing target inclusion and target damage states.

Examining the high CCDP/CLERP scenario dominant cutsets will assist in developing the context the operators will face while trying to determine whether to abandon when faced with a loss of control situation. Starting with cutsets related to high CCDP/CLERP scenarios can identify scenarios where shutdown will not be possible from the MCR and the benefit of crediting LOC procedures will be apparent. When used in combination with the fire impact tables,[8] it will also provide information on exactly what the operator will "see" in the control room (in terms of indications) that can be discussed during the interviews in terms of what combinations the crew would consider to be part of the process of diagnosing a loss of control (that is, could they interpret what they see as a LOC). For cases where some indications are not damaged by the fire and are therefore providing accurate information, it will be necessary to consult the thermal-hydraulic analysis to specify what the operators will see (in terms of gauges and alarms) and when they will see it. The plant fire response procedure may even provide a list of MCR instrumentation that is protected (or, conversely, not trustworthy) in case of fire. Since at this point the operators have not yet been interviewed as to what they may use to diagnose a loss of control, it is necessary to go into the interviews with this information for any cues that they *may* use.

As a side benefit, providing specific example scenarios from real plant cutsets can alleviate potential operator bias to remain in the MCR. Operations staff can be asked the question "how would you shut down the plant in this scenario?" This may also lead to a change in thinking as to what indications would be used for the diagnosis.

4.3.2 Consideration of Timeline

There are certain timeline related considerations that need to be addressed during the interview process because, per NUREG-1921 [1], "... the decision to leave the MCR—and the timeliness with which this decision is made—can have serious ramifications for reaching safe shutdown, analysts will need to provide as reasonable an estimate as possible for the time at which the decision to abandon would be made." Fundamentally, the issue in the decision process is not whether or not the decision to abandon is made, but whether or not it is made in time to restore control and prevent core damage (i.e., before core damage is inevitable regardless of what is done).

Specific guidance for the development of the timeline for the decision to abandon is provided in Section 7.3.3. Figure 7-1 discusses the three phases (time period before abandonment decision,

[8] The cutsets generally do not show the direct fire-induced failures caused by the fire scenario since these are set to "TRUE" in the quantification process and subsumed out of the results. However, the cutsets will indicate which fire scenario is involved. By consulting the fire impact tables for the scenario it will be possible to determine which indications are affected and will provide false or misleading information. Fire impact tables relate each scenario to the equipment that fails to perform its function through a relational "chain of links" from ignition source to fire model to affected cable trays to affected cables to component functional failure, thereby providing a list of functional failures associated with each scenario. In addition to including all the front line and support components failed by the scenario, this list will be inclusive of all controls, indicators, and alarms that are failed.

time period for decision to abandon, and time period after abandonment during which transitional and post-abandonment shutdown actions are performed) that occur during an abandonment scenario.

4.3.3 Operator Interviews

When the procedure's entry criteria do not contain specific, objective cues to be used for determining whether to abandon, the standard HRA process to interview the operations staff takes on a greater role in the cognitive HFE definition and assessment for MCRA. It is, in fact, the only way to determine with any level of confidence what, if any, conditions could exist that would lead operators to abandon the control room. Thus, the decision to abandon on LOC is a plant-specific question. As discussed in Section 4.2, the goal is to establish that in the absence of explicit cues in the procedure for when to abandon that the operational staff has a consistent interpretation of what would be considered to be a loss of control, and so the interviews are intended to accomplish that. Therefore, multiple interviews may be involved in this process in order to gain the perspective of different operations crews to establish the existence of this consistent interpretation. The bias exists for partial MCR abandonment given the familiarity and comfort operators may have while dealing with plant transients from the MCR. Specific questions should be asked in order to determine what equipment (including controls and indications), if any, would direct an operator to lose confidence in the ability to safely shut down the plant from the main control room.

Follow-up discussions by phone or e-mail are likely to be needed to clarify information from the interview or to ask additional questions. These follow-up inquiries should also be organized to make the best use of limited operator availability.

4.3.3.1 Interview Questions

The interview process needs to be structured in order to be effective and complete. Below is a suggested list of questions that address the information needed from the operators in order to formulate the qualitative (and eventual quantitative) analysis of the decision to abandon for loss of control. While useful in guiding the discussion, they are not intended to tie the analysts' hands. The analysts should (in fact must) allow the discussion to follow a course dictated by the answers in order to have sufficient depth of understanding of the decision process. However, the analyst should return to the questions once each question has taken its course to make sure that they are all addressed.

1. What procedure(s) are used for this situation? How do they interact with the plant fire procedure and EOPs/AOPs?
2. What are the entry criteria for abandonment?
3. Which staff person makes the decision to abandon? Does the procedure specifically indicate the conditions for which abandonment for fire is required? If not, is there a set of systems or functions which if lost due to fire would be the conditions for abandonment?
4. How often is training performed on MCR abandonment? For fire? Do you train on the decision to abandon (what it means to have a loss of control)? Does training on the decision involve simulator exercises?

5. Do you have a feeling for how long it would take to make that decision to abandon? Is this covered in training (and timed)?
6. Using the fire PRA, we have identified the most likely scenarios that would lead to a situation where remaining in the main control room would ultimately lead to core damage. We are going to describe the conditions you would face in these scenarios (what you would see on your indications). We will ask you what you would do in such situations. [Option to add the following: Note that we may include scenarios that would not lead to core damage if you remain in the MCR.][9]

This last question, and how it is handled, is particularly important. It would not be surprising to get the response "I will never leave the control room on loss of control." This response can be reinforced by the fact that there has never been any actual simulator training on a true loss of control situation. Training is generally focused on the "Appendix R" scenarios that are designed to be recoverable while remaining in the control room. Years of training on these scenarios, which are often (erroneously) referred to as "worst case," may make it impossible for the operators to envision a situation where there is even such a thing as a fire that cannot be responded to successfully from the MCR. It is important to re-direct the conversation from generalities to the very specific risk-significant scenarios and the associated equipment failures and walk through the procedures step-by-step explaining what they will see (or not see) happening. If the interviewer gets the reaction "That's not possible" they need to remain on track and make clear that the PRA shows it is not only possible, but it is a high risk if the response is not successful.

4.3.3.2 Post-interview Assessment

The post-interview assessment is focused on the determination of feasibility of the diagnosis, which to a large extent relates to the impact on performance shaping factors (PSFs). Overall guidance on fire PSFs is provided in Section 4.6 of NUREG-1921[1]. These PSFs are applicable to varying degrees when modeling the cognitive decision to abandon the MCR. Section 4.4.5 provides additional specific insights on PSFs associated with the decision to abandon in a loss of control situation. PSF insights for the execution portion of the MCR abandonment action (i.e., actions taken after abandonment) are outlined in Section 8. Note that if the determination is made based on the interviews that a consistent interpretation of loss of control does not exist and cannot be justified, then abandonment on loss of control would not be credited. Command and control would be assumed to remain in the control room regardless of how many operators may be dispatched to perform local operations, and the modeling and HRA for all non-LOH scenarios would be performed in accordance with NUREG-1921, not this document. As stated previously, the scope of this document does not include guidance for situations where the MCR is not abandoned.[10]

[9] In cases where the decision guidance is particularly vague or the answers vary quite a bit, it may be useful to add this and to have available some scenarios that are quite serious, but would be best served by staying in the MCR. This can provide a good perspective on the "transition point" for their decision.

[10] However, the scope does cover the situation where command and control is transferred out of the MCR, but an operator either remains in or is dispatched to the MCR to perform actions under the abandonment procedure. In this case, this operator is treated in the same way as other operators who perform local actions under the direction of the individual who has command and control authority under the abandonment procedure at the new location.

4.3.4 Key Feasibility Considerations

As this section focuses on the decision to abandon, the issue of feasibility is the answer to the following question:

- *Are the characteristics of the abandonment decision sufficiently clear such that it is feasible that the decision to abandon would be made in time to successfully shut down from outside the control room?*

So, the key to this is time – the only human action we are interested in is the decision to abandon, and that this decision be made in time. As noted in Section 4.3.2, the initially available timeline information for the decision consists of a single time parameter that combines the delay time (until the cues are available) with the time to make the decision once the cues are available. That is because until the interviews are conducted we do not know what cues will actually be understood by the operator to represent a loss of control nor do we know how the decision will be made or the biases of the operators that could either encourage or delay a timely decision. There are two key considerations that could result in a determination that the decision cannot be made in time.

- The minimal combination of cues that the operators say would lead them to determine that a loss of control has occurred and that they should consider abandonment will not occur within the total time available to make the decision (or perhaps ever). If this time is less than the total time available, it becomes the delay time in the timeline (T_{delay}; see Section 7).[11]
- The total time until this minimal combination of cues is available plus the estimated time for the operators to make the decision to abandon will not occur within the total time available to make the decision. If this sum is less than the total time available, then the estimated time for the operators to make the decision becomes the cognition time (T_{cog}; see Section 7).[12]

This feasibility determination needs to be made in the context of the key scenarios that were identified by the PRA (Section 4.3.1), which were used in the interview process. In general, it would be expected that a single determination would be sufficient to cover all of the abandonment scenarios (LOC being a defined condition based on the interviews), but it may be necessary to bin the scenarios in some cases and the feasibility determination (and associated delay time and cognition time) is determined for each bin.

[11] Example: Fire causes total loss of FW because control circuits of all AFW pumps are impacted. FW must be re-established in 60 minutes. It takes 25 minutes from the time when the decision is made to abandon until feedwater can be re-established, leaving 35 minutes to make the decision. The operators state that they would not consider control lost until they had attempted to try bleed-and-feed and it did not work. The time it takes to get to the point where they would try bleed-an-feed and would have indication it would not work is 45 minutes. The cue is too late.

[12] Example: Fire causes total loss of FW because control circuits of all AFW pumps are impacted. FW must be re-established in 60 minutes. It takes 25 minutes from the time when the decision is made to abandon until feedwater can be re-established. The operators state that they would consider control lost if they could not operate any AFW pumps from the MCR, because they are sure that cables needed to bleed-and-feed would also be affected. The time it takes to get to the point where they would know AFW controls were not working is 30 minutes. The estimate from the interviews and simulator observations is that there would be a discussion about whether to abandon that would take 10 minutes. The decision comes too late.

Only two of the PSFs are directly relevant to this feasibility determination as discussed above (that is, these two considerations play directly into the determination of these two time elements). The other PSFs associated with the decision (discussed in the next section) would form the full characterization of the HFE and affect the subsequent determination of the HEP.

- **Cues and indications** will vary on the effect of the fire on the associated cables. There may be a number of "soft cues" such as spurious cycling of plant equipment due to fire damage or unreliable indications. Due to the nature of the scenario, there is generally not a single clear cue or set of clear cues to direct the abandonment of the MCR. The decision may be based on the inability to operate equipment from the main control board (MCB), visible MCB panel damage, loss of indications, or spurious equipment operation AND the fire is of such a nature that there is concern about maintaining the ability to safely control the plant. Cues to inform the operations staff that they have lost the ability to control the plant from the MCR should be identified based on the interviews.

- **Procedures and training**, in particular the latter, since the focus of this section is when the fire damage related conditions that would result in the Shift Manager/Shift Supervisor calling for MCR abandonment are not well specified in the procedure. The basis for determining how the procedures are interpreted and implemented in making the decision to abandon need to be based on interviews with operations and training personnel, as previously discussed. This information is needed in order to describe and model the scenario(s) properly, identify relevant fire compartments and equipment impacted and to determine the crux of the cognitive abandonment decision. The HRA analysts need to review both the procedures and the training discussed during the interview to understand the level of detail provided to the Shift Manager in aiding the decision to abandon. When the decision criteria for abandonment is ambiguous, the decision to abandon may be at the discretion of the Shift Manager, which would influence the cognition time associated with the abandonment timeline.

4.3.5 Other PSF Considerations

In addition to the issues that directly affect feasibility of the decision to abandon, there are other PSF considerations that can affect the reliability of the decision even when it is feasible. As discussed previously, this section primarily focuses on the qualitative HRA evaluation of the decision to abandon when the cues for doing so are vague rather than explicit. When the cues are explicit, there is likely to be less (but not zero) influence on the reliability of the task from factors such as complexity, stress and crew communication. However, when the cues for abandonment are vague, these PSFs are likely to take on greater importance. The HRA analysts must include discussion of PSFs as part of the operator interview process and assess the degree of their influence when compared to other HFEs in the fire PRA. Guidance for the types of questions to ask and considerations to make are discussed below.

- **Complexity** is more of an issue for the post-decision actions than for the abandonment decision itself. For the decision it relates to the diagnosis strategy and can be described in terms of the effect of the strategy on the behavior type used in HCR/ORE and some of

the parameters used in CBDTM quantification methods.[13] So, the complexity of the decision needs to be evaluated by the HRA analysts based on responses to questions during the operator interview(s) and then documented in the qualitative analysis. Considerations include:

- Is the response to cues (1) upon the occurrence of a condition (i.e., "if x, do y"), (2) delay following the receipt of one or more cues until a given parameter or condition is reached, or (3) after the occurrence of one or more initial cues, but before a certain condition is reached?
- Does the abandonment procedure makes it clear that the decision must be made within a specific period of time in order to be effective?
- Does the procedure provide any guidance on things to consider when making the decision (e.g., loss of certain equipment, indications or some combination thereof)?
- Does the procedure provide cautions about possible false indications and/or about which indications can be trusted?

- **Workload, Pressure, and Stress** are already addressed in the fire HRA methodology in accordance with NUREG-1921. This will be sufficient for the decision HFE because there is minimal difference between the workload, pressure and stress of a very serious non-abandonment scenario and an abandonment scenario and the associated decision process. After abandonment, the actions required would result in increased workload, pressure and stress, which is discussed in Section 8.

- **Environment** is already addressed in the fire HRA methodology in accordance with NUREG-1921, which consider both fires outside and inside the MCR. The fact that a scenario might lead to loss of control does not alter this guidance.

- **Crew Communications, Staffing, and Dynamics** are for the most part sufficiently addressed in the fire HRA methodology in accordance with NUREG-1921 to cover the needs of the MCRA on LOC case. While communication between the control room and the fire location is essential for determining the severity and controllability of the fire if that assessment is part of the abandonment strategy, this generally applies to the assessment of all fires as part of the fire procedures (whether or not the scenario leads to loss of control). The one special consideration that needs to be given to crew dynamics is because the decision to abandon is based on discretion as opposed to clearly mandated. The crew dynamics in this case may be different than for other decisions made in the MCR during fire scenarios. The extent to which this is an important aspect of the decision depends on both the way the procedure is written (who has the authority to make the decision) and also the culture of the operating crew (e.g., would such a decision be made in an "executive" fashion by the Shift Manager, would they consult with one or more senior operations staff or managers, or would the decision be more of a consensus process). This clearly affects the potential for recovery from the wrong decision (i.e., incorrectly deciding to stay in the MCR when the only viable course of action is to

[13] Although this report is not focused on quantification, our understanding of the eventual needs of the quantification helps to define what needs to be included in the qualitative evaluation.

abandon). This type of information will have been obtained through interviews and/or simulator exercises.

- **Additional PSFs** are outlined in NUREG-1921. However, no special considerations need to be taken for the Human-Machine Interface (HMI), Special Equipment or Special Fitness Needs as these PSFs typically affect execution and will not impact the cognitive decision to abandon the MCR.

4.4 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.

5
IDENTIFICATION AND DEFINITION FOR MCR ABANDONMENT

5.1 Introduction

The objective of this section is to provide guidance on how to identify and define the operator actions credited for MCRA scenarios. The identification and definition tasks work in conjunction with the fire PRA modeling presented in Section 3 and the MCRA timelines presented in Section 7 in order for the analyst to understand the expected progression to safe shutdown and to identify the representative set of actions needed in the fire PRA to evaluate the reliability of safe shutdown given an MCRA fire scenario.

This section is organized as follows:

- Section 5.1 Introduction – objectives and organization of this section.
- Section 5.2 Background
- Section 5.3 Understanding of expected plant response for MCRA scenarios
- Section 5.4 Information gathering using talk-through and walk-throughs
- Section 5.5 Examples of plant specific shutdown strategies.
- Section 5.6 Identification of MCRA operator actions
- Section 5.7 Definition of MCRA HFEs
- Section 5.8 References

5.2 Background

The basic process for performing a MCRA analysis in a fire PRA is described in Section 11.5.2 of NUREG/CR-6850 [1], and the fire PRA modeling of MCRA is expanded upon in Section 3 of this report. Additionally, Sections 2 and 3 of NUREG-1921 [2] outline the HRA process, the general considerations regarding HRA in a fire PRA (such as the relationship with other NUREG/CR-6850 tasks and spurious operations following cable failures), and the identification and definition process for fire HRA. That process outlined in NUREG-1921 has been augmented in this document to provide specific guidance for MCRA.

As described in NUREG-1921, MCRA actions are a special case, or a subset, of fire response actions. What is different from NUREG-1921 is that the MCRA actions are a collective set of actions that typically involve more coordination and communication than other fire response actions (as described in Sections 1 and 2). Section 3 of this report describes the PRA modeling strategies to: 1) first identify if and how the fire PRA model needs to be modified based on the

operator actions, and 2) to identify critical actions whose failure will be modeled as human failure events.

The following steps summarize the identification and definition steps documented in NUREG-1921. Notes have been added to indicate those steps that are further described in this report.

- Identify and categorize HFEs:
  - Internal events HFEs that are also used in the fire PRA. MCRA HRA may credit some actions taken before operators leave the main control room and these actions may already have been modeled in the internal events HRA. Additionally, the internal events HRA may provide useful insights into some of the critical tasks needed to accomplish the actions modeled in the MCRA HRA.
  - Fire response HFEs – These are new actions added to the fire PRA. Actions taken once the decision to abandon has been made fall into this category. MCR abandonment or alternate shutdown is typically addressed by a separate, stand-alone procedure (or set of procedures).
  - HFEs corresponding to undesired operator responses to alarms and indications – this category is addressed in NUREG-1921 and is not addressed in this report.
- Define the context and initial conditions for evaluating the HFE. This includes an initial assessment of the feasibility of the operator action.
- Feasibility - Because feasibility is crucial in MCRA, the topic is discussed in greater detail in Section 6. However, the feasibility check will be an ongoing step throughout the MCRA HRA process.

5.3 Understanding of Expected Plant Response for MCRA Scenarios

The first step of the MCRA HRA process is to understand the expected plant response for MCRA scenarios. In order to build this understanding, the deterministic safe shutdown analysis for MCRA is reviewed in conjunction with the fire PRA's plant response model and timelines, specifically considering the fire progression, accident progression and procedure progression (modeling the operator actions)[14]. The deterministic safe shutdown analysis begins with the decision to abandon and does not include any actions taken inside the MCRA before the decision to abandon has been made. The fire PRA may consider both actions taken before MCRA occurs, in addition to the actions taken after the decision to abandon the MCR. See Section 7 for additional discussion of time phases of MCRA. In order to understand the integration of the Fire PRA and safe shutdown strategy, the following process is recommended.

- Review the list of fire scenarios that may cause MCRA. The HRA/PRA analyst needs to understand what components/systems are impacted by the fire and which fire-induced initiating events the MCRA scenario is trying to mitigate. For example, fire induced initiating events could include:
  - Loss of MFW

[14] The deterministic safe shutdown analysis is an assessment of the ability of the plant to achieve a safe shutdown given a fire that affects the entirety of a designated fire area. In the United States, these are referred to as the "Appendix R fires," some of which are fires that assume MCRA is required.

  - Transient
  - Loss of offsite power

- Review and comparison of the fire PRA description of the expected sequence of events versus the safe shutdown strategy. In reviewing the MCRA procedure, the HRA analyst must understand that the strategy followed by each plant after MCRA is heavily controlled by the plant-specific installed features and controls. The existence (or not) of a remote shutdown panel (RSDP), the extent of its functionalities, and the need for actions at other locations will dictate the format of the procedure (use of MCRA procedure attachments dedicated to establishing certain functions, for example) and therefore the development of logic structure for modeling MCRA in the fire PRA. See Section 3 for additional discussion. This interaction is what makes MCRA HRA uniquely challenging.

- Review and comparison of the initial conditions assumed by the fire PRA and safe shutdown. This review should also include which systems are assumed to be failed at the start of the event. For example, the safe shutdown scenario may assume main feedwater is unavailable for all scenarios whereas the fire PRA may credit main feedwater in scenarios for which it is known to be available.

- Specifically review operator actions related to LERF, since LERF was not addressed during the plant updates to meet Appendix R fire protection requirements.

- Review of the expected MCRA procedure response in comparison to the fire PRA expected response and safe shutdown response. The fire PRA response is developed based on fire PRA success criteria and this may or may not align with expected MCRA procedure response (see also Section 3.3). This is done to identify what positive and/or negative impacts the operators' expected response can have on the scenario even if the actions are not explicitly modeled for MCRA.

5.4 Information Gathering using Talk-Throughs and Walk-Throughs

The expected plant response for MCRA scenarios is typically evaluated by the HRA analyst by conducting walk-throughs, talk-throughs and discussions with operators, operator trainers, and other operations personnel[15] in order to understand the following:

- Proceduralized operator actions expected during the accident sequence progression through the fire scenario, for both the success path as well as failure paths. This includes operator actions in both CDF and LERF scenarios.

- Any assumption(s) with respect to the expected plant behavior and system or equipment and operator response (e.g., equipment assumed to be unavailable, single failures of systems assumed to have occurred).

[15] This collective set of plant personnel is used to represent anyone at the plant familiar with the expected plant response for MCRA. It is often helpful to get multiple points of view so in many cases more than one individual is interviewed. Appendix C provides additional tips on the collection of plant-specific information, including interviews, talk-throughs, and walk-throughs.

This section provides a brief overview of information gathering using talk-through and walk-throughs, but further details including templates for questions and information collection are provided in Appendix C.

The operator interviews should include a discussion of the expected plant response during the three time phases of MCRA as described in Section 7. Phase I includes the expected response before the operators leave the MCR, Phase II, includes the decision to abandon and how this decision will be made, and Phase III includes the expected plant response after the decision to abandon has been made.

The emphasis during the talk-throughs is to understand how the procedures are used, some of the key decision points and time constraints of the process and in general, gaining a sense of the operations and training perspective on the scenario, how it evolves and how it has been trained.

In comparison, the walk-through provides the analysts the opportunity to view the locations, conditions and interfaces with the RSDP and other equipment cited in the MCRA procedure steps. It allows the analysts to identify particularly challenging actions due to equipment location (e.g., time required to get there), access (e.g., cramped workspace or up a ladder), or physical workload (e.g., number of turns and force required to manually align a valve). Insights can be gained into the travel times from one point to another and performance times for key tasks. Knowing what needs to be done in a timely manner in the MCR prior to abandonment and at the RSDP afterwards could even feed into plant modifications (e.g., installation of kill switches) that could simplify actions, save time, and impact operator reliability.

As part of this walk-through preparation, there is a key interface between the PRA and the HRA that needs to take place. Since the talk-through will have gone over all the actions in the procedure, and an understanding will have been developed regarding all of the actions and the operators' perspective on why the actions are performed, it is necessary to get the PRA perspective on the risk significance of the various actions so that during the walk-through a conversation can be started with the operators regarding those actions that are detracting from the swift completion of the actions that are shown in the PRA to be the critical ones.

Based on the initial talk-through, the analysis team should have identified the locations associated with the PRA-relevant procedure steps in the MCR abandonment process that they would like to see during the walk-through. These will have to be identified prior to the walk-through to ensure that the appropriate access is obtained. The walkthrough needs to be organized, even if informally, so that the analysis team can see what they need to see during the time allotted. Viewing the RSDP and other local action locations is crucial since the analysts must understand the plant-specific displays, capabilities and limitations.

The travel time and procedure step performance time for each key procedure step identified during the talk-through should be clarified and noted during the walk-through, including the time required for communication with other remote operators and to confirm actions taken. The timing should be recorded for future use during qualitative/quantitative analysis (including feasibility assessment) by a PRA/HRA member of the walk-through team. Since the walk-through will focus on the execution portion of the actions, any particularly challenging or

difficult actions should be noted; for example, is access to the equipment time consuming or does a valve take many turns of a handwheel to close? Actions that require some decision-making and those that go beyond simple execution of procedure steps, such as electrical bus load shedding actions in preparation for starting a diesel generator, should be noted as well since the cognitive portion will have to be addressed in the HFE during the detailed HRA. Information that will be useful to the assessment of the PSFs discussed in Section 8 should also be considered during the walk-through. These include the nature of the HMI (e.g., presence of mimics, type of display being read and type of manual control), whether the equipment is one among many in a similar grouping, and whether there is clear and unambiguous labeling of equipment.

The walk-through also provides an excellent opportunity to gather information to assess feasibility criteria such as communications, lighting, and accessibility of tools/keys/personnel protective equipment. See Section 6 on Feasibility for further details.

5.5 Actions Required for MCRA Safe Shutdown

Each plant should have a pre-defined deterministic safe shutdown strategy for MCRA.

This section describes some of the different approaches identified at different plants. It is the HRA analyst's role to develop and/or identify the plant specific strategy; reviewing other plants' approaches can be helpful in this development. It is extremely important to understand that the variations discussed in this section are not necessarily mutually exclusive within the plant's abandonment strategies. For example, it is entirely possible that a plant may have different types of installed features used for recovering different functions, different communication strategies for implementing different parts of the abandonment procedures, etc. In preparing the qualitative assessment, each variation in the plant, and the role it plays, needs to be discussed.

5.5.1 Actions Taken Before Command and Control Transfer Outside the Control Room

Most fires will not lead to immediate abandonment following the start of the fire and reactor trip, so the operators will have the time to implement some actions. For slower progressing scenarios, the crew may have time to perform many EOP actions. This could be, for example in PWRs, tripping the reactor coolant pumps (RCPs) (to minimize the risk of a seal LOCA in case RCP seal cooling is lost), tripping the turbine, and closing the MSIVs (to ensure there is no uncontrolled steam flow), etc.

Once the decision to abandon has been made, most plants require that a few actions be completed in the MCR just prior to abandonment. These actions could include:

- Trip the reactor, if not already tripped
- Activate and transfer control to the RSDP or equivalent
- Obtain keys inside the MCR which are then used to power up the RSDP, and actuating disconnect switches that isolate key controls of the MCR.
- Disconnecting power switches to isolate the MCR from additional spurious operations.

5.5.2 Actions Taken After Command and Control Transfer Outside the Control Room

Once the MCR is abandoned and command and control has been established outside the MCR, bringing the plant to safe shutdown will rely on actions taken away from the MCR.

Most, if not all, RSDPs do not have all the functionalities of the control room. Severe fire scenarios could cause damage that, to be mitigated, would require controls beyond those available at the RSDP, or actions that might otherwise be performed locally. In order to reach safe shutdown, actions may need to be performed at multiple locations. Performing multiple actions at multiple locations will require communication among operators because in most cases there is not enough time for a single operator to perform all actions sequentially.

To address timing requirements, the majority of remote shutdown strategies require the coordination of multiple operators performing actions at different locations at the same time. Actions required at multiple locations will require the role of each operator to be well defined; otherwise, a timely execution may not be achieved. The abandonment procedures may stipulate the assignment of each crew member, while others may assign a specified role only to some key personnel (for example, reactor operator, turbine building operator), giving leeway to other personnel to provide assistance where needed. In cases where the site has several units and one of the units is not adversely affected by the fire, some crew members of the non-impacted unit may be assigned to the affected unit.

Once outside the MCR, the best communication plan would be to have all operators performing communications face-to-face. However, this is not always possible due to multiple actions being performed at multiple locations. There are various communication strategies that have been implemented in abandonment procedures, which can be summarized into three broad groups.

- Face-to-face communication is used where the individual controlling the abandonment process is co-located with individuals performing the abandonment actions.
- Hard-wired communication is used when the individual controlling the abandonment process is not co-located with individuals performing the abandonment actions, but the action locations are well-delineated (i.e., compact) and equipped with fixed dedicated communication stations.
- Radio communication is used when the individual controlling the abandonment process is not co-located with individuals performing the abandonment actions, but either (1) the action locations are well-delineated but not equipped with fixed dedicated communication stations or (2) the action locations are not well-delineated and so the actions must be performed at numerous locations.

It is not unusual for a plant to have a combination of these communication strategies within their overall abandonment strategy.

Another way in which time critical actions can be addressed is to minimize the time needed to establish control at the RSDP by making an advance preparation of the RSDP before a decision is made to abandon the control room. In the first minutes that the fire is detected, operators will get briefed on the apparent severity of the fire. For fires that are assessed as being high severity, an operator is dispatched to the RSDP to pre-stage it for potential operation. This pre-staging

typically consists of ensuring that switches at the RSDP are in their appropriate initial position and performing all the steps required to ensure that, when notified, the RSDP can immediately be made operational. Because this strategy is performed concurrently with the decision-making process of abandoning the control room, it gives shift supervision additional time to decide whether or not to abandon. A drawback of this approach, however, is that it removes an operator from the control room, which will require other operators to assume his/her role.

5.5.3 Actions Taken While Command and Control Remains in the Control Room

The strategy discussed in this section is not a MCRA scenario, but involves use of the RSDP to achieve safe shutdown. In this strategy command and control remains in the MCR, but operators are dispatched to the RSDP and other equivalent locations to perform local actions. It is only applicable to scenarios in which the MCR remains habitable. This strategy draws its appeal from the fact that the control room 1) remains the central hub for communications in the plant, 2) is a location that the operators are used to working in with well-established communication protocols, and 3) has the entire set of procedures needed for safe shutdown, which helps for informed decision making. A drawback of this strategy is that, for severe fires, it can be expected that key monitoring parameters will be lost in the control room, or will provide misleading information. The designated command operator will need to remain aware that only monitoring instruments that are known to be unaffected by the fire (typically, parameters available at the RSDP) should be used as reliable cues for action, and will need to communicate with individual operators at local stations where reliable indicators are available in order to control the plant. Another drawback is that the abandonment procedure may be different for the two abandonment cases, so the various assignments and related attachments will be different. This creates challenges for operator training. Since this is not a MCRA situation, this document does not provide detailed guidance on modeling or HRA. The existing guidance in NUREG-1921 and NUREG/CR-6850 is deemed sufficient.

5.5.4 Actions Taken That Use the Main Control Room as Local Station During Abandonment

A variation on Section 5.5.3 is the use of the control room as one of the local stations manned by an operator when the control room is abandoned on loss of control. This allows for the potential to operate equipment or observe other plant parameters that cannot otherwise be operated or observed from the RSDP and is not electrically isolated when the RSDP is fully activated. This provides potential additional response options should the fire (while being large and significantly damaging) not cause failure of non-safety equipment that could back up a safety function.

5.6 Identification of MCRA Operator Actions

Once the expected plant response following MCRA is understood then the MCRA operator actions that are to be included can be identified, defined, and incorporated into the overall fire PRA model.

The same HRA identification steps apply as for other fire response actions described in NUREG-1921:

- Review of plant procedures, identify proceduralized actions.

- Review of the PRA model, specifically the accident sequence development and success criteria portions, in order to understand
    - Context for the actions including the fire-induced initiating event(s) and the fire damage.
    - Human failure events already identified as being a part of the fire PRA.
- Review of the PRA results to identify actions that could mitigate fire-induced failures. This could include identifying actions that are currently not in the procedures, but if added could provide a reduction to the overall risk. For example, the fire PRA is required to consider multiple spurious component failures for a given fire scenario and these scenarios are not considered for safe shutdown and therefore procedure guidance may not currently exist.

These steps are typically conducted in an interactive manner. Before the procedure review can be effective, the fire progression and impact on SSCs should be understood, including how the progression fits with the MCRA timeline described in Section 7 of this report.

For MCRA, the HRA analyst will need to first identify MCRA scenarios included in the PRA and for each scenario and identify a set of operator actions required by the PRA to mitigate each scenario.

For MCRA scenarios, there are several types of actions to consider, which are summarized below. Their potential mapping to human failure events are shown in Table 5-1:

- Decision to abandon for loss of control scenarios (further details provided in Section 4):
- Actions in the MCR taken after the decision to abandon has been made but before the operators leave the MCR. These actions can include reactor trip, turbine trip and isolation of the MCR.
- Actions to establish command and control at the RSDP (or other control station outside of the MCR) including establishing instrumentation.
- Actions to start-up and control support systems and front-line systems as needed in order to fulfill the following key safety functions. (Note that the fire impact will range from only needing one function to challenging several safety functions. These functions implicitly include the support systems and instrumentation needed to start and sustain the function for the mission time modeled in the MCRA analysis.)
    - Ensure subcriticality
    - Provide injection
    - Ensure decay heat removal
    - Mitigate fire damage such as shut a primary PORV block valve
    - Provide containment isolation
- Actions to establish long term control support systems and front-line systems. These long term control actions are often considered to be negligible contributors for internal events HRA, but long term control at the RSDP could be more challenging and these actions should not be screened from consideration initially. Examples of long term actions could include:
    - Maintain RCIC control RSDP or Maintain RPV level by any means necessary
    - Maintain decay heat removal at RSDP

- Maintain RPV pressure and/or depressurization
- Maintain EDGs by either load shedding systems or refilling fuel tank.

Not all plants and/or fire PRA scenarios require all the types of actions identified above; the need for these types of actions is based on the fire PRA success criteria and the plant's specific MCRA strategies (see Section 3). Only after the fundamental strategy for how to achieve shutdown is understood can the analyst then identify which portions of the strategy are feasible or not (as discussed in Section 6), given the capabilities of the RSDP, the procedural and training guidance provided to the operators, and the time available for the procedure-driven actions to be performed.

5.7 Definition of MCRA HFEs

Once the scenarios and associated actions have been identified, the next step is to define the operator actions that will form the basis of human failure events (HFEs). MCRA is different from internal events HRA in that MCRA requires a collective set of operator actions. That being said, there is no difference in the definition of each HFE. For a given fire PRA scenario, the success (and associated failure) criteria need to be defined for each human failure event. This includes the definition of critical tasks and the time window for operator response. HFE definition uses input provided in support of the MCRA timeline described in Section 7.

The definition of HFEs modeling individual MCRA operator actions will follow the same guidance as for fire response actions. This is described in Section 3 of NUREG-1921. The human failures of fire response actions are defined to represent the impact of the human failures at the function, system, train, or component level as appropriate, consistent with requirement HRA-B1 of the ASME/ANS PRA Standard [3]. The definition should start with the collection of information regarding the context of the fire scenario. This comes from the PRA accident sequence, success criteria and associated engineering analyses such as the following:

- The high-level (train level) task required to achieve the goal of the response (that should form the basis for the individual HFE)
- Applicability to accident sequences based on the initiating event, the fire damage and the subsequent system and operator action successes and failures (see Section 3)
- Accident sequence–specific procedural guidance (including MCRA, fire procedure and EOPs/AOP)
- Cues, instrumentation and other indications for detection and evaluation
- Accident sequence–specific timing of cues and the time available for successful completion (as discussed in Section 7)
- Locations where the actions are taken
- Systems and components needed for success
- Communications plan and systems
- Command and control, including staffing assignments and roles

Because each HFE is part of a collective set of actions for a given MCRA scenario, part of the definition should include a discussion on dependencies among actions. This includes defining

when coordination among actions is required, identifying actions that are based on the same cues and indications, and identifying situations in which actions will be occurring simultaneously. Section 9 provides a detailed discussion on how to account for dependencies.

For MCRA actions, the definition goes beyond that typically needed for non-MCRA HFEs, in that it should include a description of the following.

- Communication strategies that would be employed once outside the MCR,
- Command and control structure once outside the MCR.
- For plants that share a MCR between units, the impact on the non-fire damaged unit should be defined.
- For a shared control room, if both units leave the MCR due to habitability concerns, the impact on staffing, and command and control structure once outside the MCR should be defined.

The definition task initially scopes out these various HFE characteristics and allows individual HFE designations to be made within the context of the MCRA scenarios. These same characteristics, however, become the topics for further qualitative analysis to flesh out the initial skeleton by assessing the HFE-specific aspects in greater detail, as discussed in Section 7 on Timelines and Section 8 on PSFs.

Table 5-1 provides an example of the types of operator actions (similar to the list shown in Section 5.6) needed to respond to different MCRA scenarios, followed by the identification of the operator actions required for success and identification of potential human failure events. As seen in Table 5-1, actions such as those taken to establish decay heat removal occur in several different scenarios and can be modeled using the same development process, provided that the performance shaping factors affecting the action are similar, such as the same timing parameters.

Table 5-2 provides a second example showing how operator actions associated with specific scenarios can be identified and defined. Using one HFE for all MCR abandonment scenarios can often times be overly conservative. In order to remove unnecessary over-conservatism, several scenario bins can be analyzed and a different recovery factor based on bin-specific differences in the HRA and equipment failure can be used for each scenario, as appropriate. The following are examples of bins that can be developed:

- **Bin 1:** AC power recovery **not** required (non-LOCA scenarios). This bin only includes the actions that take place at the RSDP and the associated equipment reliability.
- **Bin 2:** AC power recovery required (non-LOCA scenarios). This bin includes both the actions that take place at the RSDP and the actions that take place locally to re-power the credited AC power train, and the associated equipment reliability.
- **Bin 3:** AC power recovery not required (LOCA scenarios). This bin only includes the actions that take place at the RSDP and the associated equipment reliability.
- **Bin 4:** AC power recovery required (LOCA scenarios). This bin includes both the actions that take place at the RSDP, follow up actions that take place to recover from LOCA scenarios, and the local actions to re-power the credited AC power train and all of the associated equipment reliability.

In addition to the bin approach, different actions can be credited at the RSDP or locally for recoveries at a system functional level, such as recovery of Auxiliary Feedwater (AFW), recovery of charging, recovery from stuck open PORVs and recirculation. These actions are selected based on procedure guidance and RSDP capabilities. Any combination of these actions may be used in different scenarios based on the plant damage state.

Table 5-2 lists an example of the combinations that can be used when considered appropriate for various MCR abandonment scenarios in the fire PRA model. In this example, the Bin 3 for AC power recover NOT required for LOCA scenarios is used. The PRA functions are identified in the header of the table, then the application of the HFEs that implement these functions to specific scenarios is shown in the body of the table.

Following Table 5-2, Section 5.8 provides examples of HFE definitions.

