DISSERTATION

DEVELOPMENT OF A HUMAN FACTORS HAZARD MODEL FOR USE IN SYSTEM SAFETY ANALYSIS

Submitted by

Dustin Scott Birch

Department of Systems Engineering

In partial fulfillment of the requirements

For the degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2021

Doctoral Committee:

Advisor: Thomas Bradley

Erika Miller
James Cale
Mehmet Ozbek

ABSTRACT

DEVELOPMENT OF A HUMAN FACTORS HAZARD MODEL FOR USE IN SYSTEM SAFETY ANALYSIS

Traditional methods for Human Reliability Analysis (HRA) have been developed with specific applications or industries in mind. Additionally, these methods are often complicated, time consuming, costly to apply, and are not suitable for direct comparison amongst themselves. The proposed Human Factors Hazard Model (HFHM) utilizes the established and time-tested probabilistic analysis tools of Fault Tree Analysis (FTA) and Event Tree Analysis (ETA), and integrates them with a newly developed Human Error Probability (HEP) predictive tool. This new approach is developed around Performance Shaping Factors (PSFs) relevant to human behavior, as well as specific characteristics unique to a system architecture and its corresponding operational behavior. This updated approach is intended to standardize, simplify, and automate the approach to modeling the likelihood of a mishap due to a human-system interaction during a hazard event.

The HFHM is exemplified and automated within a commercial software tool such that trade and sensitivity studies can be conducted and validated easily. The analysis results generated by the HFHM can be used as a standardized guide to SE analysts as a well as design engineers with regards to risk assessment, safety requirements, design options, and needed safety controls within the system architecture. Verification and evaluation of the HFHM indicate that it is an effective tool for HRA and system safety with results that accurately predict HEP values that can guide design efforts with respect to human factors.

In addition to the development and automation of the HFHM, application within commonly used system safety Hazard Analysis Techniques (HATs) is established. Specific utilization of the HFHM within system or subsystem level FTA and Failure Mode and Effects Analysis (FMEA) is established such that human related hazards can more accurately be accounted for in system design safety analysis and lifecycle management.

Lastly, integration of the HFHM within Model-Based System Engineering (MBSE) emphasizing an implementation into the System Modeling Language (SysML) is established using a combination of existing hazard analysis libraries and custom designed libraries within the Unified Modeling Language (UML). The FTA / ETA components of the hazard model are developed within SysML partially utilizing the RAAML (Risk Analysis and Assessment Modeling Language) currently under development by the Object Management Group (OMG), as well as a unique recursive analysis library. The SysML model successfully replicates the probabilistic calculation results of the HFHM as generated by the native analytical model. The SysML profiles developed to implement HFHM have application in integration of conventional system safety analysis as well as requirements engineering within lifecycle management.

ACKNOWLEDGMENTS

I would like to thank my advisory committee Dr. Thomas Bradley, Dr. Erika Miller, Dr. James Cale, and Dr. Mehmet Ozbek for their support of my research activities. I would also like to thank Dr. Daniel Herber and Jayesh Narsinghani for their essential contributions to the SysML component of this work. Everyone's expertise and insight have been invaluable in my efforts to complete my research project and add to the knowledge base in Systems Engineering, and particularly in safety analysis. I'm grateful to Colorado State University for their dedication to student success, and the world class instruction I received while completing my degree program. Additionally, I would also like to thank the College of Engineering, Applied Science, and Technology at Weber State University, and particularly Dr. David Ferro, Dean, for their support of my educational endeavors. Without this key support, I would not have completed my degree program. Finally, I must thank my wife Wendi, my children Alaina, Elise, and Jace, as well as my parents Keith and Susan and brothers, Brody and Barton, for their continuous support, encouragement, and confidence in me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACES	The Applied Computational Electromagnetics Society
AIAA	American Institute of Aeronautics and Astronautics
ASEE	American Society for Engineering Education
ASME	American Society of Mechanical Engineers
BA	Barrier Analysis
BDD	Block Definition Diagram
BPA	Bent Pin Analysis
CAST	Causal Analysis based on STAMP
CCA	Cause-Consequence Analysis
CCFA	Common Cause Failure Analysis
CD	Conceptual Design
DD	Detail Design
EASA	European Union Aviation Safety Agency
EDC	Engineering Data Compendium – Human Perception and Performance
EHA	Environmental Hazard Analysis
ETA	Event Tree Analysis
FAA	Federal Aviation Administration
FHA	Functional Hazard Analysis or Fault Hazard Analysis
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FMRI	Final Mishap Risk Index
FTA	Fault Tree Analysis
HAT	Hazard Analysis Technique
HAZOP	Hazard and Operability Analysis
HD	Health Design
HEP	Human Error Probability
HFHM	Human Factors Hazard Model
HFTE	Human Factors Triggering Event
HHA	Health Hazard Assessment
HRA	Human Reliability Analysis
IMRI	Initial Mishap Risk Index
INCOSE	International Council on Systems Engineering
IBD	Internal Block Diagram
ISSS	International System Safety Society
JHA	Job Hazard Analysis
MA	Markov Analysis
MBSE	Model-Based Systems Engineering
MORT	Management and Oversight Risk Tree
NASA	National Aeronautics and Space Administration
OD	Operations Design

OMG	Object Management Group, Inc.
O&SHA	Operating and Support Hazard Analysis
OUR	Office of Undergraduate Research
PD	Preliminary Design
PHA	Preliminary Hazard Analysis or Process Hazard Analysis
PHL	Preliminary Hazard List
PNA	Petri Net Analysis
PRA	Probabilistic Risk Analysis
PSF	Performance Shaping Factor
RAAML	Risk Analysis and Assessment Modeling Language
RHA	Requirements Hazard Analysis
RD	Requirements Design
RE	Requirements Engineering
RPN	Risk Priority Number
RSPG	Research, Scholarship, and Professional Growth
RQ	Research Question
SCA	Sneak Circuit Analysis
SD	System Design
SE	Systems Engineering
SHA	System Hazard Analysis
SoSHA	System of Systems Hazard Analysis
SSHA	Subsystem Hazard Analysis
STAMP	Systems-Theoretic Accident Model
STPA	Systems-Theoretic Process Analysis
SwHA	Software Hazard Analysis
SysML	Systems Modeling Language
T	Task
THA	Test Hazard Analysis or Threat Hazard Analysis
UML	Unified Modeling Language

INTRODUCTION

An engineered system is comprised of numerous human, electrical, mechanical, and software components and subsystems. These system building blocks are combined together into a larger, more complex system, that is used to perform a function per a specified design intent. Human beings (human actors), along with all other components in the design, can interact with the system to respond to off-design behavior to avoid a hazardous situation that may evolve into an accident / mishap [10]. These human-system interactions play a significant role in determining the reliability and safety of a system throughout its lifecycle [11]. The combined functionalities and associated interactions of all system elements, including human elements, must be modeled, analyzed, and documented as a matter of Systems Engineering (SE) best practice. System Safety analysis asserts that the reliability and hazard characteristics of the system design must be evaluated and analyzed, then all of the identified potential hazards eliminated or minimized, such that a failure might avoid resulting in a catastrophic outcome. To be considered complete, this engineering analysis must consider the interactions and risks posed by all human actors within the system context. A consistent and uniform approach to analyzing the human contribution to safety throughout the system lifecycle management process is preferred.

The contemporary inductive perspective of System Safety analysis tends to emphasize scrutiny of the non-human elements (electrical, mechanical, software) that are combined into the larger system architecture [14][41]. Typically, the probabilistic failure rates of these various elements are determined, and then accounted for in the larger system arrangement using established Hazard Analysis Techniques (HATs). The prospective failure modes and safety

related concerns of a system are evaluated based on the results of these HAT activities and documented for future abatement during subsequent design and testing activities [14]. In addition to the electrical, mechanical, and software elements that are commonly recognized as the core building blocks of a system design, human actors and their respective influence on system operations can be of equal or even greater importance, to the performance, reliability, and safety within the system lifecycle [11]. Accident rates attributable to human activity in system operations range from 10% to as high as 80% depending on the industry and application [15][21]. For example, the National Highway Traffic Safety Administration (NHTSA) reports that human error is the cause of up to 94% of all ground transportation accidents [50]. Although sometimes overlooked or minimized during system analysis and design, the various human interactions within the system context, and their possible impact on safety, should be properly scrutinized, with potential hazard probabilities being quantified explicitly [21].

There is no universal or general technique to evaluate the hazards associated with human-system interaction [15][19]. Several Human Reliability Analysis (HRA) approaches have been developed, but they are typically complicated and time consuming to implement and are not designed to be applied across engineering disciplines or applications [22]. Instead, HRA approaches generally have specific application within certain industries, environments, or operational activities [15]. For example, HRA techniques such as the Technique for Human Error Rate Prediction (THERP) and Success Likelihood Index Method – Multiattribute Utility Decomposition (SLIM-MAUD) have their origins and primary usage in the nuclear power industries, with an emphasis on control room activities. A technique such as Maintenance Personnel Performance Simulation (MAPPS) focus primarily on human hazard analysis as it relates to maintenance activities, and Aeronautical Decision-Making (ADM) is an analysis

technique specific to pilot-flight control interface analysis [22][23][47]. Considering the HRA approaches as currently evaluated, the proposed Human Factors Hazard Model (HFHM) is intended to provide a systematic, automated, and efficient approach to assessing system risks associated with human interactions. With this new approach to predicting human hazard risk, comprehensive safety analysis of an entire system can be performed with improved accuracy, consistency of approach, and thoroughness.

As a complementary development to an improved modelling technique for HRA, an approach to implement this within the most state-of-the-art lifecycle management tools would be desirable and necessary to enable application of the technology. In keeping with this philosophy, clear advantages are evident in the application of Model-Based Systems Engineering (MBSE) into design activities [31]. As opposed to the document-based approach to systems engineering, using MBSE, and particularly the System Modeling Language (SysML) establishes an integrated and coherent virtual model of the system design that captures nearly all of the system design definition within a single overarching model that is parametrically linked for real-time management. Conversely, the traditional document-based approach to system design can present significant challenges when applied to complicated or highly dynamic systems. Document-based systems engineering will typically include information spread over many organizations in formats unique to those organizations. Each group will likely be performing lifecycle design activities using tools unique to themselves (spreadsheets, diagraming tools, etc.). The characteristics of this management technique are prone to ‘siloing’ or ‘stove-piping’ where each organization operates with limited contact and communication with each other, and information is not readily available or shared, nor is it often in its most current iteration for other systems engineers to utilize. The model as defined in MBSE is established as a single entity, wherein all

relevant Systems Engineering information and data reside and can be shared amongst all interested parties. The model is essentially a single virtual prototype representing system structure, behavior, requirements, and parametrics [31]. Therefore, theoretically, if any stakeholder revises a model element or relationships between elements, the underlying model will account for this change, and propagate all relevant data and altered system behavior throughout the system architecture as established by MBSE. This parametric model behavior promotes more effective communication of data, uniformity of design, repeatability, and efficiency [31]. All of these intended features of MBSE promote a more direct method for validation and verification of system requirements such that a design meets all of the specified intent. However, it is important to note that regardless of the applied approach to Systems Engineering, the same lifecycle management activities are performed [33]. As a result of the advantages of MBSE, organizations become much more focused on a single, shared model, that exists as the single virtual representation of the system configuration and design [33][32]. Model-Based Systems Engineering (MBSE) is the recommended approach to lifecycle management as proposed by the International Council on Systems Engineering (INCOSE), as well as a growing number of government entities and industry partners. The natural progression of systems architecture approaches must include reliability and safety analysis, including human factors, in keeping with the 'model-centric' philosophy associated with MBSE [7].

One critical element of the 'system-think' associated with lifecycle design is the consideration of the system reliability and safety. This would include all electro-mechanical-software elements, as well as human actors that reside within the system context. Currently, very few techniques and tools exist to effectively and efficiently implement comprehensive Human

Reliability (HRA) within system-wide safety analyses, especially within the structure of Model-Based Systems Engineering (MBSE) and associated modeling languages such as SysML.

Currently, efforts are underway to develop standardized software tools to effectively integrate system reliability and safety analysis within MBSE. Beginning in 2016, the Object Management Group (OMG), which is an international software standards consortium, has been working to establish a common approach to modeling reliability within the system safety domain. These efforts include standardized tools for use in developing Fault Tree Analysis (FTA) as well as Failure Mode and Effects Analysis (FMEA) within MBSE. Other reliability and safety methods being explored for integration into MBSE include Hazard and Risk Analysis (HARA), Goal Structured Notation (GSN), and System Theoretic Process Analysis (STPA). The current family of analytical tools being developed are being produced by the commercial software company No Magic. As a note, No Magic has been a member of OMG for nearly two decades. As a result of these current development efforts, a new reliability modeling standard has been developed. This standard is called Risk Analysis and Assessment Modeling Language (RAAML). The RAAML provides functional libraries in the Unified Modelling Language (UML) for use in conjunction with the System Modeling Language (SysML) extension [27][28][29][30].

BACKGROUND

Classic System Safety Hazard Analysis

System safety analysis as an activity within Systems Engineering (SE) has its origins in the early 1960's, with the earliest contributor being the Department of Defense (DOD) under MIL-STD-38130 (Safety Engineering of Systems & Associated Subsystems) which was later superseded by the current MIL-STD-882 (Standard Practice – System Safety) [14][25].

Following the development of these guidelines, other agencies were quick to adopt these system safety philosophies including the Nuclear Regulatory Commission (NRC), as well as the National Aeronautics and Space Administration (NASA). These techniques have gained widespread acceptance and use across government and commercial industries. It is common to perform detailed safety analysis using one or more of the various analysis techniques that have been developed [14][25].

Numerous Hazard Analysis Techniques (HAT's) have been developed over the past several decades for use in system safety analysis. Each HAT employs a specific approach to hazard identification, analysis, documentation, as well as recommended remedial action. Each individual HAT is classified by three basic characteristics. These include:

1. Primary or Secondary Analysis
    - Primary analysis techniques are designed to be thorough and formal methodologies intended to identify as many of the latent system hazards as possible.
    - Secondary techniques act as supporting and supplemental analysis to primary techniques.

2. Inductive or Deductive

    - Inductive reasoning is an approach where fundamental observations develop into a more specific higher-level theory or conclusion. Thus, when inductive reasoning is based on reasonable initial inferences, the top-level theory has a high probability of being true. However, it is important to note that the derived conclusion, although based upon informed and reasoned information, is still arrived at via conjecture. Thus, the logical outcome is more broad, and presents a conclusion that may imply more than the initial observations support completely [14].
    - Deductive reasoning is a logical approach where a general theory develops into a confirmed conclusion. In deduction, if the initial inferences postulated are all demonstrably true, then the final assumption based on those inferences is therefore logically true and always accurate [14].

3. Qualitative or Quantitative

    - Qualitative analysis relies on information that can be difficult to objectively compare and is subjective in nature. The information is typically not numerical, and does not lend itself to direct mathematical analysis or evaluation.
    - Quantitative analysis relies on information and data that is numerical, often related to measurable quantities of interest. The information is easily ranked and compared using standard mathematical approaches and methods.

Typically, analyses that rely upon deductive reasoning as well as quantifiable data are considered more accurate and can be verified and validated easier. However, all analysis techniques, regardless of type, are asserted to be useful in identifying and minimizing hazards.

Over 100 HATs are listed in *The System Safety Analysis Handbook* published by the International System Safety Society (ISSS) [14]. However, only 10-20 different unique HATs are currently widely used by system safety experts. Many of the unused analysis techniques are deemed obsolete, redundant, less effective, or incomplete, and therefore are not commonly used. All of the currently defined HATs are associated with a type or category of the system design process. These types refer to the analysis timeframe, detail level, and coverage of the system. As defined, the seven different system safety analysis types are:

- Conceptual Design (CD)
- Preliminary Design (PD)
- Detail Design (DD)
- System Design (SD)
- Operations Design (OD)
- Health Design (HD)
- Requirements Design (RD)

Most of the system safety analysis types listed above are named for their primary application within the SE lifecycle model. For example, Conceptual Design (CD), is primarily utilized during the conceptual design phase of the engineering effort. However, it does have

secondary application later in the SE process. One instance of a HAT without a distinct application within the lifecycle model is Health Design (HD). HD refers to a safety analysis type that is specific to human health concerns within the system design, and can have applications that span multiple stages of the design process. HD considers human health hazards during system test, operation, maintenance, and disposal. It examines such potential hazards as materials, chemicals, radiological substances, biological pathogens, and ergonomic concerns.