Table 5-1
Example of HFE Identification for MCR Abandonment Scenarios

Reason for Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
Loss of Habitability	**Scenario 1** Fire with no SSC damage so no fire-induced initiating events. Reactor trip occurs due to the decision to conduct manual shutdown as required by the decision to abandon.	Decide to abandon Electrically isolate the main control room and transfer control to the RSDP. Establish and maintain control of decay heat removal outside the MCR for PRA mission time. Establish containment isolation	Decision to abandon is not modeled following a loss of habitability	
			Operators fail to transfer control from MCR to RSDP	The action to transfer control to the RSDP would involve electrical isolation of the MCR. The electrical isolation could be performed from the MCR or at the RSDP depending on plant design.
			Operators fail to establish instrumentation at RSDP	Establishing instrumentation at the RSDP could be defined as a single HFE or it could be included as part of the success criteria for other HFEs. Most operator actions will require some instrumentation and by defining an HFE to establish instrumentation at the RSDP the dependency concerns among HFEs which share the same set of instrumentation can be explicitly addressed.
			Operator fails to start-up a feedwater pump, including restoration of support systems, and control feedwater for 24 hours	Long term control actions should be considered following abandonment. Long term control actions are typically considered to be negligible for fire scenarios which do not require abandonment.
			Operators fail to shut containment purge line	Containment isolation actions would impact LERF and the identified set of operator actions should include both CDF and LERF actions.
	Scenario 2	Same actions as in Scenario 1 to transfer	Same actions as in Scenario 1	

Reason for Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
	Fire-induced LOCA due to open Primary Relief Valve	control outside of the MCR and establish decay heat removal; plus the following: Mitigate stuck open Primary Relief Valve	Operators fail to shut stuck PORV or block valve	
			Operators fail to start and control Safety Injection (SI) Operators fail to terminate SI after PORVs are closed Operators fail to establish long term decay heat removal	The HFE for failure to establish long term decay heat removal would only be required if operators fail to close PORV or block valve.
	Scenario 3 Fire-induced Station Black Out (SBO)	Same actions as in Scenario 1 to transfer control outside of the MCR and establish decay heat removal; plus the following: Start and maintain EDGs for PRA mission time.	Same actions as in Scenario 1	
			Operators fail to locally start emergency diesel generators (EDGs) or re-establish some other source of electrical power	
			Operators fail to restore power to hydrogen ignitors	
	Scenario 4 Fire-induced spurious SI	Same actions as in Scenario 1 to transfer control outside of the MCR and establish decay heat removal; plus the following: Terminate spurious safety injection.	Same actions as in Scenario 1	
			Operators fail to terminate spurious SI	
			Operators fail to mitigate the LOCA given PZR overfill	
Loss of Control	**Scenario 5** Fire with significant SSC	Decide to abandon	Decision to abandon is modeled following a loss of control	

Identification and Definition for MCR Abandonment

Reason for Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
	and instrumentation disablement due to fire-induced initiating events; automatic reactor trip.	Electrically isolate the main control room and transfer control to the RSDP. Establish and maintain control of decay heat removal outside the MCR for PRA mission time. Impact of fire on instrumentation and control may affect the actions needed start-up a feedwater pump, including restoration of support systems, and control feedwater for 24 hours. Establish containment isolation.	Operators fail to transfer control from MCR to RSDP	The action to transfer control to the RSDP would involve electrical isolation of the MCR. The electrical isolation could be performed from the MCR or at the RSDP depending on plant design.
			Operators fail to establish instrumentation at RSDP	Establishing instrumentation at the RSDP could be defined as a single HFE or it could be included as part of the success criteria for other HFEs. Most operator actions will require some instrumentation and by defining an HFE to establish instrumentation at the RSDP the dependency concerns among HFEs which share the same set of instrumentation can be explicitly addressed.
			Operators fail to start-up a feedwater pump, and control feedwater for 24 hours	Long term control actions should be considered following abandonment. Long term control actions are typically considered to be negligible for fire scenarios which do not require abandonment.
			Operators fail to shut containment purge line isolations	Containment isolation actions would impact LERF and the identified set of operator actions should include both CDF and LERF actions.
	Scenario 6 Fires that include: LOCA or Station Black Out (SBO) or Spurious SI	Same actions as in Scenario 5 to transfer control outside of the MCR and establish decay heat removal; plus the following: Start and maintain EDGs for PRA mission time.	Decision to abandon is modeled following a loss of control.	
			Operators fail to mitigate a LOCA Operators fail to restore electrical power or EDG	

Reason for Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
			Operator fail to terminate SI given instrumentation is impacted by the fire.	

Table 5-2
Example of MCRA scenario functional relevance for identifying individual operator actions for MCRA Scenarios that involve PORV LOCAs when AC power recovery remains available

PRA Sequence	Abandonment Decision	Transfer of Control	Recovery of AC Power	Closing Spuriously Open PORVs	Recovery of AFW	Recovery of Charging	Local Action for Cold Leg Recirculation	HFEs Required By the Scenario
1	MCRAHFE1 Operators fail to abandon on LOC	MCRAHFE2 Given the decision to abandon has been made operators fail to transfer control to RSDP	AC Power Available. No recovery needed and no contribution to overall HEP	MCRAHFE4 Operators fail to remove power to stuck open PORV	MCRAHFE5 Operators fail to start and maintain AFW at RSDP	MCRAHFE6 Operators fail to start and maintain charging at RSDP	MCRAHFE7 Operators fail to provide longer term make-up	MCRAHFE1 MCRAHFE2 MCRAHFE4 MCRAHFE5 MCRAHFE6 MCRAHFE7
2	MCRAHFE1 Operators fail to abandon on LOC	MCRAHFE2 Given the decision to abandon has been made operators fail to transfer control to RSDP	AC Power Available. No recovery needed and no contribution to overall HEP	MCRAHFE4 Operators fail to remove power to stuck open PORV	MCRAHFE5 Operators fail to start and maintain AFW at RSDP	MCRAHFE6 Operators fail to start and maintain charging at RSDP	Recirculation unavailable due to hardware failure.	MCRAHFE1 MCRAHFE2 MCRAHFE4 MCRAHFE5 MCRAHFE6
3	MCRAHFE1 Operators fail to abandon on LOC	MCRAHFE2 Given the decision to abandon has been made operators fail to transfer control to RSDP	AC Power Available. No recovery needed and no contribution to overall HEP	MCRAHFE4 Operators fail to remove power to stuck open PORV	MCRAHFE5 Operators fail to start and maintain AFW at RSDP	Charging available. No recovery needed and no contribution to overall HEP	MCRAHFE7 Operators fail to provide longer term make-up	MCRAHFE1 MCRAHFE2 MCRAHFE4 MCRAHFE5 MCRAHFE7

5.8 Examples of HFE Definitions

This section provides examples of detailed HFE definition for three of the seven HFEs shown in Table 5-2:

- MCRAHFE1: Operators fail to implement decision to abandon MCR
- MCRAHFE2: Operator fails to transfer controls to RSDP after decision to abandon MCR
- MCRAHFE5: Operator fails to perform DHR Function via MD AFW Pump 3 at RSDP (non-LOCA scenarios)

MCRAHFE1: Failure to Implement Decision to Abandon MCR

Summary of HFE:
Fire scenarios in the main control room (MCR) and cable spreading room (CSR) may involve damage to redundant trains of safe shutdown equipment.

The MCR will need to be abandoned due to loss of control.

This HFE constitutes the cognitive (i.e., diagnosis and decision-making) error for failing to abandon in time to successfully shut the plant down from outside the MCR.

The consequence of failure of this action is core damage.

Cues and Indications:
Primary Cue: Alarm for fire in CSR

Additional Cues:
Pressurizer level unavailable from MCR
RCS temperature unavailable from MCR
Steam generator level unavailable from MCR
Fire suppression system initiated
Normal charging indications unavailable from MCR
Local verification of CSR fire by Nuclear Operator

Operators will get an indication of fire in the CSR; once this alarm is identified by operators in the MCR, they will send a nuclear operator to visually verify the presence of a fire (flames) in the CSR.

The SRO communicated during interviews that indication parameters never fail as is; instrumentation would either fail erratic, high, or low. It would therefore be very obvious to operators that instrument indications have failed. The procedure also has sufficient cautions that indications can become unreliable in fires, and also the operators would clearly understand that conflicting and nonsensical indications cannot be trusted. This is considered equivalent to warning/alternates in a procedure. It was stated that this is also covered in training.

However, the cues in the procedure for abandonment are not completely definitive (the Shift Manager still has to make a determination based on judgment that the plant cannot be controlled from the MCR).

Procedures:
Cognitive: Fire Response- Cable Spreading Room
There are two possible entry conditions into the CSR fire procedure; automatic fixed suppression actuation or visual confirmation of CSR fire.

Step: 11

Instruction: ASSESS IF CONTROL ROOM EVACUATION REQUIRED

Normal Charging in-service and controlling pressurizer level between 20% and 60%

RCS Pressure Stable or Trending to 2235 psig

RCS Temperature Trending to 547F

All vital 4KV Buses Energized

Steam Generator levels in at least 2 generators trending to 65% Narrow Range Level

Shift Manager determines plant control not available in the MCR

This action models cognition only. There are no execution sub-tasks required for success.

Assumptions:

High workload is assumed due to fire conditions.

Timing:

The operator must abandon the MCR within 25 minutes of the start of the fire.

It will take approximately 10 minutes from the start of the fire until the cues for the decision to abandon will be established in the MCR. Once cues for abandonment are present it will take the shift supervisor approximately 1.5 minutes to make the decision to abandon.

Training: MCRA scenarios are trained on in the class room once every two years at a minimum.

Manpower: The shift supervisor is responsible for making the decision to abandon.

Communications:

While command and control is inside the MCR, face to face communication with 3 way communication will be used. Once the shift supervisor has made the decision to abandon, he will hold a short crew brief to inform all control room operators what is going on. Then just prior to abandoning, an RO will make an announcement that the MCR is being abandoned due to a fire.

Location: This action takes place in the MCR.

MCRAHFE2: Operator Fails to Transfer Controls to RSDP After Decision to Abandon MCR

Summary of HFE:

This action is predicated on the operators successfully making the decision to abandon. This HFE addresses the actions operators take inside the MCR prior to leaving the control room (e.g. tripping the reactor and reactor coolant pumps, dispatching an operator to be stationed at the RSDP, isolation of letdown) and the subsequent implementation of procedure steps to set up control from the RSDP.

The high level task required for success of this action include:

1. Ensure reactor trip from inside the MCR

2. Close the MSIVs and bypass valves from inside the MCR

3. Trip all RCPs from inside the MCR

4 Transfer charging suction to the RWST from inside the MCR

5. Establish control at the remove shutdown panel. This involves turning three hand switches at the RSDP.

The consequence of failure of this action is core damage.

Cues and indications:

This action is predicated on the operators successfully making the decision to abandon. Once the decision to abandon has been made then the expected plant response is that operators will following the MCRA procedure. Therefore, this action models execution and cognition is based on the decision to abandon.

Procedures:

Procedure OP 1 directs operators to commence procedure OP 2A upon the decision to abandon MCR. Operators need to Implement Att. 4 and Appendix F of OP 2A to set up for control from the RSDP.

OP 1,

Step 4. Ensure Reactor Trip

Step 5. CLOSE the MSIVs and Bypass Valves

Step 6. TRIP ALL RCPs

Step 8. TRANSFER Charging Suction to the RWST

OP 2A - Step 12. ESTABLISH Control from Remote Shutdown Panel

Timing:

Operators have 60 minutes from the start of the fire to avoid core damage by starting an MD AFW pump and/or a charging pump. It was estimated that operators will have 25 minutes from the start of the fire to determine if abandonment is required and the remaining 35 minutes are allotted to the execution portion of abandonment. The execution portion was estimated by using operator simulator data. An average of 4 minutes is conservatively used as the manipulation time for the in-MCR actions and an average of 3.25 minutes for the actions to establish control at the RSDP. However, operator interviews indicated that operators have often times delayed execution of actions because of increased stress because of the limited capabilities of the RSDP. Conservatively an estimate of 6.5 minutes is used for the actions to enable the RSDP, leading to an overall manipulation time of 10.5 minutes.

Training:

There is bi-annual training on the fire and MCRA procedures, which covers the topics in the OP 2A Lesson Guide and the System Training Guide for the RSDP. The simulator includes a real mock-up of the RSDP and it actually transfers control from the MCR. The simulator training staff interject realism into the simulations by saying how overloaded people are and sometimes telling the operators that someone is no longer available if they have been tasked with too much to do during the simulation. They also interject time delays to allow time for task performance.

Manpower:

The shift supervisor is responsible for making the decision to abandon and for giving the cue to the other operators to take the actions to enable the RSDP. The actions required in OP1 will be performed by a

single RO and peer checked just before leaving the MCR. Once at RSDP the shift manager will designated a specific person responsible for manipulation of all

Location: This action takes place in both the MCR and the RSDP.

The MCR is on the 140' level of the Aux Building. The stairs would take the operators down to the RSDP on the 100' level.

MCRAHFE5: Failure to Perform DHR Function via AFW MD Pump 3 at RSDP (Non-LOCA scenarios)

Summary of HFE:
After successfully transferring control to the RSDP, operators will go through procedure OP 2A and will realize the need to provide Decay Heat Removal to the RCS, then operators will start AFW.

The high level tasks required for this action include

1. Diagnosing the need to start AFW.

2. At RSDP Take MAN-AUTO switch to MANUAL and start the AFW pumps and place AFW Supply to Manual for Affected SG.

The consequence of failure of this action is core damage.

Cues and Indications:
Initial Cue:
AFW Flow (Low)

Additional Cues:
Steam Generator Level (RSDP indications: LI-201 through LI-204)

Procedures:
OP 2A, Step 20. CHECK AFW System Status

Step 20.a (RNO). Take MAN-AUTO switch to MANUAL and start the AFW Pumps

Step 20b. (RNO). Place AFW Supply to Manual for Affected S/G

Timing:

Operators have 60 minutes from the start of the fire to avoid core damage by starting an MDAFW pump and/or a charging pump.

Decision to abandon is made at T= 25 minutes

Time to Transfer Control to the RSDP after the decision to abandon is 35.5 minutes from the start of the fire.

The cue for the AFW action becomes available at 4.5 minutes, based on the time it takes for operators to get to step 20 of procedure OP 2A from simulator exercises. The time operators take to monitor the parameters described in Step 20, AFW pumps running, until they realize that they need to recover the secondary heat removal capabilities via AFW pumps is estimated to require only 0.5 minutes since it is a very easy and straight forward step.

The time it will take once operators transfer control and realize that they need to start AFW pumps is estimated as 10 minutes, based on the allotted time operators have to complete JPM-055.

Training:

There is bi-annual training on the fire and MCRA procedures, which covers the topics in the Lesson Guide and the System Training Guide for the RSDP. The simulator includes a mock-up of the RSDP and it actually transfers control from the MCR. The simulator training staff interject realism into the simulations by saying how overloaded people are and sometimes telling the operators that someone is no longer available if they have been tasked with too much to do during the simulation. They also interject time delays to allow time for task performance.

Manpower:

The shift supervisor is responsible for making the decision to abandon and for giving the cue to the other operators to take the actions to enable the RSDP.

Communications:

Once command and control is outside the MCR the communication protocol is to communicate via face-to-face is possible. In some instances, local operators (not at the RSDP) will need to communicate with operators at the RSDP and in these actions radios will be used. Prior to leaving the MCR each operator will pick up a pre-staged radio. For starting the AFW pumps at the RSDP face-to-face communication is all that is required.

Location: This action takes place at the RSDP.

5.9 References

1. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
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.

6
FEASIBILITY ASSESSMENT FOR MCR ABANDONMENT

This section provides overall guidance for performing a feasibility assessment for MCRA scenarios and associated HFEs. Certain aspects of feasibility assessment are also discussed in the following sections of this report:

- Section 3, Modeling MCR Abandonment in Fire PRA
- Section 4, Analysis of Decision to Abandon
- Section 5, Identification and Definition for MCR Abandonment
- Section 7, Timing and Timelines for MCR Abandonment
- Section 8, Performance Shaping Factors for MCRA Scenarios

6.1 Introduction

Section 4.3 of NUREG-1921 [1] discusses feasibility assessment in the broad context of operator actions during a fire at a NPP. Specifically, in NUREG-1921, within the context of fire HRA, *feasibility assessment* is the qualitative consideration of whether the operator action is go/no-go, considering the most influential PSFs. A review of NUREG-1921 Section 4.3 is recommended to better understand the considerations inherent in a feasibility analysis done as part of a fire HRA.

Additional guidance is provided in NUREG-1852 [2] on assessing the feasibility of local fire operator manual actions (OMAs)[16] performed outside the MCR— upon detecting a fire to either protect critical safety equipment that might be failed or might be spuriously affected and rendered unavailable by the fire, or to manually align locally critical safety equipment to perform its function when needed. NUREG-1852 defines a feasible OMA as one "that is analyzed and demonstrated as being able to be performed within an available time so as to avoid a defined undesirable outcome." It should be noted that NUREG-1852 combined feasibility criteria with reliability criteria such that if all the criteria are met the operator action would be highly reliable. However, NUREG-1852 does not provide a definition for "highly reliable." Therefore, in some cases, the feasibility criteria for the HRA, provided in this report or in NUREG-1921, may be less restrictive than what is specified in NUREG-1852, since the ultimate goal of the HRA is to quantify the reliability rather than simply make a distinction between deterministic concept of "highly reliable" versus "not highly reliable."

The basic purpose of a feasibility assessment per NUREG-1921 is unchanged for MCRA scenarios. Also, as discussed in NUREG-1921 and in Section 5 of this report, MCRA feasibility

[16] Note that for plants transitioning to NFPA 805, there are special considerations for MCRA OMAs and their treatment as NFPA 805 recovery actions, as discussed in RG 1.205, Section 2.4, Recovery Actions.

assessment will be an iterative process throughout the MCRA HRA. In other words, MCRA feasibility is likely to be performed initially when operator actions and HFEs are first identified, then again as further information becomes available to the qualitative HRA (and later, during HRA quantification).

However, there are some important differences that are unique to MCRA feasibility and further discussed in this section. Namely,

1. Because an unfeasible MCRA HFE or scenario may not be an acceptable final result for the HRA/PRA, the HRA analyst maybe involved in identifying and defining what improvements could be made that would change the assessment to "feasible." This role for MCRA HRA analysts is different than that for analysts performing HRA for other fire HRA scenarios and HFEs.
2. Feasibility assessments should be performed at the individual HFE AND at the scenario level for MCRA scenarios.
3. Criteria for MCRA feasibility assessment have been expanded to address additional factors that are important to the MCRA context. In addition, both these expanded criteria and the different context(s) for operator activities outside the MCRA require additional information collection and assessment. (See Appendix C for more guidance on information collection.)

6.2 Feasibility Assessment – Scenario Level versus Human Failure Event

Feasibility assessments are usually performed at two points in the development of the PRA models. The feasibility of scenarios is assessed when first developing the accident sequence (event tree) models to determine if potential branches in the tree could occur or were infeasible (and therefore not modeled further). An operator action feasibility assessment is performed once the accident sequences have been developed in the PRA model to determine whether specific operator actions can be considered for detailed assessment using HRA methods or should be not represented since they are infeasible.

6.2.1 Scenario Feasibility Assessment

In internal events PRA and most of fire PRA, scenario-level feasibility is typically performed in the accident sequence analysis task, and may not involve input from the HRA analyst.

However, for MCRA, the level of involvement by the HRA is different. As discussed in FAQ 13-0002 [3], "Main control room abandonment is a complex issue in that the PRA modeling consists of a wide range of scenarios and the plant response consists of a collective set of operator actions." Consequently, a different approach is needed for scenario feasibility assessment. Namely, the HRA analyst **will need** to be involved in this assessment.

Section 3 provides guidance on the interaction required between various fire PRA tasks to define MCRA scenarios, including the consideration of situations where success is not possible given the plant design and current operating approach.

Scenario feasibility assessment begins with the accident sequence development and ends with the HRA quantification of individual actions and is evaluated by demonstrating that the following criteria can be met:

- The plant design and shutdown strategy can mitigate the PRA scenario. This includes review of the procedures to ensure that actions required by the fire PRA are included in the procedure guidance and review of systems and components operability and availability with respect to the given scenario.
- There is sufficient time to complete the collective set of actions. This includes all actions required after the start of the fire.
- A walk through or talk through of the given scenario confirms that there is sufficient manpower available to support all required actions within the required time.
- Once outside the MCR, the plant has identified and defined a command and control structure and operators have been trained on their expected roles and responsibilities following MCRA.
- If communication is required once outside the MCR, then the plant has defined a communications strategy and has shown that any required hardware (e.g., radios or phones) will be available and not impacted by the fire.
- For loss of control scenarios, the criteria for abandonment have been defined and the operating crew is aware of the need to abandon for the given scenario.

Examples of MCRA scenarios that were determined not to be feasible by a fire PRA are:

- Based on a review of procedural guidance and capabilities of the RSDP, it was determined for one plant that feed and bleed actions were not feasible from the RSDP. This action was not analyzed further and was not credited in the abandonment portion of the fire PRA model.
- At another plant, closure of MSIVs from the RSDP was not credited for MCRA. Even though these actions were included in the MCRA procedure, the operator actions were not developed for the fire PRA/HRA because a circuit analysis showed that MSIV control from the RSDP could be lost.
- For a loss of control scenario, 11 SRVs spuriously open at the same time as reactor trip and the start of the fire. With 11 SRVS opening at the same time, the operators only have 13 minutes to respond before core damage. Closing 1 SRV (outside the MCR) takes approximately 15 minutes and therefore the overall scenario is determined to be not feasible.

In summary, the HRA analyst obtains information from the accident sequence analysis and the fire modeling task on fire-induced failures that may lead to abandonment and that may make certain scenarios infeasible, as well as the variations of functions that are required to be implemented for successful safe and stable shutdown. The MCRA HRA analyst then conducts the initial review of the MCRA and related procedures to identify functions that can or cannot be implemented at the RSDP.

Using this information, the HRA analyst then scopes out individual MCRA HFEs and subjects them to the feasibility criteria discussed in the following subsection.

There are iterations that occur between the scenario feasibility and the individual HFE feasibility assessments. NUREG/CR-6850 [4] Task 11.b guidance suggests that timelines developed for MCRA scenarios should be evaluated for feasibility as follows. "…accident sequence timing modeled in the plant model (i.e., fault trees and event trees) should be compared with the alternate shutdown procedure timeline. The comparison should ensure that the planned operator action times upon which alternate shutdown procedures are based will be less than the operator actuation or recovery times postulated for the applicable fire-induced accident sequences."

Within a given MCRA scenario bin, there may also be different configurations involving various combinations of credited or non-credited functions, which may in turn be subsequently developed as individual HFEs, as shown in Table 5-2. Scenario feasibility assessments on the basis of time cannot be calculated until the individual HFE timing is developed and the combination of actions is compared to the overall timeframe by which the actions must be accomplished. Sufficient time must be assessed at the scenario level (i.e., for the collective or entire set of actions), taking into consideration potential dependencies between actions (e.g., "hold points" where Operator A waits to complete his/her actions until Operator B's actions are complete, as reported by the shift supervisor).

Examples of these timing evaluations are provided in Section 7.

6.2.2 Human Failure Event (HFE) Feasibility Assessment Criteria

Once MCRA scenarios have been identified (these can be grouped or binned, depending upon the strategy of the analysis[17]), the HRA identifies the relevant operator actions for the scenarios using the MCRA procedures.

The evaluation of feasibility is then performed at the operator action level, generally associated with a human failure event (HFE) as discussed in Section 6.4.

6.3 MCRA Scenarios – What to do if "feasible" is the only acceptable answer

Similar to other fire HRA/PRA scenarios, there may be MCRA scenarios and associated HFEs for which an assessment of "not feasible" is acceptable with respect to the fire PRA results. For example, the fire PRA for a specific NPP may not credit (per discussions in Sections 4 and 5) loss of control (LOC) MCRA scenarios because the actions are not feasible from the RSDP based on detailed circuit analysis or fire modeling. There may also be instances when "not feasible" is considered unacceptable for the overall fire PRA results.

In such cases, the fire HRA analyst along with PRA analysts, fire protection analysts and operations staff may be involved with identifying improvements in any of the following areas to ensure the PRA scenario is feasible:

[17] See Section 3.7 for guidance on grouping and binning MCRA scenarios.

- Remove initial modeling conservatisms from the PRA scenario description. This could include:
    - Refinements to detailed fire modeling to better understand the fire impacts.
    - Refinements to PRA model to credit additional systems/components, if required.
    - Refinements/improvements to the thermal hydraulic analysis to show additional time is available.
    - Review and confirmation of assumptions associated with the scenario/or action.
    - Collection of additional information to support the timeline.
    - Additional demonstrations (more than walk through or talk through) to show feasibility criteria can be met. A demonstration could also be used to collect or verify timing of key actions which may have been based initially on analyst judgment.
- Recommend procedure modifications, which could include:
    - Additional guidance on communication and command and control structure once outside the MCR.
    - Revisions to ensure the procedure guidance is in alignment with the PRA scenario.
    - Recommend that new procedure guidance be developed for actions/scenarios not currently included in the procedures.
- Recommend plant modifications be made to ensure action/scenarios are feasible.
    - Recommend that cables for important components be wrapped or re-routed to ensure they are not impacted by the fire.
    - Improve HMI of the RSDP if actions are currently not feasible from an HMI standpoint. NUREG-0700 [5] provides guidance on human factors and ergonomic design for main control room operator response to reactor trips that can be used as a measure for creating an environment for highly reliable operator response.
    - Improve plant design such that the scenario can be mitigated. For example, add additional back-up systems or automatic actuation features to the plant.

Being able to provide such feedback to the plant is one of the most important benefits of HRA/PRA. (Section 10 provides more discussion on examples of the kind of feedback to the plant that fire HRA/PRA can provide.) However, there may be some aspects of the MCRA scenario/HFE context that are unalterable (e.g., time available for operator actions, accessibility of the action location, operability of relevant components and systems), making it unlikely that the scenario and/or action can be credited in the fire PRA.

The approach taken by the HRA/PRA team will be highly plant-specific and could be resource intensive, depending on the level of detail required to ensure feasibility. Operations staff are likely to be the most useful resources in identifying workable improvements. However, there

may be resistance to some improvements (e.g., modifying procedures). It may be necessary to demonstrate the source of the infeasibility to operations (e.g., show them the timeline that indicates there is insufficient time to complete the tasks) to get their feedback and buy in on these changes.

6.4 MCRA Feasibility Assessment Criteria

The criteria presented in this section guide the analyst through the conditions likely to affect feasibility of an action. If the action is not feasible, an HEP of 1.0 is assigned, or the HFE is not credited in the fire PRA. For actions determined to be feasible, further qualitative assessment is performed as discussed in the Timeline (Section 7) and PSF (Section 8) sections that provide input to the quantitative evaluation of the likelihood of success of the operator action.

Note that the feasibility assessment criteria align closely with the PSFs discussed further in Section 8 and may inform the PSF analysis, but the focus is different. The feasibility assessment uses the criteria to make a “go/no-go” evaluation of an HFE; this should not be substituted for the more in-depth analysis of the PSFs that is done once an action has been determined to be feasible.

Feasibility assessment criteria for MCRA are discussed in this section as follows:

1. Additional criteria specific to MCRA, and
2. Feasibility criteria from NUREG-1921 clarified to address the context of MCRA.

In addition, Section 4.3.4 discusses some feasibility considerations that are specific to modeling the decision to abandon.

6.4.1 Human Failure Event (HFE) Feasibility Assessment Criteria

For non-abandonment scenarios, the command and control structure is well established and communications inside the MCR are generally considered to be face-to-face, leading to a negligible PSF. However, based on review and understanding of MCRA scenarios, additional feasibility assessment criteria are needed to address: (1) changes that occur in the shift in location of command-and-control (discussed in detail in Appendix B) when the MCR is abandoned and (2) the fact that communications can become a significant PSF, and in some cases prevent the success of the action. These issues are discussed further below.

6.4.1.1 Command and Control

Command-and-control is simply defined as "the exercise of authority and direction" [6], and more specifically, as the need for a central body of authority to make decisions but have them carried out by a distributed group. In the MCR, the shift supervisor, supported by the STA and shift manager, is the focal point for command-and-control. Following a reactor trip the shift supervisor's direction in implementing the EOPs is the expected and principal display of command-and-control.

In contrast, depending on the RSDP capability and plant procedures, changes in command-and-control for MCRA with respect to the existing feasibility assessment factors for in-control room may include:

- Staffing:
    - Fewer staff available to directly support command-and-control (e.g., STA and shift manager may have other duties and be assigned at different locations)
    - Command-and-control must direct, and possibly coordinate, more staff than were needed in the MCR for the same shutdown activities
- Cues:
    - Instrumentation supporting decision-making by command-and-control may not be available (e.g., no alarms at remote shutdown panel) or only available at a local panel
- Procedures and Training:
    - Command and control structure may not be defined in emergency response plans or procedures
    - Training for MCRA may not include specific command-and-control activities at the RSDP (e.g., communications/coordination with field operators) or specific delegation of field operator responsibilities

Criteria: In order for an action or scenario to be feasible, there must be a pre-defined plan for command and control once outside the MCR. Additionally, operators should be aware of their expected roles following abandonment.

As a result of the above considerations, staff responsible for command-and-control are likely to experience a need for more and different communication (e.g., phone or radio, rather than mostly face-to-face). For this reason, "Sufficient Communications" has been added as a feasibility assessment criterion for MCRA.

6.4.1.2 Sufficient Communications

NUREG-1921 did not consider communications as a separate feasibility criterion and instead addressed parts of it under ‘Sufficient Manpower’. However, given the importance of communication between multiple crew members across multiple locations for MCRA actions, it is called out as a separate factor. For MCRA scenarios, the likelihood that the crew are primarily reliant on two-way radios or other forms of distance communication (e.g., sound-driven phones) is greatly increased with the need to distribute crew around the plant both to perform local actions and to potentially monitor cues and parameters. Communications are required for relaying tasks and for ensuring sequential tasks or tasks requiring coordination are performed correctly. As NUREG-1852 states, “therefore, effective communications equipment, to the extent it is needed, should be readily available and meet the functionality and accessibility criterion.” In addition, assessment of communications should include consideration of possible background noise and inter-unit communications using the same frequency (if a two-unit shutdown is required).

Criterion: Feasibility in this case means that the plant has a clear communications plan in place and any equipment (radios, phone) required to implement the communication plan is available and not impacted by fire damage.

6.4.2 MCRA Specific Issues in Existing Fire HRA Feasibility

This section summarizes the MCRA-specific differences in evaluating the feasibility assessment criteria given in NUREG-1921.

6.4.2.1 Sufficient Time

Determining that sufficient time exists for diagnosing and completing a given action or a set of actions for a particular HFE is critical for assessing its feasibility. Section 7 on timeline development provides detailed guidance for assessing scenario and HFE timing for MCRA.

For MCRA, the time required to make the decision to abandon is particularly important and factors into the subsequent ex-MCR actions as well. In addition, extra time needed for communication between operators, or between operators and command-and-control, must be included in the time required to complete the action. This extra time should include consideration of the potential workload increase related to command-and-control.

Criterion: If the time required to perform all the task(s), taking into account any dependencies and/or coordination between actions, is less than the time available (including time required to access necessary plant locations), the MCRA scenario/HFE is determined to be infeasible.

6.4.2.2 Sufficient Staffing

The feasibility assessment for MCRA should consider whether there are sufficient personnel available to support the varied and dispersed actions. For a fire scenario this becomes critical in the consideration of a sufficient number of trained personnel that will not be concerned with other duties such as serving on the fire brigade. For MCRA actions, the number of crew members required may be increased due to the significant number of local actions and ex-control room locations to be visited. Also, staffing for command-and-control should be addressed.

Once the decision to abandon has been made, all U.S. plants have procedure guidance to ensure that for the design basis MCRA scenarios there will be sufficient staff available to fight the fire and perform the required actions. However, there could be PRA scenarios that require more actions than the design basis scenarios and the availability of crew members must be verified to ensure there is sufficient manpower.

Criterion: Following MCRA, there should be sufficient staff available to support command and control at the RSDP and to perform all the required local plant actions. Crews should be able to demonstrate this during walk-throughs or simulator exercises that include simulation of local actions in order to validate that the crew can be positioned at all required plant locations to complete all the tasks in the various MCRA scenarios properly and in time.

6.4.2.3 Primary Cues Available / Sufficient

In general, this criterion for feasibility follows the same definition and concerns as identified in NUREG-1921 and focuses on the assumption in HRA that all operator actions are taken in response to cues.[18] Following MCRA, the crew may be relying upon cues and indicators that are less obvious (e.g., no alarms like that in the MCR at the remote shutdown panel) than those presented in the MCR or less easily used (e.g., cues are only available on local panels). It will be even more important in these settings that sufficient cues be available for directing the operators' actions. The analyst needs to identify the cues necessary for diagnosing the required MCRA actions and whether the instruments supporting the necessary cues:

- Are available to support the decision to abandon the MCR, and
- Have been verified to be protected from the fire effects to support post-abandonment actions.

The fire PRA equipment (component) selection task is responsible for determining the availability and functionality of these cues, so the MCRA HRA analyst needs to interface with that task.

Examples of the types of cues that need to be evaluated for availability and functionality are:

- Fire alarm in the Cable Spreading Room (CSR), MCR, or other potential abandonment location.
- Indications of:
  - Automatic fixed suppression initiated;
  - Pressurizer Level;
  - RCS Temperature;
  - Vital 4Kv Buses Energized;
  - Steam Generator Level;
  - Normal Charging.

Criterion: If all cues required for success of an action (or scenario) are unavailable then the action is considered to not be feasible. For those actions occurring after abandonment has occurred, the cues necessary at the RSDP must be available at the RSDP or be available to locally stationed operators to allow credit for the action.

6.4.2.4 Proceduralized and Trained Actions

NUREG-1921 discusses that the feasibility assessment should address the availability and applicability of procedure guidance. There are some fire PRA MCRA scenarios for which the existing procedure guidance does not include the required actions and if the procedure guidance is followed, the PRA scenario will still result in core damage. Therefore, all actions required by the fire PRA should either be addressed by procedure guidance or be considered skill of the craft

[18] A cue may be instrumentation, a procedure step, or a plant condition.

actions in order for the action to be deemed feasible. The MCRA HRA analyst should note that procedure and training guidance could come from a variety of documents, such as:

- MCRA Procedure
- AOP for Fire Response – Fire in Cable Spreading Room
- Instructor Lesson Guide on MCRA
- System Training Guide: Remote Shutdown Panel

The coordination of actions required after MCRA can be complex due to coordination required among operators at various locations (see also Command and Control). The procedure guidance should account for this coordination and communication.

Criteria: There are two sets of MCRA criteria related to proceduralized and trained actions:

Criterion 1: Each of the following needs to be affirmative for the procedure and other trained actions to be considered feasible:

- Procedures exist for the MCRA scenarios identified by the PRM/FSS tasks and include the actions needed for the MCRA scenarios.
- Training covers the procedure steps included in the MCRA scenarios and have been demonstrated to be viable through walk-throughs or observation of simulator exercises to account for coordination and communication.

Note that feasibility is determined based on whether the procedures and training are so deficient that the MCRA actions would not be able to be performed. Otherwise, the evaluation would be related to procedure and training PSFs as part of the qualitative analysis that evaluates action reliability.

Criterion 2: Other non-PRA actions incorporated in the procedures should not prevent the PRA-related actions from being completed in time. (Note that this criterion correlates to the timeline development discussed in Section 7).

6.4.2.5 Accessible Location

The location(s) where the action(s) must be completed, the location of command-and-control, and any travel path must be evaluated to determine feasibility of the action. If any of these locations are inaccessible, the operator action should not be considered feasible. In addition, the travel path(s) of the operators should be reviewed to ensure that the defined access route is not blocked for any of the following reasons:

- Smoke and toxic gas effects caused by the fire
- Obstruction, such as from charged fire hoses
- Heat stress
- Radiation. For the feasibility analysis, the analyst needs to determine whether the radiation level or rating of an area would preclude access or otherwise prevent the action from being feasible. Also to be considered is any extra time that may be needed to prepare for entering such areas (e.g., the need to done personnel protective clothing).

- Locked doors. The fire may cause electric security systems to fail locked. In this case, the operators will need to obtain keys for access. If all operators do not routinely carry the keys to access a secure area, the HRA analyst must ensure that there is enough time for the operators to obtain access. Normally locked doors should also be considered.
- Lighting. Analysis should determine that the lighting is adequate for the action area as well as the areas to be traversed.

Criterion: Each MCRA action location, including command and control actions, must be shown to be accessible through a detailed walk-through or talk-through that addresses: (1) reaching the location, and (2) remaining in place for the needed duration of the action(s).

6.4.2.6 Availability and Accessibility of Equipment and Tools

The only difference for this criterion for MCRA beyond the guidance provided in NUREG-1921 is that since the RSDP will (most likely) be where command-and-control is located, keys (and other equipment and tools, such as radios and flashlights) that are ordinarily the responsibility of MCR staff must be obtained during the actual MCR abandonment and taken to the RSDP. In addition, HRA analysts must verify that the tools and equipment required for local MCRA actions will be available and functional when needed.

Criterion: The ability to gather necessary tools and equipment (including protective gear such as SCBA), get them in place, and demonstrate their use should be shown in a detailed talk through, walk down, or training exercise to be considered feasible within a MCRA scenario.

6.4.2.7 Operability of Relevant Components and Systems

Beyond what is already stated in NUREG-1921, the key point for MCRA in determining feasibility is an evaluation of the availability of the required controls at the RSDP or at local control stations and a confirmation of their functionality during MCRA fire scenarios (the latter may require input from the fire PRA and fire modeling tasks).

6.5 Example Feasibility Assessment

Table 6-1 provides an examples of feasibility assessments for MCRA according to the feasibility criteria presented earlier. These are intended to illustrate to the analyst the thought process involved in performing the assessment. Summaries such as these provide useful documentation tools for feasibility assessment.

Table 6-1
Example MCRA Scenario Feasibility Assessment Summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
1	Command and Control	A central body of authority has been identified to make decisions for MCRA but have them carried out by a distributed group.	The MCRA procedure is organized with the main body of the procedure associated with Control Room Supervisor (CRS) actions to direct the evacuation process and the actions taken by the other operators through the use of separate attachments of the procedure. The CRS remains stationed

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
			at the RSDP and communicates with and coordinates the actions of the following operators, each of which follows a specific procedure attachment: 1. Reactor Operator 2. Balance of Plant Operator 3. Aux Building Operator 4. Intermediate Building Operator 5. Electrical Maintenance Technician
2	Sufficient Communications	The communications system should be evaluated to determine the availability of communication, where required for coordination of actions.	As referenced in the administrative procedure, communications consist of pre-job briefs, three-way communication, and use of the phonetic alphabet during any communication having to do with the operation or manipulation of plant equipment. A new plant Radio Repeater System for use by plant Operations, Maintenance and Fire Brigade personnel is being installed to meet emergency communications requirements. The existing plant paging system is considered as a back-up system.
3	Sufficient Time	Sufficient time to travel to each action location and perform the action should exist. The action should be capable of being identified and performed in the time required to support the associated shutdown function(s) such that an unrecoverable condition does not occur. Previous action locations should be considered when sequential actions are required.	The most conservative times from the timed plant walkdowns conducted by plant operations were utilized to evaluate the feasibility and reliability of the HFEs in the MCRA HRA.
4	Sufficient Staffing	Walk-through of operations guidance (modified, as necessary, based on the analysis) should be conducted to determine if adequate resources are available to perform the actions within the time constraints (before an unrecoverable condition is reached), based on the minimum shift staffing. The use of essential personnel to perform actions should not interfere with any collateral industrial fire brigade or control room duties.	The minimum staffing consists of 2 SROs (control room supervisor and the shift supervisor), 2 Reactor Operators (ROs), an STA, and 5 non-licensed operators. Three of the five non-licensed operators are on the fire brigade. The five non-licensed operators consist of a control building operator, upper and lower auxiliary building operators, intermediate and turbine building operators. The shift manning sheet ensures that operators who have fire brigade duties are not responsible for emergency manual actions. The MCRA procedure is organized with the main body of the procedure associated with Control Room Supervisor (CRS) actions to direct the evacuation process and the actions taken by the other operators and the Electrical Maintenance technician through

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
			the use of separate attachments of the procedure. The MCRA procedure has been evaluated through timed walkdowns to validate that the actions can be performed properly and within the time required with the staff assigned.
5	Primary Cues Available/Sufficient	Consider availability of cues and indications essential to perform the action.	The operator actions credited after MCRA are either taken at the RSDP or locally so the indications at those remote locations have been validated as being available through the Fire PRA cable routing and circuit analysis, as documented in the Fire PRA Equipment Selection Notebook.
6	Operability of Relevant Components and Systems	Consider availability of systems and components essential to perform the action.	The availability of systems is addressed by the fire PRA model and the scenario to which the MCRA HEP is applied. For example, separate SBO-related HEPs were developed to address the unavailability of power and the need to locally start the diesels and strip loads from the associated busses. The operability of the RSDP and remote action locations for the MCRA fire scenarios have been verified through circuit analysis and cable tracing.
7	Proceduralized and Trained Actions	Written procedures and training should be provided. The proposed actions should be verified in the field to ensure the action can be physically performed under the conditions expected during and after the fire event. Furthermore, periodic drills should be conducted that simulate the conditions to the extent practical (e.g., communications between the control room and field actions, the use of SCBAs if credited, the appropriate use of operator aids).	The HRA team participated in an interview and a plant walkdown of the key steps of the MCRA procedure with a Senior Reactor Operator (SRO) to collect information on the MCRA process, procedures, and training. The MCRA procedure provides step-by-step instructions for the operations crew for the actions required to successfully avoid core damage by bringing the plant to a safe and stable condition. Operators receive Licensed Operator re-qualification training every 5 weeks. With Administrative weeks (such as Fire Brigade training), this positions operators in the simulator about 7 times/year (depending on refueling outage schedules). Subsequent to the site visit, the operations staff conducted several timed walkdowns of the procedure. The timing and insights obtained from the site visit walkdown and the operations walkdowns validated the feasibility of the actions and provided input to the information used in the HRA

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
			Calculator files to estimate operator action reliability. The MCRA procedure is part of a new set of safe shutdown procedures. The walkdowns by operations were used to optimize the procedure and insights from these walkdowns are being factored into the training process. Operators are commonly re-trained on fire procedures every two years. The walkdowns of the MCRA procedure provided drills in that they simulated the communications, tools implementation and SCBA use to the best extent possible. The walkdowns were timed to evaluate feasibility and efficacy of communications and use of operator aids and were used to optimize the procedure to ensure that operators could efficiently enact the procedure steps required. Going forward, the plant will conduct drills on this procedure as part of bi-annual training.
8	Accessible Location	The area being visited and any areas required to be traveled through should be shown to be tenable and the fire or fire suppressant damage should not prevent the action from being performed. Specific elements within the area (e.g., lighting level, locked doors, and radiation level) should be evaluated.	The MCRA procedure is implemented for the case of fires that occur in fire areas that impact the control room and cable spreading room. All MCR scenarios were walked down by the PRA/HRA team to identify the travel path and identify any accessible issues which may be caused by the fire. Emergency lighting is controlled by a fire protection procedure, which currently requires monthly operational testing of each 8 hour emergency lighting unit and following maintenance to verify that all lamps illuminate the appropriate equipment / target or means of access / egress. The walkdowns of the MCRA procedure evaluated the availability of adequate emergency lighting in the locations where the MCRA actions are performed. A plant modification will include relocation of lights in switchgear rooms to ensure the cubicles for the RCPs are illuminated. Impacted maintenance and test procedures will be updated based on identification of the required emergency lighting units and their mission duration.