For comparison and clarity, the "type" of analysis establishes the when and what is being analyzed, where the analysis occurs in the lifecycle of the design, as well as the desired output of the analysis. It is possible that all seven types be performed during the safety analysis of a system design to maximize hazard identification and to minimize possible mishaps. Adapted directly from an Ericson illustration, the system safety hazard analysis types align temporally with the system design lifecycle as illustrated in **Figure 1** [14].

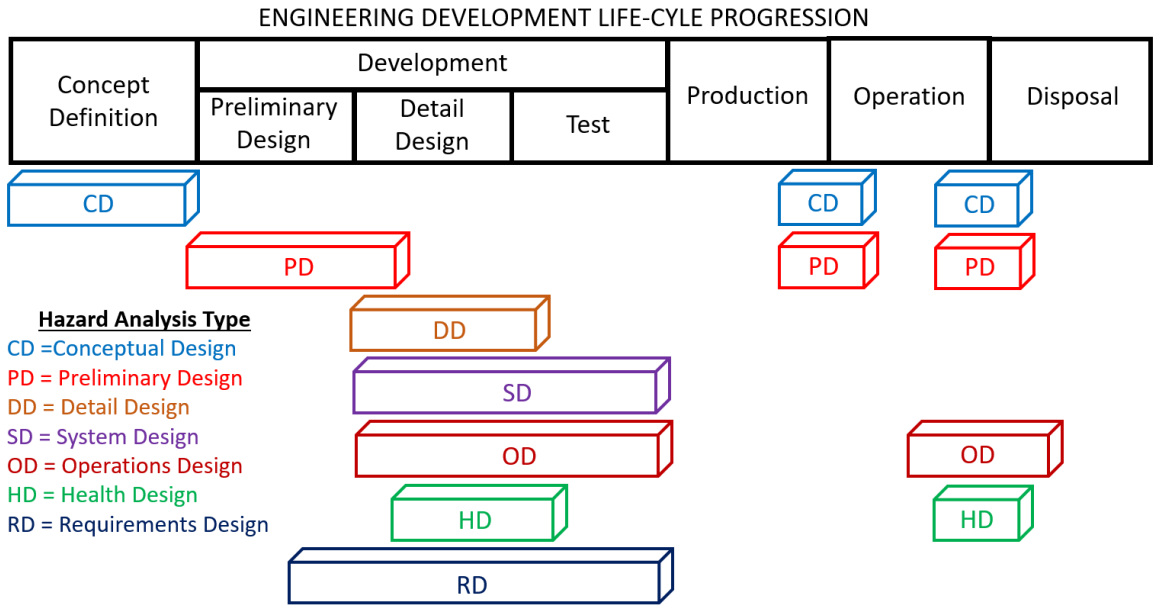


Figure 1: Hazard Analysis Type Relationship to System Lifecycle Design Process

This application of system safety analysis types would align and overlay with the classic V-Model used extensively in systems engineering as illustrated in **Figure 2**.

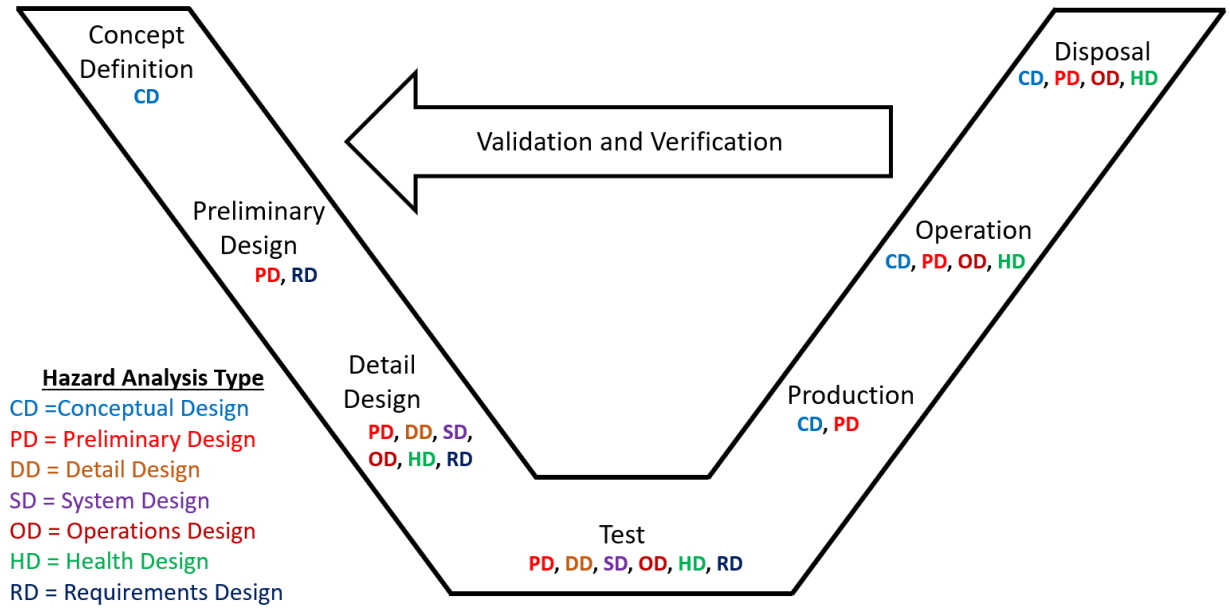


Figure 2: System Safety Type Overlay on the Lifecycle V-Model

Contrary to the analysis "type" noted above, the hazard analysis "technique" denotes how the analysis is to be performed and the specific methodology of the analysis. A list of commonly applied Hazard Analysis Techniques (HAT's) includes the following [14]:

- FHA – Functional Hazard Analysis
- PHL – Preliminary Hazard List

- PHA – Preliminary Hazard Analysis[1]
- SSHA – Subsystem Hazard Analysis
- SHA – System Hazard Analysis
- O&SHA – Operating and Support Hazard Analysis
- HHA – Health Hazard Assessment
- RHA – Requirements Hazard Analysis
- EHA – Environmental Hazard Analysis
- FTA – Fault Tree Analysis
- FMEA – Failure Mode and Effects Analysis
- FMECA – Failure Mode and Effects and Criticality Analysis
- HAZOP – Hazard and Operability Analysis
- ETA – Event Tree Analysis
- CCA – Cause-Consequence Analysis
- CCFA – Common Cause Failure Analysis
- SwHA – Software Hazard Analysis
- PHA – Process Hazard Analysis[1]
- THA – Test Hazard Analysis[2]
- FHA – Fault Hazard Analysis
- SCA – Sneak Circuit Analysis
- MA – Markov Analysis
- PNA – Petri Net Analysis
- BA – Barrier Analysis
- BPA – Bent Pin Analysis

- MORT – Management and Oversight Risk Tree
- JHA – Job Hazard Analysis
- THA – Threat Hazard Analysis[2]
- SoSHA – System of Systems Hazard Analysis

[1] *Note that the acronym of "PHA" is used for both Preliminary Hazard Analysis and Process Hazard Analysis.*

[2] *Note that the acronym of "THA" is used for both Test Hazard Analysis and Threat Hazard Analysis.*

It is important to note that some of the HAT's described in literature are actually reliability analysis tools, and not necessarily specific indicators of safety hazards. For example, a Fault Tree Analysis (FTA) will generate the probability of failure for the examined component, sub-system, or system. However, it does not establish explicitly whether that failure will result in an accident, thus precipitating human death, human injury, system damage, economic loss, data loss, or environmental harm. Therefore, the HAT output needs to be further evaluated with respect to the consequences of a predicted failure. It is important to understand that a follow-on evaluation in most HAT analyses must include assessment of accident likelihood and specifically its relationship to system safety. If a safety hazard is identified from the result of reliability analysis, this information should be used to improve the engineering design.

Human Reliability Analysis

Almost all engineered systems have some expectation of human interaction during their intended lifecycle. At one extreme, this interaction can be very limited, where human actors existing within the system context are able to influence system function, but are not expected to be active participants in system function. At the other extreme, human actors can be intended participants in system function, and are required to provide continuous input into the system operations to ensure proper function. In this case, the human actor can be considered a necessary component, critical to intended system function. As previously noted, human behavior within the system design or present within the system context, can be difficult to predict, and human responses to system cues are not as simple to model as a typical automatic control system response.

Human factors contribute to a significant fraction of the unpredictability, safety risk, and failures that occur in complicated systems. For example, human factors are currently estimated to contribute to between 50% and 70% of the risk identified in the nuclear power industry [15]. As was illustrated in the Three Mile Island accident in 1979, human error exacerbated the reactor meltdown event when operators misinterpreted instrumentation readings, and due their proximity to the unfolding event, mis-diagnosed the failure mode, and contributed to its severity by intervening in an incorrect manner [53]. Another example, to illustrate human contributions to a system failure, is the crash of Asiana Airlines Flight 214 in 2013. The flight originated in Seoul, South Korea, and crashed on landing at San Francisco International Airport (SFO). The pilots performed a series of incorrect steps involving the flight controls and made mistakes communicating standard checklist procedures to each other that resulted in the aircraft encountering the runway threshold at too low of an altitude and breaking up on impact. [24]. In

both of these cases, the human actors in the system that contributed to the accident were apparently well trained and certified to perform their job duties. In spite of their knowledge, training, and practice, errors were committed by the human actors that resulted in a very serious mishap.

The modeling of human behavioral characteristics for the purpose of improving system safety has been studied for the past several decades. The first serious efforts to establish human factors risk models began in the late 1970's and early 1980's. The field of Human Reliability Analysis (HRA) is conducted with two primary goals: first, derive a description of human interaction with an electro-mechanical system and the risks associated, and second, identify and define strategies to lower the risk associated with human actors [15]. Of current interest in the field of safety is the use of HRA within Probabilistic Risk Assessment (PRA) to better model human factors and how they relate to the likelihood of accidents in systems operation. There are approximately 38 different HRA methodologies documented in the public domain. Among these HRA methodologies summarized in this particular text are the following approaches [15][47]:

- Confusion Matrix
- Expert Estimation
- Micro-MAPPS (Micro Maintenance Personnel Performance Simulation)
- SLIM-MAUD (Success Likelihood Index Method-Multiattribute Utility Decomposition)
- THERP – Technique for Human Error Prediction
- SRM – Sandia Recovery Model
- ORCA – Operator Reliability Calculation and Assessment

- ADM – Aeronautical Decision-Making

Of the HRA methods listed, the THERP method is the most commonly used and referenced in HRA activities [15]. As such, the Human Factors Hazard Model (HFHM) being proposed in this research effort is established using THERP as a primary comparative baseline. Additionally, other commonly used methods will be referenced to and used as a guide for HFHM development. Specifically, the Expert Estimation approach will be utilized in establishing a standard scale of probabilities used in the automated HFHM user interface. Note that definitions of specific system safety and HRA terminology are presented in **APPENDIX A**. The THERP method as detailed in NUREG/CR 1278 is composed of five fundamental steps [16]. These include:

- Define the system failure of interest. These specifically relate to man-system interface points that can be influenced by human factors.
- List and analyze the related human operations within the system functions.
- Estimate the relevant error probabilities associated with the human factors.
- Estimate the effects of human errors on the system failure events. This typically involves the integration of the HRA with a system reliability analysis.
- Recommend revisions to the system design and reevaluate system failure probabilities.

Although developed primarily to evaluate HRA as it relates to the operations and maintenance of nuclear power plants, the basic THERP method has been adapted and used to

model human factors effects and reliability in other engineered systems. The Human Factors Hazard Model (HFHM) proposed as part of this research effort establishes a simplified and more universal hazard model that has broad application throughout Systems Engineering (SE). The proposed HFHM and THERP approaches to hazard modeling share similar approaches, including:

- Both models utilize a behavior paradigm that considers a human response to a hazard as to how it is perceived, processed cognitively, what corrective action (if any) is attempted, and feedback based on system reaction to human input.
- Both models integrate a probabilistic analysis of human interaction, and attempt to assign a reliability or probability of failure based on the human responses documented.
- The probabilistic model of human response is based on Human Error Probability (HEP) evaluated for specific operational scenarios using Performance Shaping Factors (PSFs) determined by various human factors considerations and analysis.

Although the proposed HFHM and established THERP approaches share similarities, the HFHM and THERP do have several differences. The HFHM seeks to build upon the strengths of THERP, and simultaneously address some of the limitations of the original methodology. Some of the identified limitations of THERP include:

- The THERP method can be complex, time consuming, and costly to apply.
- The THERP method was developed within the nuclear energy industry, with an emphasis

on control room environments. It approaches HRA and system safety from that standpoint. Thus, there is limited content and flexibility in the HEP and PSF data presented.

- The THERP method is not simple and generalized enough to allow for direct and efficient sensitivity analysis to identify the most likely safety hazards related to human factors.
- HEP and PSF data presented in THERP does not account for some contemporary instrumentation and control systems currently used in the modern computerized system environments.
- The THERP method does not account for possible malevolent behavior. It only assumes well intentioned actors within the system.

Human Factors and Hazard Analysis within Model-Based Systems Engineering

Human Reliability Analysis (HRA) within the Model-Based Systems Engineering (MBSE) paradigm is an emerging field of study. Some scholarly works have been published describing efforts to establish Probabilistic Risk Analysis (PRA) tools within UML for use in MBSE, particularly in conjunction with industry standard system modeling tools such as SysML. The Object Management Group, Inc. (OMG), has developed, and is in the process of beta testing a library of MBSE tools under the title Risk Analysis and Assessment Modeling Language (RAAML) [27][28][29]. RAAML includes development tools for various Hazard Analysis Techniques (HATs), including Fault Tree Analysis (FTA). The FTA capabilities within RAAML have application in HRA associated with the Human Factors Hazard Model (HFHM) proposed in this work. Currently, a universal and systematic approach to implementing HRA

within SysML has not been established. Using the tools provided in the planned RAAML extension and new profiles developed to establish Event Tree Analysis (ETA) in SysML, the probabilistic analysis tools present in the HFHM are stereotyped, and can be modeled efficiently.

RESEARCH QUESTIONS

Based on the current state-of-the-art in the field of human factors within system safety, and its relationship to the principles of Systems Engineering (SE) and Model Based Systems Engineering (MBSE), we can generate the following research questions. These research questions will address the areas in which the approaches and techniques of human hazard analysis within system safety can be improved upon and new techniques and tools be proposed. Additionally, a theoretical framework by which these new approaches can be implemented within MBSE will also be proposed.

Research Question 1 (RQ1): Can a new model used to evaluate human reliability, specifically with regards to its application in system safety, hazard analysis, and accident avoidance be developed to address limitations in current approaches? What characteristics of this new Human Factors Hazard Model (HFHM) can be validated against current models, and how can gaps in those analysis approaches be identified? What characteristics will determine if this new HFHM meet the needs of modern human factors design within SE approaches?

> Task 1 (RQ1-T1): Analyze existing human factors models as well as human performance characteristics relevant to system safety analysis from existing research literature, and determine what the limitations to current analysis approaches are, and what improvements can be made to create a model with more broad application and usage in the SE discipline.

Task 2 (RQ1-T2): In response to the requirements and needs identified in Task 1 (RQ1-T1), develop a new analytical model to predict the likelihood of an accident due to a Human Factors Triggering Event (HFTE).

Task 3 (RQ1-T3): Perform analytical simulations and/or analytical evaluations to compare and validate HFHM outputs as compared to existing Human Reliability Analysis (HRA) and Human Error Probability (HEP) models.

Task 4 (RQ1-T4): Develop the new hazard model such that it is as practical and simple to use as possible. The hazard model will have near universal application within system safety analysis, and will not be designed for a specific industry or system type. The model is to be automated utilizing a commonly available computational software tool so that it can be used quickly, efficiently, and be compared directly to other Human Reliability Analysis to validate its utility.

Research Question 2 (RQ2): In what ways does the proposed HFHM result in improvements to established system safety Hazard Analysis Techniques (HAT's)? Does use of the HFHM in conjunction with established HAT's result in a change to system safety analysis outcomes? How much does use of the HFHM enhance or improve the value of the conventional technique as it relates to the SE process?

Task 1 (RQ2-T1): For a relevant application, develop a combined HFHM/HAT analysis and corresponding default HAT analysis for a direct comparison. This comparison will utilize a traditional HAT as illustrated in **Table 27**, with the specific method being dictated by relevance and ease of use.

Task 2 (RQ2-T2): Based on the outcome of HFHM integration within a conventional HAT as noted in Task 1 (RQ2-T1), determine the specific results and how the analysis outcomes compare.

Research Question 3 (RQ3): Can the implementation of the HFHM within the System Modeling Language (SysML) enable the benefits asserted by MBSE integration, namely improved reusability, communication, consistency, and execution?

Task 1 (RQ3-T1): Identify reliability and safety reference models available for common MBSE applications, and develop a protocol for inclusion of the HFHM outputs into the system modeling environment.

Task 2 (RQ3-T2): Develop an approach and architecture to establish human actors, other system components, their respective attributes, and parameters to integrate the HFHM into MBSE methods.

Task 3 (RQ3-T3): Synthesize a standardized approach for requirements documentation and associated parameterization related to reliability and safety metrics within the MBSE requirements domain.

Task 4 (RQ3-T4): Evaluate a standardized stereotype approach such that the HFHM methodologies can be easily and quickly adapted to example MBSE processes.

NOVEL ASPECTS OF RESEARCH

By answering these research questions, we hope to demonstrate and justify the value of this new hazard modeling approach, and show the value it brings to not only traditional safety analysis techniques, but within MBSE and System Modeling Language (SysML) libraries and stereotypes. The proposed Human Factors Hazard Model (HFHM) developed in support of this research effort provides the following improvements and advantages over the Technique for Human Error Rate Prediction (THERP) approach:

- The HFHM is simplified and generalized for broad application in HRA activities related to system design.
- The HFHM analysis can be quickly performed, with minimal training in system safety analysis or hazard modeling.
- The HFHM can quickly and efficiently perform sensitivity studies, and identify areas within the system design for improvement and optimization with regards to system safety.
- The HFHM utilizes Human Error Probability (HEP) and Performance Shaping Factor (PSF) data drawn from multiple sources and industries for a more comprehensive library of probabilistic data for accuracy, and minimal reliance on expert judgement or estimating risk to establish reliability baselines.
- The HFHM is a "tunable" model that can operate using baseline values or accept user specified HEP and PSF values for customization of the probabilistic model to suit more specialized and detailed analysis.

- The HFHM is automated within a commercial software tool for improved speed, accuracy, and utility.
- The HFHM has direct application within Model Based Systems Engineering (MBSE), and can be adapted into SysML and related modeling languages.

DEVELOPMENT OF A HUMAN FACTORS HAZARD MODEL

Referencing Research Question 1 (RQ1), a new Human Reliability Analysis (HRA) method, namely the Human Factors Hazard Model (HFHM), has been developed to provide an efficient and standardized approach to hazard analysis with respect to human actors within a system design or system context. In support of Task 1 and 2 (T1 and T2), existing HRA literature was utilized to establish baseline Human Error Probability (HEP) values used in the new hazard model.

The HFHM is a systematic analysis approach to determining the human actor probability of correctly reacting to an associated Human Factors Trigger Event (HFTE). The architecture of the HFHM is comprised of three basic elements. These include:

- Performance Shaping Factors (PSFs)
- Fault Tree Analysis (FTA) of each pivotal event
- Event Tree Analysis (ETA) of entire hazard pivotal event sequence

In the general functionality of the HFHM, the PSFs are used to establish the Human Error Probability (HEP) values associated with various human and system characteristics unique to the system design and nature of the hazard event. To establish HEP values, three sources of probability are utilized. The first source of PSF information available in the HFHM are baseline values of HEP from published literature. Most of this data is derived from values published in the Technique for Human Error Rate Prediction (THERP) and the Engineering Data Compendium – Human Perception and Performance [16][1]. Other secondary sources of

information from industry and governmental agencies are also cited for relevant PSF data. The second key source of HEP values for use in the HFHM is specified through Expert Estimation. In the literature, five different types of Expert Estimation are currently cited [15]. These include:

- Paired Comparison
- Ranking and Rating
- Direct Numerical Estimation
- Indirect Numerical Estimation
- Multi-attribute Utility

For the Expert Estimation methods listed, several limitations are identified. Paired comparison and ranking / rating approaches produce equivocal results. Indirect numerical estimation will establish a HEP by relative comparison based on the probabilities of failure determined for other events. The direct numerical estimation technique produces a specific HEP based on an expert or group of expert's estimations of the likelihood of a specific error due to the relevant human factors as well as system characteristics. The HFHM uses a simplified version of direct numerical approach to specify HEP and associated error factors from a pre-defined standardized scale of HEP and error factors. The standardized scale utilized in the HFHM is presented in **Table 1** [37].

Table 1: Expert Estimation Standard HEP and Error Factors for the HFHM

EXPERT ESTIMATION DESCRIPTION		HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
PROBABILITY OF FAILURE	PROBABILITY OF SUCCESS		
Certain	Impossible	1.000	1.000
Extremely Likely	Extremely Unlikely	0.999	1.001
Very Likely	Very Unlikely	0.990	1.010
Likely	Unlikely	0.900	1.100
Moderately Likely	Moderately Unlikely	0.700	1.300
Marginal	Marginal	0.500	1.500
Moderately Unlikely	Moderately Likely	0.300	2.000
Unlikely	Likely	0.100	3.000
Very Unlikely	Very Likely	0.010	5.000
Extremely Unlikely	Extremely Likely	0.001	10.000
Impossible	Certain	0.000	N/A

The third source of HEP values for use in the HFHM are custom, user defined values, that are specified by the analyst. These HEP values and their associated error factors would be based on specific empirically derived HEP data, a more detailed Expert Estimation using any of the techniques listed above, or simply a value determined to be appropriate by the analyst.

Performance Shaping Factors

The likelihood that a human actor will fail to perform or incorrectly perform a required task, possibly resulting in an accident / mishap, is referred to as Human Error Probability (HEP). The development of an analytical model used to predict HEP is primarily dependent on consideration of human factors and system characteristics. These two elements are referred to as Performance Shaping Factors (PSFs). PSFs are used to calculate HEP relevant to specific operational scenarios. For example, the complexity of a system design, the human actor's knowledge of system operation, the actor's distraction and stress levels, and the nature of the current behavior of the system, will all contribute to the probability that the actor will react

correctly to the system signals, and successfully avoid a mishap [16][17]. Typically, the characteristics of PSFs are drawn from established and widely cited Human Reliability Analysis (HRA) and human factors engineering sources. A non-comprehensive list of elements that represent human factors and system factors in PSFs are presented in **Table 2** [15][19][20].

Table 2: Examples of Human and System Factors Used to Determine PSF's

HUMAN FACTORS	SYSTEM FACTORS
Training	System Complexity
Practice	Hazard Event Timing
Experience	Hazard Event Duration
Mental Acuity	Observability of System Behavior
Intellectual Capacity	Annunciation of System Behavior / Alarms
Gross and Fine Motor Skills	Instrumentation Availability to Monitor System Behavior
Sensory Acuity (Smell, Vision, Hearing, Touch)	Input Control Capabilities
Fatigue, Vigilance, and Impairment Level	Input Control Accessibility to Actor
Stress and Emotional Stability	System Behavior Feedback Characteristics
Reaction Time	Environmental Conditions (Temperature, Illumination, etc.)
Location and Orientation of Actor withing System Context	System Fail-Safes
Negligence ande Malevolent Intent	System Safeguards

Performance Shaping Factor Modifiers

The Performance Shaping Factors (PSFs) contributing to the HEP determination can be used in their baseline state, or can be modified depending on other contributing characteristics. For example, the baseline probability of failure (HEP) due to an actor's intellectual capacity can be modified by their stress level, fatigue level, impairment characteristics, and other relevant PSF values. To modify a baseline HEP value, multiplying factors are applied to adjust the probability of failure based on characteristics specific to the human actor and system design in question. This calculation is of the form:

$$P_f' = \left(P_f\right) \prod_{n=1}^{i} M_n \quad (1)$$

Where:

P_f' = Modified Event Probability of Failure
P_f = Initial Event Probability of Failure
M_n = Probability Modifier n
i = Total Number of Probability Modifiers Applied

All of the event probabilities determined in the HFHM using various PSFs will follow similar contributing factor adjustments, conditional logic, and combined probability calculations to accurately represent the likelihood of a failure for that particular event.

In the unique case of hazard event timing (event chronology), the baseline human reaction time is adjusted using a multiplier similar to the probability adjustments noted above. However, multipliers are not compounded, but applied individually, then summed to adjust the baseline human actor reaction time. If multipliers are used to modify the baseline reaction time, the calculation is of the form:

$$T_r' = T_r + \sum_{n=1}^{i} T_r(R_n - 1) \quad (2)$$

Where:

T_r' = *Modified Reaction Time*
T_r = *Baseline Reaction Time*
R_n = *Reaction Time Modifier n*
i = *Total Number of Reaction Time Modifiers Applied*

Human Factors Modeling

The Human Factors Hazard Model (HFHM) utilizes published data from a number of sources to establish the Performance Shaping Factors (PSFs) required to develop a suitable Human Error Probability (HEP) model for use in determining the basic event probabilities. The Technique for Human Error Rate Prediction (THERP) was used as a primary source to establish relevant baseline HEP values as well as modifying multipliers [16]. Another significant source of human behavioral characteristic information is derived from the Engineering Data Compendium – Human Perception and Performance (EDC), produced and published by the U.S. Air Force [1]. Tertiary sources of human factors data were derived from several other published documents as referenced. These sources of PSF and HEP data were primarily governmental agencies, academic institutions, or non-profit corporations involved in safety, risk analysis, and human factors engineering research [2][3][4][5].

Age Considerations

As a human being ages, a decrease in memory recall and cognitive processing, as well as an increase in overall reaction time is observed. Due to this trend in human performance, an older actor within a system design will have a higher probability of failure related to correctly

interpreting and reacting to a Human Factors Triggering Event (HFTE). As derived from published sources, the probability multiplier for actor mental acuity is presented in **Figure 3** [2]. The curve is a third-order (cubic) polynomial that is generated using a regression curve fit of discreet data points calculated using the published source material and a calibrated Human Factors Hazard Model (HFHM). Per the noted curve fit, for ages less than 27 years old, a multiplier of 1.0 is assigned.

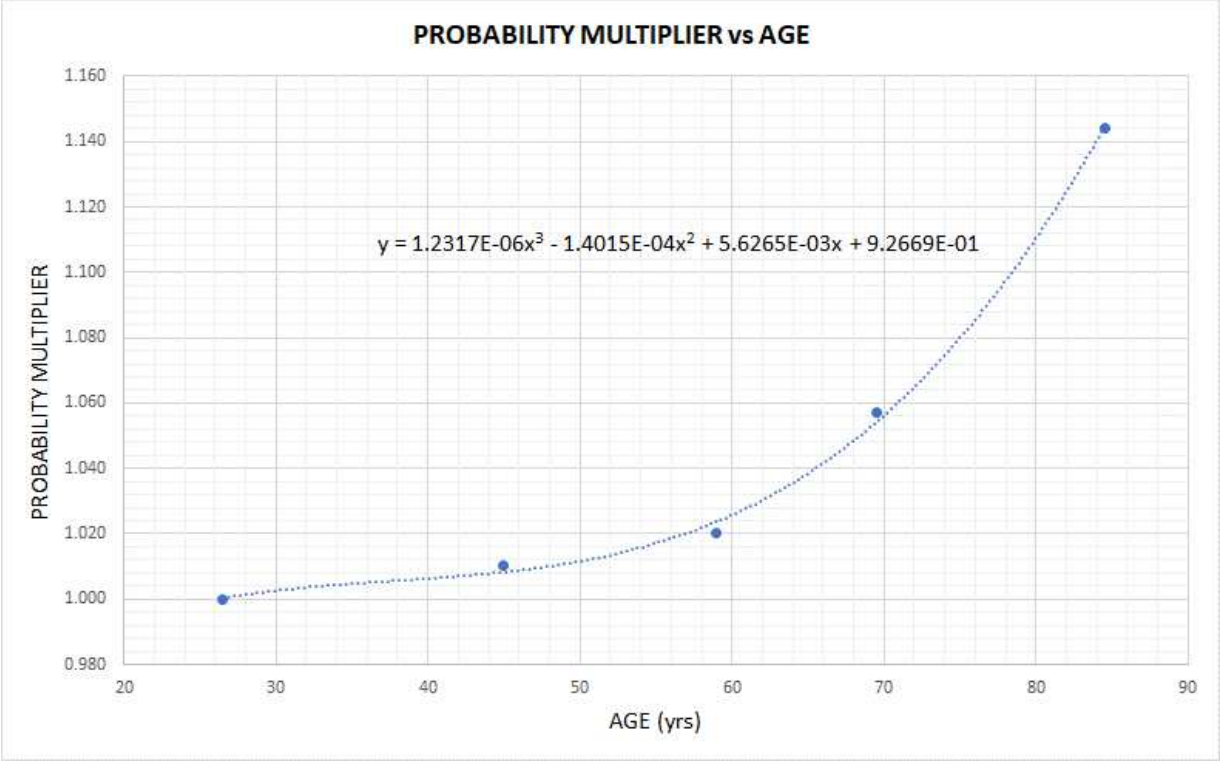


Figure 3: Probability Multiplier versus Actor Age

The adjustment of baseline reaction time as a function of human actor age was generated using a fit of published data. A linear regression is used to establish a function from the

published data. The reaction time multiplier as a function of actor age is presented in **Figure 4** [2]. Per the noted curve fit, for ages less than 27 years old, a multiplier of 1.0 is assigned.

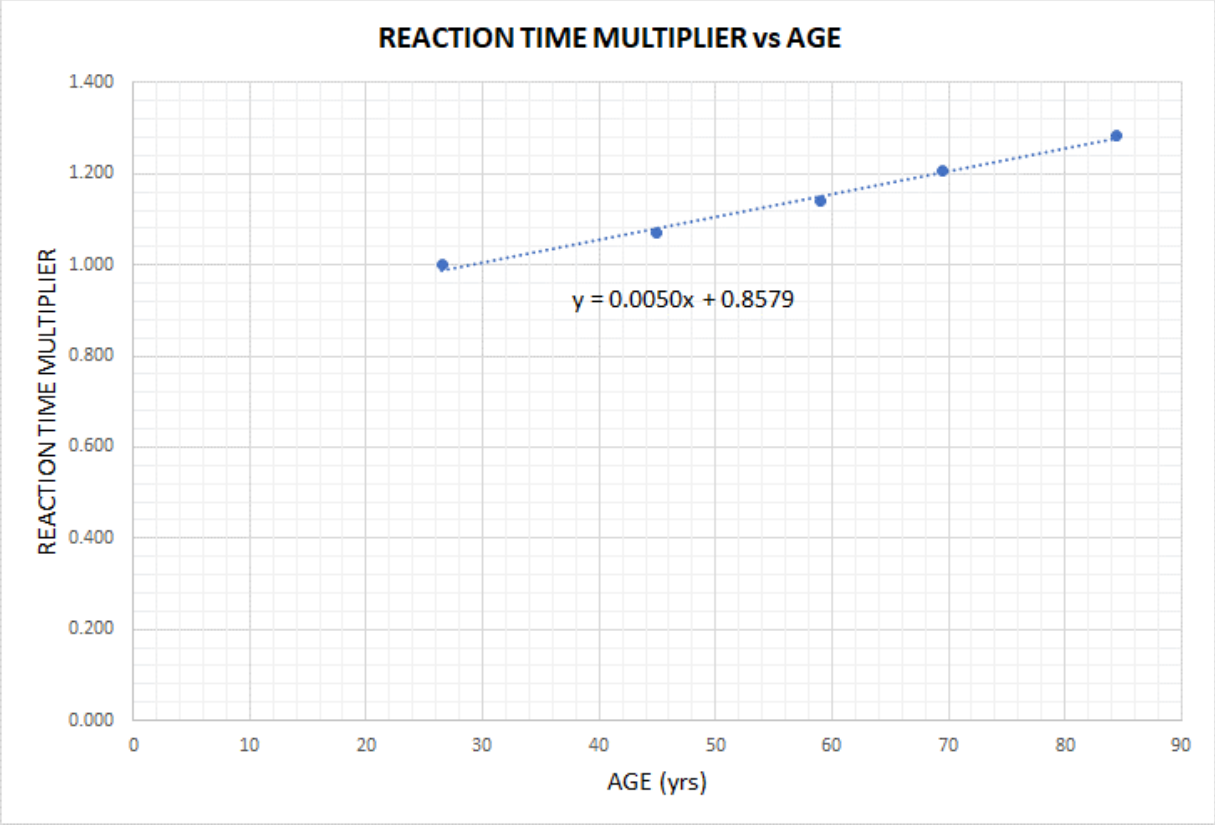


Figure 4: Reaction Time Multiplier versus Actor Age

Environmental and Extremity Temperature Considerations

The ambient temperature of the operational environment, and particularly the time that the actor is active within that environment, affects the human actor's mental acuity and reaction time. The probability multiplier for mental acuity related to environmental temperature and the time an actor spends in that environment is presented in **Figure 5**. The mental acuity curves are developed using a linear regression fit of data derived from the published data [1].