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
			To perform all actions credited after abandonment, the expected travel routes do not included any locked doors or special access restrictions.
9	Availability and Accessibility of Equipment and Tools	Any tools, equipment, or keys required for the action should be available and accessible. This includes consideration of SCBA and personal protective equipment if required. (This includes staged equipment for repairs).	A fire protection procedure provides the LCOs/Actions/Surveillances for fire protection-related emergency tools. The tools and equipment used in the MCRA procedure are implemented using an administrative procedure, which provides an example of the equipment that is contained in the RSDP emergency tool locker and is inventoried on a quarterly basis. The availability and accessibility of tools required for the actions, as cited in the MCRA procedure steps, were verified during the timed walkdowns performed by plant operations. The site walkdown also verified that the tools and equipment required for the MCRA actions were available per the fire protection and administrative procedures.

6.6 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.:2012. 1023001/NUREG-1921.
2. U.S. Nuclear Regulatory Commission. NUREG-1852*, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,* Washington, D.C. October 2007.
3. Nuclear Energy Institute, Fire PRA Frequently Asked Question (FAQ) 13-0002, "Modeling of Main Control Room (MCR) Abandonment on Loss of Habitability," August 2013. Available through ADAMS Accession Number: ML13249A249.
4. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD: 2005. EPRI 1011989 and NUREG/CR-6850.
5. U.S. Nuclear Regulatory Commission. NUREG-0700 Revision 2*, Human-System Interface Design Review Guidelines,* Washington, D.C. May 2002.
6. Globalsecurity.org, Mission Command: Command and Control Army Forces. Last retrieved February 1st from: http://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm

7
TIMING AND TIMELINES FOR MCR ABANDONMENT

7.1 Introduction

In order to be consistent with the rest of the Fire PRA, the analysis of MCRA scenarios must adhere to the same fundamental considerations as the Fire PRA evaluation of fire areas and different fire scenarios, including timing considerations. The concepts that the *Time Available* must exceed the *Time Required* and that the amount of exceedance impacts the reliability of the action remain valid for MCRA. That being said, there are several differences, primarily additional considerations, that must also be taken into account in order to ensure that the MCRA actions are both feasible and reliable. The purpose of this section is to describe the timing considerations associated with MCRA, and to present an approach to overlay the various timing sources (timelines) into a single MCRA timeline. Note that throughout this document the term "MCR Abandonment" is meant to apply to evacuation of the main control room due to loss of habitability or transfer of command and control from the MCR due to fires in other areas that could lead to MCRA.

The development of the MCRA timeline serves several purposes. First, it helps the analyst to understand the plant response following a fire as it develops from ignition to damage followed by the actions associated with safe shutdown. Second, the timeline helps with the qualitative analysis by providing a means to check feasibility and providing insights on performance shaping factors (such as the relationship between procedures, training, communications and cues and the time required). Additionally, the timeline supports the quantitative analysis by providing a measure of the margin between the time required to complete all MCRA actions and the time available for response.

The timing considerations associated with MCRA HRA are different from fire HRA or internal events HRA because there are many overlapping relationships, primarily because multiple operators are involved in a collective, but distributed, response. There are normal fire PRA considerations for fire growth and suppression, plant thermal-hydraulic progression after the initiating event, component failure times (such as time to fire damage or time to battery depletion), and the operator response. However in MCRA, there are additional considerations for what happens in the MCR before abandonment, what happens during the decision to abandon, and what happens outside of the MCR after abandonment. Each of these phases typically consists of actions by multiple operators. NUREG/CR-6850 [1] Task 11.b requires that a planned timeline, with variations be developed for MCRA. Section 3.2.2 describes the link between the fire PRA modeling and the development of a timeline for MCRA scenarios.

Section 4.6.2 of NUREG-1921 [2] provides guidance on developing a timeline, but this guidance was limited to defining parameters associated with an individual action such as the system time window, the time of the cue and the time required for response. The guidance in this section builds upon that basis but will also address considerations due to a severe fire occurring in the

MCR or in a fire area that renders the MCR inoperable, and considerations for analyzing a collective set of operator actions that likely involve coordination, communications and long term control of plant parameters.

The MCRA timeline helps the HRA analyst understand the complex relationships between fire, plant response and the interactions among operators. By incorporating additional timing considerations into a single "picture", the HRA analyst will develop a better understanding for the plant response, which will improve the qualitative analysis and provide input to a better operational narrative; ultimately improving the feedback to plant operations, procedures and training as described in Section 10.

Development of the MCRA timeline includes integrating timing information from several different sources; fire progression, accident progression, procedure progression are all linked via a common reference point or reference points. The MCRA timeline collects information from each of these sources and provides a chronological description of the scenario progression. Each source must be considered with regard to its potential impact as part of the overall MCRA analysis. This timeline, in conjunction with the detailed scenario description, provides the required context for the qualitative analysis.

To understand the collective set of operator actions required for MCRA, the timeline can be conceptualized as consisting of the following three time phases. Each phase is described further in Section 7.2.

- Phase I – Time period before the decision to abandon.
- Phase II – Time period for the decision to abandon
- Phase III – Time period after the decision to abandonment has been made.

7.2 MCRA Timeline and Time Phases

The MCRA timeline requires integrating timing information from the following sources:

- Fire progression, from ignition to damage including detection and suppression.
- Accident progression (event tree sequence) given the fire-induced initiating event, including the time of reactor trip.
- Procedure progression consisting of the expected operator response in transitioning through procedures (emergency procedures and/or fire response procedures) and executing the appropriate steps. This includes
    a. Time of abandonment
    b. Time of the cue for individual actions.
    c. Time each individual action is started
    d. Time at which critical procedure steps or procedure transfers are reached, including coordination among different operators
    e. Time each action is to be completed.

The MCRA timeline starts with fire ignition. Not all timing inputs are collected from the same starting point. For example, typically the thermal-hydraulic plant response timeline will define

T=0 as reactor trip, but the fire growth timeline will define T=0 as the start of the fire, and the operator response timeline sometimes start once the decision has been made to take an action. Using the same reference point helps the analyst to capture the complexity and multiple interactions of the MCRA scenarios. To understand the collective set of operator actions required for MCRA, the timeline can be conceptualized as consisting of the three time phases shown in Figure 1 below.

- Phase I – Time period before abandonment decision
- Phase II – Time period for the decision to abandon
- Phase III – Time period after abandon during which the transitional and post-abandonment shutdown actions are performed

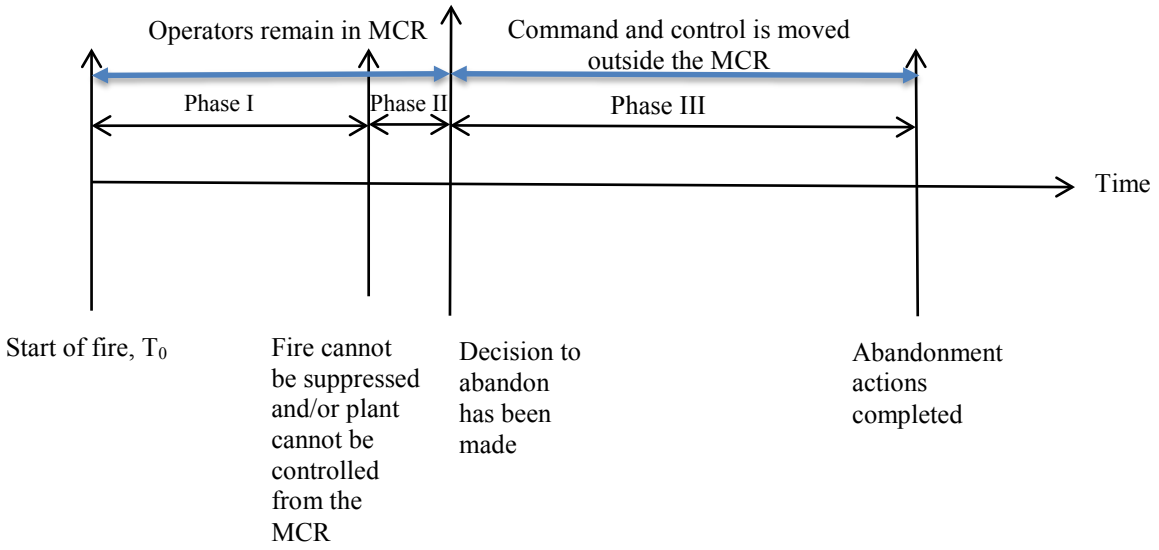

Figure 7-1
Three time phases of MCRA

Phase I is the time period before the operators recognize that abandonment may be required. This phase begins at the start of the fire and ends when operators recognize the severity of the fire damage. The cue(s) for MCRA could be one or more of the following:

- The fire cannot be suppressed and the smoke levels are becoming life threatening,
- Operators begin to believe that the plant cannot be controlled from the MCR, or
- The MCRA procedures direct the operators to abandon.

While in the MCR, command and control remains in the MCR and the operators inside the control room will be interacting with the fire brigade and performing any necessary control room actions, such as EOP and plant fire procedure actions.

Phase II is the time period associated with the decision to abandon. This phase starts when the operators receive the cue that indicates the severity of the fire and access the MCRA procedure to evaluate whether the criteria for abandonment have been met. Phase II ends when the decision

to abandon has been made. This time period includes the three elements of cognition: detection, diagnosis, and decision making. The detection of the fire should be obvious and will be completed in Phase I. The detection in Phase II is related to detecting fire damage and fire growth such that loss of control can be diagnosed. Detection of fire damage may require local confirmation of operability of a system if its status cannot be determined in the MCR.

As discussed in Section 4, LOH in the MCR can result due to a fire in the MCR or due to a fire in a nearby compartment wherein smoke may enter the MCR rendering it uninhabitable. The decision to abandon the MCR is assumed to be forced due to untenable environmental conditions within the MCR. Therefore, it is assumed that there is no contribution from the failure to diagnose and decide to abandon the control room in time to execute a successful shutdown (i.e., the decision to abandon is considered to always be successful).

For loss of control scenarios, the time required to diagnose and make the decision that a particular fire has impacted the MCR to the point of requiring abandonment could be complex, depending upon the level of guidance provided in the MCRA procedure. At many plants, specific cues for abandonment are not provided in the MCRA procedure and the simulator training often does not specifically cover the decision-making process, with trainers instead providing the cue to abandon to the crew being trained. This leads to significant uncertainty in the operators' ability to reliably make the decision to abandon in time to safely shutdown the plant. For this reason, the HRA analyst should work with the PRA modeling team to identify the equipment and functional failures leading to MCR inoperability and recommend the inclusion of more specific abandonment cues based on these equipment/functional failures to the MCRA procedure. Detailed information on modeling the decision to abandon the MCR is provided in Section 4.

Phase III starts once the decision to abandon has been made. Most MCRA procedures contain specific actions that are required to be performed just before leaving the MCR. These actions could include reactor trip (if not automatic or already manually done), turbine trip, and isolation of critical MCR panels to allow control to be transferred to the RSDP. The time it takes to perform these actions should be incorporated into the overall operator response timeline and are considered to be in Phase III.

When the operators leave the MCR, command and control is moved from the MCR to the RSDP and locally at equipment manipulation points. The plant response typically consists of the following sub-parts:

- Actions required for completing the transfer of control to the RSDP, alternate shutdown panel, or local control stations (depending upon the plant-specific MCRA set-up).
- Local actions to implement systems and functions required for safe shutdown.
- Long term control of plant parameters.

Phase III should consider the time it would take to travel from the MCR to the RSDP. This time can range from less than a minute to greater than 5 minutes depending upon the plant layout. Once at the RSDP, it is not uncommon for the SRO[19] to review the next steps of the MCRA

[19] SRO is used here as an example of the person leading command and control after the decision to abandon has been made. Each plant will specify a person assigned to this role. It could be the SRO, RO, STA, or shift supervisor. SRO has been used here as an example title.

procedure with the crew before delegating procedure steps to them, often organized into specific procedure attachments. Then, the main objective is to establish control of the plant at the RSDP so that it can serve as the new command and control center to which the other operators report the status of their local actions. The operations team then takes actions to implement systems and functions, which may include time-critical actions, to bring the plant to a safe and stable condition. Further, depending on the plant's licensing basis these actions may, or may not, be defined as NFPA 805 recovery actions.

Phase III ends once the required systems and functions have been implemented, and operators are maintaining long term control of the plant. These long term control actions have a mission time based on the function or system being modeled, for example, the time to reach safe and stable conditions.

7.3 Timing Sources Used as Input to MCRA Timeline

The MCRA timeline integrates several individual timelines based on different information sources. This section identifies the different sources to review and incorporate as appropriate into the MCRA timeline.

7.3.1 Fire Progression Timeline

The fire progression timeline consists of fire ignition, growth, propagation, detection, suppression and times to component damage. The fire growth and suppression times are typically a function of the heat release rate, geometry of the MCR, and control room HVAC system line-up.

The fire progression timeline is used to develop inputs for both Phase I and Phase II of the MCRA timeline and provides the following key times within the MCRA timeline.

- Time the fire starts. This is typically defined at T=0.
- Time the fire is detected. In many cases this may be T=0. However, in other cases, it could take several minutes for smoke or component failures to develop.
- Time of the cue. The fire may provide a direct cue, for example fire in Cabinet X leads to specific section of fire procedure. Additionally, the fire may indirectly provide a cue via fire-damage to an SSC, such as when the fire fails an electrical bus causing reactor trip.
- Time at which fire suppression starts, to the extent that it is required to ensure realism in the dominant MCRA scenarios. Manual suppression is not addressed by the fire HRA but in the fire modeling task. Even when plant staff are used as part of the Fire Brigade (or until the fire brigade arrives), the staffing for MCRA has usually been specified such that sufficient personnel are available for safe shutdown actions, but this should be verified by reviewing the plant fire procedures and discussions during operator interviews.
- Time at which loss of habitability criteria are met. This time is based on when the smoke levels become life threatening and is primarily a function of fire damage, but it could also

be a function of the operability of the Control Room HVAC system and associated system alignment.

For loss of habitability scenarios, CFAST calculations or other fire modeling techniques can be used to determine the time at which the smoke levels becomes life threatening.

- Time at which fire is extinguished.
- In some cases, detailed fire modeling may be able to provide the times at which key components are impacted by the fire. However, in most Fire PRA MCRA scenarios the time to component damage is modeled conservatively such as "all components failed at the start of the fire". The expected operator response is highly dependent on when components are failed. If all components are assumed failed at T=0 then the operator response should reflect this assumption.

  In some scenarios, a component may spuriously start and run for a defined amount of time. In some cases, the spurious start may provide additional time for recovery of the system following failure. For example, in a PWR a spurious start of safety injection may provide additional time to core damage due to overfill of the pressurizer. If these times are known, they can be used in the MCRA timeline to provide a best estimate timeline.

In general, the fire progression timeline requires inputs from detailed fire modeling and the fire PRA fire modeling task. The more detailed fire modeling information is available, the less uncertainty there will be related to the timeline development.

7.3.2 Accident Progression Timeline

The accident progression timeline consists of the thermal-hydraulic modeling of the event tree sequence. As such, this consists of the progression from the initiating event, through success or failure of systems and actions modeled in response to the initiating event, to the point of core damage or a safe, stable end state. The progression includes the PRA success criteria for systems, components and operator actions. The accident progression includes the following timing information:

- Time of reactor trip
- Time of cues (T_{delay}) for individual actions
- Times for successful operator actions (if applicable)
- Times that component failures are modeled as occurring (if applicable)
- System time window (T_{sw}) for individual actions

The accident progression timeline links to the fire progression timeline through the times when components are failed, and the time of reactor trip. In most MCRA scenarios, the fire starts and all components affected by the fire are assumed to be failed at the same time.

It is important to identify the time of reactor trip with respect to the start of the fire because most thermal-hydraulic data collected to support the system time windows consider T_0 as reactor trip.

If the fire damage causes reactor trip, then the clock starts for many operator actions. However, if the reactor trip is delayed, then the clock starts later.

For most MCRA scenarios, the severity of the fire and loss of functionality of the MCR and significant systems and functions would be expected to lead to fire-induced reactor trip shortly into the scenario, if not immediately, and is therefore taken to occur at T_0.

The system time window (Tsw, See Section 7.4) start time for an individual HFE that models the implementation of a system or function after the MCR has been abandoned may be based on when SSCs are impacted by the fire. For example, an action to restore power to a DC bus by locally re-aligning the power supply could have success criteria based on battery depletion time. The time to battery depletion only starts when the batteries are demanded. This may or may not be the start of the fire, or may start once the operators remove power from the MCR just before abandoning. In addition to potential shifts such as these, the system time window may be longer depending on the system or function being implemented, such as long term control actions.

The accident progression timeline produces timing information related to cues that are a function of parameters being monitored by instruments, for example, RCS pressure, temperature and level (or SG level). The accident progression timeline generally starts with the success criteria from the internal events PRA model and uses additional thermal-hydraulic cases developed for the Fire PRA. The accident progression timeline is usually linked to the other timing sources at the time of reactor trip. This timeline is typically produced by the thermal-hydraulics group, which may or may not be directly involved with the Fire PRA project.

7.3.3 Phase II Timing Associated with the Decision to Abandon

For loss of habitability scenarios, the time associated in the decision to abandon is negligible. The fire PRA and HRA both assume that when the habitability criteria (defined in NUREG/CR-6805 Task 11b) are met then abandonment begins. After the habitability criteria are met, then the operators will perform any required control room actions such as reactor trip, or turbine trip and leave the MCR. For loss of habitability scenarios the phase II timing will be negligible.

The time required for the diagnosis and the decision to abandon for loss of control scenarios is complex and could take several minutes. The decision to abandon will be based on procedure cues, training and is typically at the discretion of the SRO in charge of the operating crew. For most U.S nuclear plants, the criteria for abandonment are typically not clearly defined and are often ambiguous. Section 4 provides additional guidance on the decision to abandon for loss of control scenarios.

7.3.3.1 Phase II Timing Parameters

In Phase II of the MCRA timeline, there are four timing parameters which should be identified.

- Time at which the abandonment criteria are met relative to the start of the fire.
- Time required for the control room to make the decision to abandon.
- Time available for Phase II.
- Time available for recovery or time margin.

For loss of habitability scenarios, the time at which the habitability criteria for abandonment are met will be based on the fire progression timeline

For loss of control scenarios, the time available for the decision to abandon is defined by the HRA analyst by first identifying how long it will take to perform all actions (both cognition and execution of each action need to be considered) after abandonment and working backwards to determine the latest time at which the operators must leave the MCR. (Phase III timing will therefore need to be developed before Phase II timing.) This time will be based on how well the abandonment criteria are defined in the MCRA procedure, interviews with operators and the HRA and PRA analysts' understanding of the scenario. This time may rely heavily on engineering judgment.

In contrast to the time available for the decision, the time required for making the decision to abandon is the expected time it will take the MCR crew to make the decision, which could range from one minute to several minutes depending on the clarity of the guidance in the procedures and whether it is covered in training. This time could also include obtaining approval from others outside the MCR, or obtaining confirmation of the severity of an ex-MCR fire or of the systems that are failed or available. For loss of habitability scenarios, this time will be negligible.

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

7.3.3.2 Example Approach for Phase II Decision to Abandon Time Estimation

It should be noted that in most cases the timing associated with the decision to abandon will be determined by engineering judgment. One approach to determining these timing parameters is described as follows.

First, the total time available for Phase III is determined and compared to the time required to complete Phase III actions (cognition and execution). See Figures 7-2 through 7-5 for an example.

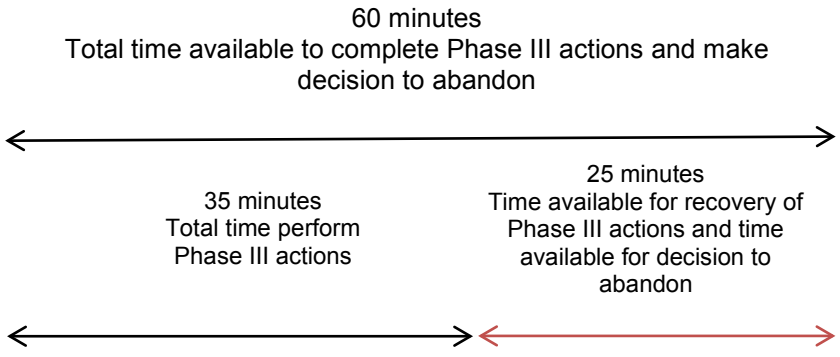

Figure 7-2
Time available for recovery of Phase III actions and time available for decision to abandon

The total time available for recovery of Phase III is calculated by subtracting the total time available from time required. In Figure 7-2 this is shown by the red line.

Based on the time available for recovery of Phase III actions and time available for decision to abandon, the time is split to define the time at which the operators must leave the MCR. This split is defined by the analyst and will be based on their understanding of the timing impact on the quantification of the HEPs.

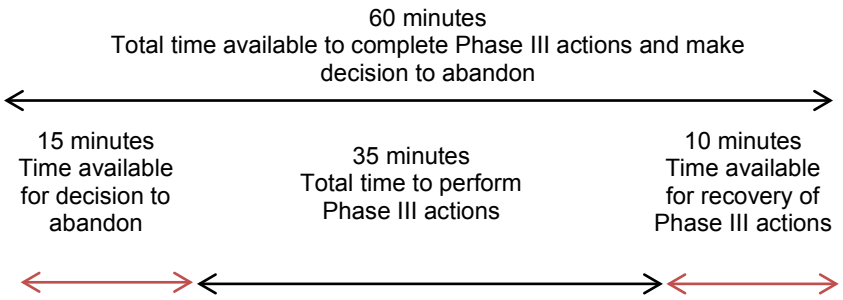

Figure 7-3
Split between time available for recovery of Phase III actions and time available for decision to abandon

Based on the defined time available for the decision to abandon the analyst must then define the time required to make this decision and the time available for recovery. The time available for recovery is calculated as Time available – Time required.

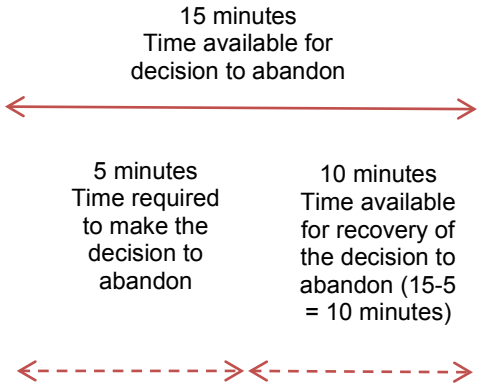

Figure 7-4
Time required and time available for recovery for the decision to abandon

For the purposes of the MCRA HRA, all timing parameters associated with the decision to abandon should be identified as best estimate point estimates because many of the actions required after abandonment are predicated on the time at which abandonment occurs. In reality, however, it is recognized that there is significant uncertainty associated with each timing input related to the decision to abandon.

When determining the timing associated with the decision to abandon, the time for recovery must be greater than zero in order to show that the MCRA scenario is feasible. Section 9 provides additional discussion on this uncertainty.

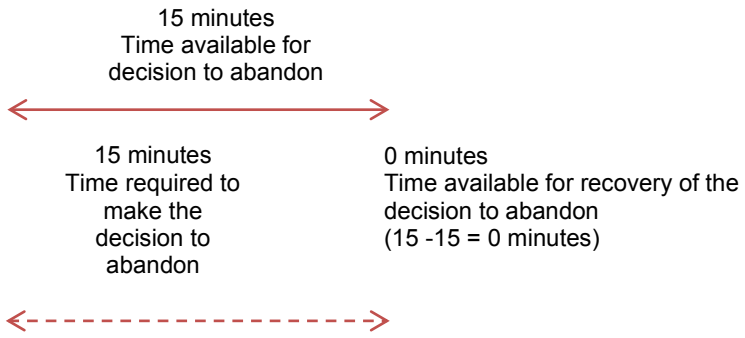

Figure 7-5
Decision to abandon is not feasible

After the initial best estimate timing parameters have been developed, the MCRA HRA can consider doing sensitivity studies to determine the impact of the uncertainty associated with the decision to abandon. One way to assess the sensitivity of the uncertainty in the timing values is to conduct a trial increase in the time parameters to see how much the HEP is impacted. It may be prudent to utilize a conservative value initially to see what the impact is to the fire PRA results. If the conservative HEP is not acceptable, then the HRA analyst can assess what would be needed qualitatively to improve the time estimate, whether it is clearer MCRA criteria or better training, and discuss this with operations, training and fire PRA project team.

7.3.4 Procedure Progression Timeline (Operator Response)

The timing sources described above primarily define the time available for operator response and provide additional information such as cues and plant parameters occurring during response. This section focuses on the time required for response.

As described in NUREG-1921, the time required for response consists of the time for cognition and the time for execution. The time required for response depends on what procedures are being used, including the time to transition through and to different procedures, as well as the time needed to implement the procedures.

For all phases, the procedure progression timeline is typically constructed by the HRA analyst with input from the plant operations staff. Operational input is essential in order that the plant response times reflect the "as-operated" or "as-to be operated" plant. Input is collected from the operators based on the talk-through/walk-through guidance in Appendix C. As part of this discussion, the HRA analyst should review the modeled timing of the fire and hardware failures associated with Phase I with plant operations in order to understand the context and development of timing for both Phase II and Phase III.

During Phase I, typically, the plant EOPs/AOPs remain in effect and are used in conjunction with the plant fire procedure and the modeling of the time required for response follows the same

considerations as described in NUREG-1921. During Phase I the fire-induced initiating event and the associated reactor trip are affected by the fire growth timeline (Section 7.3.1) and accident progression timeline (Section 7.3.2).

During Phase II (making the decision to abandon), the plant is typically following EOPs and or AOPs and fire procedures, and accessing the MCRA procedure to decide whether MCR abandonment is warranted. For Phase II, the time at which abandonment occurs should be based upon the specific criteria the crew will use for making the decision to abandon, as discussed in Section 4 and Section 7.3.3.

Most MCRA procedures typically include several actions that are performed just before leaving the MCR. These actions typically can be accomplished quickly and include reactor trip (if not already done), turbine trip, and isolation of critical MCR panels as a first step to transferring control to the RSDP. The time it takes to perform these actions should be incorporated into the overall operator response timeline. When conducting these steps, the actions are typically accomplished independently without the need for communications, coordination or command and control.

During Phase III the operators may be using only the MCRA procedure or may still be using EOPs/AOPs and the plant fire procedure. This is one of the questions that should be asked of operators during the interviews (as noted in Section 4). The evaluation of the Phase III portion of the MCR timeline requires a combination of both talk-throughs and walk-throughs of the MCRA procedures with knowledgeable plant staff since the control room simulator has limited use for actions outside of the MCR. If the plant has a simulator for the RSDP this can be useful for determining the time to complete actions at the RSDP, but actions taken away from the RSDP will need to be based on walk-throughs and talk-throughs and should cover the time it takes to perform each action individually as well as the collective set of actions.

The MCRA procedure may contain steps that are not considered essential by the PRA, but are done to facilitate the ability of the operators to restart the plant at a later time. These steps, however, can take time and attention away from the critical actions and could compromise the ability of the operators to complete the PRA-relevant steps in time to bring the plant to a safe condition. Conducting timed walkthroughs can identify the time constraints on the entire MCRA process and can help demonstrate to operations and training the importance of focusing on the PRA relevant steps of the procedure. The HRA analyst can then recommend moving the non-essential steps to a later point in the procedure after the critical steps are completed.

The MCRA procedure needs to be evaluated not only in terms of individual actions (and HFEs; see Section 5 on Identification and Definition), but as a collective set of actions to ensure that the entire set of actions can be completed in time to avoid core damage. 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.

The MCRA timeline ends once the Phase III actions have been completed. However, operators will need to maintain long term control of the plant, typically of decay heat removal and

injection systems. For these long term control actions, the duration is the mission time of the function or system being modeled; this is not included in the MCRA timeline but should be included in the fire PRA as actions required for success. In contrast, for internal events HRA, the time available generally looks at the time at which the system must first be started, and actions for long term control are often not required or are considered negligible. For MCR abandonment MCRA, the long term control portion may no longer be negligible. The operator may need to control the system multiple times in order to comply with the PRA mission times. When modeling these steps, the actions typically require some level of communications, coordination, and/or command and control and the time required to accomplish these actions must be addressed

The timing considerations and sources of data in Section 4.6.2 of NUREG-1921 apply to MCRA; specifically, the following sources may be useful in determining the time required to complete each action.

- Job performance measures (JPMs). Many plants have a specific JPM for each MCRA action. The JPM can provide a reasonable estimate for the time it takes to perform an action. However, the HRA analyst should review what is and is not included in the time required to perform this action. Often times the coordination between operators is simulated via a phone call and not actually walked down as part of the training. Additionally, the JPM training may use a different starting point than the fire PRA. For example, the JPM T_0 may start once the operator is already in the field whereas the MCRA T_0 should be the start of the fire.
- Training exercises
    - Times recorded during simulator exercises can help estimate the overall time the MCRA process takes or time points for when key actions need to be started and completed.
- Appendix R feasibility demonstrations. As cited in NUREG-1852 [3], Section III.I.2 of Appendix R states the following:

    > Practice sessions shall be held for each shift [crew] to provide them with experience in [performing the operator manual actions] under strenuous conditions encountered [during the fire]. These practice sessions should be provided at least once per year for each [operating crew] ... [and] performed in the plant so that the [crew] can practice as a team.

- Information from the assessment of a similar action in which the following characteristics exist:
    - The actions themselves are similar
    - The timing related to when the actions have to be performed and how long it would take to implement the actions is similar
    - Locations of the actions are not so different that travel time to the locations is not significantly affected
    - Similar environments exist for the locations of the actions

Timing information from the assessment of similar actions can also be used as a bounding case when it is clear that the actions being evaluated would not require more time than the similar action.

Evaluation of time required to complete the actions should consider the time to travel to each action location, as well as the time necessary for performing the action, including communications if necessary. This may be complicated if multiple locations are visited in the course of sequential actions, in which case the various action locations need to be considered. This is especially important for post MCRA actions for which a large number of actions will be distributed.

The evaluation of time required to complete the actions should include the time required for coordination and communications. Once outside the MCR, each plant has a unique communications strategy (or strategies). Consideration of the command and control structure at the plant should be made as part of the communication and operator dynamics assessment; see Section 8 on PSFs and Appendix B on Command and Control. The HRA analyst should identify the times at which key communications would be required between stations outside of the MCR.

For example, starting a pump may require one operator to start the pump locally and a different operator to control the pump flow at a different location. Starting and controlling the pump could require one operator to start the pump and then communication with the RSDP to determine the flow rate. The flow rate indicators may or may not be available at the pump. The time at which this communication occurs is dependent on how long it takes the operator to travel to and start the pump. For example, the flow rate of the charging pumps may not be determined until after instrumentation and control has been established at the RSDP.

Section 4.2.2 of NUREG-1852 mentions equipment access, environmental conditions, and expected variability between individuals and crews as potential contributors to timing uncertainty. It is therefore important that the analyst recognize the potential for uncertainty in the time estimates and be vigilant for cases in which a small change in the estimation of the time required could change the operator action from feasible to infeasible. See Section 6 for additional discussions on feasibility.

7.4 Individual HFE Timeline

Section 7.3 described the evaluation of the overall MCRA timing and the different timing sources available to the HRA analyst. This section discusses the evaluation of timelines for the individual human failure events (HFEs) modeled in the fire PRA to represent the system and function implementation for the MCRA scenarios, as discussed in Section 5 on Identification and Definition. In addition to the overall MCRA process timeline, for each HFE modeled in the fire PRA, an individual timeline should be developed. The HRA analyst should work together with operations staff to identify the time required to perform each action individually, but also the timing relationships between the actions, all with respect to the same reference point. The time required must include the transit time as well as the time required for coordination and communications. If the action involves the longer term control of plant parameters, then a mission time is also needed.

In addition to the time required, the MCRA HRA evaluates the time available for response using the considerations provided in Section 7.3. Once the individual HFE timeline is constructed, it is used for feasibility and quantification.

The individual timeline for each action should be defined following the basic guidance and timing concepts in NUREG-1921, which is repeated below for completeness, but with specific MCRA examples added. During Phase I (before the decision to abandon) this modeling is the same as in NUREG-1921. During Phase III, the time of the cue may be the modeled as the time when the operators leave the MCR. Each of these timing parameters is discussed below and has been annotated to provide a reference back to the timing considerations presented in previous sections.

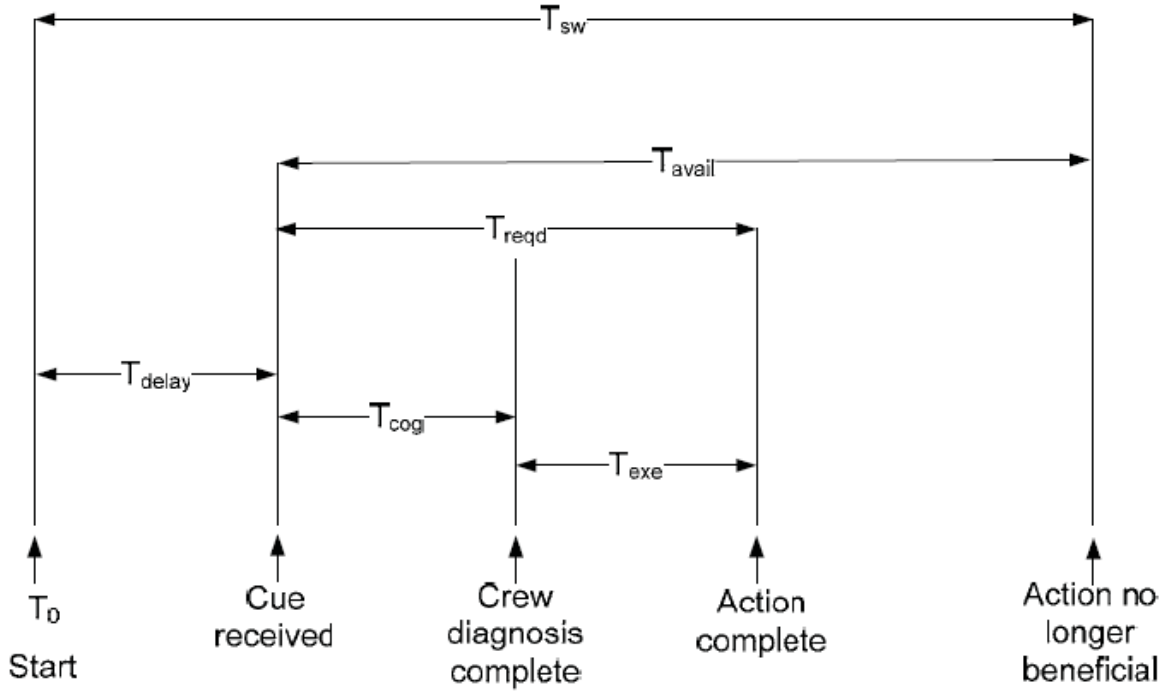

Figure 7-6
Illustration of Individual HFE Timing Concepts from NUREG-1921

The terms associated with each timing element are summarized what is unique to MCRA with respect to what is provided in NUREG-1921.

- **T_0** = start time = start of the event. This may be the start of the fire or reactor trip as described in Sections 7.3.1 and 7.3.2.

- **T_{sw}** = system time window – (T_{SW}) is defined as the start of the fire until the action is no longer beneficial. This time typically derived from thermal-hydraulic data and, for HRA quantification, is considered to be a static input. The system time window represents the maximum amount of time available for the action.

In many cases, T_{sw} is determined based on a thermal hydraulic calculation for the most limiting conditions. For example, consider the operator action to recover AFW outside the MCR after the decision to abandon has been made. A thermal hydraulic calculation is performed for a scenario in which all secondary cooling (AFW, MFW, and condensate is lost at the start of the fire) to determine the longest time to steam generator dry out assuming no feed and bleed. This time was calculated to be 60 minutes and represents the total time available from the start of the fire until this action must be completed. Note that 60 minutes represents the most limited case and there could be scenarios in which the most limited case is overly conservative. For example, if T=0 is defined as the start of the fire and AFW successfully runs for 20 minutes before operators trip the pumps inside the MCR, as directed by the MCRA procedure then T_{SW} would be longer than 60 minutes. At a minimum, in this case, T_{SW} = 20 + 60 minutes = 80 minutes.

For the HFE associated with the decision to abandon, the system time window is defined as the time from the start of the fire until the point at which operators must make the decision to abandon in order to successfully perform all Phase III actions. As described in Section 7.3.3 this time will be defined by the HRA based on how much time is required for the Phase III actions.

Two examples, illustrate how T_{sw} is determined for decision to abandon.

Example 1 – PWR example for T_{SW} associated with decision to abandon

Scenario description: Fire starts in cable spreading room, AFW is failed, MFW is failed, one PORV fails open, charging pumps are failed, and feed and bleed cannot be performed from the MCR.

Based on a thermal hydraulic calculations, operators have 60 minutes to avoid core damage by starting an MD AFW pump and/or charging for other scenarios. In order to establish and control AFW and charging the control and instrumentation must first be established at the RSDP. The Phase III actions credited in the PRA and time required to complete (T_{cog}+T_{exe}) are summarized in Table 7-1:

Table 7-1
Example 1: Actions credited and time required

Action	T_{cog}+T_{exe} (Minutes)	Basis
Establish control at RSDP	15	The JPM allotted time is 15 minutes. This time includes both cognition and execution.
Establish AFW locally	15	This time was obtained from simulator training session data the time to go from Step 11. Implement Appendix Y to Step 22. Check reactor sub critical,
Establish charging locally	20	Obtained from operator talk-through.
	Total time for Phase III actions = 50 minutes	

T_{SW} for the decision to abandon equals 60 minutes – 50 minutes = 10 minutes. This 10 minutes assumes that the time available for recovery of the Phase III actions is 0. See Section 7.3.3 for additional discussion.

Example 2 – BWR example for T_{SW} associated with the decision to abandon

Scenario description: Fire starts in the cable spreading room. At T=0, all sources of injection are lost, 3 SRVs spuriously open, and power to bus A is lost.
Based on a thermal hydraulic calculation, operators must establish low pressure injection within 20 minutes of a loss of all high pressure injection. The Phase III actions credited in the PRA and time required to complete (T_{cog}+T_{exe}) are summarized Table 7-2:

Table 7-2
Example 2: Actions credited and time required

Action	T_{cog}+T_{exe} (minutes)	Basis
Establish control at RSDP	10	Talk through of abandonment procedure steps 1-10
Re-establish power to bus	3	1 min cognitive and 2 min execution based on talk through. Same timing as used for internal events action.
Start low pressure injection at the RDSP	4	2 min cognitive and 2 min execution based on talk-through of procedure steps.
	Total time for Phase III actions = 17 minutes	

T_{sw} for the decision to abandon is calculated as 20 minutes –17 minutes = 3 minutes. With a system time window of only 3 minutes, the HRA analyst must ensure that this scenario is feasible. If the time required to make the decision to abandon is greater than 3 minutes then this scenario is not feasible. The T_{sw} of 3 minutes assumes that the time available for recovery of the Phase III actions is zero. See Section 7.3.3 for additional discussion.