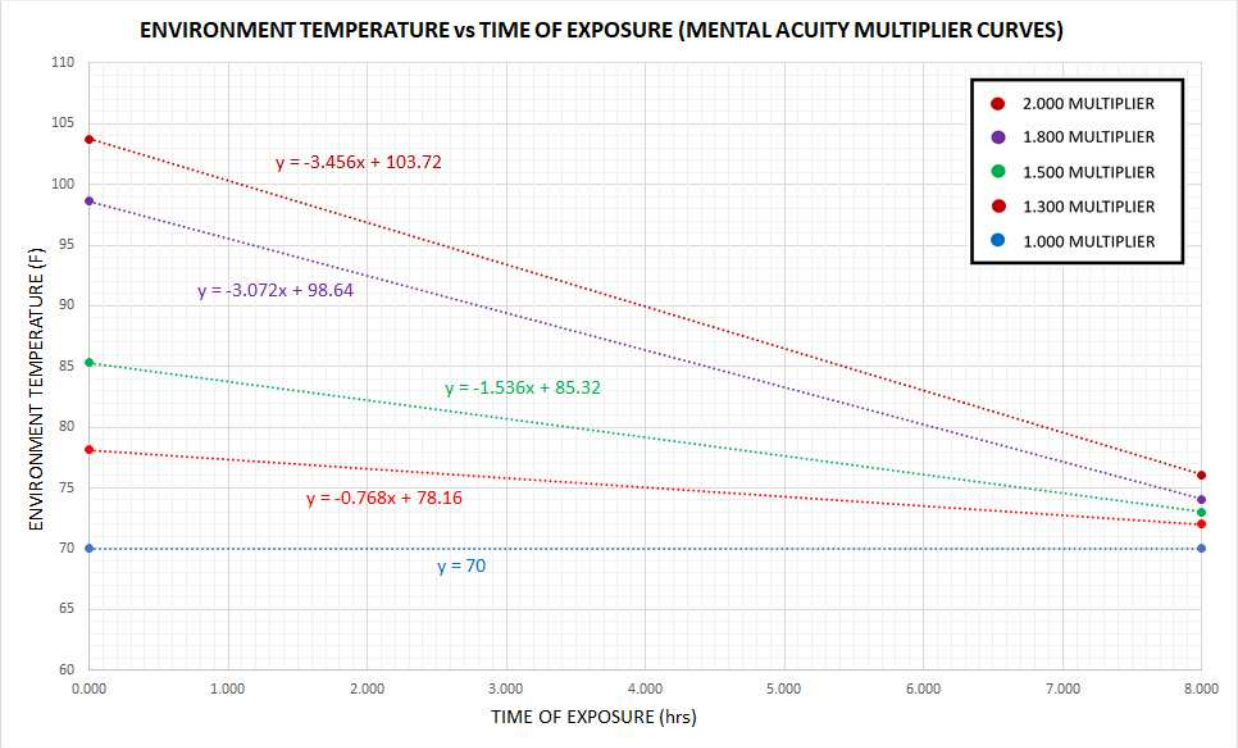


Figure 5: Environmental Temperature Exposure Mental Acuity Probability Multipliers

The reaction time multiplier for human actor time of exposure at a specific environmental temperature is presented in **Figure 6**. Each function associated with a respective reaction time multiplier curve is represented by a power function generated using a regression fit of the published data [1].

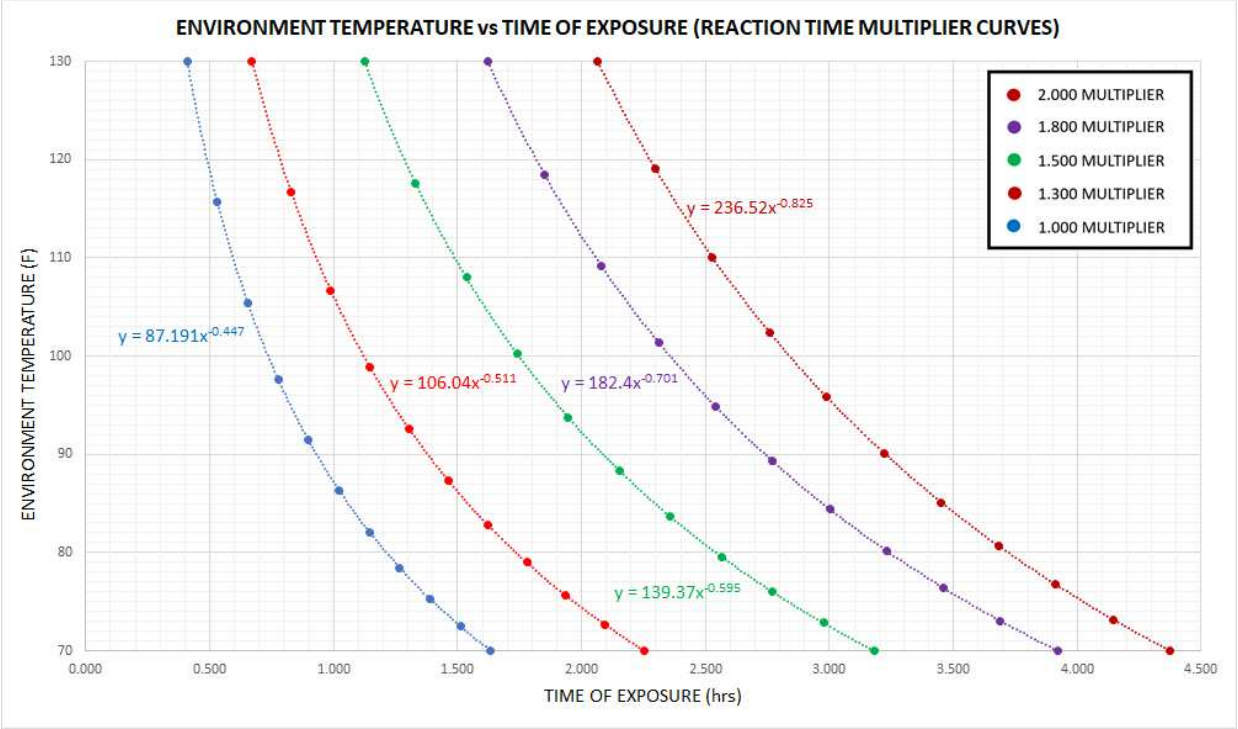


Figure 6: Environmental Temperature Exposure Reaction Time Multipliers

In conjunction with environmental temperature, and it effects on mental acuity and reaction time, the skin temperature of the extremities of the human actor can affect fine motor skills in extremities, specifically the hands and fingers. For example, if the hands and fingers of an actor manipulating instruments and controls are at a low temperature, and the person is called upon to make fine adjustments or manipulations, loss of fine motor control is likely to be exhibited. This is a source of potential error as it relates to providing correct control inputs to system operations. Extremity skin temperature with associated probability multipliers was developed from published human factors engineering data. The temperature classifications and associated multipliers is presented in **Table 3** [1].

Table 3: Extremity Temperature Probability Multipliers

REDUCED EXTREMITY SKIN TEMPERATURE	PROBABILITY MULTIPLIER
NORMAL	1.000
SIGNIFICANT	1.300
EXTENSIVE	1.500
SEVERE	2.000

Vigilance Considerations

The level of vigilance associated with the human actor will affect the reaction time to a hazard event stimulus. For example, if the actor is cognizant a certain hazard event is likely to occur, and has mentally prepared themselves to act when the hazard presents itself, the reaction time required will be considered optimal. If the actor is not prepared, or enough time has passed without a hazard event presenting itself, the level of initial vigilance will decrease as a function of time. Without observable system behavior revealing evidence of an impending hazard event, over time, the perceived level of threat will decrease, even in an individual that began their system interaction with a reasonably high level of vigilance. The curve indicating the vigilance probability multiplier as a function of time is presented in **Figure 7** [16].

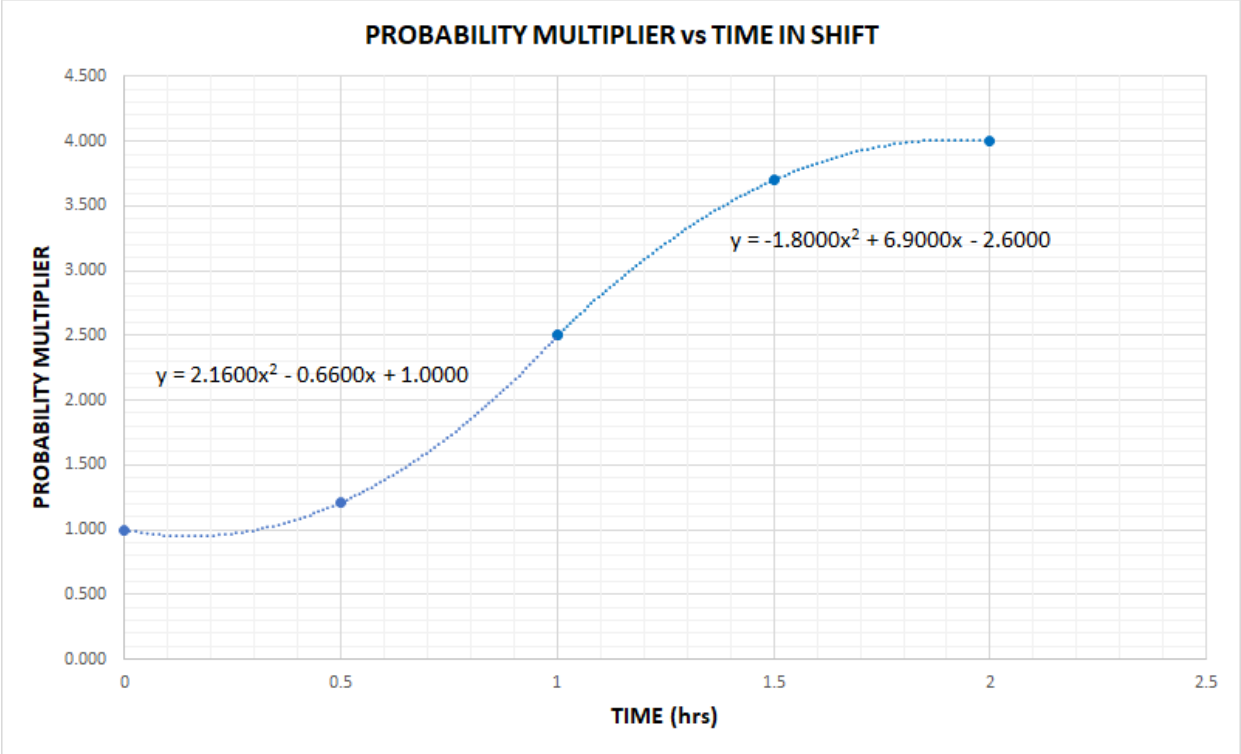


Figure 7: Vigilance Probability Multiplier versus Time in Shift

Note that the vigilance curve is a combination of two different second order (quadratic) polynomials that are based on vigilance relationships described in the Technique for Human Error Rate Prediction (THERP) [16].

Distraction Considerations

Closely related to human actor vigilance with respect to system behavior, and particularly to hazard event recognition, are distraction factors. Distractions are cognitive diversions due to external influences, that direct attention away from required monitoring and assessing of system operational behavior. Distractions will affect a human actor's ability to center their thought process to the task at hand, and will lengthen reaction time when responding to a threat [3][4][5].

Distractions can be, but are not limited to, any of the following activities while attempting to simultaneously focus on a required system operation task:

- Text messaging or other mobile device activities.
- Composing e-mails.
- Internet browsing.
- Listening to music.
- Playing videogames.
- Conversations with other people.
- Watching television or movies.
- Reading a book, magazine, newspaper, or other media.
- Personal grooming.
- Eating or drinking.
- Dialing or speaking on a telephone.
- Cleaning or organizing a work area.
- Performing repairs or maintenance activities on equipment in work area.

By referencing published values for distraction types as well as Human Error Probability (HEP) values related to accident rates, a schedule of distraction level with associated probability and reaction time multipliers is developed [3][5][4]. The distraction levels and associated probability and reaction time multipliers are presented in **Table 4** and **Table 5**.

Table 4: Distraction Level and Probability Multiplier

DISTRACTION LEVEL	PROBABILITY MULTIPLIER
Very High	136.732
High	43.857
Moderate	20.402
Low	1.164
None	1.000

Table 5: Distraction Level and Reaction Time Multiplier

DISTRACTION LEVEL	REACTION TIME MULTIPLIER
Very High	18.000
High	13.750
Moderate	9.500
Low	5.250
None	1.000

Stress Considerations

Mental acuity and how it relates to a human actor's ability to respond to a hazard event is dependent on the level of stress the human actor is experiencing. A stressor is defined as any external or internal influence that causes bodily or mental tension. The typical human response to that tension is manifest as the stress that is experienced [16]. Stress is typically classified as either psychological or physiological, and either or both can contribute to the ability of a human actor to correctly respond to a hazard stimulus. A non-comprehensive list of psychological factors that can become stressors include [16]:

- Sudden onset of hazard event (surprise or startled reaction of actor)
- Required task speed
- Required task load

- High level of jeopardy from risk (high level of negative consequence of failure)
- Tedium from non-engaging work
- Conflicting or inconsistent system cues
- Lack of job motivation
- Low job satisfaction

A non-comprehensive list of physiological factors that can become stressors include [16]:

- Pain or discomfort
- Illness
- Hunger or thirst
- High G-forces / Accelerations
- Restriction of movement / Confinement
- Oxygen deficiency
- Radiation exposure

As specified in the literature, the categories of stress used for Human Error Probability (HEP) evaluation is classified into the following categories [16]:

- Very low stress resulting from insufficient arousal.
- Optimum stress (step by step). The step-by-step tasks to resolve the hazard event are anticipated to be routine and procedurally guided. The hazard event is

considered to be an expected event with a well-defined corrective action prescribed.

- Optimum stress (dynamic). The hazard event requires decision making, keeping track of multiple functions, and controlling multiple functions. The hazard event is considered to be typically abnormal without a well-defined corrective action prescribed.
- Moderately high stress that is slightly disruptive to normal human response to the hazard event.
- Extremely high stress that is very disruptive. This is considered to be perceived as a threat to the human actor, and panic is likely.

It is important to note from the categories above that the lowest level of stress experienced by the actor does not correspond to the minimum Performance Shaping Factor (PSF) multiplying factor for Human Error Probability (HEP) adjustment. As noted in the literature, the optimal level of stress corresponds to the maximum effectiveness of a human response to a hazard event. If the stress is too low or too high, then an increase in HEP can be expected. A hypothetical representation of this stress / performance relationship curve is presented in the Technique for Human Error Rate Prediction (THERP) [16]. This visualization is presented in **Figure 8**.

Figure 8: Hypothetical Performance Effectiveness versus Stress Level

The Human Factors Hazard Model (HFHM) utilizes the stress classifications as noted in the literature [16]. As noted above, each anticipated level of stress, as experienced by the human actor, has an associated probability and reaction time modifier assigned. These values are based on the values noted in THERP and adjusted using a calibrated HFHM. Specified stress levels with the corresponding HEP and reaction time modifiers is presented in **Table 6**.

Table 6: Stress Related Probability and Reaction Time Multipliers

	MENTAL ACUITY MODIFIERS			REACTION TIME MODIFIERS		
STRESS LEVEL	SKILLED	NOVICE	NO EXPERIENCE	SKILLED	NOVICE	NO EXPERIENCE
Very Low	6.005	6.005	6.005	2.000	2.000	2.000
Optimum (Step by Step)	1.000	1.000	1.000	1.000	1.000	1.000
Optimum (Dynamic)	1.000	6.005	16.248	1.000	2.000	4.000
Moderately High	6.005	16.248	34.405	2.000	4.000	8.000
Extremely High (Panic)	21.491	35.672	37.720	5.000	10.000	20.000

As noted in **Table 6**, the experience and skill level associated with the human actor can affect the stress level modifiers. Typically, the higher the skill level and training, the lower the resulting effects of stress on overall HEP multipliers and reaction time.

Impairment Considerations

The mental acuity of the actor will be negatively affected by the level of impairment due to an intake of alcohol, drugs, or other substances. Typically, as the concentration of an impairing substance increases in the bloodstream of a human actor, the more likely it becomes that mental function and baseline reaction time will be affected. The negative effects related to impairment include, but are not limited to [42][43][44]:

- Loss of judgement
- Lower alertness level
- Lower muscle coordination
- Loss of balance
- Longer reaction time to stimuli
- Short term memory loss

- Altered mood and exaggerated emotions
- Confusion
- Reduced information processing capability (signal detection, visual searching, visual signal processing)

There are numerous intoxicating substances, both legal and illegal, available for human consumption. These include such substances as alcoholic beverages, prescribed pharmaceuticals, sanctioned and illicit drugs, as well as a number of over-the-counter medications that may have impairing side effects. All of the various substances or combinations of substances would be impractical to catalog or account for in the Human Factors Hazard Model (HFHM). To simplify the HFHM with regards to Performance Shaping Factors (PSFs), human impairment characteristics are communicated to the model as an equivalent blood alcohol percentage (%BAC) only. If any intoxicating substance is assumed to be present in the human actor, the level of impairment must be bookkept in the model with the analyst specifying an equivalent effect, as if it was due exclusively to alcohol blood content. Curves representing impairment related probability and reaction time multipliers are presented in **Figure 9** and **Figure 10.**

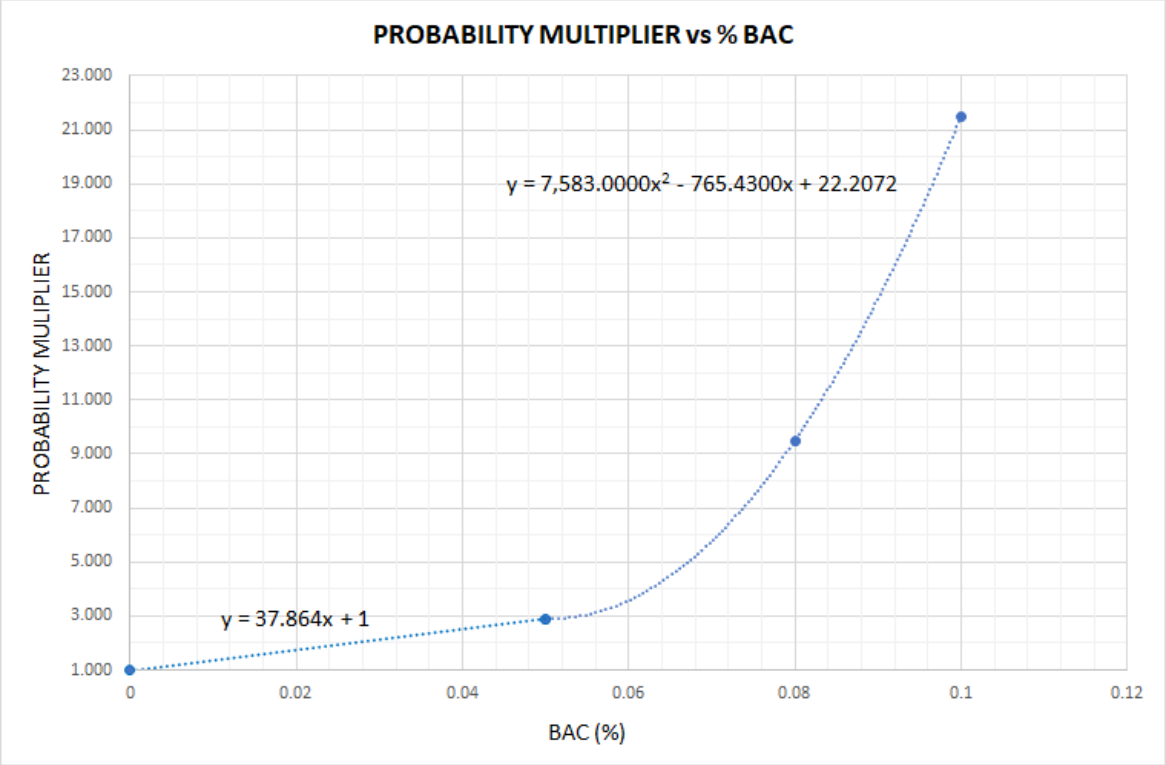


Figure 9: Impairment Probability Multiplier versus Equivalent Blood Alcohol Content Percentage (%BAC)

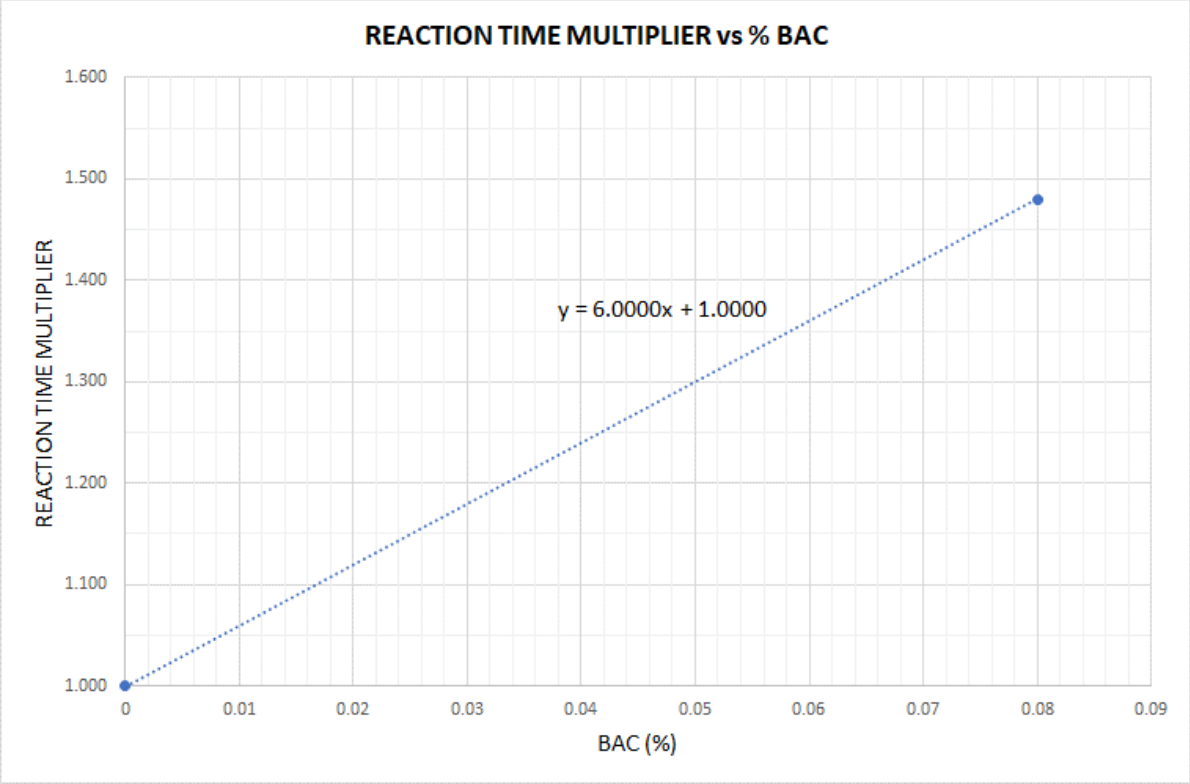


Figure 10: Impairment Reaction Time Multiplier versus Equivalent Blood Alcohol Content Percentage (%BAC)

As noted in **Figure 9** and **Figure 10**, regression curves are used to fit the data associated with probability and reaction time multipliers [42][43][44]. The probability multiplier illustrated in **Figure 9** is actually represented by two individual trendlines. The first is a linear relationship, followed by a second order (quadratic) polynomial. For the reaction time multiplier, a single linear curve fit is applied.

Fatigue Considerations

As a human actor becomes more fatigued due to a lack of adequate rest, the general trend is for the time required to react to a given stimulus to increase. Based on experimental data as well as accident rates reported in the literature due to drowsy driving a multiplier curve for baseline reaction time adjustment is developed [1][45][46]. The curve utilized by the Human Factors Hazard Model (HFHM) to compensate for actor fatigue is presented in **Figure 11**.

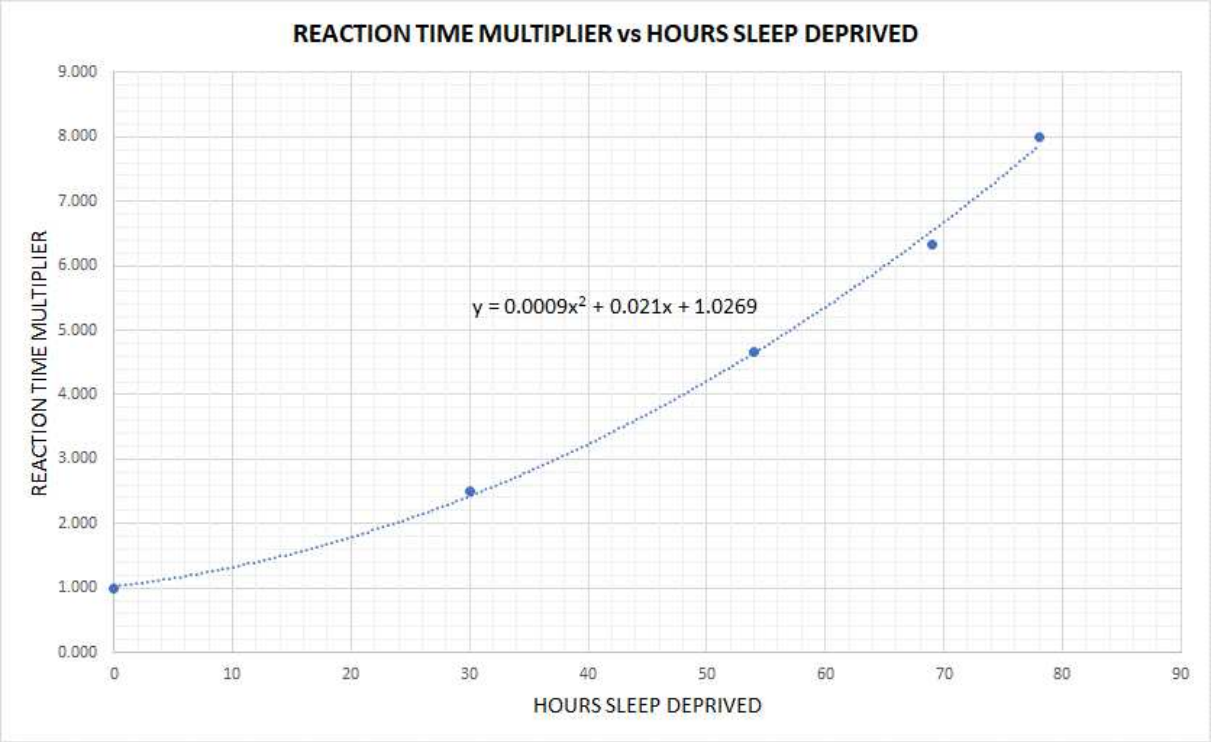


Figure 11: Fatigue Reaction Time Multiplier versus Hours Sleep Deprived for Actor

As noted in **Figure 11**, the fatigue data is modeled using a regression curve fit. A second order polynomial (quadratic) is used to establish the reaction time multiplier as a function of continuous hours spent without adequate rest.

Hearing Acuity Considerations

Hearing acuity and how it relates to a human actor's ability to respond to a hazard event is dependent on the sound characteristics of the system hazard event. System behavior and instrumentation that creates an audible signal as a reaction to hazardous behavior, must be perceptible to the human actor. Additionally, the audible signal must have characteristics that the human actor can interpret and correctly use in the diagnosis of the hazard event. If not detected and interpreted correctly, any audible signal generated will fail to contribute to the human response the Human Factors Triggering Event (HFTE).

The extents of the human hearing range are based upon two characteristics related to the sound properties: first, the intensity (loudness) of the sound, typically measured in decibels (dB), and second, the frequency of the sound, typically measured in hertz (Hz). Both of these characteristics will factor into whether the sound can be detected and interpreted correctly by a human being. Sound intensities greater than 0 dB can be detected by human beings with normal hearing. Sound intensities greater than approximately 100 dB for sustained amounts of time can damage hearing and will grow increasingly uncomfortable to the human actor as they increase. A sound intensity of 200 dB is equivalent to the shock wave of an explosion and can be fatal to a human being [38]. The frequency range with respect to human hearing thresholds are 20 to 20,000 Hz. However, hearing is typically most sensitive in the 2,000 to 5,000 Hz frequency range [39]. Depending on the human's gender and age, hearing acuity can be variable. Hearing typically deteriorates as a person's age increases, with the largest declines observed in subjects beginning at ages 45 to 54 years old. It has also been observed that males typically have a higher

incidence of hearing loss than females [1]. The minimum hearing thresholds, in decibels (dB), for male and female actors of various age ranges are presented in **Table 7** and **Table 8**.

Table 7: Minimum Hearing Thresholds (in dB) for Sound Frequencies (in Hz) and Age Ranges of a Male Subject

	AGE	AGE	AGE	AGE	AGE	AGE	AGE
FREQUENCY	8-24 YEARS	25-34 YEARS	35-44 YEARS	45-54 YEARS	55-64 YEARS	65-74 YEARS	75-84 YEARS
125	0.0	1.7	2.6	4.8	8.7	10.1	11.5
250	0.0	1.0	1.7	3.2	6.5	9.6	12.7
500	0.0	0.7	1.7	3.9	7.0	9.7	12.4
1000	0.0	1.0	1.7	4.7	5.6	12.8	20.0
2000	0.0	0.4	2.5	5.5	12.1	25.1	38.1
3000	2.1	5.8	8.6	18.2	31.5	40.9	50.3
4000	3.5	7.5	12.6	22.2	37.8	45.5	53.2
6000	2.5	5.3	12.4	23.1	49.5	50.9	52.3
8000	0.0	3.3	7.2	20.7	53.5	57.2	60.9
12000	0.0	5.2	14.4	41.7	64.2	70.0	75.8

Table 8: Minimum Hearing Thresholds (in dB) for Sound Frequencies (in Hz) and Age Ranges of a Female Subject

	AGE	AGE	AGE	AGE	AGE	AGE	AGE
FREQUENCY	8-24 YEARS	25-34 YEARS	35-44 YEARS	45-54 YEARS	55-64 YEARS	65-74 YEARS	75-84 YEARS
125	4.3	5.5	6.1	9.5	13.1	17.1	21.1
250	2.9	5.3	5.6	7.6	11.6	16.4	21.2
500	4.0	4.1	5.7	8.7	12.8	20.8	28.8
1000	3.7	4.1	6.4	9.5	10.0	24.7	39.4
2000	4.6	4.8	6.9	10.9	14.9	26.6	38.3
3000	4.6	6.9	10.3	18.2	20.2	40.6	61.0
4000	4.3	8.5	10.0	18.9	26.3	45.6	64.9
6000	5.8	8.8	13.6	22.4	28.7	47.2	65.7
8000	5.6	9.6	15.7	28.4	39.7	52.2	64.7
12000	9.2	17.6	28.5	58.0	70.0	70.0	70.0

As noted in the tables above, for a given age range for both male and female subjects, at a specific sound frequency (in Hz), the minimum detectable sound intensity (in dB) is reported. The Human Factors Hazard Model (HFHM) interpolates this data when comparing audible signal data (sound intensity and frequency) with the human factors minimum thresholds of hearing used to determine Human Error Probability (HEP) values. If the minimum threshold of hearing for a particular sound is not achieved using the hearing data incorporated into the HFHM, then a probability of failure of 1.0 is designated for that event. Otherwise, the probability of failure is assigned to be equal to 0.0, indicating that there is no chance of failure due to hearing limitations related to the human actor.

Visual Acuity Considerations

The visual acuity of the human actor is used to establish relevant Human Error Probability (HEP) values within the Human Factors Hazard Model (HFHM). Visual acuity within the HFHM is considered in two different ways. First, the ability of the actor to accurately resolve images related to detecting and diagnosing system behavior, and second, the ability of the actor to appropriately differentiate colors and interpret them correctly. The inability to observe system behavior, and accurately see instruments or input controls or to distinguish between color hues will have a direct influence on the actor's ability to correctly perceive and interpret system hazard behavior. Therefore, widely accepted and utilized methods for vision assessment are used to evaluate visual acuity and color blindness [1][40].

With regards to visual acuity, and the ability to see objects correctly, the HFHM requires the analyst to establish the visual characteristics of the human actor being evaluated using standard Snellen test designations. Normal vision is defined as having a ratio of 20/20. The

numerator in the ratio corresponds to the distance at which the subject can correctly read an eyechart optotype character and the denominator corresponds to the equivalent distance the control with normal vision can read the same character. For example, an actor with 20/60 vision can read a character accurately at 20 feet where an equivalent subject with normal vision can read the same character at 60 feet. Therefore, the actor being examined has less visual acuity than what is considered to be normal. The HFHM allows for a selection of visual acuity ranging from normal 20/20 up through 20/200 which is considered to be legally blind in the United States of America. The option for a complete lack of vision, beyond legal blindness, is also available for selection in the model.