- **T_{delay}** = time delay = time of the cue = duration of time it takes for an operator to receive and acknowledge the cue.

  For MCRA scenarios, the time of the cue could be the time of abandonment, the time to reach a procedure step (or if coordinating with another operator, the time the associated operator reaches a procedure step) or the time a parameter reaches a certain level.

  Figure 7-3 shows the inputs to the estimation of T_{delay} for starting an injection system following MCRA:

  T_{delay} for the injection HFE corresponds to the time from the start of the fire to the arrival of the cue that they are losing inventory and need to start charging pumps. Review of the fire procedures and discussions with operators shows when the actions are expected to occur all relative to the start of the fire.

Table 7-3
Inputs to estimation of T_{delay}

Action	Expected timing (minutes)	Basis
Start of the fire	0	
Decision to abandon has been made	25	Time at which the decision to abandon has been made.
Time at which control is established at RSDP	7	Once the decision to abandon has been made it will take the operators 7 minutes to establish control at the RSDP. This is based on walk-through and talk-through of the MCRA procedure. Establishing control at the RSDP is a prerequisite for injection.
Cue for injection	3.25	Time from simulator training session data for going from Step G: Check vital buses energized to Step H: Check charging flow normal = 3.25 minutes. Therefore time of the cue is 32+3.25 = 35.25.
	T_{delay} = 25+7+3.25 = 35.25 minutes	

- **T_{cog}** = cognition time consisting of detection, diagnosis, and decision making. Typically after the decision to abandon the MCR, each operator action is largely execution. Even so, there are still cognitive considerations including command and control, coordination and communications which must be included in the time required for response. If the MCRA procedure is written such that each action must be performed in chronological order and the action requires no additional information other than what is written in the procedure, then T_{cog} could be short (e.g. under a minute). However, if the operator performing the action must obtain additional information by either communicating with an additional operator or interpreting hard to read indicators, then this time could be on the order of minutes. Any travel time related to obtaining information should also be included in the cognitive time.

- **T_{exe}** = execution time including travel, collection of tools, donning of PPE, and manipulation of relevant equipment. This time should also include time for communication. For HFEs modeling the long term control of plant parameters, the time required for execution should be extended to cover the mission time required for the action.

  In Phase I, most actions will be occurring in the MCR and the execution time can be based on simulator observations for MCR actions or JPMs for local actions. For Phase II, there will be no execution time associated with the decision to abandon, the decision to abandon is considered to be cognition only. For Phase III actions, the execution time can come from walk through, talk through and JPMs if available. In many cases, a combination of several sources will be needed to obtain an estimate, as shown in Tables 7-4 and 7-5.

  Example 1: The execution time associated with the operator action to locally start an EDG.

Table 7-4
Example 1: Collection of timing information associated with locally starting EDG

T_{exe} for starting EDG locally	Source of timing information
10 minutes	JPM – Allocated time required to be met by all operators
7 minutes	Operator interviews indicated that it would take no longer than 7 minutes to start diesels from the beginning of the fire scenario
6.5 minutes	Walkdown time

In the above example, a conservative estimate of 10 minutes is used as the execution time because operators do not have a direct procedural path to locally start the diesel, the dispatch of the operator to manually start the diesel could be delayed.

Example 2: The execution time associated with establishing command and control at the RSDP contains several sub tasks and the timing associated with each sub-task can come from different sources.

Table 7-5
Example 2: Collection of timing information associated with establishing command and control at RSDP

Subtask	Time (Minutes)	Source of timing information
Transferring control in the MCR to RSDP prior to leaving MCR	2	A simulator observation was performed to observe how long Steps 1-8 of the abandonment procedure would take prior to leaving MCR
Travel from MCR to RSDP	6	Walk down
Enabling control at RSDP	2	Walk down
	Total T_{exe} = 10 minutes	

- T_{avail} = time available = time available for action = (T_{sw} - T_{delay}). This time is one of the two inputs used to evaluate feasibility.

- T_{reqd} = time required = response time to accomplish the action = (T_{cog} + T_{exe}). This time is one of the two inputs used to evaluate feasibility. In discussion with HRA practitioners the term time required is used to describe how long it would take to complete this action. By definition, time required includes both cognition and execution but in many cases the cognition time is minimal compared to the execution time and/or the cognition time cannot be observed separately from the execution time.

When the individual HFE timeline is developed using the approach described above then sufficient timing parameters have been collected to evaluate feasibility, and to identify the amount of time available for recovery. An action is feasible when the time available is no less than the time required.

7.5 Integrating All Timing Sources into MCRA Timeline

As described in Section 7.2 the MCR timeline consists of three phases. Table 7-6 outlines the key timing parameters in each phase and describes how the information is linked together to form the complete MCRA timeline.

Table 7-6
Integration of timing sources into MCRA timeline

MCRA Timing Phase	Timing Parameter	Timing Sources	Links to other MCRA timeline parameters
Phase I	Start of the fire (T_0)	Fire response timeline	All timing inputs in the MCRA timeline should be estimated with respect to the same T_0
	Time of reactor trip	Fire response and/or operator response timeline	In most LOC scenarios there are major failures of equipment, and thus reactor trip will occur at T=0. For LOH where equipment failures have not caused a reactor trip, this defines the start of system time window and time at which the operators enter the EOPs.
	Following reactor trip, time at which key EOP and fire PRA actions are started and the time at which the cue for each of these actions is received.	Operator response timeline	The procedure progression can be used to define the cues for many individual actions.
	Time at which fire is suppressed and times at which firefighting occurs	Fire response timeline	If crew members used for the fire brigade take staff away from MCRA staffing, the time at which fire is suppressed could impact the time at which crew members (fire fighters) become available to take additional PRA actions.[20]
Phase II	Time at which the abandonment criteria are met relative to the start of the fire	Fire response / accident progression timeline	Identifies plant-specific cue to operators (T_{delay} with respect to T_0) of need to abandon MCR

[20] All U.S plants have procedure guidance to ensure that for design basis MCRA scenarios there will be sufficient staff available to fight the fire and perform the required actions. However, there could be PRA scenarios that require more actions than the design basis scenarios and the availability of crew members must be verified. See Section 6 and 8 on staffing.

Timing and Timelines for MCR Abandonment

MCRA Timing Phase	Timing Parameter	Timing Sources	Links to other MCRA timeline parameters
	For LOC, time required for the control room to make the decision to abandon	Decision to abandon	Does not apply to LOH. Determined by defining the LOC abandonment criteria, if not already specified in the MCRA procedure and through operator interviews. If well specified, could be only a matter of a minute for the decision process.
	Time available for Phase II	Decision to abandon with input from accident progression and fire response timeline	The time available for Phase II is informed by the accident progression timeline and fire response timeline but is 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 and stable condition. See Section 7.3.3 for additional discussion.
	Time to perform any required actions just before leaving the MCR	Operator response timeline	
	Time available for recovery, if operators delay abandonment.	Decision to abandon timeline	This time must be greater than zero in order for the entire MCRA scenario to be feasible. The more time for recovery in Phase II, the less time available to perform actions in Phase III.
Phase III	Time at which operators leave the MCR.	Decision to abandon	The time at which the operators leave the MCR will be used to determine how much time the operators have to perform actions once outside the MCR.
	Time each action included in the MCRA procedure is started	Operator response timeline	T_{delay} for the individual HFEs depends upon the time required for the decision to abandon and take actions required to leave the MCR. In some cases, the MCRA procedure is linear. In these cases, one action cannot be performed until the preceding action is completed.

MCRA Timing Phase	Timing Parameter	Timing Sources	Links to other MCRA timeline parameters
	Time required to complete each action listed in MCRA procedure, including travel times to action locations	Accident progression / fire response timeline	The accident progression model determines the time based on time of fire failures and reactor trip. The time of fire failures and reactor trip is based on the fire progression model.
	Timing of possible 'hold points' required by operators not co-located	Operator response timeline	In some cases, the procedure may have a 'hold point' (i.e., a note or a caution), calling for an operator to wait for communication that prerequisite actions have been completed
	Timing of key communications required by operators not co-located	Operator response timeline	In some cases, communications between operators can delay an action from being performed due to the need to confirm one action's completion before another can be started.
	Time available to complete each MCRA action	Accident progression timeline	The time available to complete each action will be dependent on the accident progression model and the scenario-specific timing of when the action is no longer useful to prevent core damage. The time available for each fire PRA action will be used directly in quantification.

7.6 Examples of MCRA Timeline and Individual HFE Timelines

Tables 7-7 and 7-8 and Figure 7-7 present an example of an MCRA timeline for a loss of habitability scenario following different formats. Tables 7-7 and 7-8 show the timeline as a running list of events starting with the start of the fire. Figure 7-7 presents the timeline as a Gantt chart following MCRA, while Figure 7-8 displays the relative timing of the individual HFEs used to model the LOH MCRA scenario. The information in all three examples is identical and the only difference is the format in which the material is presented.
In comparison, an example of an MCRA timeline for a LOC scenario is presented in Table 7-9.

Table 7-7
Example MCRA timeline for loss of habitability (format 1)

Time Phase	Clock time	Description
Phase I	T =0	Start of fire
	T =0	Reactor trip
	T =0	Control room is aware of a fire in the control room.
	T =0	Fire brigade summoned.
	T = 5 minutes	Operators enter E-0 and complete first 4 steps within 5 minutes. No SSD equipment is damaged by the fire.
	T = 5 minutes	Fire brigade continues to fight fire unsuccessfully. Operators open MCRA procedure, but fire has not yet progressed sufficiently to enter procedure.
	T = 5-18 minutes	Operators work in ES-01 and try and assess damage caused by fire. The fire brigade continues unsuccessfully to suppress fire.
	T=15	Operators will have seen the smoke building, and at the 15 minute point will decide to implement the MCRA procedure. The 15 minute point was modeled based on the following: • CFAST calculations showing the evacuation criteria are met at 18 minutes • Operators have stated that they will remain in the MCR as long as possible. • Operators see smoke building, respond to the reactor trip using EOPs until the point where abandonment is imminent
Phase II	T =15-17 minutes	Operators perform the first 8 steps of MCRA procedure. Most of the actions associated with these procedure steps will have already been performed since the plant has been shutting down since the start of the fire. Although the fire is causing smoke and hot gas, it has damaged only components associated with the panel where the fire has started. Upon completion of the first 8 steps of the MCRA procedure, AFW and Reactor Coolant Pumps (RCPs) are all stopped as directed by the procedure and the electrical power feed from offsite power is tripped.
	T =18 minutes	For this fire, CFAST calculations show the evacuation criteria have been met and force the operators out of the control room. At the same time one RO goes the RSDP and Aux Building Operator starts to align breaker to restore power to charging.
Phase III	T=20 minutes	RO arrives at RSDP
	T = 22 minutes	RSDP instrumentation is established.
	T = 25 minutes	Aux Building operator reaches required location and begins to restore AFW. The Aux Building operator must verify valve alignment and then start pump at RSDP.
	T = 27 minutes	AFW is established and Aux Building operator must radio back to RO at the RSDP that AFW flow has been established. Once started, AFW can be controlled at RSDP by a single operator.
	T = 35 minutes	Aux Building operator radios to operator at RSDP to determine charging flow. The flow indicators are not available locally.
	T = 38 minutes	Charging is re-established

Table 7-8
MCRA timeline example (format 2)

Time (Minutes)	**T =0-15**	**T =15-18**	**T = 20**	**T=22**	**T=25**	**T=27**	**T=35**	**T=38**	**T= 38 minutes to 24 hrs.**
	Phase I	**Phase II**	**Phase III**						
Operators									
SRO	Starts working in both EOPs and fire procedures Activates fire brigade.	Leaves MCR	Arrives at RSDP						
RO1	Starts working in both EOPs and fire procedures	Leaves MCR	Arrives at RSDP			AFW flow is established by Aux operator Now AFW flow must be controlled from the RSDP. Communicati on required with Aux operator	Communication required with Aux operator to determine charging flow.		
RO2	Starts working in both EOPs and fire procedures	Leaves MCR	Arrives at RSDP	Instrumentation Established at RSDP					Monitoring AFW and Charging flows

Timing and Timelines for MCR Abandonment

Time (Minutes)	**T =0-15**	**T =15-18**	**T = 20**	**T=22**	**T=25**	**T=27**	**T=35**	**T=38**	**T= 38 minutes to 24 hrs.**
Aux Building Operator	Reports to ready room for additional instructions	Leaves ready room			Reaches Aux building	AFW restarted	Communication required with RO1 to determine charging flow.		
Plant Parameter									
AFW	Running as expected	Stopped by operators just before leaving MCR				AFW restarted			
Charging	Running as expected	Stopped by operators just before leaving MCR						Charging flow restarted	
Description of milestones	Start of the fire	Decision to abandon is made	RSDP is staffed	RSDP is operational		AFW flow restarted	Communication	Charging flow re-established	Plant control from RSDP
	Fire brigade is altered								
	Reactor trip								
	Smoke fills up the MCR	Loss of habitability criteria are met							

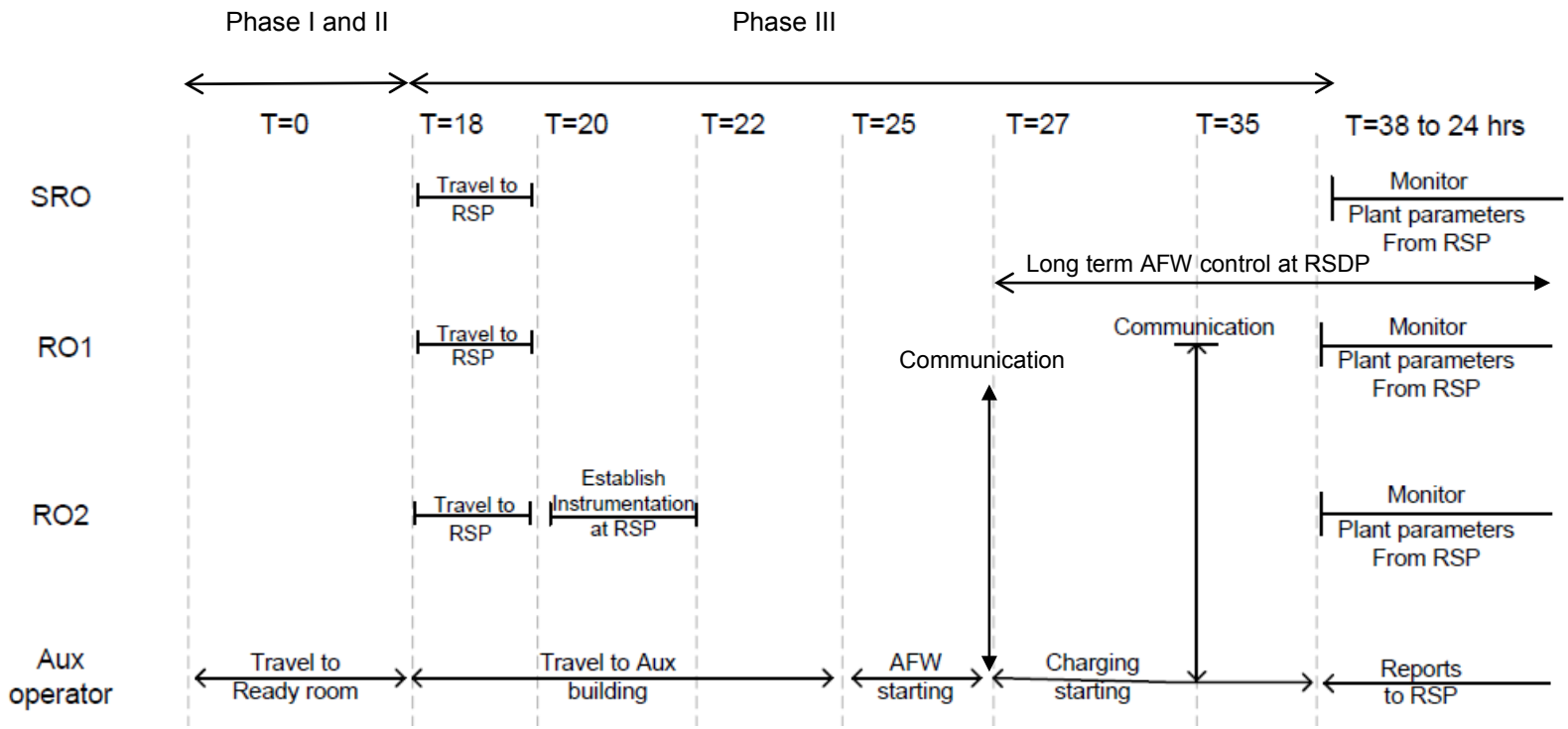

Figure 7-7
MCRA timeline after the decision to abandon has been made

Timing and Timelines for MCR Abandonment

For each of the individual HFEs credited in the fire PRA for MCRA, an individual timeline was developed. In the MCRA timeline above the fire PRA credits three unique operator actions:

- Establishing control at the RSDP
- Establishing and controlling AFW
- Establishing and controlling charging

Because the example was for a loss of habitability scenario, the decision to abandon was not included as a required operator action. The PRA assumes that the decision to abandon is negligible for loss of habitability scenarios.

The individual timelines are based on the following scenario: reactor trip with a loss of feed water followed by no MFW or AFW, no sprays/fans and no feed and bleed.

HFE 1: Operators fails to establish control at RSDP

T_{sw} = 38 minutes - Tsw is based on T-H analysis where the most limiting bounding scenario was selected
T_{delay} = 18 minutes
T_{cog} = 1 minute
T_{exe} = 3 minutes (T_{exe} includes travel time)

HFE 2: Operators fails to establish AFW

T_{sw} = 1 hr. and 8 minutes
T_{delay} = 18 minutes
T_{cog} = 1 minute
T_{exe} = 10 minutes (T_{exe} includes travel time)

HFE 3 Operators fails to establish charging

T_{sw} = 1 hr. and 38 minutes
T_{delay} = 27 minutes – In this example, starting charging is delayed until AFW is established. T_{delay} is the time it takes for the Aux Building operator to reach the step in the abandonment procedure which directs them to start the charging pumps. For this example, the abandonment procedure prioritizes the order of actions based on the success criteria timing.
T_{cog} = 1 minute
T_{exe} = 8 minutes (T_{exe} includes travel time)

In the AFW and charging operator actions, the PRA timing requirements only start once the pumps are switched off by the operators before they leave the MCR. If pumps are running at the beginning of fire and continue to run throughout the scenario, then the operator actions to recover pumps would not be required by the PRA success criteria. For the AFW example, the PRA success criteria say that AFW must be recovered within 50 minutes to prevent steam generator dry out. The time at which AFW runs successfully needs to be included in T_{sw}. T_{SW} = 18 minutes + 50 minutes = 1 hr. and 8 minutes.

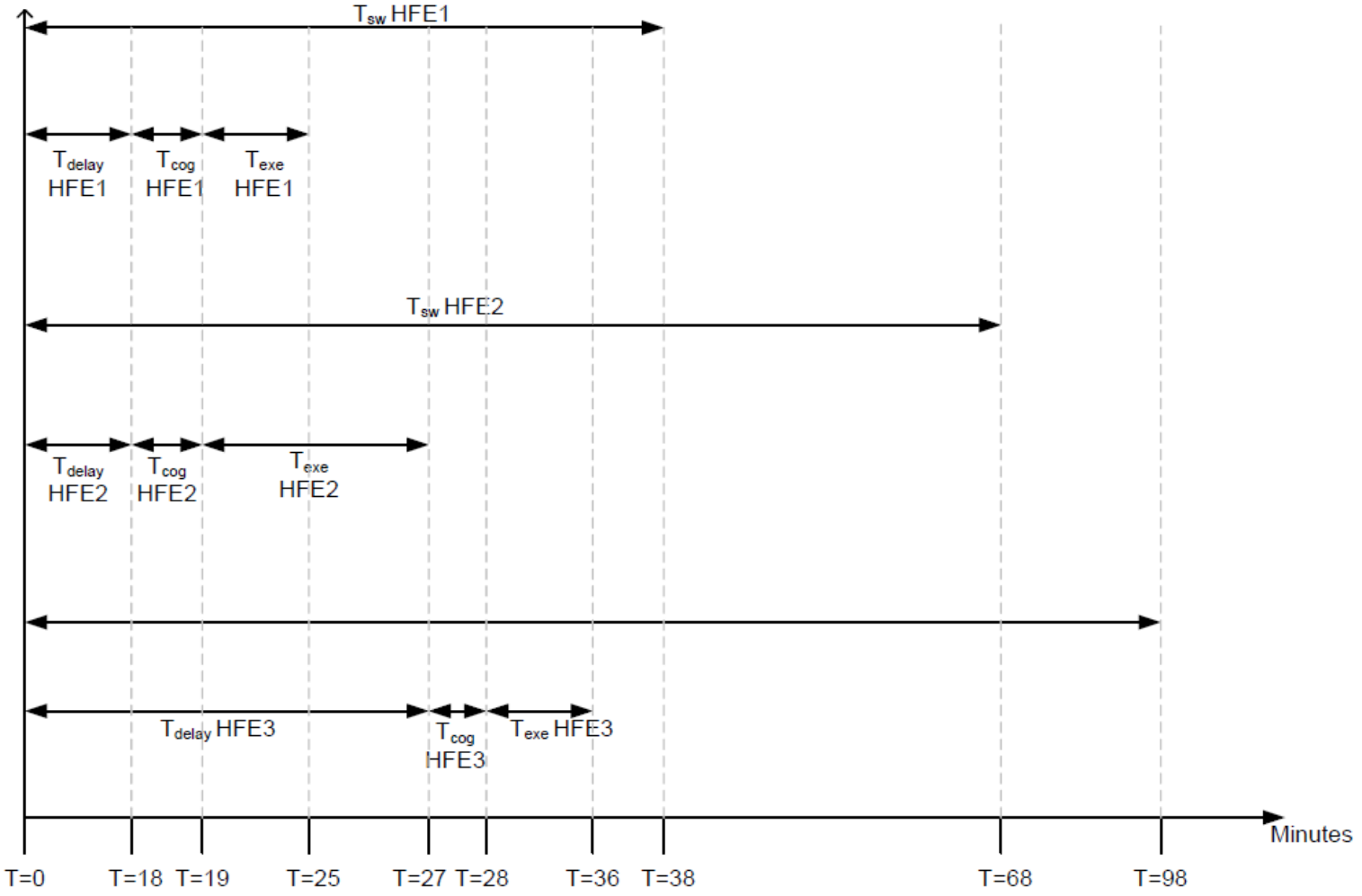

Figure 7-8
Timing of individual HFEs with respect to the same time origin

Table 7-9
MCRA timeline example for LOC scenario (format 1)

Time Phase	Clock time	Description
Phase I	T =0	Start of fire
	T =0	Reactor trip
	T =0	Control room is made aware of a severe fire in the cable spreading room.
	T =0	Fire brigade summoned.
	T = 5 minutes	Operators enter E-0 and plant fire procedure; they complete first 4 steps of EOP within 5 minutes. The EOP response timing was developed from talk through. There is major SSD equipment damage, including AFW failures, charging/safety injection failures, and MSIVs are spuriously open.
Phase II	T = 5 minutes	Fire brigade continues to fight fire unsuccessfully. Operators open MCRA procedure and read the following criteria for abandonment: No decay heat removal systems are available from the MCR.
	T = 5-14 minutes	Operators work in EOPs E-0, E-1, FR-H.1 trying to determine the status of the failed systems for abandonment.
	T= 15 minutes	Operators make the decision to abandon MCR. Operators perform the first 8 steps of MCRA procedure. Most of the actions associated with these procedure steps will have already been performed since the plant has been shutting down since the start of the fire. Upon completion of the first 8 steps of the MCRA procedure, AFW and Reactor Coolant Pumps (RCPs) are all stopped as directed by the procedure and the electrical power feed from offsite power is tripped. Most of these components are already failed due to fire damage.
Phase III		
	T =16 minutes	Operators leave the MCR.
	T=20 minutes	Operations team arrives at RSDP; SRO distributes MCRA procedure attachments to ROs and Aux Building Operator.
	T = 22 minutes	Control is established at RSDP by SRO.
	T = 25 minutes	The Aux Building operator must verify valve alignment and then start pump.
	T = 27 minutes	AFW is established and Aux Building operator must radio back to RO at the RSDP that AFW flow has been established. Once started, AFW can be controlled at RSDP by a single operator.
	T = 29 - 34 minutes	RO2 closes breaker to close spuriously open MSIVs
	T = 35 minutes	Aux Building operator radios to operator at RSDP to determine charging flow. The flow indicators are not available locally.
	T = 38 minutes	Charging is re-established

Timing associated with individual actions
The time available for each action following abandonment is determined by subtracting T_{delay} from T_{SW} in the loss of control example in some cases T_{delay} is defined as the time of abandonment.

HFE 1: Operators fail to establish instrumentation at RSDP

T_{sw} = 38 minutes
T_{delay} = 20 minutes – Based on time of abandonment.
T_{cog} = 1 minute
T_{exe} = 3 minutes (T_{exe} includes travel time)

HFE 2: Operators fail to establish AFW

T_{sw} = 50 minutes
T_{delay} = 20 minutes
T_{cog} = 1 minute
T_{exe} = 10 minutes (T_{exe} includes travel time)

HFE 3: Operators fail to establish charging

T_{sw} = 1.5 hours
T_{delay} = 27 minutes – In this example, starting charging is delayed until AFW is established. T_{delay} is the time it takes for the aux building operator to reach the step in the abandonment procedure which directs them to start the charging pumps. For this example, the abandonment procedure prioritizes the order of actions based on the success criteria timing.
T_{cog} = 1 minute
T_{exe} = 8 minutes (T_{exe} includes travel time)
In the AFW and charging operator actions, the PRA timing requirements start at the start of the fire due to fire and cable damage.

HFE 4: Operators fail to close spurious MSIV

T_{SW} = 1.15 hours
T_{delay} = 29 minutes
T_{cog} = 1 minutes
T_{exe} = 4 minutes including travel time

7.7 Uncertainty Associated with Timing

Both the MCRA timeline and individual HFE timelines should be based on best estimates, to the extent possible. Ideally, each scenario should be talked-through and walked-through with operators in order to determine the time it takes to perform the actions (including travel time). In addition, all times are typically presented as point estimates for convenience of understanding the scenario. However, each point estimate could be replaced with a timing range if a range of times is determined to be more appropriate. The ranges in response time can also be collected as part of the talk-through and walk-through collection of data. The upper bound of the response time

ranges can be used initially and then refined as needed depending upon the impact on the HEP, and the degree to which a conservative HEP impacts the fire PRA results.

In general, there will likely be greater uncertainty associated with timing information that is based on assumptions than the timing data which is simulated or observed via a JPM or walk-through. Examples based on assumption include:

- Time to abandon
- Timing associated with coordination of multiple concurrent actions.
- Timing associated with key communications

It is recognized that MCRA scenarios are complex and there is more subjectivity associated with these scenarios than with internal events scenarios. Once a base MCRA scenario has been constructed, the HRA analyst can perform sensitivity studies on individual time parameters to determine the overall impact on the timeline.

7.8 References

1. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,* U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
2. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.:2012. 1023001/NUREG-1921.
3. U.S. Nuclear Regulatory Commission. NUREG-1852*, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,* Washington, D.C. October 2007.

8
PERFORMANCE SHAPING FACTORS FOR MCRA SCENARIOS

8.1 Introduction

This section provides guidance for evaluating performance shaping factors (PSFs) in the HRA task for MCRA scenarios. The guidance provided herein is not meant to duplicate material that was already given in NUREG-1921 [1], but to provide those items and issues specific to the evaluation of PSFs that are particularly relevant for MCRA. Typically the evaluation of the PSF impacts are evaluated following the definition of the HFE and the feasibility assessment; however, the qualitative analysis should be considered an iterative and cyclical process. Note that the process of reviewing timing and PSFs also provide an initial qualitative analysis for input to the HFE quantification.

The guidance for evaluating PSFs is primarily derived from the list of PSFs developed in NUREG-1921 [1] and the experience of PRA analysts in identifying the kinds of MCRA sequences modeled in those PRAs. The impact of the PSFs on human actions is based on several sources: (1) the literature review of the bases for human performance assessment [2], (2) interviews with current and former operators and trainers, (3) the experience of analysts in using various different HRA methods and what these methods indicate about the effects of different PSFs and the contexts in which they are influential, and (4) the experience of analysts in performing fire and MCRA HRA and PRA studies.

A proper foundation of information gathered through, for example, talk-throughs or walk-throughs, is crucial for an accurate portrayal of the scenario and context and is necessary for understanding PSF impacts. Therefore, Appendix C, which describes the information gathering process, should be revisited prior to applying the guidance described in this section. Appendix C also offers guidance on how to conduct the operator interviews, plant walk-throughs and talk-throughs.

8.2 PSFs Relevant to MCRA

Although the core list of PSFs relevant for MCRA is similar to that focused on in NUREG-1921 [1], there are special considerations for each of these PSFs as well as overarching themes that must be considered.

Command and control has been identified as a “meta-PSF” (meaning that it transcends and has overarching effects on a number of individual PSFs) unique to MCRA and is therefore not discussed in NUREG-1921. It describes the need for a central body of authority to make decisions but have them carried out by a distributed group. A discussion of this topic is provided

in Appendix B, but certain command and control elements are discussed below under individual PSFs.

NUREG-1921 identifies the following PSFs as relevant for fire HRA:

- Complexity
- Crew dynamics
- Crew communications
- Cues and indications
- Procedures
- Training
- Timing
- Time pressure and stress
- Human-machine interface
- Environment
- Staffing & Availability
- Special equipment
- Special fitness needs

NUREG-1921 provides guidance on each of these PSFs that generally applies equally to the MCRA cases as well as the non-abandonment scenarios. Guidance specific to the abandonment cases is identified below for the PSFs. In some cases, NUREG-1921 included guidance for abandonment cases, and that is included below as a reminder, along with additional guidance where relevant.

In general, assessment of the PSFs for MCRA needs to consider: (1) the decision to abandon the MCR, (2) actions at the RSDP, (3) local actions in the plant, and (4) command and control issues. These topics are discussed for each PSF category.

8.2.1 Complexity

There are several possible sources of complexity associated with MCRA scenarios beyond those that apply for the non-abandonment situations. Two of the most obvious sources are: the challenge of deciding to leave the MCR (discussed further in Section 4), and, after leaving the MCR, the complexity of controlling the plant from multiple local positions coordinated via a distributed communication system. In addition, the concurrent use of multiple types of procedures (e.g., AOPs and EOPs usually prior to MCRA) will make the response more complex.

The issue of complexity arises with the combined effects of multiple PSFs. In general, operations in the event of a fire involving MCRA will be more complex than for a non-abandonment event, involving additional PSF influences not normally considered in the case of non-abandonment.

These are mostly because of the change in the command and control environment caused by the operating crew being dispersed to multiple locations rather than being co-located in the MCR. As a result, additional PSF characteristics need to be considered, not only individually but also in combination, to understand how the reliability of the operations will be affected. Appendix B goes into more depth on the issue of command and control and how to consider the effects on PSFs.

Issues that need to be addressed in evaluating the degree of complexity are:

While in the MCR:

- The extent of guidance provided in the procedures or training on the decision and when to abandon the MCR (for loss of habitability and loss of control)
- The potential for spurious (false) cues and indications that may occur in the MCR because of fire-related damage that may cause a delay in deciding that abandonment is necessary.
- The degree to which the AOPs associated with abandoning the MCR are coordinated with the EOPs directing the response to the plant shutdown. For example, do the AOPs direct the MCR crew to take copies of the EOPs with them during abandonment? Do they provide guidance on how the procedures interact in terms of priorities?

After abandoning the MCR:

- The number of different locations that require manual positioning for taking plant readings and local control actions; also the number of movements of plant personnel between different locations during implementation of the MCRA procedure.
- The degree to which the control actions required of operators involve challenging calculations or control actions that have indirect effects (for example, controlling a rapidly changing level by means of a manual flow-restricting valve) or involve physical challenges (accessing equipment in cramped spaces or using ladders or multiple turns of a difficult/large handwheel).

Complexity generally feeds into timing considerations in the HRA, since more complex and challenging cognitive or execution actions are expected to require more time to perform. Reflecting complexity in the timing can become an important factor in the assessment of MCRA action feasibility given the time constraints for when the actions need to be completed. These issues are discussed further in the MCRA timeline in Section 7 of this report.

8.2.2 Crew Dynamics

Because command and control is different for MCRA than in the MCR, these factors are considered to be even more influential. As has been discussed with the impact of other PSFs (e.g., complexity), further guidance on the special consideration of the impact of crew dynamics should be considered within the overarching theme of command and control covered in Appendix B.

At some plants, in addition to the Shift Supervisor (SS) providing command and control at the RSDP, the Shift Technical Advisor (STA) may play a role in maintaining the “big picture” of the situation and may even assist with monitoring parameters and following the procedure(s). At

other plants, the STA may be deployed as a field operator to take actions as directed by the SS. This use of STA resources is plant-specific and needs to be determined based on interviews and simulator exercise observation.

The distribution of crew members who take an MCRA procedure attachment and perform it independently with potentially no additional crew backup (as would be available for actions performed in the MCR) is another factor for consideration.

8.2.3 Crew Communications

Section 4.6.10.3 of NUREG-1921 [1] discusses the issues of communications related to operations at local panels and at the RSDP. For local actions, communication may be much more important because of the possibility of a less-than-ideal environment or situation. The way in which equipment faults caused by the fire could affect the ability of operators to communicate as necessary to perform the desired act(s) should be understood. For instance, having to set up equipment and talk over significant background noise and possibly having to repeat oneself several or many times should be considerations, even if only as possible "time sinks" for the time to perform the act. In addition, the operators' level of familiarity and training to use any special communication devices needs to be assessed.

Following MCRA, the RSDP and the locations of required related actions in plant may be in numerous places. Therefore, the ability to communicate from different places should be considered and addressed. Furthermore, if SCBA is required to be worn, the apparatus might interfere with clarity in communications among team members. The ability of operators to communicate with one another during the initiation and execution of the tasks and after their completion is critical. The role and significance of communications in command and control is discussed in Appendix B.

Specific considerations when evaluating crew communications should include:

- The command and control structure for MCRA and how communication is proceduralized, trained upon, and implemented during simulator exercises
- Whether field operators are required to simply report back what's been done or if more complicated communication and coordination is required
- Whether or not the operators are using 3-way communication
- What type of equipment is being used, the number of redundant and backup systems available, and related issues for ensuring operability (e.g., the need for extra batteries for the radio, or paging systems that are not functional in certain areas or during loss of offsite power events)
- The assignment of radio frequencies or other methods for avoiding cross talk.

8.2.4 Cues and Indications

NUREG-1921 [1] provides a comprehensive description of issues associated with indications and cues for ex-control room actions including those taken at alternate or remote shutdown panels. That material should be reviewed when addressing this PSF.

However, it should be recognized that each plant and each RSDP is different, so the guidance below needs to be considered within that context and plant-specific cues, displays and annunciators (or the lack of them) need to be analyzed.

Prior to abandonment, the primary cue for diagnosis of a fire – aside from a fire in the MCR itself - is the fire alarm. Analysts should note the location of the fire alarm panel(s) in the MCR, whether they are on the front or back panels, and how easy or difficult it is to determine the fire location and severity (often an operator is sent out to locally verify these). Another important cue for the HFE decision to abandon the MCR due to loss of control is that plant parameter indications in the MCR would be giving conflicting and nonsensical readings,

Specific to MCRA actions, the functionality at the RSDP and the potential need to get cues and indications from another location should be considered. Regarding RSDP functionality, it is important to ensure that the fire PRA circuit analysis task has verified that RSDP functions remain available for the fire scenarios where MCRA is likely to occur. At some sites, the indications on the RSDP (such as reactor level, reactor pressure, suppression pool level, etc.) are functional even with the master transfer switch in the "normal" position. At some plants, taking the transfer switch to the "transfer" position will isolate the cables associated with these instruments from the MCR or the cable spreading room (CSR) to assure the instruments will be unaffected by a MCR/CSR fire.

Note that the analyst may decide to identify a separate HFE for the actions associated with transferring control from the MCR to the RSDP, including the case where “pre-staging” activities are taken prior to leaving the MCR altogether. If cues and indications inside the MCR are impacted by the fire, but abandonment is not yet required, then some plants may implement a strategy where they can send an operator to the RSDP and communicate back to the MCR plant information as necessary. If this strategy is implemented the HRA should consider instrumentation fidelity at the RSDP in-conjunction with the MCR.

Analysts should also check whether the system parameter indications are easy to locate on the RSDP and whether they present any human-machine interface deficiencies.

The RSDP may only have a small annunciator panel or no alarms at all, and there may or may not be a safety parameter display system (SPDS) available there. This can impact awareness of parameters and conditions, and should be analyzed as part of the limitations of command and control at the RSDP versus the MCR.

Another important task for the analyst is to conduct a comparison of the cues and indications presented on the RSDP and the information required to be monitored by the MCRA procedure itself, or other procedures either called out by the MCRA procedure or identified during operator interviews as being used at the direction of the Shift Supervisor (SS). The availability of the Technical Support Center (TSC) and the resources of the Shift Technical Advisor (STA) to provide input and guidance on parameters should be assessed and the “big picture” guidance that is usually available in the MCR, but is not at the RSDP.

Operator interviews of the MCRA process usually determine that operators would be sent as considered necessary to look locally at equipment and indications. NUREG-1921 [1] points out

that the crew may have less or even limited familiarity with the local panels (those that are not RSDPs) and the way in which cues for actions are presented there (in terms of layout, demarcation and labeling). These issues must be considered during walkthroughs and interviews in evaluating the adequacy of relevant cues for post-MCRA actions. As with the RSDP, analysts need to ensure that there are cues on the local panels consistent with those required by the procedures. In addition, the potential effects of crews no longer having access to all of the information in the MCR (such as the full set of annunciators/indicators, plant drawings and other documentation) need to be evaluated.

As a result of this evaluation, the analyst should be able to assess:

- The availability of information required by the procedures and the tasks
- The fidelity of this information for various fire scenarios (as determined by circuit analysis)
- The information that is available at the RSDP versus locally

In addition, from the perspective of command and control, the limited information available at the RSDP may leave the SS concerned that there are conditions in the plant that he/she cannot observe and may act to distract him/her. The analyst can inquire during interviews as to whether there any concerns by the SS or staff as to plant conditions for which they may not be able to observe, and which might act as a distraction or source of stress.

8.2.5 Procedures

Unlike EOPs that are by-and-large standardized for each of the vendor groups, the procedures that would govern the evacuation of the MCR are written on a plant-by-plant basis, and therefore do not necessarily meet the same stringent criteria (for example, the formatting) associated with EOPs and other similar procedures. As a result, the individual plant MCRA procedures need to be reviewed for:

- Identification of the location of the fire – Some plants have detailed procedures indicating actions required given a fire in a particular area based on the fire alarm panel identifiers and stipulate that local verification of the fire location and severity must be made. The question to analysts is: will the operators have enough time to confirm the location and severity of fire given the MCRA scenario timeline(s)? [See Section 7 for more discussion of timelines and timing.]

- Identification of appropriate and actionable criteria to guide the decision of when to evacuate the main control room because of a fire

- Identification of actions to be taken before formal abandonment of the MCR (control actions like tripping the plant, etc., announcements of change in control status to plant areas, isolation of controls in MCR, identification of unreliable indications, etc.)

- Relevance to the fire PRA scenarios for MCRA and the associated PRA scenario feasibility criteria - historically, U.S. fire procedures were written to address the 10 CFR Part 50, Appendix R criteria [3], which may or may not match the PRA success criteria.

- Inclusion of the collective set of MCRA actions for all operators in all locations - For example, are communication points clearly identified in the procedures? Are multiple appendices supposed to be performed at the same time? Understanding of the structure of the MCRA procedure, its relation and application with EOPs, AOPs, ARPs, and how they will actually be implemented by operators. For example, are there separate attachments for individual operators to use in separate locations? Is the procedure structured by fire area, equipment impacted and equipment required?

- Inclusion of clear "kick outs" from the MCRA procedure to other procedures required to implement the actions needed to reach a safe and stable condition

- Specification of who goes where and what to take (such as EOPs, radios, keys, etc.)

- Description of how the command and control of the proceduralized actions will be carried out and by whom.

The review of the MCRA procedure(s) should ensure that they contain sufficient information in a clearly laid out format and written in a readily understandable language that facilitates their use during the high stress conditions of the event. Interviews, table top discussions, and walkthroughs can inform how the procedure(s) would be implemented by the operators and can reveal any disconnects in how the procedure is described versus how it would be applied by the operators.

8.2.6 Training

In the case of plant fires and especially for MCRA scenarios, training is typically given on a less frequent basis than for EOPs and in a less realistic simulator setting; often talk-through training with some visits to plant areas is provided once per year. Very few plants have a simulated remote shutdown panel for training, instead using anything ranging from just a cabinet or perhaps a computer terminal up to the use of a full mockup.

Consistent with discussions in the Procedures PSF Section 8.2.5, the training should be reviewed to verify inclusion of the collective set of MCRA actions for all operators in all locations. The interview template provided in Appendix C may be useful when interviewing the operators to understand how the integrated training incorporating training on MCRA and use of the RSDP is accomplished.

Given the wide variability in training, the following issues need to be reviewed for a specific plant to assess the plant-specific PSF for training:

- The frequency and comprehensiveness of training for MCRA, including training on making the actual decision to abandon the MCR, and ensuring that the necessary tools, procedures, knowledge of work locations, etc., have been preplanned
- The use of any kind of learning aid(s), such as a simulator or mock-up of the RSDP
- Whether the training involves visits to plant areas to:
    - Become familiar with access routes and any limitations, including consideration of locked doors, security barriers, radiation and other environmental access controls, etc.

    - Identify the location of local controls and indications
    - Evaluate communications tools (radio signals, sound-powered telephones, etc.)
- Donning and wearing of SCBA or other PPE

It is strongly recommended that the HRA analyst attend a simulator training session for MCRA to see how it is conducted, what the operator response is like, how the decision for MCRA is made and how actions at the RSDP and local panels are trained upon. Some feeling for the timing of the scenario can also be gained as well as insights to procedure use and other PSFs. Attending the post-training exercise briefing is important as well to obtain insights on what went well or not so well, in the trainers' eyes.

A separate walkthrough of the MCRA process should also be conducted to access local areas where actions will be taking place.

8.2.7 Timing

Timing is discussed extensively in Section 7 of this report and is also covered in NUREG-1921. When considering timing, the HRA task needs to consider (particularly for the LOC events) the three phases of abandonment described in Figure 7.1 as well as the actions taken following abandonment.

For MCRA actions or alternate shutdown approaches, enough time must be allowed for the operators to perform the required actions to achieve and maintain a safe and stable plant condition (e.g., hot shutdown) from an alternate shutdown location(s) or panel(s). Included in this required time is:

1. The travel time to reach the required destination, considering the starting point of the travel (e.g., starting from the MCR, the RSDP, or an ex-plant location where operators report in case of fire?),
2. Time needed to diagnose the plant conditions, and
3. Time needed to execute the required responses.

Uncertainties in other PSFs (discussed in other subsections of this section) that could affect the completion of actions within the time available (such as the uncertainty in cues and indications, the need to access other procedures, or the environmental conditions that might require SCBA to be donned) must be considered. Section 9.4 on Uncertainty discusses the consideration of parameter uncertainty, including PSFs.

Section 4.2.2 of NUREG-1852 [4] mentions equipment access, different travel paths resulting from the fire location, and expected variability among individuals and crews as other contributors to timing uncertainty.

8.2.8 Time, Pressure, and Stress

This combination of factors is treated as a single discussion because they are so integral to each other; it makes little practical sense to try and separate them. Interviews of operations and training staff at various plants have confirmed that MCRA will be a stressful situation for the operators. Timing of actions and how quickly the operators must respond may also increase the

pressure and stress felt; however, the impacts will be different for long-term versus short-term actions.

The issues associated with this PSF for MCRA are:

- Stress of leaving the MCR
- The amount of work that is required by each plant operator involved in fulfilling tasks in the procedure(s), especially where travel to plant areas (either initially or during the response) is involved.
- The effort required to reach the areas, including the physical and administrative demands, coupled together with the time urgency and requirement for the actions to be taken.
    - This includes the need to identify an alternate travel path to avoid any areas that the operators recognize as potentially hazardous.
- The experience of having to don SCBA or other PPE seldom used.
    - Narratives from other settings indicates that some fraction of people become panicked when using SCBA due to claustrophobia or similar afflictions[21].
- The effects of possible distractions on the cognitive tasks of the shift supervisor (SS), including:
    - Interruptions and unnecessary calls from staff not directly related to immediate plant responses
    - The need to perform proceduralized tasks that are not essential to the PRA-modeled tasks

8.2.9 Human-Machine Interface

The issues of interest with human-machine interfaces can be quite varied depending on whether the particular plant has a RSDP for MCRA or whether all or most actions must be taken at local controls distributed in plant areas. It is possible to evaluate the design of the interface and layout at the RSDP in terms of the kinds of human-factors criteria used for MCR designs, such as the use and layout of mimics, readability of indications, provision of feedback to confirm control actions taken have been effective (e.g., valve positions and motor states) and so on. (In some cases, the panel's design is similar to the layout of related panels in the MCR, which should simplify the operators' understanding of the panel.) For actions in plant areas separate from the RSDP, the concerns include whether the indications can be read with sufficient accuracy and the controlling devices (including manual valves) can be operated sufficiently easily and promptly to accomplish the requirements of the EOP steps. For both locations (i.e., actions at RSDP and at local panels), the feasibility of executing long term control actions should be also be considered.

A walkthrough of the MCRA process should therefore be conducted to see the RSDP, access local areas where actions will be taking place and to note the key parameter indicators and interface points at each location to see whether they appear clear or confusing. It is recommended that this walkthrough be done after the HRA analyst has reviewed the MCRA

[21] Anecdotal information from military fire training, for example.

procedures and has become familiar with the MCRA scenarios identified in the PRA to know which parameters and controls are of particular significance.

A specific issue unique to fire PRA is the potential disablement due to fire of the IN 92-18 motor-operated valves [5]. Spurious operation of these valves can cause their motors to be damaged and render them unable to be operated further. It is unlikely that controls for 92-18 valves will be located on the RSDP, however local actions may be included in the plant fire or MCRA procedure to manually reclose them after a fire. The HRA analyst should therefore interface with the fire PRA component selection task cited in NUREG/CR-6850 [6] and the plant engineering staff to identify any such valves to ensure that local operator actions to manipulate such valves after a spurious operation are NOT credited.

The items, therefore, to be evaluated for this PSF are:

1. *For plants <u>with</u> remote shutdown panels*:
    - Are the parameters cited in the MCRA procedures provided at the RSDP and do they present the information in a way that facilitates operator understanding of the conditions? In other words, are parameters that must remain below a particular level displayed digitally or are parameters that involve a trend shown as a graph?
    - Are control provided for key MCRA scenario equipment at the RSDP or must they be manipulated locally?
    - How well does the layout of indications and controls on the panel comply with the human-factors guidance for MCR panels? Section 12.2 of NUREG-0700 [Ref. 7] presents guidelines for the design of local control stations (including RSDPs) in terms of HMI design requirements. These are less detailed than for the MCR, however, and therefore it is necessary for the HMI to be reviewed for the potential for errors. (See also the discussion in Section 4.2 of Appendix B.)
    - Is there sufficient space at the panel to place procedures and other documents to allow the operators to consult the documents when taking actions or directing others via communications?

2. *For plants <u>without</u> remote shutdown panels or where actions must be taken other than at the shutdown panel*:

    - Is feedback to field operators provided for local actions?

    - For <u>each</u> indication used in responding to the initiating event via the EOPs, is the display clearly identified, adequately clear, and sufficiently readable from where the operator will be to make the judgments of the value compared with the EOP requirements? (It is recognized that the requirements of Section 12.2 of NUREG-0700 [7] for the HMI design of local control stations set minimum standards for indications and controls)

    - For <u>each</u> control used in responding to the initiating event via the EOPs, is the location of the control device (switch, breaker, valve, etc.) clearly labeled and accessible/visible to take the necessary action without non-installed access aids (e.g., a portable ladder not required to be located by the control or portable lighting to illuminate the RSDP area).

8.2.10 Environment

Section 4.6.7 of NUREG-1921 [1] identifies the issues associated with actions required outside the MCR. Of special consideration for MCRA are long term actions. Specifically, would heat or radiation have an impact on how long someone could keep going in a particular area (i.e., mission time given environmental changes)?

8.2.11 Staffing and Availability

Issues related to sufficiency of staffing and the availability to respond to events may be of concern for MCRA scenarios. More operators than are normally in the MCR may be needed to take actions close in time in multiple plant areas, and the time needed to travel between locations may prevent operators being able to accomplish multiple actions. Additionally, operators may be required to coordinate actions in multiple locations. The possibility of using staff from another unit may be considered. This will not be practical, however, for plants having a single MCR for multiple units, nor in the event of a multi-unit fire.

8.2.12 Special Equipment

As described in Section 4.6.8 of NUREG-1921 [1], operators will likely need to be prepared with portable equipment for locally accessing and operating equipment. In addition, means for accessing secure areas (e.g., keys, any special badges, etc.) will be required. These items must be taken to the RSDP from the MCR upon abandonment (if they are not provided at the RSDP). Beyond these considerations, there are no significant issues apparent for MCRA that were not already covered in the discussion in NUREG-1921.

8.2.13 Special Fitness Needs

In order to implement actions outside the MCR, the operators will need to be capable of reaching and taking actions in areas that may be difficult to access or need PPE such as SCBA. This capability may require the operators to be suitably fit to accomplish these actions. NUREG-1921 explains that the HRA analyst should verify that unique fitness needs are not introduced due to the fire and its effects (e.g., needing to move and connect hoses, especially if using a heavy or awkward tool).

8.3 Special Considerations for Decision to Abandon on Loss of Control

While the PSFs related to the decision made by the operators to abandon the MCR on LOC have been highlighted in the previous sections for the individual PSFs, the issues and factors important for the cognitive decision to abandon the MCR in LOC scenarios are summarized here. Modeling of this decision to abandon is discussed in detail in Section 4.

Timing estimates during LOC situations will be more difficult to ascertain as the decision to abandon will be based on cues of system and function loss due to the severity of the fire, procedure direction clarity on how these cues translate into abandonment criteria, and training on the decision process itself. Ultimately, the decision is typically at the discretion of the operating crew. Section 7 describes the calculation of the timing elements considering that, for most U.S. nuclear plants, the criteria for abandonment can vary widely from simply abandoning upon

confirmation of an MCR fire to not being clearly defined to allow a timely abandonment decision.

In addition to the uncertainty in estimating the timing of the decision to abandon, the decision to abandon during a LOC scenario also has increased complexity. In particular, the complexity of the diagnosis needs to consider that the behavior type during the diagnosis process may not fit into the typical nominal behavior types used for most actions, primarily because of the non-specificity of the cues. Therefore, the complexity aspect should be described in terms of the effect of the strategy on the behavior type, and whether it is a nominal example of that type or a "degraded" one.

Finally, crew communications, staffing, and dynamics may be unusually impacted during LOC situations. While the procedures will state who makes the decision, it may not be clear how the decision is reached since the decision is a function of the culture of the operating crew and how they interpret the level of damage to key plant systems and functions that render the MCR inoperable. Interviews and simulator exercises play a significant role in defining the crew dynamics of the decision process, for example, the extent to which it is consensus versus declarative.

8.4 Guidance for Evaluating PSF Impacts

This section provides guidance on how to assess the reliability of human actions in a qualitative manner. While the ultimate goal is to provide the means for quantifying the error probabilities of HFEs modeled in the MCRA PRAs, assessing the reliability qualitatively will provide a basis for identifying: (1) which kinds of accident sequences are most affected by which PSFs and scenario characteristics, and (2) the kinds of PSFs that need to be incorporated in an HRA quantification model to be used for these sequences.

This guidance was developed by first considering how different kinds of scenarios that are modeled in the MCRA PRAs will affect the various types of PSFs. Second, the guidance considered what effects these PSFs will have on the reliability of the human actions in these scenarios. For example, the likelihood of success in a scenario that requires actions at many plant locations would likely be challenged by a low-staffing PSF, and that low-staffing PSF needs to be accounted for in assessing the overall HEP for the collective set of response actions. In contrast, the effect of this PSF may not be important for scenarios that do not require so many actions at plant areas but are simply controlled from the RSDP.

In some cases the interaction of the scenario and one or more of the PSFs may be adverse, resulting in a lower likelihood of success, and in other cases it may be beneficial. For example, a well-designed remote shutdown panel that even mimics the MCR will take advantage of the training the crew has received on the instrument and cues in the MCR.

The assessment guidance provided here was influenced by the list of PSFs developed in NUREG-1921 and expanded upon in the above sections as well as the experience of MCRA PRA analysts in identifying the kinds of sequences modeled in those PRAs. In addition, the guidance was heavily influenced by the interviews of current and former operators and trainers conducted by the authors of this report. The ex-operators interviewed represented experience at BWRs and PWRs, and several also had experience as operator trainers. Several themes arose

during these interviews helping the authors to better understand the context surrounding MCRA as well as better define the situations and performance shaping factors that may have the biggest impact. Feedback was received on various issues such as how a two-unit shutdown is handled, what parameters might be difficult to control locally, how training is conducted, if the determination of timing used during training is realistic, and differences in the distribution of RSDP capabilities at a sampling of plants.

Tables 8-1 and 8-2 provide tools for the PSF assessment. Table 8-1 provides examples of the type of PSF impacts that an analyst might see for certain characteristics that were identified as distinguishing factors from the HRA perspective for MCRA scenarios. While it is possible that a PSF can be better than optimal and this can be noted in the documentation as a "kudo" to the plant design or practices, these positive PSF influences only influence the HRA as compensatory factors for other detracting PSFs. For this reason, Table 8-1 lists the potential detracting PSFs for a given scenario and their associated compensating PSFs. For example, the degree of capability of the RSDP has a significant impact on the HRA evaluation of an MCRA scenario. When the analyst is assessing the capability of the RSDP, one of the key attributes to evaluate is whether the RSDP provides indications for the parameters that need to be monitored and controlled by the operators during MCRA scenarios, as defined by the MCRA procedure. Therefore, Table 8-1 advises the analyst that the HMI for the RSDP or local stations could differ significantly from the MCR, providing a detracting PSF (negative impact upon the analysis). However, the analyst also needs to assess whether the Procedures and Training provide an adequate compensating PSF to counterbalance the detracting HMI PSF. These evaluations will be based upon procedure reviews as well as operator and training staff interviews/walkthroughs/talkthroughs. In this sense, Table 8-1 provides 'things to look for' both in terms of MCRA scenario characteristics and PSF issues that matter most to the qualitative analysis of these scenarios. The intent of Table 8-1 is to provide a bridge between the qualitative analysis of PSFs discussed in this section and the quantification process to come.

Table 8-2 assists the analyst in determining which PSFs are the most significant contributors to the qualitative analysis of a particular MCRA scenario. For each of the PSF categories, the table identifies the issues that make a PSF consequential and why. For example, if a procedure is poorly worded, then it may not be executed when needed, or another procedure it calls upon may not be entered when necessary. Table 8-2 also indicates scenario-specific elements that should be considered for the PSF categories. Carrying on with the procedure example, if the scenario for which a poorly worded procedure is used is risk-significant, then a procedure modification may be recommended if agreed to by operations and training. Finally, Table 8-2 offers a selection of offsetting factors that may exist in the scenario to compensate for the negative effects of the consequential elements for each PSF category. Offsetting factors for poorly worded procedures would be the demonstration during walkthroughs that the action is simple enough not to require strong procedural direction, or the shift supervisor clearly directs the action anyway, or skill of the craft is evident. These offsetting factors would therefore soften the negative impact of that PSF's contribution to the qualitative analysis of an HFE/scenario.

The suggested application process is for the HRA analyst to identify the characteristics of the particular accident sequence being analyzed and see how they compare with the scenario characteristics presented in the first column of Table 8-1. It may be that more than one characteristic matches the sequence being analyzed. The analyst then uses the examples in Table

8-1 for each PSF category as triggers for the type of considerations needed to qualitatively evaluate each PSF. This assists the analyst in identifying which PSFs may be important influences for the reliability of human actions as indicated by the entries for the most closely matching scenario description.

Table 8-2 then helps the analyst evaluate the degree of each PSF's influence on a scenario or HFE, to either drive it to a greater or lesser concern from a risk perspective. Offsetting factors that mitigate the PSF's influence should be noted and documented. Particularly dominant adverse PSFs might even be candidates for modification (such as procedure changes or physical modifications to add capability the RSDP) to better ensure reliability.

If more than one set of characteristics matches, it is the HRA analyst's task to select either the most closely matching description or to consider more than one set of characteristics and then evaluate the overall result. If the differences warrant separating into multiple scenarios or HFEs, this should be coordinated with the fire PRA model development of MCRA scenarios, discussed in Section 3.

Table 8-1
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Compensating PSFs
Time Constrained Scenario or Scenario involving rapid response Examples BWR: Fire causes multiple stuck open SORVs. Operators must locally close stuck open SORV before TAF occurs (~6 to 30 minutes depending on how many SORVs are open). PWR: Fire causes loss of RCP seal cooling. Operators must trip RCPs within 13 minutes on loss of seal cooling to avoid RCP seal LOCA.	Timing: The less time available for recovery, the lower the reliability.	Procedures and Training: • Clear (unambiguous) direction in procedure to reduce variability in diagnosis and execution time • Timed training runs (e.g., JPMs) with emphasis on key actions Crew Dynamics/Command and Control: Clear plan in place for communicating priorities and coordinating operator actions and ensuring time critical actions are addressed when needed, despite distractions
	Procedures and Training: Actions in the MCRA procedure that are not deemed critical in the fire PRA could delay time-critical fire PRA actions and reduce the time available for recovery	Procedures and Training: • Timed training runs (e.g., JPMs) with emphasis on key actions • Re-shuffling of procedure steps to move non-risk significant ones to end of procedure
	Complexity: Challenging cognitive or difficult physical task to perform in time to prevent core damage	Procedures and Training: • Training, either in classroom or simulator exercises, that specifically address the challenging cognitive diagnosis and decision making rather than just telling the crew what the scenario is • Timed training runs (e.g., JPMs) that include actual physical manipulations

Scenario Characteristics	Detracting PSFs	Compensating PSFs
	Environment: Conditions that could make actions more difficult and require more time, such as: -Emergency or portable lighting - Heat - Cramped spaces or difficult access to locations	Procedures and Training: Timed training runs (e.g., JPMs) that include actual physical manipulations at location with discussion of possible lighting/heat issues
	Special Equipment: Equipment that could make actions more difficult and require more time to access and implement, such as: - Donning and working in SCBA - Acquiring and using special tools (location of lockers; have they been replaced/maintained) - Acquiring and using Keys or key cards for secured areas	Procedures and Training: Timed training runs (e.g., JPMs) that include actual physical manipulations at location using gear Special Equipment: Pre-staging required tools and gear to ensure they are readily available when needed
	Staffing: Staff may be allocated to fire brigade or other tasks so that insufficient staff is available to perform the required actions	Procedures and Training: Plan for MCRA covers allocation of staff and appropriate prioritization to ensure all required actions are covered
Long timeframe or delayed action <u>Examples</u> BWR: Any fire scenario that requires containment venting. PWR: Fire causes transient. AFW runs for several hours until the CST depletes and operator must then refill the CST.	Cues and Indications: Cue presented earlier in scenario but not repeated at time when action is required (and can be forgotten)	Procedures and Training: • Procedure includes clear reminder step • Training highlights need for Shift Manager/Supervisor to provide cue reminder
	Procedures and Training: Numerous essential actions in the procedures can take attention away from the essential actions identified in the fire PRA.	Cues and Indications: An additional cue presented when parameter reaches action point can be credited as a reminder to the crew to perform the required action Procedures and Training: • Procedure includes clear reminder step • Training highlights need for Shift Manager/Supervisor to provide cue reminder
	Workload, Pressure and Stress: Interim complacency or lack of vigilance until action is suddenly needed	Cues and Indications: A relevant second cue presented (again) when parameter reaches action point can compensate for complacency Procedures and Training: • Procedure includes clear reminder step after interim procedure steps can compensate for lack of vigilance

Scenario Characteristics	Detracting PSFs	Compensating PSFs
		• Training highlights need for Shift Manager/Supervisor to provide cue reminder later in scenario and also compensate for complacency
	Staffing: Staff delegated to other tasks in the interim and is occupied with other tasks when required for the action	Command and Control: Plan in place for supervisory monitoring and control of staffing
Includes actions to maintain control (initiate, actuate, stop) of a system or function (rather than a one-time action) Examples BWR: Maintain long term RCIC control (vs. start RCIC). PWR: Maintain long term AFW control (vs. start AFW).	Cues and Indications: Not all cues required for the control action are co-located at the action location(s) Complexity: Control action is distributed among various plant locations Timing/Workload, Pressure and Stress: The longer the time between each control iteration, the greater the chance that the operator will become distracted	Crew Dynamics/Command and Control: Plan exists for coordinating control actions and for providing verbal cues for control steps Communications: Supervisor (in charge of Command and Control) communicates with staff performing distributed control actions to ensure and verify that actions are taken Procedures and Training: • Procedural reminders are provided for control actions to reduce distraction • All steps of control actions are covered in JPMs/simulator training
	HMI: Parameters to be controlled are presented poorly or poorly annunciated (if at all)	Procedures and Training: • Procedure steps include specific parameter indications for reminders and actions • Training includes time at mockup or actual RSDP or local stations with highlighting of parameter presentation
Capability of RSDP (whether or not indications or controls needed are on the RSDP or whether need to access multiple plant areas instead) Examples BWR: For starting Torus cooling, The procedures direct the operators to flush the system to prevent voiding. The system is flushed by listening for water flow thru and pipes at multiple locations. The RHR pumps can be started at the RSDP.	HMI: Layout and/or controls/annunciators on RSDP differ significantly from MCR	Procedures and Training: Procedural direction and/or training notes that prepare operators for the differences between the RSDP and MCR capabilities and highlight the need to access local stations for information
	Complexity: • Not all functions can be performed at the RSDP and therefore operators must travel to and perform actions away from the RSDP • Multiple actions required in parallel at multiple locations	Timing: With enough time any number of actions can be completed. Time available for recovery can offset the multiple actions at multiple locations Crew Dynamics/Command and Control:

Scenario Characteristics	Detracting PSFs	Compensating PSFs
PWR: Starting Charging vs. another LPI system		• Clear coordination plan is in place that involves communication of action completion OR • Actions are independent and do not require significant coordination or associated communication for successful performance Cues and Indications, HMI: Action locations have all of the necessary cues/indications and controls needed for successful performance
Loss of Control, especially the Decision to Abandon	Cues and Indications: "Soft cues" such as spurious cycling of plant equipment due to fire damage or unreliable indications may not be sufficient to trigger the need to abandon	Procedures and Training: Guidance related to the inability to operate equipment from the main control board (MCB), visible MCB Panel damage, loss of indications, or spurious equipment operation AND the fire being of such a nature that there is concern about maintaining the ability to safely control the plant
	Timing: The less time available for recovery, the lower the reliability	Procedures and Training: • Clear (unambiguous) direction in procedure • Timed training runs (e.g., JPMs) with emphasis on when the decision to abandon needs to be made
	Procedures: Fire damage related conditions that would result in the Shift Manager/Shift Supervisor calling for MCR abandonment are not well specified in the procedure	Training: Guidance is provided during training (as identified through operator interviews) that gives operators a basis for determining how the procedures are interpreted and implemented in making the decision to abandon (e.g., loss of certain equipment, indications or some combination thereof)
	Staffing: Culture of the operating crew may impact the decision to abandon (e.g., would such a decision be made in an "executive" fashion by the Shift Manager, would they consult with one or more senior operations staff or managers, or would the decision be more of a consensus process)	Procedures and Training: The person who has the authority to make the decision to abandon is clearly identified in procedures and training

Scenario Characteristics	Detracting PSFs	Compensating PSFs
Reliance of skill-of-craft actions	Procedures and Training: Procedural direction limited, requiring reliance on skill-of-craft actions.	Procedures and Training: Lack of detailed procedure steps may be offset by skill-of-the-craft if (a) cue for action is prioritized through procedures and training and (b) training quality and frequency and/or experience exists and has been demonstrated Cues and Indications: Cue for action is clear and distinct
Multi-Unit site	HMI: Different RSDP and local interfaces for the different unit(s)	Procedures and Training: Training involves time at the other unit's RSDP
	Staffing: More personnel to coordinate for an already complex scenario can lead to confusion about roles and tasks	Procedures and Training: • Procedures and/or plans include clear direction of the unit in charge given the impacted unit and staff responsibilities • Multi-unit staffing and responsibilities are clearly covered in training (as indicated by Operations and Training responses to interview questions)
Other concurrent initiators/special conditions in addition to fire, e.g., Station Blackout (SBO) resulting in additional recovery actions for emergency diesel generator start and associated bus load stripping <u>Examples</u> BWR and PWR: Fire causes MCRA with SBO, Transient , LOCA, LOOP, RCP seal LOCA (PWR only)	Workload, Pressure and Stress: Concurrent initiators typically result in high workload for the operators because these scenarios usually require the use of multiple procedures Cues and Indications: SBO impacts instrumentation availability	Procedures and Training: • Procedure provides alternative indications and warnings of indication impacts in case of SBO • Training includes time at mockup or actual RSDP or local stations highlighting parameter fidelity in case of SBO
	Workload, Pressure and Stress: Multiple actions needing to be performed within a specific timeframe	Procedures and Training: • Procedural reminders for control actions • All steps of control actions are covered in JPMs/simulator training
	HMI: Concurrent initiator scenarios could require manipulation of equipment which is not frequently trained upon or not manipulated frequently. The HMI for components may not be ideal. For example, breaker cabinet labeling could be similar and could cause confusion about which breakers to manipulate	Procedures and Training: • All steps of control actions are covered in JPMs/simulator training to provide familiarity with tasks • Actions are similar to non-MCRA SBO actions that are trained upon more frequently
	Environment: Concurrent initiating events may result in less than ideal environmental conditions such as lack of normal lighting, high	Special Equipment: Emergency and portable lighting is available at specified locations

Scenario Characteristics	Detracting PSFs	Compensating PSFs
	radiation areas or high temperatures.	Procedures and Training: High radiation or temperature environmental conditions may be addressed in procedural warnings or during training
	Staffing: Staff may have multiple tasks to perform and may not be available to perform required actions concurrently and may need to sequence /prioritize actions	Procedures and Training: Plan for MCRA covers allocation of staff to ensure requirements are met
	Communications: Additional field locations from which operators must relay information on status of task(s)	Crew Dynamics/Command and Control: Plan in place for supervisory monitoring and control of communication and coordination

Table 8-2
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Offsetting Factors
Procedures and Training	1) Do not exist	Potentially insufficient guidance for required action(s)	If risk significant, consider procedure modification	Training/experience/procedure mod
	2) Do not match situation	Inappropriate guidance for required action(s)		Training/experience/procedure mod
	3) Take too long	• Find out why • Nice to have vs. must do actions	Depends on scenario timing	See Timing
	4) Insufficient training (also training)	• Classroom vs. realistic (communications) • Integrated (field operators & communications included) • Security drills	If scenario involves coordination of multiple operators and communications, training should cover it	• Simplicity of action • Strong supervision • Skill of the craft • General training
	5) Poorly worded	• Not entered • Not executed • Insufficient level of detail • Attachments	If risk significant, consider procedure mod.	• Simplicity of action • Strong supervision • Skill of the craft • General training
Cues and Indications	1) Ambiguous	Event parameters inconsistent with design of indications		• Simplicity of action • Strong supervision • Skill of the craft • General training • Clear procedural directions
	2) Spurious indications	Fire-induced effects		• General training • Specific training • Clear procedural direction of indications impacted or not impacted by fire
	3) Located in hard-to-see locations (also HMI)	HMI issues at plant area or RSDP		• Strong supervision • Skill of the craft • General training • Specific training

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Offsetting Factors
	4) Absent	HMI issues at plant area or RSDP		• Strong supervision • Skill of the craft • General training • Specific training • Clear procedural directions
Complexity	1) Need for challenging calculations or complex control actions	• Coordination between fire procedures, AOPs and EOPs • High workload can exacerbate		• Strong supervision • Skill of the craft • General training • Specific training • Clear procedural directions
	2) Coordination at multiple work locations (also communications)			
Workload, Pressure, and Stress	Number of tasks is inconsistent with time available	Can't complete actions in time	Should have been evaluated via JPMs and simulator exercises for MCRA training, but these may not have included time required for LOC cognitive portion	May be nothing else to do but see if there are any "nice to do" actions that can be removed, procedure mods that can be made, or physical mods that can be installed
HMI	Capabilities of RSDP do not match MCRA tasks required	Requires local checking or manipulation	Should have been evaluated during MCRA training sessions	Physical plant mod of alternate cable runs to make action feasible on RSP? Alternative local action(s)?
Environment	Fire is in work area itself		Not usually an issue for MCRA, but should be checked; if so, HEP is set to 1.0 for that fire area	Physical plant mod of alternate cable runs to make action feasible? Alternative action in accessible area?
	Heat conditions exist			limit time the worker can be in the area
	Poor lighting			Emergency lights available and where needed or have to use flashlights/headlamps

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Offsetting Factors
Special Equipment	SCBA required	Limitations on visibility, movement, time to implement task		Additional staff available to take over task?
	Tools required	Stored in lockers and regularly maintained/put back? (usually a process/procedure for this)		Communicate need for tool
	Keys required	Access permissions and where keys are located (f not on belt)		Notify Supervisor who in turn calls Security
Special Fitness Needs	Climbing ladders; difficult access to equipment	Impacts timing of task and reliability		Sufficient/extra time available
Crew Staffing / Availability	Crew diverted to fire brigade	Not usually an issue for MCRA, but should be checked		• Emergency planning (prior preparation for number of staff needed) • Sufficient/extra time available
Communications	Radios do not function properly in task areas	No diversity or functionality of communication systems (should be a procedure for this)		• Emergency planning (prior preparation for communication needed)
	Protocols for communication are not used	Procedural direction/confirmation or other instructions not clear/verified		• Strong supervision
Timing	Time required > time available	Could be infeasible	Look at JPMs and simulator exercises for MCRA training	May be nothing else to do but see if there are any "nice to do" actions that can be removed, procedure mods that can be made, or physical mods that can be installed
	No clear cues for abandonment	Requires additional diagnosis and decision-making time		LOH cues are clear; LOC can be identified through discussions with Operations and insights from fire PRA and fed into procedure

8.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. U.S. Nuclear Regulatory Commission. NUREG-2114, *Cognitive Basis for Human Reliability Analysis.* Washington, D.C.: January 2016.
3. 10 CFR Part 50, Appendix R, Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979.
4. U.S. Nuclear Regulatory Commission. NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, Washington, D.C. October 2007.
5. Information Notice No. 92-18: *Potential for Loss of Remote Shutdown Capability During a Control Room Fire*, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC: February 28, 1992.
6. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
7. U.S. Nuclear Regulatory Commission. NUREG-0700, Revision 2, *Human-System Interface Design Review Guidelines*, Rockville, MD: 2002.

9
RECOVERY, DEPENDENCY, AND UNCERTAINTY

9.1 Introduction

This section provides guidance on recovery, dependency, and uncertainty for MCRA HRA. The fundamentals of each of these steps in the HRA process are not unique to fire HRA or MCRA HRA. As with previous sections, this section builds upon the existing information provided in NUREG-1921 and cites the differences and corresponding approaches to address these differences.

9.2 Recovery

NUREG-1921 cites the following definition for a *recovery human failure event*: "the failure to restore failed equipment or find alternative equipment or configurations within the time period required" [1][22]. NUREG-1921 also says, "After the initial fire PRA model quantification, recovery actions may be identified to restore or reconfigure a function, system, or component initially unavailable in the scenario. Accounting for such a recovery would reduce the frequency of the scenario." The recovery actions considered in NUREG-1921 are those that were not added to the fault trees and event trees as part of the initial, planned plant response. Instead, these actions are added at the sequence or cutset level to realign the affected system or to provide an alternative system, such that success of these actions would have prevented core damage and/or large early release.

Recovery, however, has two different meanings, both of which are noted in NUREG-1921: 1) the PRA-based version mentioned above and 2) the recovery *within* an action, such as the self-check by the operator him/herself performing the action or review by other operations crewmembers that catches an error. Recovery according to meaning 1) is not really applicable to MCRA because MCRA itself is fundamentally the recovery. That is, in the context of the PRA, MCRA is a set of recovery actions for responding to a situation where the normal plant response procedures will not work, and MCRA is used to recover from that condition. The MCRA procedures encompass all the possible actions that can be used to accomplish that recovery, so there are no additional recovery human failure events to consider (i.e., there is no "recovery" from a failure to successfully implement MCRA, whether due to human or equipment failure).

Opportunities for recovery within an HFE for MCRA scenarios do exist. They may be less likely due to the lack of "backup" when operators are distributed among multiple locations (rather than all in the MCR), but this will depend upon the structure of the procedure and the capabilities of the remote shutdown "command-and-control" (C&C) location. When an action

[22] This definition of recovery, which has been in common use in PRA for many years, is ***not*** to be confused with the definition of "recovery action" used in NFPA 805.

takes place at this C&C location, additional co-located staff would have similar "checking" ability as in the MCR and could be credited in a similar fashion. When an action takes place in another location, the "checking" would be more like a local action when C&C remains in the MCR and would be implemented through communication from the local operator and confirmation based on the more limited set of indications available at the C&C location. Such opportunities are not separate HFEs, but are generally treated as dependencies between operators within an HFE. This is addressed further in Section 9.3 on dependency analysis.

Aside from those plants where the cues provided for the decision to abandon are not well defined, the MCRA actions are generally clearly proceduralized and trained upon. The actions are therefore less likely to be *ad hoc* than recovery actions in internal events and fire PRA, which often require procedure changes to fully credit. Depending upon the nature and duration of the event and the plant-specific definition of what constitutes a safe and stable condition, MCRA-related recovery actions in longer term scenarios may even be directed by the Technical Support Center (TSC), such as implementation of FLEX options.

9.3 Dependency Analysis

The ASME/ANS PRA Standard [2] requires that multiple human actions in the same accident sequence or cutset be identified, an assessment of the degree of dependency performed, and a joint human error probability be calculated. This requirement focuses upon the quantitative aspects of dependency, but the underlying qualitative dependency must also be evaluated.

One way in which dependency is qualitatively addressed for MCRA is through the development of the MCRA timeline, as discussed in Section 7. This process ensures that the timing of individual MCRA operator actions that model the critical MCRA tasks are correlated to each other and that the combined set of actions is feasible within the total timeframe available to bring the plant to a safe and stable condition.

Another facet of dependency is the treatment of recovery within an action, discussed as meaning #2 in the Recovery subsection above. Self-checking and peer checking recovery actions reflect an implicit amount of dependence between the initial cognition or execution failure and the checking action(s) that can reduce the likelihood of the initial error. The dependency level between the initial and recovery actions is assessed qualitatively according to a scale from zero to complete dependency (see discussion above Figure 9-1) and is ultimately translated into quantitative dependence that modifies the substep probabilities within an HFE. There are unique considerations for the MCRA case in this type of dependency, for example, the extent to which self-check and extra crew checking apply to cognitive decisions that occur after leaving the MCR and to the degree to which peer checking can be credited when everything is occurring through communications between local stations. Some specific considerations are:

- Where is the action being performed? Is it within the capability of the panels at the Command and Control (C&C) location? The dependency model for recovery within a HFE taken solely at this location would be similar to one taken in the MCR, while one taken elsewhere would be modeled like actions taken outside the MCR.
- How many people (and who) are at the C&C location? This goes to whether credit can be given to extra staff and/or STA.

- What indications are available at the C&C location to achieve recovery? This relates the extent of credit (dependency level to assign) for self-check, extra staff, and/or STA. The ability to check the success of the action may be less at the C&C location than in the MCR because of fewer parameters being available.
- For actions that take place away from the C&C location, the direct indications of success may only be at the location where the action takes place, thus limiting initial recovery to self-check. Whether a subsequent recovery is possible within the available timeframe would depend on whether a secondary indication is available and whether it is timely.[23]

Another way in which dependency analysis is evaluated for MCRA is through the decision-making by the HRA analyst on the definition of HFEs, as discussed in Section 5 on Identification and Definition. The HFE definition for MCRA depends in large part upon how the procedures are organized and implemented and the overall MCRA modeling strategy in the fire PRA.

If the HEPs for individual operator actions, including the decision to abandon, are combined together into a single MCRA HFE/HEP to be included in the fire PRA model, then the dependency between the individual actions should be appropriately accounted for in the logic and data associated with that single HFE/HEP.

However, if separate HFEs are defined for the MCRA actions, then the interdependencies between the MCRA HFEs may need to be assessed as described in NUREG-1921. In many (if not most) MCRA modeling in the PRA, each of the defined HFEs will lead to a failure of MCRA (i.e., all the modeled actions must be successful in order for MCRA to be successful). This is because the limited set of equipment used in the MCRA procedures provides only one path to success. In this case, there will be at most one MCRA HFE in a cutset and so there would be no dependencies to be addressed. However, this may not always be the case, for example where the procedure says to try to start and load EDG A and if that doesn't work, to try to start and load EDG B. If the HFE is defined as failure to start and load any EDG (functional), there would not be a dependency issue. If, however, there are two HFEs – one for EDG A and one for EDG B (operator action) – then the dependency would need to be addressed.

It should be noted that the individual HFEs in this approach can be defined from a functional or an operator action standpoint. In the functional case, multiple operators can be working together to restore a function and the relevant tasks performed by the various operators may be embedded in a single HFE. The HRA analyst must determine whether the timing of the single functional HFE covers the time required to perform all the embedded tasks necessary to restore the function. This is a similar evaluation as for the MCRA timeline, but is done on an individual HFE basis. Timing for these evaluations generally comes from thermal-hydraulic (T-H) analyses for the overall time available and from simulator data or training walkthroughs for the task performance timing. This is a form of dependency analysis since it addresses dependency within

[23] For example, take the case when an AFW pump needs to be started at a local station. Flow indication is only available at the local station. The C&C location only has SG level. Initially only a self-check would be possible to confirm flow. If an error is made, eventually the lack of flow would be checked at the C&C location because the SG level would not be coming up. This may provide a second opportunity for recovery if this conclusion could be reached soon enough, and an appropriate dependency level could be assigned.

an HFE, but does not address the interdependencies between the various MCRA HFEs that collectively restore all the necessary functions.

In the operator action case, individual HFEs are defined for different operator actions, such as when Operator A takes Attachment A of the MCRA procedure and performs those actions independently and Operator B does the same with Attachment B. The MCRA timeline is used to evaluate whether all the operator actions can be performed in time, but again, does not address other interdependencies between the operator actions.

The various ways in which MCRA is modeled in the fire PRA are discussed in Section 3 and the identification and definition of HFEs for MCRA is discussed in Section 5. In general, when individual HFEs, whether defined by function or operator action, are included in the MCRA portion of the model, the solution of the PRA model results in cutsets in which multiple HFEs may appear. The dependency between these multiple HFEs must be reviewed and assessed, consistent with the process followed for internal events or fire HRA, as discussed in NUREG-1921 and demonstrated in Figure 9-1. The dependence levels shown in the far right column (ZD for zero dependency, LD for low, MD for medium or moderate, HD for high and CD for complete) ultimately correlate to a quantitative process to ensure that the multiplication of multiple HFEs in a cutset does not result in a lower than credible combined human error probability.