With regards to visual acuity and the actor's ability to see, resolve, and interpret color correctly, the HFHM requires the analyst to establish the characteristics of the human actor being analyzed using standard color blindness classifications. Color blindness typically falls into three separate categories, with a number of sub-classifications for two of them. These types of color blindness are [40]:

- Red-Green Color Blindness
    - Deuteranomaly: The most common type of red-green color blindness. To the subject, green appears more red.
    - Protanomaly: To the subject, red appears more green and less bright.
    - Protanopia and Deuteranopia: The subject is unable to tell the difference between red and green.
- Blue-Yellow Color Blindness
    - Tritanomaly: The subject has difficulty telling the difference between blue and

green and between yellow and red.

  - Tritanopia: The subject is unable to tell the difference between blue and green, purple and red, and yellow and pink. Colors also appear less bright.

- Complete Achromatopsia: The actor has total color blindness, and cannot distinguish any hues of color.

Whether due to a visual acuity or color blindness issue, if the HFHM determines that the actor will be unable to detect a signal, either from the system behavior or instrumentation, then the associated event probability of failure for that event will be established at 1.0, indicating certain failure. Otherwise, the probability of failure is assigned to be equal to 0.0, indicating that there is no chance of failure due to visual limitations related to the human actor.

Tactile Acuity Considerations

Depending on system design, configuration, and operational parameters, the ability of the human actor to detect system behavioral characteristics using tactile senses will factor into Human Error Probability (HEP). The system may issue perceptible tactile signals such as accelerations, forces, vibrations, or thermal cues that will be detected via the actor being in physical contact with system components. Additionally, the human actor may be required to use tactile feedback to interface with the input control system. For example, if input control is necessary, but the actor lacks the sense of touch to ascertain contact with the input controls, or sense the appropriate amount of force required to actuate them correctly, the HEP associated with that event may increase accordingly. The probability that the actor has an adequate tactile sense for both detecting system behavior and control manipulation is accounted for in the Human

Factors Hazard Model (HFHM) by assigning HEP values using an Expert Estimation designation [1][37]. If precise HEP data is available for a specific design scenario, then the HFHM will allow a user specified value and associated error factors to be utilized in the predictive model.

Gross and Fine Motor Skills

The ability of a human actor to be mobile and have the necessary strength and dexterity to interact with the system and react appropriately to the Human Factors Triggering Event (HFTE) will have direct influent on related Human Error Probability (HEP). Depending on the nature of the hazard, the actor may be required to reposition or reorient to respond correctly to the HFTE. Additionally, the actor may be required to manipulate and exert sufficient force to provide correct input control to abate the unfolding hazard. The Human Factors Hazard Model (HFHM) relies on input regarding two types of motor function related to the human actor. These include:

- Gross Motor Skills, which correspond to the control of large muscle groups such as those found in the arms, legs, and torso. The large-scale motion and overall strength of a human actor are associated with this type of muscle function.
- Fine Motor Skills, which correspond the control of smaller muscle groups such as those found in the fingers and hand. The small-scale motions and fine muscle control to perform precise manipulations of objects are associated with this type of muscle function.

The probability that the actor has an adequate gross and fine motor skill is accounted for in the Human Factors Hazard Model (HFHM) by assigning HEP values using an Expert Estimation designation [1][37]. If precise HEP data is available for a specific design scenario, then the HFHM will allow a user specified value and associated error factor to be utilized in the predictive model.

System Factors Modeling

System Complexity, Training, and Operational Practice

The Human Error Probability (HEP) values associated with recognition, interpretation, and diagnosis of a particular, and potentially hazardous system behavior, were derived from data reported in the Technique for Human Error Rate Prediction (THERP) [16]. The failure probability values, as published, are established assuming a very complex control room environment used to control a nuclear power generating facility as the baseline. The HEP values, as recommended by THERP, are variable depending on training and practice associated with the specific hazard event. Additionally, the HEP associated with training and practice are determined as a function of time available to assess the threat, and plan a corrective action strategy. Expert Estimation is used by the analyst to assign a relative complexity within the Human Factors Hazard Model (HFHM), with the maximum value corresponding to the THERP control room configuration. As the complexity decreases from the baseline, a 10-times (10x) linear scaling factor is used to adjust the diagnostic time available for use in the cognition curve. The scaling factors based on system complexity are presented in **Table 9**.

Table 9: System Complexity Scaling Factors

SYSTEM COMPLEXITY	SCALING FACTOR
Very Complex	1
Complex	10
Simple	100
Very Simple	1000

As noted above, the HEP values from THERP data are a function of the human actor training and practice levels prior to the Human Factors Triggering Event (HFTE) as well as the time available to formulate a diagnosis and corrective action plan. Actor training refers to the level of system design and functional understanding possessed by the human interacting with it, as well as any specific understanding related to the hazard event being analyzed. The practice level describes the operational experience that the human actor has with respect to the system. This includes the development of intuition and muscle memory with regards to expected and unexpected behavior exhibited by the system. A level of expected performance for the human actor, based on training and practice, are established in the matrix presented in **Table 10**. Note that a 'FAIL' classification in the matrix would be indicative of a HEP value equal to one (Pf=1.0), which corresponds to a certainty of an actor being unsuccessful in their reaction to the HFTE.

Table 10: Human Actor Training / Practice Matrix

	ACTOR TRAINING CHARACTERISTICS		
ACTOR PRACTICE CHARACTERISTICS	NONE	SYSTEM	SYSTEM & HAZARD
NONE	FAIL	WORST	NOMINAL
INITIAL	WORST	NOMINAL	NOMINAL
CONSISTENT	WORST	NOMINAL	BEST

Depending on the performance expectation as established in the training / practice matrix detailed above, the HEP value related to an actor's ability to correctly interpret and diagnose the HFTE is established using THERP values in the literature. Using the established HFTE timeline, the probability of failure is interpolated using data presented in **Table 11**, **Table 12**, or **Table 13**. Also presented in each table are the specified error factors for each respective HEP value.

Table 11: Worst Case Actor Interpretation and Diagnosis HEP Data

	WORST CASE	
TIME (s)	HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
0	1	1
60	1	1
600	1	1
1200	1	1
1800	0.1	10
2400	0.01	10
3000	0.001	10
4800	0.0001	30
91200	0.00001	30

Table 12: Nominal Case Actor Interpretation and Diagnosis HEP Data

	NOMINAL CASE	
TIME (s)	HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
0	1	1
60	1	1
600	1	1
1200	0.1	10
1800	0.01	10
2400	0.001	10
4200	0.0001	30
90600	0.00001	30

Table 13: Best Case Actor Interpretation and Diagnosis HEP Data

	BEST CASE	
TIME (s)	HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
0	1	1
60	1	1
600	0.1	10
1200	0.01	10
1800	0.001	10
3600	0.0001	30
90000	0.00001	30

Visual Instrumentation, Input Controls, and Ergonomic Considerations

In the case of reading and interpreting standard instruments used to monitor system function, the Technique for Human Error Rate Prediction (THERP) has documented standard Human Error Probability (HEP) values. The various error probabilities and associated error factors related to a human actor reading and correctly interpreting standard industrial / commercial instrumentation are presented in **Table 14** [16].

Table 14: Human Actor Interpretation HEP for Standard Instrumentation

INSTRUMENTATION TYPE	HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
Analog Meter with Easy to See Limit Marks	0.001	3
Analog Meter with Difficult to See Limit Marks	0.002	3
Analog Meter without Limit Marks	0.003	3
Digital Readout	0.001	3
Graph Readout	0.010	3
Labeled Indicator	0.001	3

THERP also provides HEP data relevant to input control provided by a human actor that is interfacing with the system. The various error probabilities and associated error factors related

to a human actor initiating input control to the system via a standard type of control is presented in **Table 15** [16].

Table 15: Human Actor HEP for Control Input Action

INPUT CONTROL TYPE	HUMAN ERROR PROBABILITY (HEP)	ERROR FACTOR (EF)
Rotary Control (Dial/Wheel) Input	0.0010	10
Two-Position Switch or Lever Input	0.0005	10
Multi-Position Joystick Input	0.0040	10
Single Push-Button or Foot Pedal Input	0.0005	10
Numeric Keypad Input [1]	0.0004	10
Alpha-Numeric Keyboard Input [1]	0.0040	10

[1] *HEP Per Each Required Keystroke*

The HEP related to actor interpretation of instrumentation and manipulation of input controls can be modified by ergonomic factors related to the standardization and organization of the respective panels and their unique functions. As dictated by THERP, the respective probability multipliers are presented in **Table 16** [16].

Table 16: Ergonomic Multiplier for Instrumentation and Input Controls

INSTRUMENTATION & CONTROL ERGONOMICS	PROBABILITY MULTIPLIER
NEITHER ORGANIZED NOR STEREOTYPED	10
ORGANIZED	5
STEREOTYPED	5
ORGANIZED AND STEREOTYPED	1

For the characterizations as specified in **Table 16**, the following ergonomic definitions apply:

- Organized corresponds to instrumentation or a control interface that is well organized following good ergonomic principles. This includes instruments and controls that are visually prominent, properly labeled, grouped logically, and well illuminated.
- Stereotyped corresponds to instrumentation or a control interface that does not violate population stereotypes with respect to panel organization. This specifies that all displays read similarly during normal operation, and any unexpected behavior creates an easily noticeable difference as compared to companion instrumentation, that can be interpreted directly and in a timely manner by the human actor.

If values derived from the THERP HEP database are not intended to be used in the Human Factors Hazard Model (HFHM) analysis, the model allows for a value based on Expert Estimation to be used [37], or a custom user specified HEP value and associated error factor may be bookkept in the model for the human actor's interaction with the input controls of the system.

Audible Instrumentation - Alarms

In addition to visually interpreted instrumentation, that will communicate information as a result of a Human Factors Hazard Event (HFTE), an audible signal in the form of an alarm may be present to alert the human actor as to the presence and nature of the unfolding hazard. The alarm can be present simply to notify the actor of an existing hazard, or it may contain a specific sound or pattern of sounds to assist in hazard diagnosis by the human actor. Expert Estimation or a custom user defined probability is specified to establish the likelihood of an alarm signal being generated by errant system behavior. The sound intensity and frequency of the alarm

signal, as well as any possible diagnostic characteristics, are also specified in the Human Factors Hazard Model (HFHM) [37].

System Observability Characteristics

In the event of a Human Factors Trigging Event (HFTE) occurring during system operation, information specific to the characteristics of the hazard can be communicated to the human actor via the observable system behavior. Depending on the nature of the hazard event and the system design, specific information unique to the system behavior may be generated that can be detected and deciphered by the human actor. The types of system behaviors that generate a signal may include:

- An olfactory signal may be generated by errant system behavior that after a certain amount of time may be detected by the human actor. This signal may be a result of smoke, fumes, vapors, etc. that are produced by the system undergoing certain behaviors.
- A visual signal may be generated by errant system behavior. This signal may be generated by visible motion within the system, orientation or configuration of system components, deflection or deformation of system components, etc. Through direct observation, the human actor may see that the system is operating in a way that is not intended nor safe.
- An audible signal may be generated by system behavior. This may include unfamiliar or unusual sounds generated by the system, or the cessation of sound that may indicate undesired behavior. The sound or lack of sound generated by the hazard event may be

heard and deciphered by the human actor.

- A tactile signal may be generated by errant system behavior. This may include such characteristics as vibrations, accelerations, forces, etc. The tactile signal may be felt by the human actor if they are positioned and oriented correctly.

The system behavior signal generated by the HFTE used to alert the user, or be used to diagnose the hazard event, is specified within the Human Factors Hazard Model (HFHM). The probability of a system behavior signal can be specified in the HFHM using Expert Estimation or a custom user defined probability as dictated by the analyst [37].

System Environmental Factors That Can Interfere with Hazard Signals

A signal generated by system behavior or by the system instrumentation to communicate system behavior characteristics will be influenced by the environmental conditions in which the system and human actor are operating. The various environmental factors that may influence the detection or diagnosis of hazard event signals include:

- Illumination of system environment.
- Atmospheric clarity (fumes, smoke, etc.) obstructing direct observation by the human actor.
- Line of sight obstructions (walls, barriers, enclosures, physical distance from system behavior, etc.) hindering direct observation by the human actor.
- Vibrations obscuring visual or tactile reception of hazard signal.

- Acceleration of system components and / or the human actor, interfering with the reception of the hazard signal.
- Noise or other environmental sounds interfering with the actor's reception of an audible signal.
- Temperature of components in contact with the actor that may influence the receipt of a hazard signal.

Any individual factor, combination of factors, or all of the factors noted above may influence the human actor's ability to detect and then diagnose the Human Factors Triggering Event (HFTE) due to obscuring or interruption of the system behavior diagnostic signals. The environmental factors that may influence signal communication are specified in the Human Factors Hazard Model (HFHM) using Expert Estimate or custom user defined probabilities [37].

Misuse and Malevolent Intent

A hazard event can be initiated as the result of a human actor using the system in way that was not intended in the original design, by willfully disregarding signals of obvious errant and unintended behavior, or through malicious intent. If allowed to proceed without countermeasures being executed, system misuse or malevolent intent can progress into an accident / mishap. Each of these two possible scenarios are accounted for separately in the Human Factors Hazard Model (HFHM).

Misuse of the system by a human actor can include two separate use cases. First, the actor can choose to ignore system behavior signals that are communicating a hazard event is

underway. This inaction may be due to several factors. Among them are disbelief by the human actor that an actual hazard may be occurring despite the warning signs, laziness or complacency on the part of the operator, or a lack of understanding of the possible consequences due to inaction. Misuse may also include a Human Factors Triggering Event (HFTE) initiated by purposeful input action that does not follow standard operating procedures (SOPs), or a specified best practice for operation, as defined by the system design.

An example of intentional misuse contributing to a mishap resulting in loss of life and tremendous economic harm is the crash of American Airlines flight 151 at Chicago O'Hare International Airport on May 25, 1979. While accelerating down the runway for take-off, the McDonnell-Douglas DC-10-10 aircraft suffered a mechanical failure that ultimately resulted in a crash. While the aircraft was executing the take-off rotation to leave the ground, the left engine, pylon, and section of the wing leading edge separated from the aircraft. The pilot was not able to maintain control of the aircraft, and it rolled over in flight crashing into a field near the end of the runway. 271 passengers and crew onboard the plane as well as 2 people on the ground were killed, with 2 other people on the ground injured by flying debris. The aircraft, several automobiles, and structures on the ground were destroyed in the crash as well. A root cause of the structural failure can be attributed to a maintenance error due to equipment misuse during routine engine maintenance and replacement. In an attempt to save time and money, American Airlines maintenance personnel developed a procedure to remove the engine and pylon as a single assembly. The original procedure called for the engine and pylon be removed separately using specific tooling. This shortcut procedure was performed without authority from the airframer (McDonnell-Douglas) or engine manufacturer (General Electric). The modified procedure, using a forklift for engine manipulation and support, inadvertently damaged the

attachment clevis assembly of the engine support structure on the aircraft wing. This handling damage led to premature fatigue in the support structure, resulting in the engine separation during take-off. The modified maintenance procedure was not adequately reviewed by appropriate technical personnel, analyzed, tested, and approved per company policy. This example constitutes an intentional misuse of the system resulting in an accident [49].

Contrary to misuse, malevolent behavior is the intentional initiation of an accident / mishap as a result of the human actor willingly commanding system behavior to act in a known unsafe manner. The actor may be motivated for a number of reasons to act in a malevolent manner, thus intending harm. These motivations may include, mental illness, desire for self-harm, anti-social tendencies, anger or resentment towards supervisors or colleagues, etc. Ultimately, this type of behavior may lead to a catastrophic event that cannot be recovered from during system operations.

An example of malevolence on the part of the system operator is the crash of Germanwings Flight 9525 in the French Alps on March 24, 2015. The aircraft, an Airbus A320-211 was purposely flown into terrain by the copilot, killing all 150 passengers and crew. The flight that originated in Barcelona, Spain enroute to Dusseldorf, Germany was routine and uneventful until approximately 30 minutes into the flight. The copilot who had been privately seeking treatment for suicidal tendencies forcefully took control of the airplane, and flew it into the ground, crashing in the Massif des Trois-Eveches mountain range in the French Alps. The event occurred when the pilot in command momentarily left the cockpit. While absent, the copilot locked the door, and proceeded to crash the aircraft. No safeguards or fail-safes were in place to prevent controlled flight into terrain. The system designers did not anticipate this

activity as a likely threat to the aircraft, nor did they wish to remove the ultimate control authority from a human actor [48].