It should be noted that the dependency decision tree shown in Figure 9-1 was designed to be a conservative first approach to assessing the dependency levels. Since MCRA scenarios involve significant communication and simultaneous actions, using the tree may result in an initial assessment of complete dependency. In many cases, however, scenario specific inputs can be used to justify a level of dependency lower than what is explicitly given by the dependency tree.

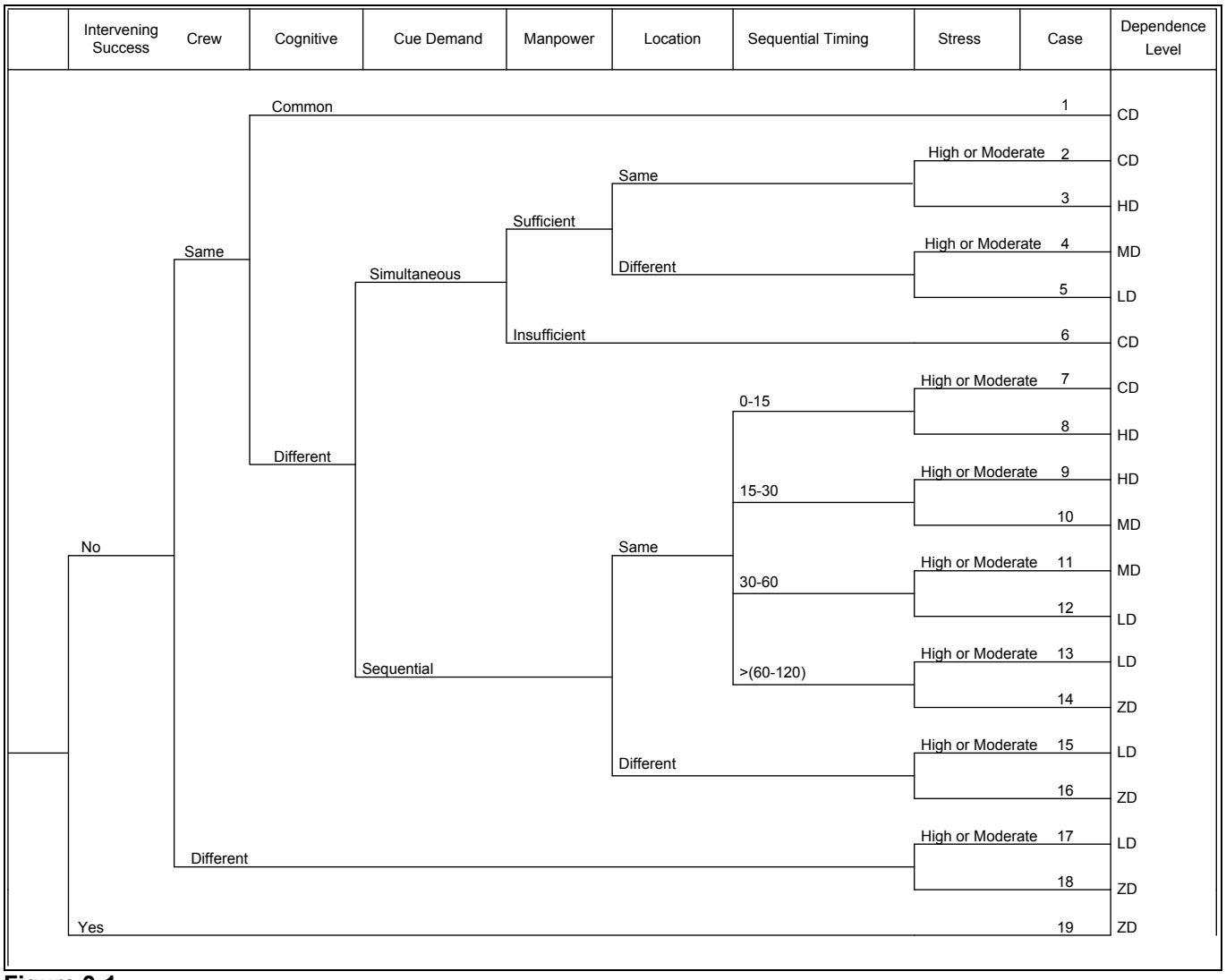

Figure 9-1
Dependency Rules for Post-Initiator HFEs

*Note: The units of the "Sequential Timing" branch are in minutes.

9.4 Uncertainty

ASME/ANS PRA Standard supporting requirement HR-G8 directs the HRA analyst to "Characterize the uncertainty in the estimates of the HEPs in a manner consistent with the quantification approach, and PROVIDE mean values for use in the quantification of the PRA results." [2] However, this does not provide much insight into the evaluation of the uncertainty of qualitative analyses for HRA.

Since the publication of NUREG-1921 in July 2012, new technical reports have been issued by the U.S. NRC and EPRI that provide guidance for evaluating uncertainty in PRA.

NUREG-1855, Revision 1 [3], provides guidance on how to treat uncertainties associated with PRAs used by a licensee or applicant to support a risk-informed application to the NRC. EPRI

1016737 [4] and EPRI 1026511 [5] provide guidance on identifying and characterizing sources of model uncertainty in an at-power reactor PRA, the former for internal events and internal flood hazards, and the latter for the internal fire hazard, seismic hazard, low-power and shutdown operational modes, and Level 2 PRA.

These documents first define the various types of uncertainty and then provide guidance for addressing them.

9.4.1 Types of Uncertainty

NUREG-1855, Revision 1 [3] provides the following overview of the types of uncertainty that are examined in PRA:

> "Generally speaking, there are two main types of uncertainty; aleatory and epistemic.
>
> - Aleatory uncertainty is based on the randomness of the nature of the events or phenomena and cannot be reduced by increasing the analyst's knowledge of the systems being modeled. Therefore, it is also known as random uncertainty or stochastic uncertainty.
> - Epistemic uncertainty is the uncertainty related to the lack of knowledge about or confidence in the system or model and is also known as state-of-knowledge uncertainty.
>
> PRA models explicitly address aleatory uncertainty which results from the randomness associated with the events in the model logic structure. The random occurrence of different initiating events with subsequent failure of components to operate and human errors lead to a large number of possible accident sequences that are accounted for in the event and fault trees used in a PRA model. The results of the PRA model evaluation (accident sequences and cut sets) represent aleatory uncertainty.
>
> Note that the exclusion of initiating events, hazards, accident sequences, systems, components, or cut sets from the PRA model results in epistemic uncertainty (i.e., in model uncertainty), and is not a contributor to the aleatory uncertainty.
>
> The different types of epistemic uncertainty are completeness, parameter, and model uncertainty."

These three types of epistemic were defined as follows in the original version of NUREG-1855 [6]:

Completeness Uncertainty – "relates to contributions to risk that have been excluded from the PRA model. This class of uncertainties may have a significant impact on the predictions of the PRA model and must be addressed. Examples of sources of incompleteness include the following:

- The scope of the PRA does not include some class of initiating events, hazards, or modes of operation.
- There is no agreement on how the PRA should address certain elements, such as the effects on risk resulting from aging or organizational factors.

- The analysis may have omitted phenomena, failure mechanisms, or other factors because their relative contribution is believed to be negligible."

Parameter Uncertainty – "relates to the uncertainty in the computation of the parameter values for initiating event frequencies, component failure probabilities, and human error probabilities that are used in the quantification process of the PRA model."

Model Uncertainty – "relates to the uncertainty in the assumptions made in the analysis and the models used…In general, model uncertainties are addressed by studies to determine the sensitivity of the results of the analysis if different assumptions are made or different models are used."

9.4.2 Relationship of Uncertainty Types to MCRA Qualitative Analysis

Each of the three types of epistemic uncertainty are discussed below in terms of their relevance to this report's mission of addressing qualitative analysis for MCRA. Input to this section is provided from presentations and discussions at the joint NRC – EPRI workshop on the treatment of uncertainty in risk-informed decision making [7, 8] held in November 2015.

Completeness Uncertainty
This category of uncertainty refers to items not included in the PRA model, which can be defined as [8]:

- Those known not to be in the model, e.g., excluded systems or equipment,
- Those not in the model because they are not known, e.g., effects of unknown failure mechanisms.

For those items that are not included in the model, the guidance from NUREG-1855, Rev. 1 [3] states that it is the responsibility of the analyst to determine the risk significance of a missing scope or PRA item by performing a screening analysis to demonstrate that the non-modeled item can be eliminated from further consideration.

Since this report focuses on the qualitative analysis of MCRA, the screening discussed here is based on the qualitative assessment of relevance.

The qualitative criteria for identifying MCRA relevant HRA scenarios will be consistent with the scope of the fire (FSS) and fire PRA modeling (PRM) tasks, as discussed in Section 3 on Modeling MCRA in the PRA logic model. In particular, Figure 3-1 shows where the guidance for the MCRA FSS/PRM and HRA fits within Task 11 of NUREG/CR-6850 [9], NUREG-1921 and this report.

Regarding the "unknown unknowns", these are beyond the capability of the qualitative analysis and are assumed to be addressed via other principles of risk-informed decision-making [8]:

- Defense-in-depth
- Safety margins
- Performance monitoring

Parameter Uncertainty

Since this category is concerned with uncertainty in the computation of the parameter values used in quantification, such as the HEPs used to quantify individual HFEs in an MCRA scenario, it is beyond the scope of this document.

However, the assumptions involved in evaluating and estimating the inputs to the calculation of these parameter values, such as timing and PSFs, are part of the qualitative analysis described in other sections of this document. These assumptions should therefore be clearly documented and may be challenged once quantitative results are obtained.

Table 9-1 lists potential sources of parameter uncertainty related to MCRA.

Model Uncertainty

The PRA standard defines a Source of model uncertainty as:

> "a source is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event). A source of model uncertainty is labeled "key" when it could impact the PRA results that are being used in a decision, and consequently, may influence the decision being made. Therefore, a key source of model uncertainty is identified in the context of an application."

Appendix A of EPRI 1016737 [4] provides tables of potential generic sources of model uncertainty for internal events, while Appendix B, Table B-1 of EPRI 1026511 [5] provides a table of potential sources of model uncertainty for fire HRA.

Table 9-1 lists the generic potential model uncertainty sources from these EPRI reports and provides an indication of the MCRA relevant issues associated with them.

Table 9-1
Potential sources of uncertainty for MCRA HRA

Category	Potential Sources of MCRA HRA Uncertainty
Parameter Uncertainty	
Timing	Timing data inputs (T_{sw}, T_{delay}, T_{cog}, and T_{exe}) where T_{delay} can be impacted by uncertainty in the data source, such as fire modeling of the time to damage based on the selected heat release rates and fire growth / spread rates, and operator action modeling such as timing for decision-making or execution (e.g. ability to collect more than one operator's input)
	Impact of timing variability on short or constrained timeframe events.
	Degree of difficulty and complexity in performing ex-control room actions.
	What to do with varying or conflicting operator input.
Stress	Ability to assess stress level.
Workload	Ability to assess what constitutes "high" workload.
Communications	Impacts to normal communications systems and processes, and the availability and effectiveness of back-up communications.

Category	Potential Sources of MCRA HRA Uncertainty
	Command and control related communication.
Training	Uncertainty associated with frequency and effectiveness of training for the collective set of MCRA actions.
Procedures	Impact of unclear cues or direction in procedures.
	MCRA procedures not in an industry standard format (like EOPs).
Cues	Impact on cues such that the indications may not be accurate.
	Compelling indications or cues that may distract the operator from the modeled task.
Model Uncertainty	
Generic HRA (from Table A-4 of EPRI 1016737)	
HFE Delineation	The discrimination of those HFEs that are to be modeled and the conditions under which they are characterized. There are hundreds of individual HFEs that could be modeled. Of these, there are HFEs that are screened or subsumed into larger groups. The larger group of HFEs is then represented by a single set of limiting conditions. MCRA relevance: decision-making on definition of individual HFEs in a scenario.
HFE Applicability	The HFE application to specific circumstances within the accident sequence may be constrained in different ways for different applications. MCRA relevance: applicability of individual HFEs to different scenarios and the definition of scenario bins.
Scenario-dependent recovery and repair	The accident sequence level of discrimination with regard to plant conditions, timing, operator interface, and use of non-safety systems. The finite nature of the level of delineation collapses the continuum of possible sequences to a limited set. Repair and recovery of failures is an area of significant judgment in the PRA model. It involves the designation of sufficient time, access, personnel, and guidance to either recovery (manual action) or repair of a failed SSC. MCRA relevance: definition of individual HFEs in a scenario based on procedure steps and equipment interfaces.
Organizational interfaces	The plant-specific organization during an event may be difficult to capture in the HRA and may strongly depend on the personalities involved, including: • Operations-Maintenance • Staff-Management • Control Room-TSC • Ex-Plant (for example, grid operator) MCRA relevance: Command and control
Errors of commission	MCRA relevance: • Failure to make decision to abandon

Category	Potential Sources of MCRA HRA Uncertainty
	• Failure to implement necessary systems and functions to prevent core damage
Procedural changes (permanent and temporary)	MCRA relevance: consideration of re-ordering or further clarification of MCRA procedure steps to improve operator action feasibility.
Human performance impact of beyond design basis conditions and environments (for example, SGTR, SBO, and ATWS)	The characterization of human performance for beyond design basis events is critical to the successful realism in a PRA. The simulator training and results from that training can support the HEP characterization. MCRA relevance: consideration of fire PRA success criteria and fire PRA scenarios applicable to MCRA based on FSS/PRM interface.
Instrumentation response resulting in degraded information flow to crew	The crew's window on the plant comes primarily from instrumentation. Failures of instrument or degraded conditions of instrumentation may significantly alter the way the crew responds to an accident, but the level of redundancy in the instrumentation should be considered as part of the performance shaping factors utilized in the HRA development. MCRA relevance: Instrumentation issues in MCR prior to abandonment; limited instrumentation available at RSDP or local control stations.
Worker-machine interface	There may be unique components, instruments, or controls that make plant operation, accident response, and recoveries significantly better or worse than the typical plant. These shaping factors are difficult to fully integrate into the HRA. MCRA relevance: limited controls available at RSDP or local control stations.
Training and procedures	Training and procedures form the basis for the HRA. MCRA relevance: clarity of procedure cues for action and degree of preparation provided by training.
Multi-unit events	Multiple units may provide both significant benefit—by virtue of the sharing of equipment and personnel—and significant challenges if all units require accident mitigation simultaneously. MCRA relevance: coordination of personnel between units and staffing availability.
Crew response times	The simulator, crew input, and JPM response times are sources of information for crew response times. All sources are not consistent and can be either optimistic or pessimistic. MCRA relevance: realism of timeline(s) constructed for MCRA scenarios.
Distractions (for example, tired, problems outside	The crew work schedule and individual crew member conditions are not generally included as part of the shaping factors of the HRA.

Category	Potential Sources of MCRA HRA Uncertainty
of work, and so on)	
Crew turnover	Period of crew turnover and the information transmittal at crew turnover is not modeled.
Crew awareness to conditions	Training can alter crew awareness. The awareness of the crew to specific accident conditions varies with the training cycle and current industry experiences that are promulgated to the crews. MCRA relevance: capture of decision to abandon in training.
Circadian clock	Time of day is not generally included in the HRA despite evidence that the most serious crew errors occur between 12 midnight and 6 a.m.
Training cycle emphasis	Training can alter crew awareness. The awareness of the crew to specific accident conditions varies with the training cycle and current industry experiences that are promulgated to the crews.
Fire HRA (from Table B-1 of EPRI 1026511)	
Impact of fire on HEP evaluation	The impacts of the fire need to be factored into the HFE analysis for the fire PRA model (e.g. added stress or limited accessibility for ex-control room actions). MCRA relevance: PSFs of stress, location
HEP Methodology	The basis for the HEP methodology utilized needs to be consistent with the internal events PRA standard requirements for HRA. MCRA relevance: quantification method selection (not in scope of current report)
Fire impacts on recovery actions	Recovery actions in the plant response model are subject to the same requirements as the internal events recovery actions. MCRA relevance: ANS/ASME PRA Standard requirements for recovery actions per SR HR-H1 and HRA-E1.
Modeling of any existing or new FPRA actions including accident sequence specific factors	Inclusion of the HFEs into the model may include modification to an accident sequence, system model, or recovery of an event. Failure to properly model the HFE impact can result in either conservatism or non-conservatism. MCRA relevance: definition of MCRA HFEs; coordination with PRM task on how to incorporate into the fire PRA model.

9.4.3 Specific Uncertainty Issues in MCRA Qualitative Analysis

Uncertainty in the input information to HRA is generally characterized in the qualitative analysis in the form of assumptions.

Assumption is defined in the ASME/ANS PRA standard as a decision or judgment that is made in the development of the PRA model. An assumption is labeled “key” when it may influence (i.e., have the potential to change) the decision being made.

Assumptions need to be clearly stated in the HRA documentation and can form the basis for follow-on operator interviews or modeling of fire response or thermal-hydraulics. Some examples of uncertainty driven assumptions related to MCRA are provided here.

As discussed in Section 4, the conditions that lead to a LOC situation involve significant uncertainty, including fire damaged cables and equipment. As a result, the timing of those fire-induced effects "complicates" the plant and operator response and may require assumptions on the part of the HRA analyst. An example of such an assumption that is a significant source of uncertainty is the case where the fire scenario, although eventually requiring abandonment to reach safe shutdown, is mild enough that the overall time window for the decision to abandon and subsequently perform the post-abandonment actions is relatively long. The source of uncertainty in that case is the time window for the decision to abandon, which can be interpreted as a time margin to recover from an incorrect abandonment decision (meaning, the operator decides not to abandon). If the analyst selects a relatively long time (effectively giving the operators additional time for recovery from the decision not to abandon), this shortens the time available for the post-abandonment actions and their own recovery and therefore these actions have a higher probability of failure. Conversely, if the analyst selects a relatively short time window for the decision to abandon, there would be more time available to perform the post-abandonment actions, but the cognitive failure to abandon would have a higher probability.

The MCRA procedures themselves can be a source of uncertainty and assumptions. Section 4 has already cited the lack of specific cues for MCRA as a source of uncertainty related to the cognitive HFE for the decision to abandon. The HRA analyst must often take the lead in defining these cues, but the time required for the abandonment decision based upon these cues is still an assumption. Some plants choose to perform an initial MCRA analysis to gain information on the key actions and time constraints, then update their procedures later, stating as an assumption of the preliminary analysis that these procedure changes will have to be made at a later date.

9.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
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. U.S. Nuclear Regulatory Commission. NUREG-1855 Revision 1-DRAFT, *Guidelines on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,* Washington, D.C. ADAMS Accession Number: ML15026A512.
4. *Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessment.* EPRI, Palo Alto, CA: 2008. 1016737.
5. *Practical Guidance on the Use of PRA in Risk-Informed Applications with a Focus on the Treatment of Uncertainty.* EPRI, Palo Alto, CA: 2012. 1026511.

6. U.S. Nuclear Regulatory Commission. NUREG-1855 Revision 0, *Guidelines on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,* Washington, D.C.: March 2009.
7. Memo from A. Gilbertson to J. Nakoski, December 23, 2015, "Summary of the U.S. Nuclear Regulatory Commission and Electric Power Research Institute Co-Sponsored Workshop on the Treatment of Uncertainty in Risk-Informed Decisionmaking. ADAMS Accession Number: ML15355A540.
8. Presentation slides, U.S. NRC and EPRI Workshop on the Treatment of Uncertainties in Risk-Informed Decision Making, November 18-19th, 2015. ADAMS Accession Number: ML15327A182.
9. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

10
CONCLUSIONS AND DOCUMENTATION

10.1 Introduction

This section summarizes conclusions identified from the development of qualitative analysis guidance to support fire scenarios that may result in MCRA. In addition to high level conclusions, this section also provides good practices for MCRA modeling and HRA, and the type of feedback that can (and should) be provided to operations during the MCRA HRA qualitative analysis process.

Within this section, discussion is provided on the requirements for MCRA HRA from the ASME/ANS PRA Standard [1], with particular emphasis on documentation of the analysis. Finally, areas that have been identified for future development are noted.

10.2 Properties of a Good Qualitative Analysis

As noted throughout this report, MCRA is a unique case of fire HRA. The high degree of interface between PRA/HRA, definition of fire-related damage criteria leading to abandonment, crew structure outside the MCR, and the coordination of many overlapping timeframes and actions necessitate a solid qualitative analysis to ultimately support quantification of HFEs. The facets of a good qualitative analysis include:

- Collection and review of plant specific information for MCRA including:
  - MCR abandonment procedure
  - Fire-induced risk model (fire PRA)
  - Fire PRA success criteria
  - Fire PRA MCR Task 11b analysis (Fire Modeling)
  - Any available feasibility study (such as from Appendix R evaluations)
- Coordination with the fire modeling task to define the criteria for MCR abandonment on LOH.
- Scoping out in clear and specific detail the criteria for MCR abandonment on LOC
  - What are the key safety functions that will determine whether the operators need to abandon the MCR due to loss of control?
  - What systems that provide or backup those safety functions are lost during a fire that leads to MCRA?
  - What systems need to be enabled or recovered to provide the safety functions?
- Coordination with the fire PRA analysts to identify relevant MCRA scenarios, including consideration of the decision to abandon, and proper treatment within those scenarios based on different functional requirements.
- Review of each MCRA procedure step and assessment of why it is or is not relevant to the analysis.

- Conducting plant-specific walk-throughs and talk-throughs of the MCRA procedure at the plant locations where the actions occur and observation of simulator exercises of the MCRA process (if possible).
- Development of a timeline for the MCRA process based on walk/talk-throughs and simulator exercises of the MCRA process, as well as timed training materials.
- Identifying and defining human failure events (HFEs) based on the relevant MCRA procedure steps and the context of the fire PRA scenarios for MCRA.
- Evaluation of HFE-specific performance shaping factors (PSFs) based on the context of the fire PRA scenarios for MCRA and other influences on operator performance observed during walk/talk-throughs and simulator exercises of the MCRA process.
- Assessment of command and control in terms of existing plans, training, and communication requirements.
- 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.

Further discussion on documentation is provided in Section 10.6.

10.3 MCRA Modeling and HRA Checklists

Earlier guidance provided in NUREG/CR-6850 [2] and even NUREG-1921 [3] may not have provided an adequate level of detail in order to consistently and properly model the relationships and elements commonly found in MCRA. The checklists in this section serve as a high level reminder of the elements to consider in the MCRA PRA modeling and the HRA process.

10.3.1 MCRA Modeling Checklist

1. Based on the HRA operator interviews and procedure review, define the plant conditions that would constitute a loss of control or loss of habitability for the plant and include appropriate logic in the model to credit abandonment only when those conditions occur.

2. Based on the fire modeling for control room fires, determine the scenarios that would result in a loss of habitability and only credit abandonment actions for those scenarios (i.e., do not credit actions in the control room that only appear in other procedures).

3. Include random failures of equipment required for remote shutdown (including the controls located at the remote shutdown panel) in the PRA model.

4. Include recoverable fire-induced failures of equipment required for remote shutdown (including the controls located at the remote shutdown panel) in the PRA model. This requires performing circuit analysis of the remote shutdown panel and control circuits to determine if any abandonment scenarios can cause failure.

5. Include non-recoverable fire-induced failures of equipment required for remote shutdown in the model. These would include MSOs that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed, etc.).

6. For scenarios modeled with detailed fire modeling, account for detection and suppression.

10.3.2 MCRA HRA Checklist

1. Start with the current abandonment procedure(s), but recognize it may be in the process of being revised so document the assumptions and identify what needs to be validated later. If it is a new procedure, then involve the procedure-writer with the FPRA efforts.
2. Conducting an interview and walkthrough of the procedure is crucial – the analyst need to actually see the Remote Shutdown Panel(s) and other local action locations. It is important for the analyst to understand the plant-specific RSDP displays, capabilities and limitations. Knowing what needs to be done in the MCR and at RSDP in a timely manner could feed into plant mods (e.g., installation of kill switches).
3. Develop a timeline for each of the MCRA actions. Bound the actions with the most relevant Thermal-Hydraulics run for the plant conditions that would result from the damaging fire that leads to abandonment. New T-H may be needed to address specific time limiting conditions (e.g., 3 stuck open PORVs and the impact on scenario timing if operators are able to close them).
4. Deduct the timing for the cognitive HFE to abandon the MCR from subsequent execution HFEs, including the time required for someone to go to visually confirm the fire. Feasibility may drive the results and require re-prioritization of tasks and revision of procedures. Utilize any JPMs or other timed training exercises to understand how long the execution actions take, including travel time.
5. Model cognitive failure to abandon as a separate HFE and only include cognitive evaluations in other execution actions if the procedure indicates that some diagnosis is involved (if/then statements) such as in controlling an SSC or function throughout the mission time.
6. Identify the smallest set of actions that capture what is done to abandon and go to safe and stable, considering the variability in actions given various damage states modeled in the PRA. For example, SBO versus non-SBO cases.
7. MCRA HRA requires close coordination with the fire PRA model – MCR abandonment is not like the rest of fire HRA that basically does tweaking of existing internal events HFEs or adding recovery actions.
8. Work closely with operations and training to walk and talk through the MCRA procedure to identify the actions that are essential for safe and stable rather than those that are just “nice to do if you have time”. It is important to get “buy-in” from Ops regarding the MCRA HRA and PRA modeling strategy (this has sometimes been met with resistance or even hostility and may require some discussion about the PRA perspective).
9. Consistent with items above, plant operations staff and the fire PRA analysts need to agree on the fire damage related conditions that would result in the Shift Manager/Shift Supervisor calling for MCRA. This is often not well specified in the procedure but is needed to model the scenario(s) properly, identify relevant fire compartments and

equipment impacted and to determine the crux of the cognitive abandonment decision. (Note that this can feed into clearer direction being provided in the procedure.)

10. Review all the feasibility items in NUREG-1921 [3] and NUREG-1852 [4] and be sure that these issues have been addressed in the HRA both qualitatively and quantitatively, such as emergency or normal lighting, keys and tools needed (and the timing needed to access them), and SCBA (plant-specific protocols for use, training on using them, location in the plant and time to access and don).
11. Thoroughly document the interview findings, cues, assumptions, and timing in the notebook/report on MCRA. Augment as necessary with interview notes and photos.
12. In addition to discussing the criteria for MCRA with the Shift Manager/Shift Supervisor, discuss how command and control is maintained and re-confirmed following MCRA. Include this in the qualitative analysis, and potentially in the credit for recovery actions.
13. Discuss the coordination and communications conducted between operators for the following phases:

    a) In the MCR before abandonment

    b) Following MCRA, during restoration of systems

    c) Following restoration of systems, during control of critical safety functions

    d) Address how requests and communications from personnel not involved with core cooling are managed.

10.4 Feedback to Operations

Performing an analysis for MCRA consistent with these guidelines provides detailed information on the process and its reliability/feasibility, as well as insights on how it can be improved. This section discusses the ways in which the findings from the analysis can be fed back into operations, training or even design to ensure the feasibility and improve the reliability of the MCR abandonment process.

10.4.1 PRA Perspective

Operators are likely to express reluctance to abandon the MCR since it provides the scope and range of control and indications they are accustomed to having during a transient or other plant upset. Consistent with this mindset, it may be difficult for operators to conceive of a fire that is large or severe enough that abandonment would be necessary. The analysts will have to assist in providing the PRA perspective regarding the severity of the fire, such as with the following explanations:

- The type of fire resulting in MCRA is such that the fire brigade reports that the fire is severe. The scenario fire modeling may show that certain large fires may affect multiple cable trays leading to damaging enough circuits to cause loss of control from the MCR.
- Risk insights from fire PRA indicate that fires large enough to result in significant effects on the availability and reliability of instrumentation will also be large enough to impact systems capable of providing sufficient cooling water flow to the reactor vessel (both

high and low pressure systems). In such cases, the operators will not be able to determine plant status from the MCR and the vessel water injection systems may not be operating and attempts to actuate those systems from the control room in accordance with the abnormal operating procedures may fail. Therefore, transfer of command and control to the RSDP(s), which will have unaffected instrumentation, will improve and reduce risk.

- Actually providing the operators with the list of equipment and indications that are in a failed state for the most risk-significant plant-specific scenarios that would trigger a MCRA can help break the "barrier of conception" of the fire severity that they may face is a very helpful approach. These can even be set up as simulator scenarios so that they can see what they would be dealing with.

As discussed in Section 2, it is common for MCR abandonment procedures to contain actions that are "nice to do" versus those that are "crucial to do" from the standpoint of the PRA required actions to reach a safe and stable plant state. These may include disablement of spuriously actuated non-essential equipment. Past experience in conducting talk-throughs has shown that Operations often considers some non-PRA critical steps to be important, because they are co-located in areas where critical actions are already being performed and/or provide a benefit to the operators when restoring equipment much later in the scenario. Further, both the procedures and training for fires have tended to be event-based, not symptom based. That is, they assume that every fire is an "Appendix R" fire in the given area, affecting all equipment and circuits in the area in the worst way possible. PRAs have shown that the most likely fires are smaller ones, and that even the most risk significant fires, while still large and significantly damaging, still do not approach the all-encompassing Appendix R fire. In addition, because there are probabilities associated with many of the fire-induced failures that occur, the Appendix R approach of "if it can happen, it will happen" has led to procedures and training that are (to say the least) not risk-informed and therefore filled with actions that are not risk-important. The analysts will have to provide a PRA perspective and emphasize that the time required to perform these steps may distract focus from the critical actions or even render the overall process infeasible. While the PRA preference would be to remove these non-critical steps, discussions with Operations sometimes result in consolidation or re-ordering of procedure step performance that might still allow for these supplementary actions in addition to the PRA critical actions. The key is establishing an understanding with Operations that balances their desire to take control of everything directly with the need to maximize the probability of avoiding core damage, which is usually achieved by establishing procedures that perform the risk-critical actions first and then, once the plant is stabilized, going back and performing the other actions that support longer-term operational goals.

10.4.2 Plant Modifications

Where time is particularly constrained and the action is essential, plant modifications may be appropriate to provide a rapid response mechanism or an improved human-machine interface. One of the more common modifications is the installation of a (or several) MCR "disconnect switch" to address spurious operation of valves (e.g., mitigates spurious opening by causing the valve to re-close). This protects the plant from spurious operations due to hot shorts and allows reactor or secondary coolant system boundary integrity to be maintained.

NRC Information Notice (IN) 92-18 [5] describes a situation discovered by a licensee where "…a fire in the control room could cause hot shorts, i.e. short circuits between control wiring and power sources, for certain motor-operated valves (MOVs) needed to shut the reactor down and to maintain it in a safe shutdown condition. If a fire in the control room forces reactor operators to leave the control room, these MOVs can be operated from the remote/alternate shutdown panel. However, hot shorts, combined with the absence of thermal overload protection, could cause valve damage before the operator shifted control of the valves to the remote/alternate shutdown panel." Some plants therefore choose to conduct plant modifications of motor-operated valves susceptible to this type of overload damage to ensure they are available for manual operation when de-energized.

Other examples of plant modifications that facilitate or prevent operator manual actions related to MCR abandonment are listed in Table 10-1.

Table 10-1
Example plant modifications for MCRA

HFE Description	Description of Suggested Plant Modification
Operator Fails to Align Fire Water for Alternate Vessel Injection	Operator response can be improved if a plant modification is implemented where fire water cross-tie spool piece remains permanently installed. This modification will eliminate the need to install the spool piece by providing a permanent spool piece and additional valves necessary to make the ability to inject fire water into the Feedwater system a permanent design feature of the system. Additionally, this modification includes a new fire hose connection to support the FLEX project.
Operator Fails to Depressurize RPV by Opening Electromatic Relief Valves (ERVs)	This design change modifies the valve control circuits for the ERVs by providing an additional local selector/control switch that will allow an operator to turn power off/close the ERVs or to open the ERVs using a new alternate power source. The selector/control switches will have three positions, "NORM PWR", "PWR OFF/ERV CLS", AND "EMER PWR/ERV OPEN". The purpose of installing this design change is to allow for ERV operation from the reactor building.
Failure to Provide AFW Decay Heat Removal During Alternate Shutdown Scenarios	Credit is taken for a modification in which the control circuits for the Diesel Driven Cooling Water Pump are protected, which eliminates the current required manual action of sending an operator to two separate locations.
Operators Fail to De-energize Source of Fire-induced LOCA using MCR Switch	Fire that forces Alternate Shutdown, hit kill switch and PORV is isolated. Procedure and training changes are necessary to ensure the decision to abandon is made within 5 minutes of the start of the event.

As the last entry the table indicates, the physical plant modifications must be correlated to procedure and training updates, as discussed in the next section, to ensure that operators have the direction and practice necessary to make the modifications effective.

10.4.3 Procedure and Training Updates

Some plants may already be in the process of updating their MCRA procedures and training, but further input from the analysis can assist in re-ordering or emphasizing certain steps to ensure they are performed in a sufficiently timely manner.

Others choose to perform the MCRA analysis first to gain information on the key actions and time constraints, then update their procedures later, stating as an assumption of the preliminary analysis that these procedure changes will have to be made.

There could be situations where evacuation is not immediately required but is anticipated, and the procedure could be modified to include steps to "pre-stage" the transfer of command and control to the RSDP. In such a case (as discussed in Section 4), one operator is dispatched to the RSDP as soon as it is determined that an active fire is occurring in an area designated as a MCRA area. This "pre-staging" allows both 1) additional support to the diagnosis of loss of control, since indications of system status and plant parameters on the panel can be compared with those observed in the control room, 2) providing additional time for making the decision to abandon the control room by shortening the amount of time to make the transfer and 3) once the decision is made, to implement initial actions at the RSDP immediately.

Other examples of procedure changes related to MCR abandonment are listed in Table 10-2.

Table 10-2
Example procedure changes for MCRA

HFE Description	Description of Suggested Procedure Change
Operators fails to cross tie Bus 15 and Bus 25	Add guidance to locally close bus-tie breakers if necessary to repower Train A 4kV bus from opposite unit.
Failure to make decision to leave MCR due to fire that causes loss of control	Revise Shift Supervisor guidance for decision to abandon MCR.
Failure to manually isolate letdown	Add steps to determine whether letdown LOCA is in progress, and if so, close letdown valve switches on main control board prior to abandonment; re-establish using local controls if feasible.
Operators Fail to De-energize Source of Fire-induced LOCA using MCR Switch	Add steps to operate isolation switches prior to MCR abandonment.
Operators Fail to Verify Containment Isolation	Add steps to require the operators to perform manual containment isolation prior to exiting the MCR, and to locally verify isolation after abandonment. Procedure changes should be optimized to speed the local isolation verification.

10.5 MCRA Requirements from the PRA Standard

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. Supporting Requirements (SRs) that are particularly relevant to MCRA actions are:

- HR-E3 (HRA-A1) on conducting talk-throughs of procedures,

- HR-E4 on using simulator observations or talk-throughs to confirm the response models used for scenarios,
- HR-G5 on basing the required time to complete actions for significant HFEs on action time measurements on either procedure walk-throughs or talk-throughs, or simulator observations,
- HR-H2 on crediting operator recovery actions only if:
    - (a) a procedure is available and operator training has included the action as part of crew's training, or justification for the omission for one or both is provided
    - (b) there are "cues" (e.g., alarms) to alert the operator to the recovery action provided procedure, training, or skill of the craft exist
    - (c) attention is given to the relevant PSFs listed in HR-G3
    - (d) there is sufficient manpower to perform the action.

The Fire Scenario Selection (FSS) section of the PRA Standard does contain two SRs related to analysis of potential fire scenarios leading to MCR abandonment under high level requirement HLR-FSS-B:

- FSS-B1 requires the analyst to "DEFINE and JUSTIFY the conditions that are assumed to cause MCR abandonment and/or reliance on ex-control room operator actions including remote and/or alternate shutdown actions."
    - Note 1 associated with this SR states that "In justifying the selected abandonment conditions, consideration should reflect the assumptions that control room abandonment may be required should the control room itself become untenable for human habitation (e.g., heat buildup sufficient to cause pain to human skin or smoke buildup sufficient to substantially impede operator performance), or as a result of a loss of a sufficient set of plant controls or indications such that operator performance would be substantially impeded, or as required by plant procedures."
- FSS-B2 requires the analyst to "SELECT one or more fire scenarios, either in the MCR or elsewhere, leading to MCR abandonment and/or reliance on ex-control room operator actions including remote and/or alternative shutdown actions, consisting of a combination of an ignition source (or group of ignition sources), such that the selected scenarios provide reasonable assurance that the MCR abandonment fire risk contribution can be realistically characterized."

The guidance provided in Section 3 on Modeling MCR Scenarios assists the analyst in meeting these SRs from the HRA perspective. In addition, the Decision to Abandon guidance provided in Section 4 addresses the need to define LOC criteria based on the distinction in Note 1 between LOH and LOC scenarios.

10.6 Documentation

Documentation of the MCRA HRA qualitative analysis should follow the basic concepts from NUREG/CR-6850 [2] and the ASME/ANS PRA Standard [1] outlined in Section 7 of NUREG-1921 [3] for the development of a calculation package or notebook. Generally MCRA HRA is documented as a subsection of the overall Fire HRA calculation, but can be done as a stand-

alone document so long as any changes to the fire HRA that might impact MCRA are updated as well.

The following outline identifies the type of information that should be included in the MCRA HRA documentation:

1. Main Control Room Abandonment (MCRA) HRA
1.1 Assumptions
1.2 MCRA Modeling and Abandonment Criteria
    1.2.1 Temperature LOH Abandonment Criterion
    1.2.2 Visibility LOH Abandonment Criterion
    1.2.3 Loss of Control Abandonment Criteria – coordinated with the Fire PRA modeling, with the plant MCRA procedure and with plant Operations and Training to specify the criteria in terms of systems and functions lost due to the extreme fire.
1.3 Actions Following MCRA – table of the MCRA procedure steps with documentation of the determination by the HRA analyst of which steps were considered relevant or not to the MCRA analysis and why.
1.4 Modeling MCRA Actions – development of the MCRA timeline(s) based on scenarios and thermal-hydraulics runs, identification and definition of individual MCRA HFEs including PSFs
    1.4.1 Long-Term Actions - table of HFEs relevant to various binning configurations
    1.4.2 Short-Term Actions - table of HFEs relevant to various binning configurations
1.5 Quantification of MCR Abandonment Human Failure Events (not covered in this report)

10.7 Areas for Future Development

The following areas have been identified as areas for future development as a result of the compilation of this document.

- Guidance for MCRA HRA Quantification

This initial supplement to NUREG-1921 focuses on the qualitative analysis portion of MCRA, but a subsequent report will be issued to address quantification of the HFEs defined for the MCRA process.

- Ways to Model Command and Control

The Command and Control (C&C) appendix and the discussion of aspects of C&C in the PSFs section identify what C&C is and how some facets are addressed through PSFs. However, there is not yet an agreed-upon method for modeling C&C. This is an area for further research and development.

10.8 References

1. 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

2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
3. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
4. U.S. Nuclear Regulatory Commission. NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, Washington, D.C. October 2007.
5. Information Notice No. 92-18: *Potential for Loss of Remote Shutdown Capability During a Control Room Fire*, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC: February 28, 1992.

A
MAIN CONTROL ROOM ABANDONMENT REGULATORY BACKGROUND AND HISTORICAL EVENTS

This appendix provides summaries relevant to MCRA on the topics of: 1) U.S. regulatory background and 2) historical events.

A.1 Regulatory Background for Main Control Room Abandonment

Although fires are the most frequently occurring event that could require MCRA, fire are not the only type of event addressed in regulatory requirements for NPPs that may require MCRA. Requirements for MCR abandonment are rooted in the Code of Federal Regulations (10 CFR 50), both Criterion 19 in Appendix A [1] (which relates to control room habitability) and Appendix R [2] (e.g., requirements G3 and L) which relates to fire protection.

A.1.1 10 CFR Part 50, Appendix A and Related Guidance

The main control room is the area of a nuclear power plant defined in the facility licensing basis from which actions are taken to operate the plant safely under normal conditions and to maintain the reactor in a safe condition during accident situations. For most plants, the criteria defined in General Design Criterion 19 (GDC 19) in 10 CFR Part 50, Appendix A [1], "General Design Criteria for Nuclear Power Plants," apply to this area.

NRC Generic Letter 2003-01 [3]: Control Room Habitability, issued in 2003 further defines issues related to the requirement to maintain control room habitability. The control room envelope (CRE) is the plant area defined in the facility licensing basis that encompasses the control room and may encompass other plant areas. Structures that make up the CRE are designed to limit the in-leakage of radioactive and hazardous materials from areas external to the CRE. Control room habitability systems (CRHSs) typically provide shielding, isolation, pressurization, heating, ventilation, air conditioning and filtration, monitoring, and the sustenance and sanitation necessary to ensure that the control room operators can remain in the control room and take actions to operate the plant under normal and accident conditions. Plant design bases and severe accident risk analyses both assume that the control room operators can remain safely with the control room to monitor plant performance and take appropriate mitigation actions. NRC Generic Letter 81-12 [4] outlines the equipment that is required to be operational so that the plant can achieve hot standby and cold shutdown for both a PWR and a BWR. Generic Letter 81-12 also outlines the requirements for alternate shutdown capabilities.

A.1.2 10 CFR Part 50, Appendix R and Related Guidance

The regulations do not specify criteria for when operators must abandon the control room. The criteria for main control room abandonment are procedurally outlined by each plant and therefore

may vary widely from plant to plant. For example, no regulatory limit exists on the amount of smoke allowed in the control room. The plant's ability to manage smoke infiltration is assessed qualitatively. Licensees should perform a qualitative assessment to ensure that the plant can safely be shut down from either the control room or the alternate shutdown panel during an internal or external smoke event [5]. The main control room evacuation procedure entry conditions may include criteria such as a fire in certain critical plant areas (e.g. the control room, cable spreading room, HVAC equipment room, etc.), loss of or unreliable operation of control room controls and indicators, spurious operation of plant circuitry exposed to a fire, or personnel safety concerns due to smoke, toxic gas, radiation, bomb threat etc.

A.2 Historical Events Involving Main Control Room Abandonment

Evacuation of the MCR of a NPP is an extremely rare and unusual occurrence. The regulations require that the control room be maintained in a habitable condition such that critical functions can be safely performed even under accident conditions. 10 CFR 50, Appendix A, General Design Criterion 19 [1] states that, "A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents." Thus the occurrence of conditions that lead to the evacuation of the control room should, by design, be extremely uncommon.

To date, there have been no evacuations of the control room of any operating nuclear power plant in the United States. One evacuation occurred at Haddam Neck Nuclear Power Plant (see Section A.2.1 below), which was permanently defueled at the time of the event.

The only known evacuation of an operating nuclear power plant control room occurred at the Narora Atomic Power Station, a non-US nuclear power plant, in Uttar Pradesh, India.

Sections A.2.1 and A.2.2 briefly summarize the two events that resulted in MCR abandonment. Section A.2.3 summaries some other incidents that involved challenging fires, but did not result in MCR abandonment.

A.2.1 Haddam Neck– Non-Fire Event with MCR Abandonment of Defueled US NPP [6]

In August of 1997, the only evacuation of a control room to date in a U.S. nuclear power facility took place at the Connecticut Yankee Nuclear Power Plant in Haddam Neck, Connecticut. At the time of the evacuation the plant was in a permanently defueled condition. At approximately 9:47 a.m. the control room Halon system was inadvertently discharged while a training instructor was taking flash camera pictures of the inside of a Halon control panel located in the control room. Because prolonged exposure to Halon, a chemical used to extinguish fires, can result in nausea and dizziness, the control room and adjacent security central alarm station were evacuated as a precautionary measure. Upon exiting the control room, operators continuously monitored the control board through a window in the viewing area located immediately outside the control room. The control room ventilation system was used to remove the Halon, the air was sampled, and operators were able to reoccupy the control room in approximately 45 minutes.

A.2.2 Narora Atomic Station – Fire with MCR Abandonment of non-US NPP [7]

The only occurrence of a main control room abandonment at an operating nuclear power facility took place in March of 1993 at the Narora Atomic Power Station in Uttar Pradesh, India. Narora is a two-unit 220 MWe PHWR (Pressurized Heavy Water Reactor). With Unit-2 shutdown, the Unit-1 turbine generator tripped from 84% power followed immediately by the sound of an explosion and the report of a large fire under the main generator. A gust of hot dusty air was felt in the MCR and, after observing the extent of the fire, 38 seconds after the turbine trip, operators manually tripped the reactor and commenced an emergency cooldown. In just under eight minutes, the fire station was called. At about eight minutes following the turbine trip, there was a complete loss of all electric power in Unit-1 and a plant emergency was declared. The fire spread quickly through a cable penetration fire barrier into the control equipment room adjacent to the control room, leading to such extensive smoke in the MCR that operators were forced to evacuate. Operators were not able to re-enter the control room for about 13 hours. The fire was brought under control in about 1.5 hours and, after an additional 4 hours, power was restored to one emergency bus via diesel generator. The fire was not completely extinguished until 9 hours after it began and the plant emergency was ended at 19 hours.

The root cause of the fire was identified in follow-up investigations to be a fatigue failure of the last stage low pressure turbine blades. This caused a severe imbalance on the rotor, leading to failure of the turbine bearing and the generator hydrogen seals. Escaping hydrogen was ignited by generator slip rings. The effects of the ensuing explosion ruptured turbine generator oil pipes, which fed the fire and helped to ignite electrical cable insulation.

The Narora incident illustrates that a large plant fire can cause control room habitability issues significant enough to necessitate abandonment of the control room even if the fire is outside of the MCR. The Narora fire also illustrated that turbine building fires, which are often screened out as being risk insignificant, can under certain circumstances present a severe challenge to nuclear safety.

A.2.3 Challenging Fire Events That Did Not Result in MCR Abandonment

A sample of fire events history must include the Browns Ferry event that resulted in some dramatic changes in U.S. fire protection requirements. This event is summarized below, followed by brief descriptions of a few other U.S. and non-U.S. fires that were smoke was observed in the control room.

Browns Ferry [7, 8]

Though no evacuation took place, there has been one challenging fire in an operating U.S. NPP that, had it occurred today may have led to the evacuation of the control room. This event took place at the Browns Ferry NPP in Athens, Alabama in 1975. The fire event at Browns Ferry forever changed how the NRC and the nuclear power industry view the threat of fire to nuclear power plant safety and prompted a new series of fire protection regulations.

Using a small lit candle to search for air leaks in penetrations between the reactor containment building and the reactor building of the plant, a technician inadvertently ignited insulation around electrical cables that supplied power to the plant's MCR and safety systems. The fire started around 12:20 p.m. and advanced from the cable-spreading room into the reactor building through the

cable-tray penetration and burned for over 7 hours before water was used to extinguish the fire. Initially hand-held dry chemical and CO_2 had been used to fight the fire, but the fire continued to smolder and re-ignite. Activation of the plant's permanently installed CO_2 fire-extinguishing system was initially delayed due to the fact that the power had been shut off as a safety measure during the leak testing and because manual activation was prevented by metal plates that had been installed under the breakout glass to prevent inadvertent activation during plant construction. The fire in the cable spreading room was eventually extinguished using the CO_2 system and chemical extinguishers, but the fire continued to burn in the reactor building, requiring use of ladders to apply the contents of hand held extinguishers. By 12:35 p.m., the smoke had become so dense that breathing apparatus was required. Problems in fighting the fire were compounded by the loss of the ventilation system and the reactor building lighting, along with a shortage of air-breathing equipment.

During the seven hours the fire was burning, operators faced several unusual situations. Around 12:40 p.m., alarms associated with the ECCS initiated but were inconsistent with the systems' status. The residual heat removal (RHR) core spray (CS) system, the high-pressure coolant injection (HPCI) system, and the reactor core isolation coolant system (RCIC) had initiated and were running. The operators stopped the pumps, but the alarms would not reset. Over the next few minutes there was other anomalous behavior of controls and instrumentation including other starts and stops of RHR, CS, and HPCI and brightening and dimming of panel lights. At one point smoke infiltrated the MCR to the extent that some operators put on breathing apparatus for a brief period. Though the MCR operators were successful in maintaining core cooling and the fire was eventually extinguished, this event challenged nuclear safety and has forever changed the landscape for fire protection.

Other Fires Resulting in Smoke in the Control Room

There have been a number of other incidents where varying quantities of smoke entered the control room from other areas of the plant. In all of these incidents the operators remained in the control room.

One such incident occurred at the Vandellos NPP [7], a graphite moderated reactor in Barcelona, Spain in 1989. In this incident turbine blades caused a rupture in several oil lines and a large oil and hydrogen fire. Smoke from the turbine building fire entered the control room and several other parts of the plant. Automatic fire suppression systems were activated in areas remote from the actual fire due to smoke and plant personnel had to wear self-contained breathing apparatus (SCBA) to enter certain areas of the reactor building. Control room operators were issued SCBA but they were never used. Portable fans were brought in to clear the smoke and provide fresh air into the control room.

Another incident occurred at the Oconee NPP [7] in Seneca, South Carolina in 1989. In this incident a switchgear failed explosively and caught fire. At some point in this incident smoke entered the control room, but the extent of the smoke and the path by which it found its way into the control room are not described in available sources.

In 1978, a fire in the turbine building at the Beloyarsk [7], a 146 MWe LWGR-1000 type nuclear power plant in Ekaterinburg, Russia resulted in fire propagation into the adjacent control building

via cable penetrations and other openings. The fire also propagated into the control panels of the MCR and caused damage. Operators had to work in heavy smoke conditions with some operators reported as being "half-conscious" due to smoke inhalation. Despite these difficulties, operators managed to start one train of reactor emergency cooling system.

A.3 References

1. Code of Federal Regulation (CFR), Title 10, Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants", U.S. Government Printing Office, Washington, D.C.
2. Code of Federal Regulation (CFR), Title 10, Appendix R to Part 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979", U.S. Government Printing Office, Washington, D.C.
3. U.S. Nuclear Regulatory Commission, Generic Letter (GL) 2003-01: "Control Room Habitability", Washington, D.C.: June 12, 2003.
4. U.S. Nuclear Regulatory Commission, Generic Letter (GL) 81-12: "Fire Protection Rule (45 FR 76602, November 19, 1980)", Washington, D.C.: February 20, 1981.
5. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Regulatory Guide (RG) 1.196 Revision 1, "Control Room Habitability at Light-Water Nuclear Power Reactors", Washington, D.C.: January 2007.
6. Licensee Event Report, LER 50-213/97-013-00, "Inadvertent Halon Discharge in Control Room Due to Camera Flash Results in Precautionary Control Room Evacuation": August 1997.
7. U.S. Nuclear Regulatory Commission, NUREG/CR-6738, *Risk Methods Insights Gained From Fire Incidents,* Washington, D.C.: September 2001.
8. A.J. Pryor, *The Browns Ferry Nuclear Plant Fire,* Society of Fire Protection Engineers Technology Report 77-2, Boston, MA: 1977.

B
COMMAND AND CONTROL

B.1 Introduction

Command and control (C&C) is a term that has evolved from military applications to common usage in systems where there is need for a central body of authority to make decisions but have them carried out by a distributed group[24]. In normal operations, during post-initiator events, and non-abandonment fires, C&C is accomplished in the MCR by the shift supervisor (SS) directing the operating crew's activities (both the MCR board operators and field operators out in the plant) to perform actions identified in relevant procedures. These include, for example, the Emergency Operating Procedures (EOPs) for post-initiating-event operations and the fire-related procedures for non-abandonment fires.

During MCRA scenarios, C&C transitions through a series of contexts whereby the person in charge of responding to the event (typically the SS[25]) must: (1) decide to abandon the MCR, (2) transition to the RSDP, and (3) be responsible for determining what actions are necessary, and communicating instructions to staff located in plant areas who are then responsible for taking the actions. These decisions can often be based on reports of indications and measurements communicated to the SS by the staff in plant areas. In addition, the method of implementing C&C needs by the plant operators at the local panels needs to be considered.

Section 2 of this report summarizes what is different about MCRA fire scenarios and how those differences relate to the PRA and HRA modeling. This appendix is intended to provide a strictly human-factors perspective of C&C in MCRA without it necessarily impacting the HRA modeling. It is therefore simply to provide an informational basis for those analysts interested. Any direct impact on PRA and HRA modeling are discussed in sections of the report (particularly Section 8, PSFs).

Section B.2 describes a human-performance perspective surrounding the concept of C&C as it relates to MCR abandonment scenarios based on models of human performance already developed for NRC. Section B.3 discusses variations between plants in how C&C may be implemented. Section B.4 summarizes an integrated perspective of the factors surrounding C&C

[24] For example, Chapter 1 of the 2003 US Army Field Manual (FM) 6.0, Mission Command: Command and Control of Army Forces, states: "*The focus of Command and Control (C2) is the commander. Commanders assess the situation, make decisions, and direct actions*." *"To implement their decisions, commanders direct coordinated actions by their forces that together accomplish the mission."[*1]

[25] This discussion assumes the common US arrangement of the SS taking control from the remote shutdown panel (RSDP) and directing field operators in the plant by communication systems. Some plants may have different arrangements. The same principles apply in these arrangements as described here, substituting the title and location of the person or people in charge for the SS and the RSDP respectively. Also, there may be special cases where two operators at local panels are in communication with only each other, with one operator designated as the decision maker.

activities in each phase and location, and Section B.5 identifies how these perspectives relate to the individual PSFs discussed in Section 8 of this document.

B.2 Human Performance, Macrocognition and Command and Control

Command and control represents the essential functions of the operating crew in a post-initiator response as described in HRA methods like ATHEANA [2]. One framework that has been developed for describing the performance of humans in process control (including the response to initiating events in nuclear power plants) is based on an understanding of macrocognition [3, 4]. Macrocognition refers to the process in real-world settings by which individuals and teams detect situations, make sense of those situations, and formulate response plans.

Roth, Mosleh et al. [5] describes macrocognition for nuclear plant operating crews as being comprised of the following activities:

- Detecting/noticing,
- Directing attention/managing workload,
- Sense-making/understanding,
- Planning/deciding,
- Communicating/coordinating (teamwork functions),
- Supervising/directing personnel, and
- Executing actions.

Figure B-1 presents a summary of these activities based on Roth, Mosleh et al. [5]. The following description is taken from Roth, Mosleh et al.

> "At the core of this model is the concept that people actively work to construct a coherent understanding of the situation they are in – this is referred to as '*sensemaking*' [c.f.,6]. The output of sensemaking is a *situation model* that represents a person's understanding of a situation. This understanding draws on both real-time information obtained from the world via perceptual processes (i.e., the macrocognitive function of *'detecting/noticing'*), as well as background knowledge stored in long-term memory (e.g., mental models). The situational model is closely related to (and subsumes) theoretical concepts such as *situation awareness* and *diagnosis*. A person's situation model may or may not be an accurate representation of the true state of the world. Another core concept of the model is that people have limited attention, short-term memory, and information processing capability. This places a premium on '*directing attention and managing workload'* functions. Attention/workload management refers to determining where to direct attention and focus activity under high workload/ high attention demand conditions. People form expectations as to what should happen next and what is highest priority to deal with based on their situation model. These expectations influence where people will direct their attention and how they will manage their workload (e.g., how they will prioritize activities under high workload conditions). These in turn will influence what people will pay attention to and therefore what they will detect/notice [7, 8]. People's understanding of a situation also

influences *planning and deciding* functions. Based on their situation model people will prioritize goals, make decisions, and plan actions.

Communicating and coordinating and other related teamwork activities, including supervising/directing personnel, are also central macrocognitive functions [9]. These functions enable the team to operate as a cohesive macrocognitive unit. The output of all these macrocognitive processes is the execution of observable physical actions."

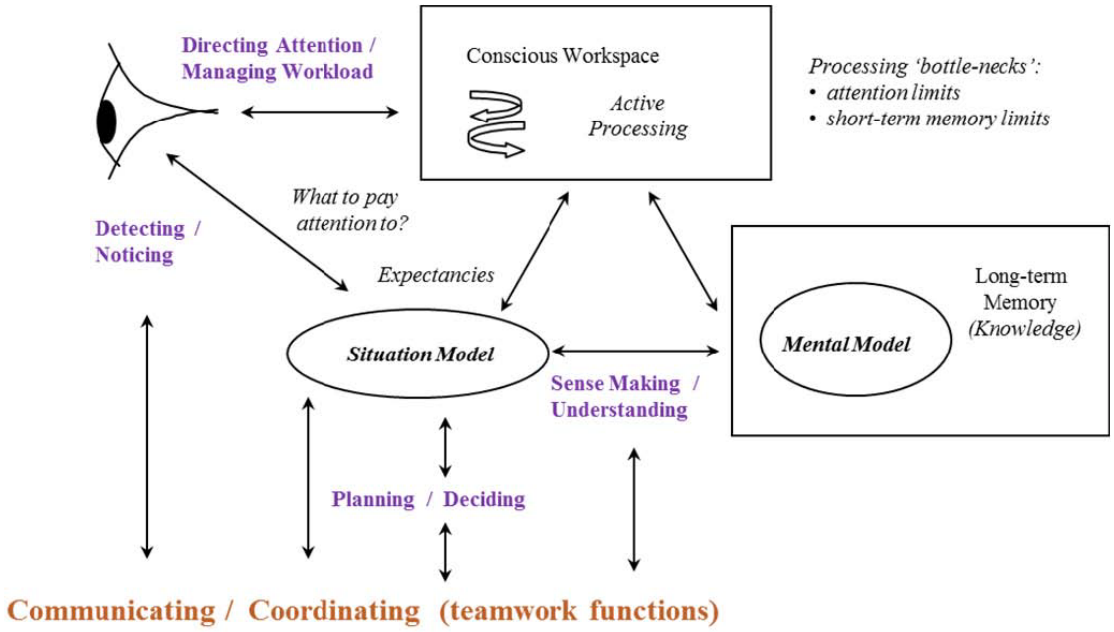

Figure B-1
A simplified model of macrocognition (based on Roth, Mosleh, et al. [5])

Using this model, Roth, Mosleh et al. developed sets of situational factors (SFs). Situational factors are those factors (or contextual elements) that are considered to make successful completion of the activities in macrocognition less likely. Compared with the more typically used performance shaping factors (PSFs) used in human reliability and performance models, situational factors are more finely grained and are connected with the particulars of the context in which the action is taking place. Table B-1 lists the sets of SFs associated with the activities identified in the paper.

Figure B-2 shows an adaptation of Figure B-1, showing the application of the macrocognitive functions to power plant operations. (This figure is an update of the model used in the ATHEANA HRA method [2]).

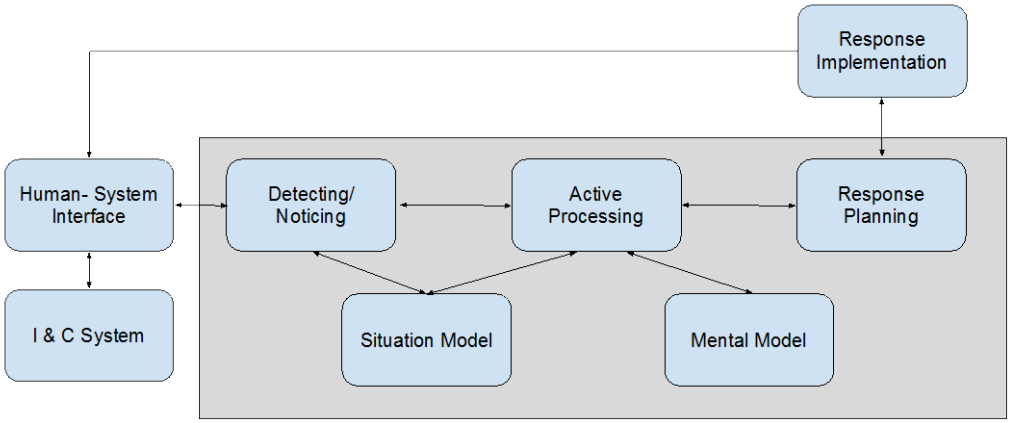

Figure B-2
Basic steps in post-event responses for non-abandonment scenarios

In terms of plant operations from the MCR (including during non-abandonment fires), much of the macrocognitive activity is the responsibility of the SS, aided by the reactor operators (ROs) providing monitoring and detecting functions and implementing actions. The STA is typically providing support to the SS in assessing the situation and adding knowledge. The MCR team is co-located allowing a level of redundancy (for example, the SS monitoring the reactor status in addition to the ROs, and the ROs discussing the situation with the SS), and face-to-face communications in a relatively quiet location. It further allows shared access to information (displays and written documentation). The SS also is typically assisted in communications responsibilities (such as making required notification calls to the NRC, taking calls from the fire brigade, security, health physics, etc.), but who provides such assistance (for example., the STA, an extra RO on shift, other operations personnel that arrive to assist the MCR) varies somewhat between plants.[26] This same model applies prior to the abandonment phase in MCRA fires.

In contrast, Figure B-3 shows the more complex situation once the MCR crew has abandoned the main control room and the SS is managing the response from the RSDP by interactions with staff at one or more local panels (the figure assumes staff in multiple plant locations). Now the detection and monitoring activities are based on a combination of direct observations at the RSDP plus communicated inputs from the operators located at the various local panels.[27] Similarly, the response implementation is carried out in part by an RO located with the SS at the RSDP and by other operators at the distributed local panels.

Where and what the STA does following MCR abandonment depends on plant-specific policies. For example, the STA may:

- Accompany the SS to the RSDP, continuing the role of assisting the SS in the

[26] The set of conditions described in this paragraph (e.g., a single procedure being followed by the entire crew; formal, face-to-face, and real-time communication; indications that can be monitored by all crew members; the expectation that other crew members will provide backup) supports the implicit assumption in most HRA methods that the MCR crew can be treated as a single operator. However, these conditions cannot be assumed to be applicable outside the context of at-power, post-reactor trip, non-fire Level 1 events.

[27] Although there are plant-to-plant variations, the indications at the RSDP are likely to be different and fewer than in the MCR. Also, RSDPs do not always have alarm panels or safety parameter display systems (SPDS). Such differences can make obtaining information from the RSDP more effortful than for the same information in the MCR.

decision-making activities

- Go to an alternate RSDP (if the plant has two - Train A and Train B), assisting the STA via phone or radio, plus performing actions at that RSDP
- Act as a field operator, going to one or more local plant panels to perform necessary actions
- Go to the Technical Support Center (TSC) to take responsibilities in the Emergency Response Organization (ERO).

In these conditions, the SS is reliant on communication systems for receiving information and directing actions; he may not have the ability to verify many readings and confirm actions, and the potential exists for him to become a "bottleneck" for conveying data between plant operators whose actions must be coordinated. In addition, the SS has same communications responsibilities at the RSDP as existed in the MCR (calls to and from the fire brigade, for example) but now may not have the same support from the STA and may not have the same amount or kind of communications equipment.

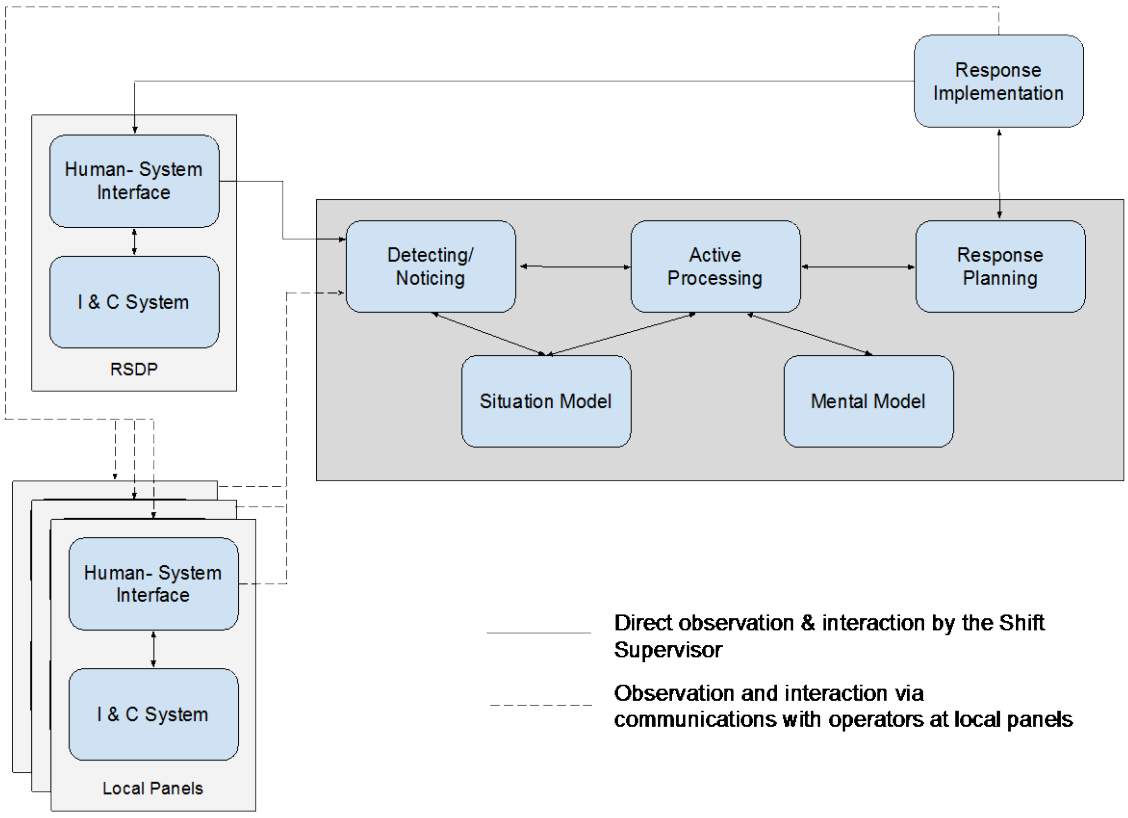

Figure B-3
Basic steps for post-event responses following MCRA

B.3 Plant Differences in Command and Control Structures

Each plant has a unique command and control structure while inside the MCR and then a different structure while outside the MCR. It is the HRA analyst's role to identify the expected

command and control structure outside the MCR. Understanding the structure is the key to understanding the impact on the reliability. The command and control structure can be defined by:

- Identifying the person or people leading the response, as well as each person's role and responsibility following MCRA.
- Identifying where the person or people leading the response will be located once outside the MCR.
- Evaluating how communications are expected to be performed,
  - Physical process, such as use of radios, sound-powered phones, or other means
  - Protocol, such as three-way communication, required reporting to SS when each step or task is performed or waiting to report until a major function or system is restored
- Identifying how procedures will be used by the person or people in charge and by the field operators – for instance, do the field operators have their own written procedures in hand in plant locations or do they rely only on directions from the person in charge.
- Identifying how many people will require interaction and communication (including plant staff and organizations beyond those needed only for safe shutdown)
- Identifying how much communication will be required to satisfy all communication needs
- Identifying who, beyond the SS, is available to help address communication needs.

B.4 Assessment of Command and Control Issues in MCRA

The purpose of this section is to provide an integrated perspective of the factors surrounding the C&C issues for each timeframe and location. Roth, Mosleh, et al. [5] developed sets of situational factors (SFs) based on the model previously described.

There are two timeframes when to consider C&C effectiveness: the time up to abandonment of the MCR, and post abandonment (the time during abandonment will be short and any significant C&C issues are not expected to occur during that time). The time up to abandonment is considered separately for loss of habitability (LOH) and loss of control (LOC) scenarios as the SFs are somewhat different. During the post-abandonment phase, C&C issues need to be considered both at the RSDP and at the plant areas. Thus there are four contexts to be assessed for C&C issues.

Situational factors related to MCRA analyses are presented in Tables B-2, B-3, B-4 and B-5. Those SFs listed in these tables are considered to make the decision to abandon less likely or delayed for LOH scenarios (Table B-2), and to have the potential to make the decision to abandon less likely or delayed for LOC scenarios (Table B-3). Those in Table B-4 are considered to make the post-abandonment responses at the RSDP less reliable or timely, and those in Table B-5 to make the post-abandonment responses at the plant locations less reliable or timely. These are discussed below.

While every plant has unique designs for the interfaces for controls, indications and manually operated devices, NRC's guidelines for the review of human-system interfaces, NUREG-0700 [10], sets standards for these and other command & control-related systems (like communications and environments). While these guidelines are primarily seen as relating to the design of the MCR, they do limit (if fully applied) the extent to which the SFs developed by Roth, Mosleh, et al. [5] can play a role in creating opportunities for human-performance problems outside the MCR. The assessment of the local control stations and the RSDP should still, of course, be assessed against the PSFs discussed in Section 8.

B.4.1 Decision to Abandon the MCR

The analysis of the decision to abandon the MCR are discussed in Section 4, Analysis of Decision to Abandon.

B.4.1.1 Loss of Habitability Scenarios

As discussed in Section 4, there is very little potential for failure to abandon during LOH events as the compelling effects of fire on the MCR environment are clear and direct. The only potential SF is the possible stress from a reluctance to abandon control from the MCR because of the change from a familiar to an unfamiliar setting. Since this is a scenario for which training is required, in practice this is not likely to be a significant issue.

1. The SS (and the rest of the crew) will likely be feeling considerable stress compared to responding to plant events for which frequent simulator training is provided (*Directing attention/managing workload*).

B.4.1.2 Loss of Control Scenarios

Unlike the LOH case that has immediate and unambiguous cues of the need to abandon the MCR, the cues for abandonment in LOC scenarios may not be so direct or obvious. As discussed in Section 4.3, there is rarely specific guidance on what constitutes the required evidence of a LOC scenario needing abandonment. In addition, the effects of the fire may be progressive, with failures of controls and indications in the MCR occurring over time and needing time on the part of the operators to understand the underlying cause of them. Depending on the location of the fire, associated plant fire alarms may provide assistance in diagnosing the cause.

1. For loss of control (LOC) scenarios, the cues and indications, components and systems required to safely shutdown the plant following EOP guidance may be impacted by the fire. When these systems or components and indications are unavailable (from the MCR) or their status cannot be determined from the MCR then operators may be forced to shutdown the plant from outside the MCR. Deciding which indications are valid and the status of key components/systems given spurious instrumentation faults due to the fire could initially delay the detection for the need to abandon the MCR. Fire damage may also create misleading or inaccurate indications not necessarily associated with safety indications but that may distract or add confusion at the time of deciding to abandon the MCR. (*Detecting/noticing and sense making/understanding*)

2. There may be a high information load on the SS associated with understanding the causes of multiple fire-induced plant indications, from comprehending possibly false equipment alarms plus the potential for verbal/phone/radio reports from plant areas associated with the fire (*Sense making/understanding*)
3. There is considerable variability in the level of guidance provided for abandoning the MCR during fires, especially when due to LOC. Deciding to abandon the MCR is likely to prove stressful in the absence of explicit training for LOC events. (*Incomplete procedural guidance*).
4. The decision to abandon the MCR will likely be taken with great reluctance as it is: (a) the place the operating crew is most familiar with and practiced in using as a team, and (b) the location where the greatest resources are available (documentation, communications, etc.). Abandoning the MCR will also likely create concern among the plant staff to whom it indicates a severe event (*Decision has foreseeable potential consequences to the plant and the staff…*)
5. During the time to decide to abandon, it is likely that the SS will be receiving much information from both the MCR and plant areas about the fire and its effects. The information and the need to decide will be fast paced and there are potentially many interruptions and distractions (*Directing attention/managing workload*).
6. Given items 4 and 5 above, the SS (and the rest of the crew) will likely be feeling considerable stress compared to responding to plant events for which frequent simulator training is provided (*Directing attention/managing workload*).

B.4.2 Post Abandonment Operations

Post abandonment operations comprise the activities necessary to ensure a safe shutdown once the MCR has been abandoned.

B.4.2.1 Operations at the Remote Shutdown Panel

1. Once the SS has left the MCR, the information available outside the MCR will, in most cases, be less than they would be familiar with in the MCR during normal operations and during non-abandonment fires. While the information at the RSDP may be adequate for the range of plant conditions encompassed in the PRA, it is likely that the SS will need to be assured that there are no conditions arising that would further complicate the response. Information in addition to the RSDP will need to be obtained from plant areas using communication systems (*Detecting/noticing*).
2. Because of the need for reported information from plant areas, it is likely that the SS will be facing a high information workload compared with operations in the MCR through having to keep track of reported values, etc., rather than rely on face-to-face reports and direct observations (*Sense making/understanding*).

3. Unlike when operating in the MCR, it may be that the SS and plant operators do not have a well-designed work place in terms of adequacy of workspace, lighting, noise, etc., and the design of the control interface that may make reviewing information and taking actions more difficult (*Manipulating/acting*).
4. To take actions, the plant personnel will not be using the normal controls with which they are most familiar (in the MCR) but other controls and indications at the RSDP and plant areas. The possibility exists that the RSDP is not designed to modern human-factors standards. While the guidelines of NUREG-0700 [10] (or equivalent) apply to control stations outside the MCR, the level of guidance is less extensive, and therefore the operators may require to be more vigilant in selecting controls or indications. (*Manipulating/acting*).
5. Perhaps the most significant SF associated with MCRA is the need for close and frequent communications and coordination between the RSDP and the field operators in the plant areas (*Communicating/ coordinating*).
6. When field operators are in multiple locations, the SS has to coordinate and oversee the activities of each individual (even if they have their own local procedures) in parallel, which involves a significant workload using communications systems (*Supervising/directing personnel*).
7. Because field operators may have to access areas that are security-protected or involve accessing radiation barriers, it may take a significant time for the staff reach their control positions and delaying their ability to respond (*Supervising/directing personnel*).
8. The need to supervise and direct the field operators during the post-abandonment period will involve multiple concurrent demands on the SS. These demands will probably be high-tempo at times while coping with interruptions from other operators (and possibly plant management). This response period will involve periods of sustained attention and monitoring to cope with the workload and the interruptions, which will be stressful. Further, the potential exists for a need to remember data in the absence of the normal MCR displays and paperwork (*Directing attention/ managing workload*).

B.4.2.2 Operations in Other Plant Areas

1. The potential exists for field operators in plant areas to have to use indications and controls that are not ideally designed from a human-factors perspective. Generally Section 12.2 of NUREG-0700 requires indications and controls at local control stations to be designed not to violate population stereotypes or to have to identify displays and indications in a confused design. However, this requirement may not

result in designs that meet the full specifications of NUREG-0700 *(Manipulating/acting)*.

2. Operations in plant areas can involve being in harsh or uncomfortable environments *(Manipulating/acting)*.
3. Frequent communications between the SS and the field operators will be required *(Communicating/ Coordinating)*.
4. In some circumstances (depending on the accident scenario and required operator actions), operators may be involved in performing concurrent or "close-in-time" actions with associated time pressure. Actions may require sustained or continuous monitoring and may be performed in the face of multiple distractions or interruptions (due to communications needs, for example. Operators may need to keep data values in mind or perform mental calculations as parameters change. *(Directing Attention/ Managing Workload)*.

B.5 Impact on PSFs

Section B.3 has identified SFs that have the potential to degrade human performance for both the period leading up to the decision to abandon (Section B.3.1), and the post-abandonment period (Section B.3.2). Actions for both sets of SFs relate to broadly similar PSFs. These are discussed below. More specific guidance on the assessment of PSFs is provided in Section 8.

B.5.1 Complexity and Stress

From the operating crew's perspective, complexity and stress are intertwined: the greater the complexity the greater the stress. The major sources of complexity and stress are:

- The need to abandon the familiarity of operating from the MCR for operations in locations that are rarely if ever used in practice
- SS having to cope with control via communications at a distance and having potentially to cope with multiple distractions and simultaneous communications
- SS coping with uncertainties about what the plant behavior is (compared with the information available in the MCR)

The analyst needs to consider the extent to which these can degrade the performance (particularly of the SS) to respond to the situation in a highly reliable and efficient manner. In many ways, complexity and stress represent challenges to C&C; the more complex the event, the greater the stress and a greater need for effective command and control. Any weaknesses, therefore, in the PSFs discussed below will likely increase the disruptive effects of complexity and stress.

B.5.2 Cues and Indications

B.5.2.1 Pre-Abandonment

1. The analyst should consider the degree to which spurious (false) cues and indications will be present, particularly for LOC events that have the potential to slow down the response of crews to decide that the fire is real and that the MCR needs to be abandoned.

B.5.2.2 Post-Abandonment

1. The limited information provided at the RSDP will require the SS to rely on information provided by field operators in plant areas. The location of such information sources may or may not be well designed in terms of access, observability, and ergonomic design. The analyst needs to assured that the relevant information can be obtained reliably and in a timely manner.
2. The limited information available at the RSDP may leave the SS concerned that there are conditions in the plant that he/she cannot observe and may act to distract him/her. The analyst can inquire during interviews as to whether there any concerns by the SS or staff as to plant conditions for which they may not be able to observe, and which might act as a distraction or source of stress.

B.5.3 Communications

B.5.3.1 Pre-Abandonment

Prior to the abandonment, it is possible that the SS in the MCR will become flooded with calls about the occurrence of the fire (depending on its location and how visible it is). These calls may become a distraction to the SS while making the decision to abandon the MCR. In addition, for the LOC case, calls may be coming in from plant operators outside the MCR who are noticing "odd" plant behavior. The analyst should discuss whether this is a potential source of delay in making the decision to abandon the MCR. This is also considered in Section 6 concerning the feasibility of communications based on a plan.

B.5.3.2 Post-Abandonment

Following the abandonment, much of the control actions will be directed by the SS from the RSDP using any or all of the communications systems available to him/her. The analysts needs to assess how reliable and effective the available communications systems are between the RSDP and all the needed control stations in the plant necessary for post-abandonment actions. In particular, the analyst needs to make a judgment as to the plant's use of techniques and protocols that increase the effectiveness of communications (like 3-way communications, for example) when the technology used for communications may not be ideal. Also, as discussed in Section 6, there should be a communications plan, including an expected level of staffing to support the amount of expected communications. There are many impacts of ineffective communication, including miscommunication of indications (i.e., another PSF), excessive workload due to

inadequate communications plan, and delay of actions (e.g., timing concern and a potential failure mode).

B.5.4 Procedures

B.5.4.1 Pre-Abandonment

The analyst should consider the amount and level of detail of guidance to operators concerning when to abandon the MCR for LOC to assess how long it will likely take to reach the point of abandoning the MCR.

B.5.4.2 Post-Abandonment

The analyst should evaluate the degree to which the procedural guidance to the SS and the field operators requires frequent or complex communications to coordinate the work during the response period. Less need for communications will ease the workload on the SS.

B.5.5 Training (Both pre- and post-abandonment)

Training for the abandonment scenarios will have the capability of reducing the stress and workload on the SS (by making the task a little more familiar) and ensuring that the necessary tools, procedures, knowledge of work locations, etc., have been preplanned. The analyst should assess the effectiveness of integrated training (if any) for abandonment in accomplishing this capability in a structured and coherent manner.

B.5.6 Time Pressure

The analyst needs to assess the levels of workload on the SS and the field operators during the period before the decision to abandon and in the control period following abandonment. The assessed timescale for actions to be taken is discussed in Section 7 and the elements associated with the decision to abandon are discussed in Section 4. Here the analyst needs to assured that the times available take account of the actual pressures on the SS in particular, including interruptions and calls, and the need to perform tasks that are not essential in terms of the PRA model.