The HFHM accounts for misuse and malevolent intent in the Fault Tree Analysis (FTA) associated with the Cognition, Action, and Feedback pivotal events. System misuse is accounted for in all three of the noted pivotal events as the actor can choose to interpret and accept system signals indicating a threat, or not. The Action pivotal event allows for consideration of malevolent intent. Because specific human-system interaction with malicious intent requires knowledge and experience with the system controls, the HFHM accounts for not only the possibility of nefarious intent, it factors in whether the actor would possess the necessary skill to cause an accident on purpose. The likelihood of misuse or malevolent behavior are specified in the Human Factors Hazard Model (HFHM) using Expert Estimation or custom user defined probabilities with associated error factors [37].

Hazard Event Spatial Factors

The location and orientation of the human actor with respect to the various system components and their behavior will affect their perception and cognition with respect to the Human Factors Triggering Event (HFTE). The location of the actor refers to the position of the actor within the system context with respect to the optimal location required to appropriately perceive, diagnose, and act upon the HFTE. In the case of orientation, the actor may be in the correct position to detect the required signals from the system behavior, but possibly not with the correct orientation. For example, the actor may be standing in front of the control panel, but with their back turned to the display and controls, thus any visual signal would not be detected, nor would they be oriented correctly to interface with the input controls. Additionally, the human

actor's ability to access and actuate input controls as well as receive feedback with regards to the impact on system behavior will also be dependent upon their location and orientation within the system context. The spatial location and orientation of the actor with respect to the system will affect their ability to detect olfactory, visual, audible, and tactile signals related to system behavior and specifically the nature of the hazard event. If all four signal types are not detected, then the HFTE will progress to an accident. If any of the signal types are detected, then it is possible for the actor to relocate or reorient during the HFTE to detect other system signals that may be communicating information specific to the hazard event that is underway.

If the Human Factors Hazard Model (HFHM) determines that the actor will be unable to detect any hazard signal, due to their location and / or orientation relative to the system components, then the associated event probability of failure for that event will be established at 1.0, indicating certain failure. Otherwise, the probability of failure is assigned to be equal to 0.0, indicating that there is no chance of failure due to spatial concerns related to the human actor's location and orientation.

Hazard Event Timeline Factors

The success or failure of the actor's response to a Human Factors Triggering Event (HFTE) is dependent upon the timeline related to the hazard event. The chronology of the hazard event is calculated and evaluated within the Human Factors Hazard Model (HFHM). Beginning at the hazard event initiation, the sequence of events is established with timing associated with each step. The HFHM breaks the timeline into two segments for evaluation. The first segment includes events from hazard initiation through the point that corrective action has been initiated via the input controls. The second segment begins after initial corrective

action has been completed via the controls, and then evaluates any system feedback and subsequent actor response. Graphical representations of the both segments of the event timelines are presented in **Figure 12** and **Figure 13**.

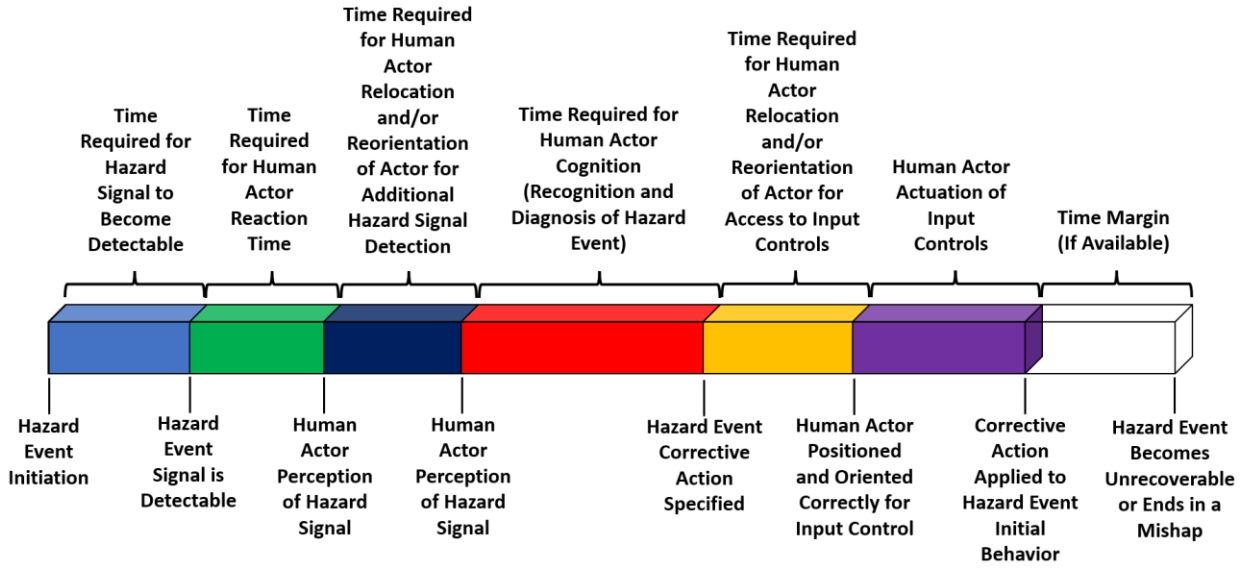


Figure 12: HFTE Timeline – Pre-Feedback Segment

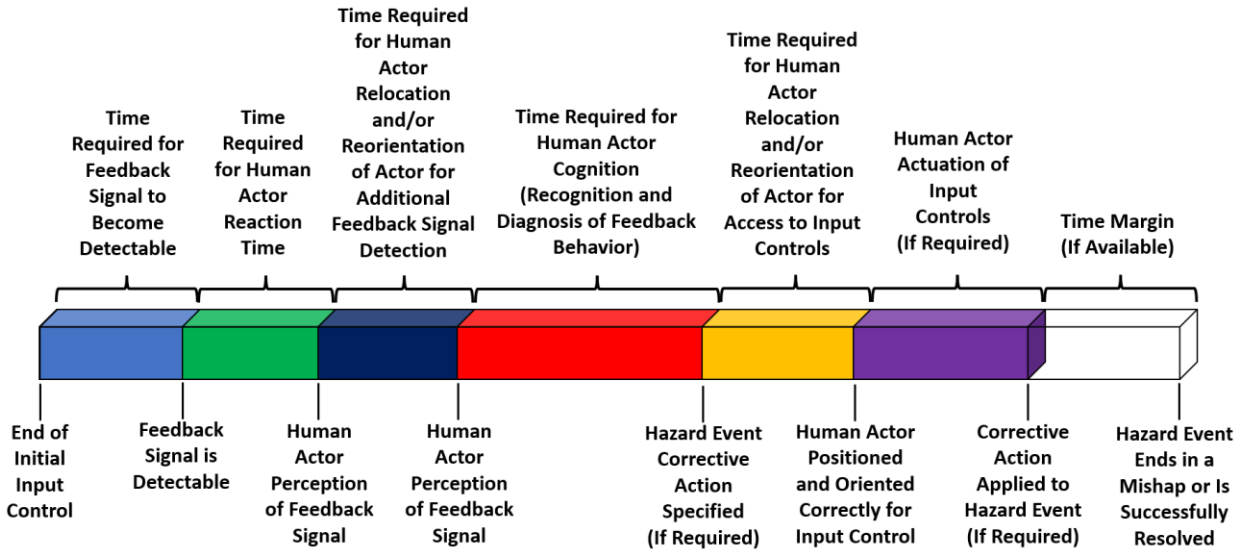


Figure 13: HFTE Timeline – Feedback Segment

As noted in **Figure 12** and **Figure 13** a timeline is bookkept beginning with the HFTE initiation, and ending with the point in time where the event has progressed to the point it becomes unrecoverable or is successfully resolved. The HFTE timeline accounts for the interval required for a detectable signal to be generated by the hazard event, for the human actor to react to the signal, relocate or reorient accordingly, and then cognitively process the hazard signal.

Once a diagnosis and planned corrective action is determined, an allowance is also made for any time required for relocation or reorientation to access the system control interface. Timing of input control action is then accounted for. The HFHM assumes that initial control action forestalls the hazard event such that feedback and subsequent input control or cessation of control inputs can occur. Note that if Human Error Probability (HEP) for HFTE diagnosis is derived from literature values, then all available time for cognition will be allocated by the software, leaving no time margin in the event. However, if cognition timing is specified by the analyst, then it would be possible to have a time margin available in the event timeline.

If the HFHM determines that the actor will be unable to provide a corrective action due to timing constraints, then the associated event probability of failure for that event will be established at 1.0, indicating certain failure. Otherwise, the probability of failure is assigned to be equal to 0.0, indicating that there is no chance of failure due to spatial concerns related to the human actor's location and orientation.

Human Redundancy and System Safeguards

Certain countermeasure characteristics unique to the system design may improve the probability of success as it relates to a Human Factors Triggering Event (HFTE). Possible countermeasure included in the system design would be a redundant actor or actors to improve the human reliability, and system safeguards that will disallow human input that may exacerbate or accelerate the unfolding HFTE, such that it can progress into an accident / mishap.

With respect to a redundant actor present in the system context, the design intent is allowing an additional human with comparable knowledge and skills to provide an alternate or additional resource for hazard resolution. An example of an application of a redundant actor in a system design, with the intent of improving reliability, would be a copilot operating an aircraft. In most cases, a single pilot can safely operate the aircraft with no assistance from another trained individual. However, by having the second pilot in place, the overall reliability of the system is greatly increased. As an illustration, if the reliability of a single pilot is established by analysis to be 99.9000% for a given task, the addition of a second equivalently trained and experienced pilot, with the same estimated reliability, would improve the probability of success to 99.9999% for the same task, assuming a simultaneous failure of both the pilot and copilot is required for an accident to occur. Or in other words, the calculated probability of failure for a

given hazard event has been reduced from an estimated 1 in 1,000 chance, to a 1 in 1,000,000 chance, simply by adding the redundant actor into the system design. Within the Human Factors Hazard Model (HFHM), the probability of failure with respect to the redundant actor is specified as an unexplored event within the Fault Tree Analysis (FTA) logic network. This means that the HFHM user will specify an overall estimate for the probability of failure related to the redundant actor or actors. Typically, if the redundant actor is specified to have equivalent training and experience with respect to systems operations, the respective probability of failure entered would be equal to that calculated by the HFHM assuming a single actor's response the HFTE. Multiple redundant actors' effect on system reliability can be determined simply by calculating each probability using "AND" logic accordingly. As a general note, the presence of redundant actors within the HFHM logic is accounted for in each contributing pivotal event, namely Perception, Cognition, Action, and Feedback. Therefore, the model is assuming that each redundant actor is contributing equally to all steps involved in the hazard response.

In addition to redundant actors, the HFHM also accounts for safeguards that are designed into the system and intended to disallow incorrect or damaging input control to be initiated by the human actor. Two different types of system safeguards are accounted for in the HFHM. First, software safeguards are present as an analysis option. These safeguards include algorithms within automatic control systems designed to recognize potentially damaging user input, and provide an active response to stop said input. Second, hardware safeguards are present as an analysis option. These safeguards include such things as physical barriers, limit switches or other limiting components, etc. that would prevent hazardous input control supplied by the actor. The analyst utilizing the HFHM to assess the HFTE will supply the probability of failure related to both software and hardware safeguards. Expert Estimation or a custom user defined

probability is specified to establish the probability of failure for either safeguard feature. A probability of failure of 1.0 would be an appropriate assignment to both, if no such safeguards exist for the specific hazard event being analyzed.

Pivotal Event Fault Tree Analysis Models

The proposed Human Factors Hazard Model (HFHM) predicts the likelihood of failure due to an actor's response to a Human Factors Triggering Event (HFTE), where the HFTE is defined as any interaction between a human being and the system which may result in a mishap [9]. The conceptual model of the steps involved in predicting the human response to an HFTE is a serial processing approach as illustrated in the schematic presented in **Figure 14**. First, the event must be perceived and recognized as a hazard. Second, the actor will cognitively process the available observed information, and then establish a corrective action plan. Third, a planned remedial action by the actor is then communicated to the system via control inputs, and the subsequent system behavior response is then observed. Fourth, based on the system feedback behavior due to control input, the actor must decide whether to terminate control input because the hazard has been resolved, or continue to provide additional control corrections in an effort to eliminate the hazardous behavior completely.

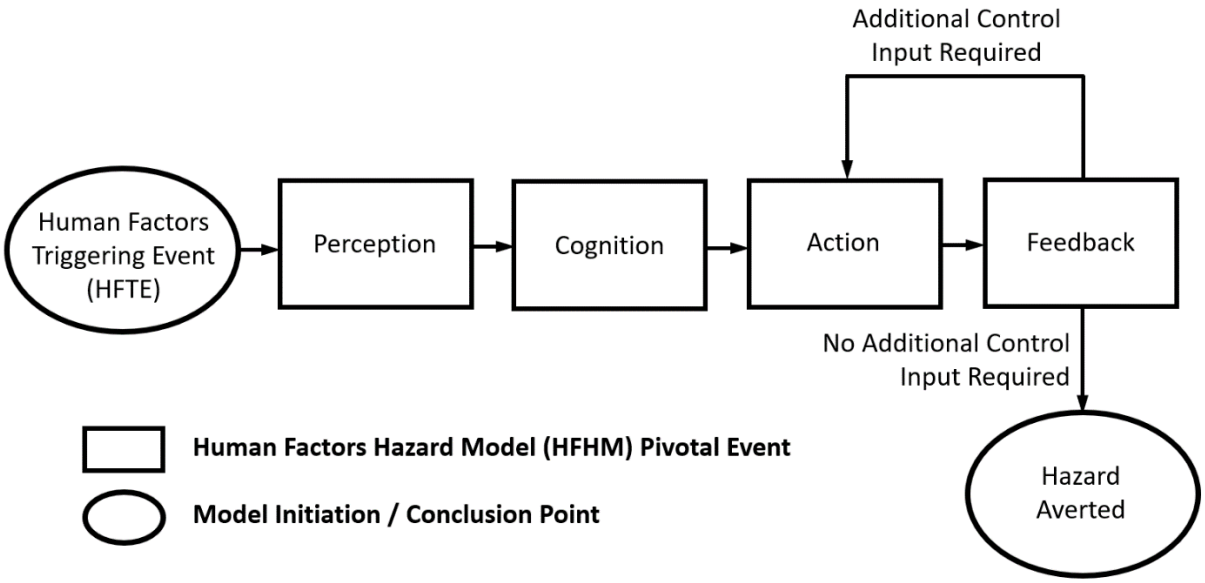


Figure 14: Hazard Event Human Response Model

Each stage of the process detailed above in **Figure 14** (Perception, Cognition, Action, and Feedback), indicates a point in the hazard sequence where a possible human failure could result in a mishap. This sequential approach to human information processing is a widely accepted model used to map a response in discrete, identifiable steps [51][52]. As an example, if the actor perceives the hazard event, but subsequently does not cognitively process it correctly, concluding that corrective action is necessary, the series of events will not progress to the action step, and thus, the HFTE will end in a mishap.

Under the proposed HFHM technique, each of the individual pivotal events noted in **Figure 14** are modeled using an embedded Fault Tree Analysis (FTA). The probability of success (or failure) for each of the four pivotal events are predicted via the FTA logic networks composed of basic events determined from the human factors and system characteristics (PSFs) unique to the problem being analyzed. The individual FTAs are each based on an evaluation of

probability of failure associated with combinations of the various contributing events due to human interaction with the system. Each basic event probability of failure is evaluated using Boolean logic, up through intermediate events, ultimately arriving at a combined top-level probability of failure [14].

The two primary logic operators used in the FTA approach are the "AND" gate, which indicates that all events must occur for a true condition to occur, and the "OR" gate, which indicates that any event, combination of events, or all events will precipitate a true condition. In the case of the "AND" logic, the corresponding Venn Diagram illustrating the joint probability of an event is presented in **Figure 15**.