Table B-1
List of situational factors identified in Roth, Mosleh, et al. [5]

Detecting/ Noticing	**Sense Making / Understanding**	**Planning/Deciding**	**Manipulating/ Acting**	**Communicating/ Coordinating (Teamwork Functions)**	**Supervising/Directing Personnel**	**Directing Attention/ Managing Workload**
□ Large number of simultaneous alarms (that make the key alarm(s) difficult to detect) □ Missing information (e.g., failed alarm) □ Degraded information (i.e., the primary info is not available and requiring use of the secondary info) □ Misleading information (e.g., valve indicates closed when actually partially open) □ Small or gradual change □ No reason to check □ Status of automatic control system/ automatic control actions	□ Ambiguous cues □ Unreliable cues (e.g., indicator has a high false alarm rate) □ Multiple malfunctions □ High information load (e.g., large number of incoming reports) □ Relevant information is distributed over time or space. □ Masked cues (e.g., a safety injection masks a small LOCA) □ Garden path (initial cues focus operators in wrong direction) □ Mismatch with expectations based on prior training or experience (wrong mental model) □ Other	□ Mismatch of event evolution with procedures (e.g., plant conditions arise after relevant steps are passed) □ Incomplete procedural guidance /Ambiguous or conflicting guidance □ Multiple competing goals to balance □ Mismatch with expectations based on prior training or experience (regarding appropriate response) □ Choice under risk and uncertainty □ Workarounds routinely expected □ Decision has foreseeable grave damage to plant properties, staff safety, and/or society □ Other	□ Complex system dynamics (e.g., shrinks or swells) □ Stimulus-response incompatibility (e.g., two controls are spatially crossed with their corresponding displays; moving lever down to increase value) □ Multi-mode displays/ controls □ Inadequate system feedback (feedback about control state is missing or too slow) □ Negative transfer - Mismatch with required response based on prior training or experience □ population stereotype violations (e.g. red for normal, green for abnormal)	□ Close/frequent communication demands within CR □ Close/frequent communication demands between CR and outside (e.g., field operators) □ Close/frequent coordination demands within CR □ Close/frequent coordination demands between CR and outside (e.g., field operators) □ Other	□ Need to supervise and coordinate multiple independent activities in parallel □ Unclear lines of authority □ Key personnel missing, unavailable or delayed in arrival □ Other	□ Multiple concurrent demands for operator attention and action □ High tempo, time-pressured tasks □ Multiple distractions and interruptions □ Demands on memory / Need for mental calculation □ Need for sustained attention/continuous monitoring □ Psychological stressors; and physical stressors □ Other

Detecting/ Noticing	**Sense Making / Understanding**	**Planning/Deciding**	**Manipulating/ Acting**	**Communicating/ Coordinating (Teamwork Functions)**	**Supervising/Directing Personnel**	**Directing Attention/ Managing Workload**
not clearly indicated (e.g., complex interlocks) □ Unfamiliar/ unrecognizable alarm pattern □ Other			□ Confusable controls / Poor control coding (multiple controllers that look alike and are next to each other). □ Less than adequate in work space design (e.g., size, orientation, and nominal lighting) □ Hazardous, harsh or uncomfortable work environment □ Specific tool (not including procedures) required for the action is not available or condition is less than adequate □ Other			

Table B-2
List of situational factors associated with decision to abandon MCR (LOH)

Detecting/Noticing	Sense Making / Understanding	Planning/Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/Directing Personnel	Directing Attention/ Managing Workload
□ None	□ None	□ None	□ None	□ None	□ None	□ Psychological stressors; and physical stressors

Table B-3
List of situational factors associated with decision to abandon MCR (LOC)

Detecting/ Noticing	Sense Making / Understanding	Planning/Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/Directing Personnel	Directing Attention/ Managing Workload
□ Missing information (e.g., failed alarm) □ Degraded information (i.e., the primary info is not available and requiring use of the secondary info) □ Misleading information (e.g., valve indicates closed when actually partially open)	□ Ambiguous cues □ Unreliable cues (e.g., indicator has a high false alarm rate) □ Multiple malfunctions □ High information load (e.g., large number of incoming reports)	□ Incomplete procedural guidance /Ambiguous or conflicting guidance □ Decision has foreseeable grave damage to plant properties, staff safety, and/or society	□ None	□ None	□ None	□ Multiple concurrent demands for operator attention and action □ High tempo, time-pressured tasks □ Multiple distractions and interruptions □ Psychological stressors; and

Detecting/ Noticing	**Sense Making / Understanding**	**Planning/Deciding**	**Manipulating/ Acting**	**Communicating/ Coordinating (Teamwork Functions)**	**Supervising/Directing Personnel**	**Directing Attention/ Managing Workload**
□ Status of automatic control system/ automatic control actions not clearly indicated (e.g., complex interlocks) □ Unfamiliar/unrecognizable alarm pattern						physical stressors

Table B-4
Hierarchical list of situational factors associated with post-abandonment responses at RSDP

Detecting/ Noticing	**Sense Making / Understanding**	**Planning/Deciding**	**Manipulating/ Acting**	**Communicating/ Coordinating (Teamwork Functions)**	**Supervising/Directing Personnel**	**Directing Attention/ Managing Workload**
□ Degraded information (i.e., the primary info is not available and requiring use of the secondary info)	□ High information load (e.g., large number of incoming reports)	□ None	□ Inadequate system feedback (feedback about control state is missing or too slow) □ Population stereotype violations (e.g. red for normal, green for abnormal) □ Confusable controls / Poor control coding (multiple controllers that look alike and are next to each other). □ Less than adequate in work space design (e.g., size, orientation, and nominal lighting) □ Hazardous, harsh or uncomfortable work environment	□ Other: Close/frequent communications and coordination between RSDP and field operators in plant areas	□ Need to supervise and coordinate multiple independent activities in parallel □ Key personnel missing, unavailable or delayed in arrival	□ Multiple concurrent demands for operator attention and action □ High tempo, time-pressured tasks □ Multiple distractions and interruptions □ Demands on memory / Need for mental calculation □ Need for sustained attention/continuous monitoring □ Psychological stressors; and physical stressors

Table B-5
Hierarchical list of situational factors associated with post-abandonment responses at plant locations

Detecting/ Noticing	Sense Making / Understanding	Planning/Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/Directing Personnel	Directing Attention/ Managing Workload
□ None	□ None	□ None	□ Inadequate system feedback (feedback about control state is missing or too slow) □ Population stereotype violations (e.g. red for normal, green for abnormal) □ Confusable controls / Poor control coding (multiple controllers that look alike and are next to each other). □ Less than adequate in work space design (e.g., size, orientation, and nominal lighting) □ Hazardous, harsh or uncomfortable work environment	□ Other: Close/frequent communications and coordination between RSDP and field operators in plant areas	□ None	□ Multiple concurrent demands for operator attention and action □ High tempo, time-pressured tasks □ Multiple distractions and interruptions □ Demands on memory / Need for mental calculation □ Need for sustained attention/continuous monitoring

B.6 References

1. Globalsecurity.org, U.S. Army Field Manual 6.0, *Mission Command: Command and Control Army Forces.* 2003. Last retrieved February 1st from: http://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm.
2. U.S. Nuclear Regulatory Commission. NUREG-1624, Revision 1.*Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA),* Rockville, MD: May 2000.
3. Klein, D.E., Klein, H.A, et al., *Macrocognition: Linking Cognitive Psychology and Cognitive Ergonomics.* 5th International Conference on Human Interactions with Complex Systems, University of Illinois at Urbana-Champaign: 2000.
4. Klein, G., Ross, K.G., et al., *Macrocognition.* IEEE Intelligent Systems **18**(3): 81-85. 2003.
5. Roth, E.M., Mosleh, A., et al., *Model-based framework for characterizing contextual factors for HRA applications.* PSAM/ESREL2012, Helsinki, Finland: 2011.
6. Klein, G., Philips, J.K., et al., *A Data-Frame Theory of Sensemaking.* Expertise Out of Context. R.R. Hoffman, Ed. New York, Lawrence Erlbaum Associates: 2007.
7. Vicente, K.J., Mumaw, R.J., et al., *Operator Monitoring in Complex Dynamic Work Environment: A Qualitative Cognitive Model Based on Field Observations.* Theoretical Issues in Ergonomic Science **5**(5): 359-384: 2004.
8. Mumaw, et al. *There is more to monitoring a nuclear power plant than meets the eye.* Human Factors **42**(1): 36-55: 2000.
9. Salas, E.D., Sims, D.E., et al. *Is there a 'Big Five' in teamwork?* Small Group Research **36**: 555-599.
10. U.S. Nuclear Regulatory Commission. NUREG-0700, Revision 2, *Human-System Interface Design Review Guidelines*, Rockville, MD: 2002.

C
GUIDANCE AND TIPS FOR MCR ABANDONMENT-RELATED INFORMATION COLLECTION

MCR abandonment is a special case of fire PRA that does not build directly from internal events HFEs (even though it may contain similar actions). MCRA abandonment is governed by unique procedures even among the fire response procedures, including the procedure that guides the decision to abandon (see Appendix A for more discussion) and the safe shutdown strategy following abandonment. Also, MCR abandonment strategies include potential for the involvement of multiple operators performing distinct but correlated tasks outside the MCR, making the abandonment scenario a challenging analysis for both the fire PRA and HRA.

For this reason, it is crucial for the analysts to begin by collecting the information they will need to evaluate the unique conditions that require abandonment, including the various documents that are involved in assessing operator response.

This appendix builds upon the foundation in the Qualitative Analysis section of NUREG-1921 to identify these required inputs.

As valuable as it is for analysts to carefully review the MCR abandonment procedure, the way it is actually used and the nature of the tasks and their environment cannot be truly known unless discussions are held with the operators and trainers who use it. Guidance is therefore provided for conducting talk-throughs and walk-throughs for MCR abandonment.

The process of analyzing MCR abandonment (MCRA) can consume significant resources if the analyst is not careful to manage time and budget. One of this appendix's subsections addresses this resource management process and provides tips on utilizing other information from the fire PRA/HRA.

C.1 Plant-Specific Information Collection for MCRA HRA / PRA

As noted above, this appendix builds upon the foundation in the Qualitative Analysis section of NUREG-1921 [1] to identify these required inputs. However, as noted in Section 2.2, MCR abandonment is a special case of fire PRA where HFEs from the internal events PRA are not used as the basis for fire HRA modeling and where the procedure used as the basis for HFE modeling is likely not a fire response procedure (or an EOP). For this reason, it is crucial for the analysts to begin by collecting the information they will need to evaluate the unique conditions that require abandonment, including the various documents that are involved in assessing operator response. This information should allow the analyst to understand the MCRA process, how it is trained and evaluated at the plant, the capability and HMI of the alternate shutdown panels (ASD) or RSDP(s), and the PSFs that influence operator performance.

All of these topics, information inputs, site visits, and talk-throughs and walk-throughs are discussed below.

C.1.1 MCRA Information Inputs

The general PRA, plant and HRA information cited in Section 4.2 of NUREG-1921 [1] applies and is assumed to be available at the start of the MCR Abandonment analysis (e.g. system descriptions), but should be augmented by the information listed in Table C-1.

Table C-1 lists several possible sources of information, however, not all sources are required to start the analysis but as the analysis progresses it may be useful to follow up with some of the more specific references. For example, the very first pieces of information the HRA analyst would want to review would be:

1) MCR abandonment procedure
2) Fire-induced risk model (Fire PRA),
3) Fire PRA MCR task 11b analysis (Fire Modeling).
4) Any available feasibility study

The identification task would require:

- MCR abandonment procedure
- Fire PRA success criteria

And for this portion it would not be necessary to review the site emergency plan.

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
Fire PRA Information		
Plant Partitioning	• Fire compartments included in the MCR Abandonment analysis (NUREG/CR-6850 Task 1)	Identifies the fire compartments relevant to MCRA and the SSCs (including cables) potentially affected by fire.
	• Plant layout information	Shows the proximity of the relevant fire compartments to the MCR and RSDP and provides input to travel path assessment for local actions.
Initiating Event/Event Tree	• Plant response (both success and failure paths)	Defines the modeled PRA context consisting of the initiating event, the successful plant response path, and the failure paths; includes the modeled plant functions and systems.
	• MSOs modeled in the fire-induced risk model (NUREG/CR-6850 Task 5)	Identifies operator actions to be credited in the MCR abandonment model. Identifies MSOs that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed, etc.).
Thermal-Hydraulics	• Plant thermal-hydraulics (e.g. MAAP) data	Provides the scenario timing for different accident sequences that may apply to MCRA, as well as information on cues such as temperatures, pressures, and levels.
Circuit Analysis and Routing Information	• Circuit failure information such as cables susceptible to spurious failure and spurious failure probabilities.	Identifies equipment susceptible to spurious failures that might cause distraction during MCRA.

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
	• Routing information for cables associated with the RSDP.	Provides input to evaluation that RSDP will function as needed during MCRA.
Fire-Induced Risk Model	• MCRA modeling strategy in fire PRA (fault trees)	Provides the modeled fire PRA context for binning decisions and for determining the nature and number of HFEs needed for MCRA.
	• MCRA modeling strategy in fire PRA	
	• Multiple-spurious operations included in the fire-induced risk model, and any associated operator actions to mitigate them (NUREG/CR-6850 Task 5).	Identifies operator actions to be credited in the MCR abandonment model.
Fire Modeling	• Fire compartments identified in fire modeling that would benefit from credit for MCRA (NUREG/CR-6850 Task 11)	Provides equipment damage and fire location information for MCRA scenarios.
	• Smoke accumulation calculations from deterministic fire modeling analysis	Provides insights to the fire progression portion of the MCRA timeline.
Plant Information		
Alarms	• Fire alarms	Identifies the fire alarms in the modeled areas of the MCR, specifically the fire alarm system panel location(s) in MCR.
	• SSC alarms	Input to the plant response (mitigation) portion of the MCRA timeline. Typically not collected initially, but may be used as secondary or tertiary cues for model refinements.
	• Indications of smoke accumulation (most likely) and flames (unlikely)	Identify additional indications of a fire that potentially requires MCR abandonment. Typically not collected

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
		initially, but may be used as secondary or tertiary cues for model refinements.
Procedures	• MCRA procedure Most current procedure for MCRA – even if not finalized – obtain draft versions and understand timeframe for changes so analysts can obtain latest information from Operations and Training. Existing procedure- As a point of reference in order to understand the Operator's inherent perspective.	Collect at the beginning of the analysis. Structures the entire MCRA HRA process and typically also identifies the roles of the different on-shift plant staff.
	• Procedures calling MCRA procedure. Other procedures that direct the operators into the MCRA procedure.	Provides input to determining the cues for the MCRA diagnosis HFE.
	• Procedures called by the MCRA procedure. Other procedures that are called out by the MCRA procedure (depends on whether EOPs are still used or whether the MCRA procedure is self-contained).	Identifies tasks to include in the execution analysis (qualitative and quantitative).
	• Site Emergency Plan	Identifies who declares the fire as a site emergency and roles of various individuals in responding to the fire; may indicate which staff becomes the fire brigade and specifies interfaces with site or local fire departments.
	• Procedures/practices for operator roles and responsibilities during power operations and following reactor trip. For example, the specification of when the STA will be available and when the TSC/ERF will be available (see also Site Emergency Plan).	Provides information for timeline, feasibility assessment, execution task development; Includes: • Site-specific fire brigade, fire department, local fire department response practices • Electrical safety practices and protective gear for high voltage breaker operation

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
		• Communication systems, testing, practices and usage preferences, keys, tools, SCBA storage location(s), upkeep and accessibility
	• Control room HVAC procedure for alignments following a fire.	In conjunction with the deterministic fire modeling analyses, identifies the smoke build-up rate.
Training	• Training schedule (typically bi-annual) • Insights or summary from last bi-annual training • Training materials related to MCR abandonment. For example, instructor lesson guide or PowerPoint slides; • Results of simulator exercises (especially timing) from MCRA training [if Training department is willing to provide]	Used in the qualitative analysis, and also in timeline development.
Job Performance Measures	• JPMs or other timed walk-throughs used in MCRA training	Provides timing information, typically related to the execution which can provide additional requirements such as special tools or PPE used as execution PSFs.
Operator Action Feasibility Assessment	• Appendix R feasibility assessments for MCRA and operator manual actions or NSCA feasibility study. This is a deterministic analysis performed by fire protection demonstrating the feasibility of operator actions credited in the safe shutdown (licensing) analysis.	Collect at the beginning of the analysis. Used in the qualitative and feasibility analyses. Typically provides the following: • Timing (but may not be as well founded as JPMs, simulator data, timed walkthroughs) • Communications • Lighting: emergency and portable lighting usage, availability and locations • Access paths

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
Remote Shutdown Panel Design Information	• List of instrumentation and controls located on RSDP(s) • See also Plant Partitioning (Plant Layout) and Circuit Information (RSDP circuit analysis)	Provides information on the RSDP capabilities for assessing operator response during MCRA scenarios (which functions can be done at RSDP vs. locally). Identifies location of RSDP in plant so that travel time can be assessed and routing of cables for RSDP to assess functionality.
HRA Information		
Internal Events and Fire HRA Notebooks and Quantitative Analysis Calculations	• HFEs for comparable local actions • Previous operator interviews (especially for fire but also for internal events PRA), walk-throughs, talk-throughs, and/or simulator data. • Time Critical Operator Actions (TCOA) information from Appendix R	Provides timing information and other plant-specific insights that have already been investigated for the baseline HRA; particularly useful for actions similar to those included in MCRA as execution actions

C.2 Site Visit Preparation

As valuable as it is for analysts to carefully review the MCR abandonment procedure and other inputs discussed above, the way operators actually use the procedure and the nature of the MCRA tasks and their environment cannot be truly known unless discussions are held with the operators and trainers who use it. Because of the uniqueness of MCRA, additional or more explicit guidance is, therefore, provided below for conducting talk-throughs and walk-throughs for MCR abandonment.

It is important to prepare for the site visit to maximize the information gathering process when there, since time with the operations and training staff will be limited. The following steps are considered to be important:

- Identify the site visit team and ensure representation from HRA, fire PRA and fire protection – not so many that it makes walk-downs difficult, but having someone with knowledge of the MCRA modeling in the PRA is helpful to provide the equipment availability and scenario perspective.
- Recommend site contacts in operations and training with familiarity with the MCR abandonment procedure (such as Shift Supervisors/SROs who would be called upon to make the decision to abandon in such a case). If the MCR abandonment procedure is in the process of being updated, then the procedure writer would be useful.
- Coordinate with the contacts provided for site operations and training regarding available days and times, especially for in-plant access.
- Determine the security access requirements and who will arrange for them.
- Prepare a work plan to structure the site visit – time is valuable and needs to be concentrated on information gathering objectives.
- Entry into the MCR, and walkdowns of the back-panel areas, typically requires a pre-job brief. This is especially true if the plant is at-power and the MCR panels have open backs.

Regarding the work plan for the operator interviews, an interview questionnaire form has been issued by EPRI as part of version 5.1 of the HRA Calculator, as shown in Table C-2. This can be reviewed against other formats and questions that have been the analysts may have used for previous operator interviews to develop a comprehensive form. It is recommended to have one interview form for the pre-abandonment phase and separate interview forms for each of the different operator roles following the decision to abandon.

Prior to the visit, the analysts should have reviewed the MCRA procedure in detail and should have familiarized themselves with other input materials, particularly potentially relevant T/H runs and fire modeling information to estimate the associated timing. Taking an initial cut at identifying the specific MCR abandonment HFEs can be very helpful in identifying questions to address during the talk-through and walk-through sessions. (The details of the draft HFEs can even be provided to the operators before the site visit.)

The length of the site visit is mainly based on the availability of operators for talk-throughs and walk-throughs and resource constraints, but if it is possible to schedule three to four days on-site to have the opportunity to ask follow-on questions while still there, that is preferable.

HRA analysts and practitioners might find the following tips, based on the authors' experience, helpful:

- Do not use HRA or HF jargon (e.g., talk about "performance shaping factors")
- Learn to "speak operations" (e.g., focus discussions on plant behavior, equipment performance, specifics of how actions are performed)
- Avoid leading questions
- Listen more; talk less (e.g., keep questions short but ask for follow-up or clarifying information)

C.3 Talk-Throughs and Walk-Throughs

As stated in Section 4.11 of NUREG-1921 on Reviews with Plant Operations, "The talk-through and walk-through processes are activities that seek to determine the likely outcome(s) of a situation based on starting conditions and the effects of decisions made—the former through structured discussions and the latter through enactments under the most realistic conditions possible."

Given the unique nature of the conditions that prompt MCR abandonment, performing "enactments under the most realistic conditions possible" is particularly challenging for the analyst, but is achieved primarily by prompting operations staff to envision the conditions they will be faced with and to recall their training and simulator run-throughs of an abandonment scenario.

Section 4.11 of NUREG-1921 also provides general background on collecting information from plant-specific interviews and discusses important aspects of conducting talk-throughs and walk-throughs. That information will not be repeated here; the following sections will focus instead on issues specific to MCR abandonment.

C.3.1 Talk-Throughs

Talk-throughs can provide valuable insights into the detection, diagnosis and decision-making associated with the cognitive portion of the operator actions. This is especially true during the MCR abandonment evaluation since the decision to abandon may not have clear cut cues or indications. For the execution portion of the analysis, talk-throughs can provide insights into access paths, personal protective equipment and tools, as well as the time to complete the actions.

The talk-throughs begin with an introduction of the team and an explanation of the reason for the visit, stressing that this is not an evaluation, but an activity that supports the PRA and provides valuable input to the realism and accuracy of the analysis. It is also important to stress that the discussion is to confirm the success path, as well as to discuss the operator response when the success path is challenged (such as when failures occur).

The discussion continues with general questions, such as normal crew composition, command and control structure during abandonment, on-site fire department capability, and operations crew required to support the fire brigade.

Once an understanding of the general operation of the crew in response to a fire is covered, the specific entry conditions for the MCR abandonment procedure are discussed. One of the key pieces of information that has to be gathered is the set of decision criteria for abandonment. Typically would include both LOH and LOC. While LOH is based on fire modeling evaluations of smoke density and air temperature, LOC is plant-specific and depends upon the specific fire compartments identified by the fire PRA where a severe fire, resulting in significant degradation of MCR function, has been postulated to occur. Generally, this is in either the MCR (primarily involving panels of the main control board itself, although there are exceptions) or the cable spreading and/or relay rooms, but other plant-specific fire compartments may also cause such functional loss.

It is important for the analysts to be familiar with the level of guidance provided by the MCR abandonment procedure to the Shift Supervisor or SRO for making the decision to abandon the MCR. Some procedures provide clear direction, while others leave the decision largely to the discretion of a designated manager. For the purposes of the PRA, it is important to elicit from the operators as specifically as possible the systems or functions that would have to be lost in order for the decision to be made to abandon, and also the means by which the decision would be made (i.e., while the decision is likely initiated at the discretion of a single individual, the extent to which that individual would solicit other input would not be specified by the procedure, and so would need to be ascertained through the interview process).

The analysts must also assist the operators in envisioning a fire of the magnitude that would require abandonment since there is often a credibility issue as well as natural reluctance to consider leaving the MCR for the lesser capability for control and monitoring provided at the RSDP(s). It is not unlikely that the initial response would be that they would "never" leave, mostly because they cannot envision the types of scenarios to which the PRA intends to apply MCRA credit, so the full extent of what they would see and be able to do (or not see and not be able to do) from the MCR needs to be clearly described. This can be aided by "queries" of the PRA model to develop a list of all the failures that are postulated to occur for the representative LOC scenarios.

Part of the abandonment decision process is likely to involve confirmation of the fire severity in fire areas outside the MCR. It is important to elicit information from the operators regarding the travel time for the individual assigned under the fire response procedure to reach the location of the fire, assess the severity/controllability, and relay that information back to the MCR – this will be factored into the delay time of the MCR abandonment cognitive HFE. Additionally, it is important to ask how the severity is assessed since many times a visual inspection may be impaired due to smoke or equipment such as cabinets or raceway covers.

Following the discussion of the decision to abandon, the talk-through continues by discussing the specific operator actions included in the MCR abandonment procedure.

It is common for MCR abandonment procedures to contain actions that are "nice to do" versus those that are "crucial to do" from the standpoint of the PRA required actions to reach a safe and stable plant state. It is therefore important for the analysts to review the MCR abandonment procedure beforehand to identify the steps that are PRA critical and ensure that the talk-through

focuses on these steps, and to be patient in explaining why these are the important items and others are not so.

Experience with such interviews has shown that Operations often considers some non-PRA critical steps to be important. The primary reason for this is that in the past operators have been trained (and procedures written) using a deterministic assessment of fire impacts, in particular with respect to the occurrence of spurious operations (i.e., if it can happen, it does happen – every time and for every fire scenario in the fire area). However, in the PRA frequencies are assigned to scenarios and probabilities assigned to failures, and it is often the case that the scenarios of concern do not include some of these failures. This requires sometimes extensive discussion to break through the paradigm and bias built up over the years, so the analysts will have to discuss these to provide PRA perspective and emphasize that the time required to perform these steps may distract focus from the critical actions or even render the overall process infeasible. Discussions sometimes result in consolidation or re-ordering of procedure step performance that might allow for these actions in addition to the PRA critical actions (see Section 10 for more guidance), but as noted previously it is important to be patient during these discussions.

During the talk-through, it is important for the analysts to identify the responsibilities of each crew member who is executing the procedure, the locations of the actions, any keys or tools needed to do the job, and the associated communication protocols. Many MCR abandonment procedures are structured with the Shift Supervisor/SRO going to the RSDP to direct the overall process and handing out procedure attachments to individual operators to perform at remote locations. For the HRA, determining which operator actions require diagnosis and decision-making versus those which are simply following procedural direction is important because that diagnosis time would need to be factored into the HFE later.

In addition to obtaining answers to the interview questions while at the site, it is important to identify a particular operator who can serve as a point of contact for post-visit questions and clarifications as the analysis progresses.

Table C-2 provides a structure for the MCRA talk-through, including introductions and the questions that are typically asked.

Table C-2
MCRA HRA talk-through structure

Introduction
My name is _____from _____ and these are my colleagues _____. We have been tasked with helping conduct the fire PRA for your plant. We know the plant has a good safety and reliability record, but we look at what systems and components could fail to operate to try to figure out how likely those combinations of failure are. We do a ranked list of these combinations of failures to see which of them are most likely to happen so we can identify where the problems are and where the focus on improvements should be. One part of plant reliability is the equipment, but we also know that operators are the ones with the training, experience and procedures to bring the plant to a safe and stable condition when the equipment failures happen.

We are here to learn from you – we can look at the procedures, but we don't get the real feeling for how things happen and what you actually do. So this is not a test or a performance review. We are just gathering information to help us figure out what you look at and how you assess the plant conditions and situations. We would like to ask you questions and take notes and also do a walk down in the plant. Our specific task is to look at fires in the plant and understand how you use the fire procedures, especially when a fire is so severe that it would make you leave the control room.
Specific Questions
1. How do you find out about a fire and where it is located?
2. Where is the fire alarm panel located in the MCR (front or back panel)?
3. Do you have to figure out where the fire is or does the fire alarm panel tell you?
4. Do you send someone to locally verify the fire severity (or contact an out-plant operator)? How long do you think it would take to get that information?
5. How many and which MCR operators are assigned to the fire brigade?
6. Do you have an on-site fire department? If not, how close is the nearest fire department?
7. Have you experienced an actual fire? How serious was it and what happened?
8. Are you trained on a fire in the MCR or cable spreading room?
9. What indications would you be getting for CSR fire (or other fire outside of the MCR that requires MCR Abandonment)?
10. What indications would be lost or unreliable due to MCR or CSR fire?
11. For an MCR fire, are there particular panels that if lost would make you more likely to leave?
12. Which procedure would you be using first? Are several procedures used in parallel?
13. Is there a list in the procedure of protected instruments that are reliable in case of fire?
14. Who makes the decision to leave the MCR?
15. The procedure doesn't specifically say if you lose X, Y, Z equipment you should go, so is there a list like that covered in training or in your experience?
16. Do you have any feeling for the time it would take to make that decision to leave the MCR, based on your training?
17. Speaking of training, how often are you trained on this scenario? Do you use the simulator?
18. Would you wait as long as possible before going to the RSDP? Would you try to stay in the MCR in SCBAs?
19. How much control and instrumentation do you have on your RSDP? Is that a factor in the decision to leave the MCR? (for positive or negative?)
20. So when you decide to leave the MCR, what happens next? Is there a disconnect switch you need to actuate? Do you need to get keys or other items before you go?
21. What is the travel path from the MCR to the RSDP and how long does it take to get there?
22. Which operator goes where? Does the Shift Supervisor/Manager go directly to the RSDP?
23. Are different people stationed in different places?
24. What communications system(s) do you use?
25. Is there portable lighting that you get and use (Flashlights? Headlamps?) or do you count on local emergency lighting?
26. If you need tools or gear, where are they located? Do you need keys to access them and if so, where are the keys and do you need time to get them? Are the tools/gear checked and replaced regularly?
27. Would fire impact the security system and would access to areas be a problem?

28. Does the Shift Supervisor/Manager go to the RSDP and coordinate the overall process? Or does each operator act independently? What is the communication process like?
29. What are the primary parameters or functions you are going to be focused on controlling?
30. Is the workload greater than for other transients you train for or have experienced?
31. Do you recall how long it takes when you run through the abandonment procedure during training?

It is a great benefit to the analysis if separate talk-through sessions can be conducted with several different operators, to see if there are differences in perspective. Any inconsistencies can be noted as topics to cover in the walk-through and to consider as sources of uncertainty in the analysis.

Aside from the questions that relate to obtaining a general understanding of the process and procedure steps, the talk-through should also collect more specific information for application to the qualitative and quantitative analysis of the MCRA HFEs. Prior experience with performing an MCRA HRA or a review of the examples in this guidelines document can be used to scope out some preliminary HFEs for major tasks, functions or operator actions. A template of topics that should be addressed for the HRA, such as the interview form from the EPRI HRA Calculator v.5.1 release notes [3] shown in Table C-3, can be used to ensure that the following items are covered during the talk-through:

- Expected cue to alert operators to the need to take the specific action
- Time to reach the specified cue from beginning of event (i.e., plant trip) where the cue is based on a specific procedure step
- Time to evaluate conditions and make decision to take the specific action
- Time to complete the action once a decision is made
- Location and complexity of action steps
- Human-machine interfaces

Table C-3
HRA interview form (from EPRI HRA calculator v. 5.1 release notes)

PRA/HRA Analysts		
Worker(s) Interviewed		
Date of Interview		
Location of Interview		
Basic Event ID	**HFE Description (indicate if all of the HFE or a portion of the HFE)**	
Initial Conditions, Initiating Event, Accident Sequence, Success Criteria [from Scenario Description field]		
Cue including Instrumentation, System signal or reading	[from Initial Cue field]	Additional Notes on Cue

Procedures including Informal Instructions, Training, or Guidance	Cognitive Procedure	Cognitive Procedure Description and Revision #
		Cognitive Step # and Instructions
	Execution Procedure	Executive Procedure Description and Revision #
		Execution Instructions
Timing	T_{sw}	Required time window for performing the action
	T_{delay}	Time from start of event to presentation of cue to worker that action is required
	T_{cog}	Diagnosis and decision-making time
	T_{exe}	Execution (manipulation) time
	Timing Notes	[from Time Window Notes field]
Manpower	[Required crew members in the HRA Calculator field]	
Stress	Stress Level	Stress decision tree outcome based on PSFs
	Workload	Yes/No based on stress decision tree
	Performance Shaping Factor (PSF)	Could be Nominal or Negative based on stress decision tree
	Notes on Stress	
Location	Cognitive Location	
	Execution Location	
Execution PSFs	Environment	
	Heat/Humidity	
	Atmosphere	
	Special Requirements such as Tools and/or PPE	
	Factors contributing to Complexity of Response	
HRA/PRA Assumptions		
1. Given the scenario description, starting with the initiating event, what is the progression required by the crew to reach the guidance for this action?		
2. Given the discussion in 1, are there other progressions possible?		

3. What signals/cues/triggers lead to the decision to perform this action?
4. How long would it take to reach the guidance for this action?
5. Who is required to perform this action?
6. Where does the execution take place?
7. Is there any special equipment required for the execution? For example, tools, flashlights, protective gear.
8. Is the location readily accessible?
9. Is the operator's environment impacted in anyway? For example, is there reduced lighting, high temperature, or smoke?
10. How long would it take to perform this action, including travel time from original to another location (T_{exe})?
11. What type of training is performed for this activity (classroom or simulator or mock-up)? How often is training performed on this activity?
12. What other activities would be required at the same time?

13. Notes
Additional MCR Abandonment-specific Notes:
14. Relationship between this action and the overall MCR Abandonment response.
15. Communications. What communications are conducted during the conduct of this action?
16. Coordination. What other actions rely on this action? What other actions are needed before this action can succeed?
17. Instrumentation.
18. Actions Needed in the first 30 minutes.
19. Actions Needed after the first 30 minutes (through the mission time)

Discussions are recommended after each talk-through among the analysts on the team to identify points that were particularly obvious, confusing, or differed between operators. These points can then be emphasized during subsequent talk-throughs as well as the walk-through.

C.3.2 Walk-Throughs

During the talk-through, the emphasis is on obtaining an overview of how the procedures are used, some of the key decision points and time constraints of the process and in general, gaining a sense of the operations and training perspective on the scenario, how it evolves and how it has been trained.

The walk-through provides the analysts the opportunity to view the locations, conditions at the RSDP as well as the interfaces with the RSDP and other equipment cited in the MCRA procedure steps. It allows the analysts to identify potential challenges to successful plant response. These challenges include, but are not limited to, the following:

- Difficult actions due to equipment location (time required to get there) and local environment (heat, noise).
- Limited access to components to be operated (cramped workspace or up a ladder)
- Physical workload such as a several hundred turns of a small operator to operate a large valve.

- Travel times from one point to another
- Performance times for key tasks including time to obtain tools, lighting and/or PPE
- Communications circuits that will be used
- Seeing what needs to be done in a timely manner in the MCR prior to abandonment and during the transfer of control to the RSDP. These insights potentially feed into plant modifications (e.g., installation of kill switches) that could simplify actions, save time, and impact operator reliability.

In other words, the MCRA process that may still be somewhat abstract during the talk-through(s) becomes more real during the walk-through.

Based on the talk-through, the analysis team should have identified the locations associated with the PRA-relevant procedure steps in the MCR abandonment process that they would like to see during the walk-through. These will have to be identified prior to the walk-through to ensure that the appropriate access is obtained. The walkthrough needs to be organized, even if informally, so that the analysis team can see what they need to see during the time allotted. Ideally, more than one local operator will be available for the walk-through in order to evaluate coordination of actions specifically to observe the time required and how the communications and coordination are conducted. Visiting the RSDP and other local action locations is crucial since the analysts must understand the plant-specific RSDP displays, capabilities and limitations.

The number of locations visited during the walk-through is highly plant-specific, dependent on the plant's remote shutdown strategy and based on a review of the MCRA procedure. There may be several locations necessary to start up the RSDP, start up support systems, and establish control. For each location, the HRA analyst should note the travel time, communication, and coordination with other operators at other locations. In addition to timing information, the analyst should also be noting insights on other performance shaping factors.

The travel time and procedure step performance time for each key procedure step identified during the talk-through should be clarified and noted during the walk-through, including the time required for communication with other remote operators and to confirm actions taken. The timing should be recorded for future use during qualitative/quantitative analysis (including feasibility assessment) by a PRA/HRA member of the walk-through team. Since the walk-through will focus on the execution portion of the actions, any particularly challenging or difficult actions should be noted; for example, is access to the equipment time consuming or does a valve take many turns of a handwheel to close? Actions that require some decision-making and not just following procedure steps, such as electrical bus load shedding actions in preparation for starting a diesel generator, should be noted as well since the cognitive portion will have to be addressed to the HFE during the detailed HRA. Key factors addressed in the THERP Chapter 20 [4] tables should also be considered during the walk-through. These include the nature of the HMI (presence of mimics, type of display being read and type of manual control), whether the equipment is one among many in a similar grouping, and whether there is clear and unambiguous labeling of equipment.

The walk-through also provides an excellent opportunity to gather information to assess feasibility criteria such as communications, lighting, and accessibility of tools/keys/personnel

protective equipment (see NUREG-1921 Section 4.3 [1] and Section 6 of this guideline on Feasibility for further details).

There should be someone taking notes throughout the walk-through, particularly on timing aspects, to ensure that these key details are preserved. It is rare to get a chance at a second walk-through.

Once the walk-through is completed, any remaining time at the site should be used to review the information already gathered, discuss it among the analysis team to gain consensus on key actions and timing, identify any scenario variations from the PRA model that should be addressed, and start applying the information to the HRA to see if there are any outstanding or follow-up questions that can be addressed before leaving the site.

C.4 Managing Resources

The process of analyzing MCRA can consume significant resources if the analyst is not careful to manage time and budget. Therefore, the discussion below addresses this resource management process and provides tips on utilizing other information from the fire PRA/HRA.

As when conducting detailed fire modeling on any area that has a large number of sources as well as a large number of targets, the MCRA analysis can become a time-consuming (and resource draining) activity due to the detail and intricacy of the process and the need for interface with the site. Most analysts do not have an unlimited resources for these studies as they are considered to be a subset of the fire PRA/HRA, so resource management is important. A balance must be struck between providing the level of detail necessary to capture the process while not overtaxing the budget and compromising project schedule.

C.4.1 MCRA PRA Scenario Binning

Discussions with the fire PRA modeling team are essential to understanding the minimum set of unique scenarios that must be evaluated by the HRA.

Aspects that must be determined are:

- Specific fire areas that cause MCRA (e.g., MCR itself and cable spreading room)
- Scenarios that should be considered as separate evaluations:
    - AC power recovery is commonly broken out since it involves operator actions to locally re-power the credited AC power train, and the associated equipment reliability.
    - Scenarios that are (or are not) relevant to achieving safe and stable plant state.
        - For example, maintaining sufficient inventory [such as in the Refueling Water Storage Tank (RWST)] to account for Reactor Coolant System (RCS) volume reductions.
- Functional situations where the MCRA procedure does <u>not</u> have the capability to achieve safe shutdown from outside of the MCR to understand what is excluded from the analysis.

For many plants, this is a LOCA condition, but may not exclude LOCA due to spurious PORV operation.

As is commonly done in PRA it is often useful to create bins within these bins to account for differences in the details of what is available in terms of instrumentation and equipment. For example, in the case of LOH there could be scenarios where the fire that forces abandonment occurs in a non-safety panel and effects very little (if any) equipment needed for reaching a safe-and-stable condition, all the way up to scenarios that effect large numbers of this equipment. The complexity of the execution actions (and the need for them) varies greatly and needs to be addressed in the qualitative assessment. For LOC, different scenarios could make the diagnosis of LOC more or less difficult of a decision.

Binning the scenarios is a mutual decision by the PRA and the HRA that allows the HRA to focus on a set of actions while still maintaining some distinctions where local actions dominate. Since not all MCRA scenarios modeled by the fire PRA will actually require all these actions, this is a conservative approach. However, there are opportunities for refining the analysis to reduce the conservatism that can be taken, if additional risk margin is desired.

C.4.2 Use of Previous MCRA HRAs

One of the ways resources are conserved in HRA is to review previous analyses to see what aspects can be carried over to a new study, or even as a reminder of the type of issues that dominate a particular type of operator action. Although MCRA is highly unique and plant-specific, there may be aspects of a prior analysis that can be re-used, such as the structure of the cognitive HFE for the decision to abandon on LOC, discussed further in Section 4, or the types of tasks the operators could be expected to execute at the RSDP or locally in the plant.

The LOC-related cognitive HFE needs to focus on the timing aspects, specifically for the cue and confirmation that there is a severe fire, the time required to make the decision to abandon, and the time needed to implement any actions in the MCR to transition to or enable the RSDP(s). Reviewing another analysis can assist in understanding the key factors that go into evaluating that timing.

Since the execution portion of the MCRA HRA focuses on the actions important for reaching a safe and stable plant state, it can be useful to review other MCRA assessments to understand the key parameters and functions that must be controlled.

Some of the actions that may have been modeled in previous MCRA HRAs include:

- Establishing control at the RSDP(s)
- Tripping the reactor coolant pumps
- Taking local control of breakers on the bus
- Locally starting the diesel generator (for station blackout scenarios)
- Locally establishing and maintaining reactor vessel level through high and low pressure systems (BWR)
- Locally establishing and maintaining SG level through feedwater pressure systems (PWR)

The analyst should also check similar or comparable operator actions already modeled in the internal events and fire PRAs to see what information is still consistent for MCRA, such as the thermal-hydraulics for the fire PRA scenario that is most constraining for MCRA to provide the overall timeframe within which the actions need to be taken. In addition, JPMs and operator interviews for actions that constitute a piece of the MCRA process can provide insights to manipulation and travel timing.

Care should be taken, however, not to carry over an approach for convenience without considering the plant-specific nature of the actions and interfaces and how they should be grouped and developed as HFEs.

C.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
3. *EPRI HRA Calculator Version 5.1.* EPRI, Palo Alto, CA. EPRI 3002003149: June 2014.
4. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* U.S. Nuclear Regulatory Commission, Washington, D.C. NUREG/CR-1278: August 1983.