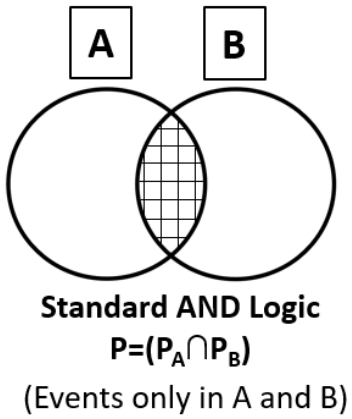


Figure 15: "AND" Logic Venn Diagram for Data Sets "A" and "B"

When applying the "AND" gate logic in an FTA network, each contributing event will have an associated probability of failure that are all accounted for in a single logic gate. The logic gate represents the associated Boolean operation, which is the intersection of data sets A &

B, to be performed on the contributing elements. This is illustrated in the FTA schematic presented in **Figure 16**.

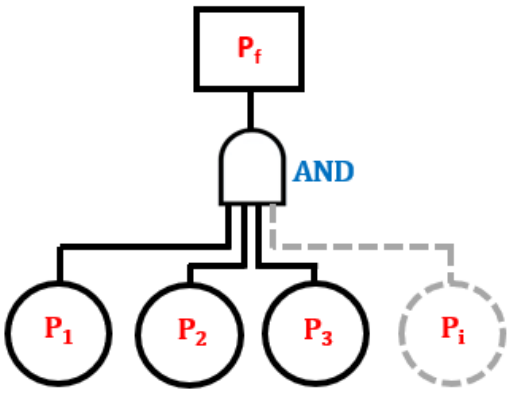


Figure 16: Fault Tree Analysis "AND" Logic Schematic

The mathematical approach used to calculate the combined probability due to the "AND" logic gate as illustrated above is noted by the equation:

$$P_f = \prod_{n=1}^{i} P_n \tag{3}$$

Where:

P_f = *Intermediate or Top-Level Event Probability of Failure*
P_n = *Contributing Event Probability of Failure*
i = *Total Number of Contributing Events*

In the case of the "OR" gate, a specific version of Boolean logic is applied to determine the combined probability. The FTA approach used in this analysis utilizes an "Inclusive OR" approach. For this type of logic, which is the union of data sets A & B, a single event, any combination of events, or all events associated with the higher-level event will satisfy the operator, thus resulting in a true condition. In the case of an "Inclusive OR" gate, the corresponding Venn Diagram illustrating the joint probability of an event is presented in **Figure 17**.

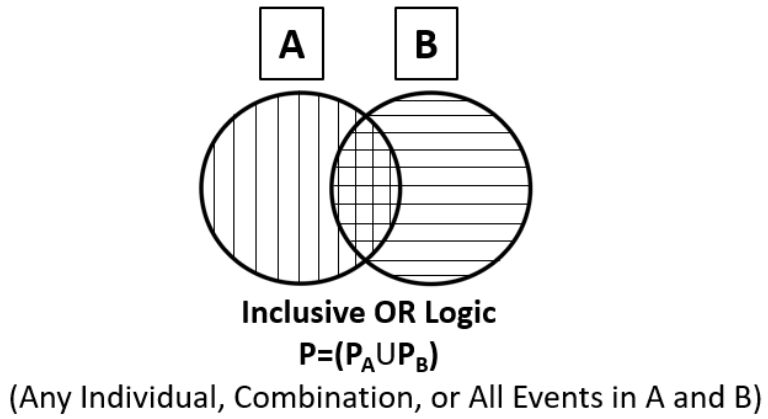


Figure 17: Inclusive "OR" Logic Venn Diagram for Data Sets "A" and "B"

When applying the "Inclusive OR" gate logic in an FTA network, each contributing event will have an associated probability of failure that all converge in a single logic gate. This logic gate represents the associated Boolean operation to be performed on the contributing probabilities. This is illustrated in the FTA schematic presented in **Figure 18**.

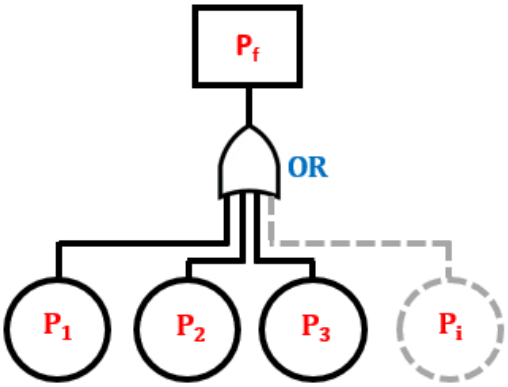


Figure 18: Fault Tree Analysis "OR" Logic Schematic

The mathematical approach used to calculate the combined probability due to the "Inclusive OR" logic gate as illustrated is noted by the equation:

$$P_f = \sum_{n=1}^{i} (-1)^{n+1} \left[\sum \left(\prod CP_n \right) \right] \tag{4}$$

Where:

P_f = *Intermediate or Top-Level Event Probability of Failure*
P_n = *Contributing Event Probability of Failure*
i = *Total Number of Contributing Events*
CP_n = *Each Combination of n Elements for Contributing Event Probability*

As an example of "Inclusive OR" logic and the associated mathematics to establish the combined probability, consider a scenario with four contributing events (P_1, P_2, P_3, P_4). The equation to calculate the combined probability (P_f) of the intermediate event is:

$$P_f = (P_1 + P_2 + P_3 + P_4) - [(P_1)(P_2) + (P_1)(P_3) + (P_1)(P_4) + (P_2)(P_3) + (P_2)(P_4) + (P_3)(P_4)] + [(P_1)(P_2)(P_3) + (P_1)(P_2)(P_4) + (P_1)(P_3)(P_4) + (P_2)(P_3)(P_4)] - [(P_1)(P_2)(P_3)(P_4)]$$

Where the intermediate event combined probability of failure (P_f) is the alternating sign sum of the product of each incremental combination (ones, twos, threes, etc.) of contributing events (P_1, P_2, P_3, P_4).

As previously described, each pivotal event contributing to the human actor response to an HFTE has a corresponding FTA that establishes the Human Error Probability (HEP) related to that event. The relevant symbols used in the HFHM Fault Tree Analysis logic networks are presented in **Figure 19**.

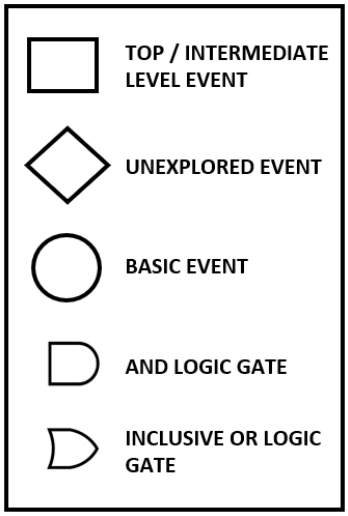


Figure 19: Fault Tree Analysis Event Symbol Key

The FTA corresponding to the Perception pivotal event is presented in **Figure 20** and **Table 17**.

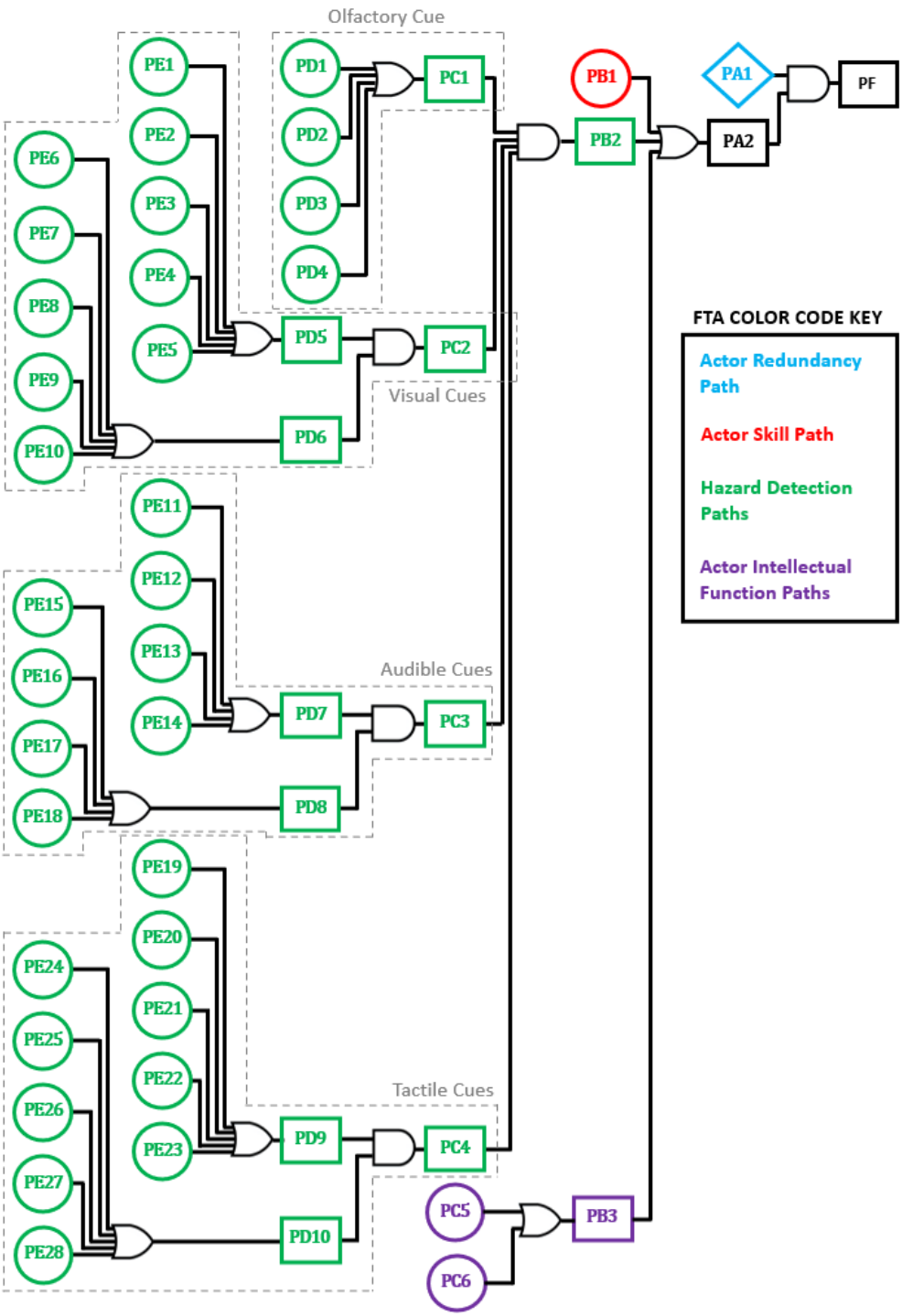


Figure 20: HFHM Perception FTA Used to Model the Probability of Fault for the Operator to be Unable to Perceive the Hazard

Table 17: HFHM Perception FTA Labels, Descriptions, and Logic Gate Types

PERCEPTION PIVOTAL EVENT FTA NETWORK		
LABEL, EVENT DESCIPTION, AND EVENT LOGIC NETWORK GATE TYPE		
PF	Top Level Event	AND
PA1	Redundant Actors	N/A
PA2	Single Actor	OR
PB1	Actor Skill	N/A
PB2	Hazard Detection Cue	AND
PC1	Olfactory Hazard Cue	OR
PD1	Timing	N/A
PD2	Location	
PD3	Sensory	
PD4	Olfactory Cue	
PC2	Visual Hazard Cue	AND
PD5	System Behavior Cue	OR
PE1	Timing	N/A
PE2	Location	
PE3	Orientation	
PE4	Sensory	
PE5	Signal	
PD6	Instrumentation Cue	OR
PE6	Timing	N/A
PE7	Location	
PE8	Orientation	
PE9	Sensory	
PE10	Signal	
PC3	Audible Hazard Cue	AND
PD7	System Behavior Cue	OR
PE11	Timing	N/A
PE12	Location	
PE13	Sensory	
PE14	Signal	
PD8	Alarm Cue	OR
PE15	Timing	N/A
PE16	Location	
PE17	Sensory	
PE18	Signal	
PC4	Tactile Hazard Cue	AND
PD9	System Behavior Cue	OR
PE19	Timing	N/A
PE20	Location	
PE21	Orientation	
PE22	Sensory	
PE23	Signal	
PD10	Control System Cue	OR
PE24	Timing	N/A
PE25	Location	
PE26	Orientation	
PE27	Sensory	
PE28	Signal	
PB3	Actor Intellectual Function	OR
PC5	Actor Mental Acuity	N/A
PC6	Actor Attention	

The FTA corresponding to the Cognition pivotal event is presented in **Figure 21** and **Table 18**.

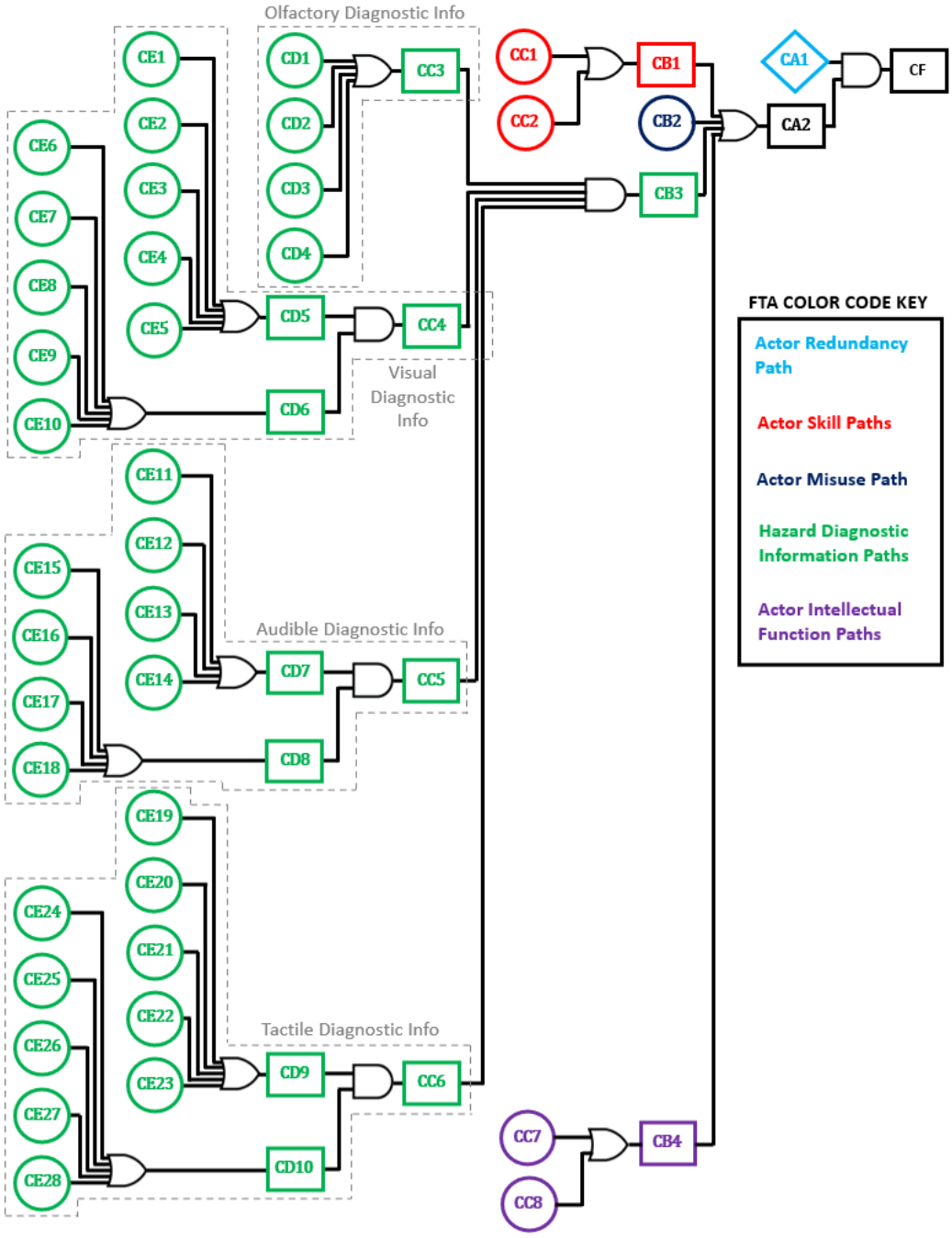


Figure 21: HFHM Cognition FTA Logic Network Used to Model the Probability of Fault for the Operator to be Unable to Cognitively Process the Hazard

Table 18: HFHM Cognition FTA Labels, Descriptions, and Logic Gate Types

COGNITION PIVOTAL EVENT FTA NETWORK								
LABEL, EVENT DESCIPTION, AND LOGIC NETWORK GATE TYPE								
CF	Top Level Event							AND
	CA1	Redunant Actors						N/A
	CA2	Single Actor						OR
		CB1	Actor Skill					OR
			CC1	Timing				N/A
			CC2	Diagnostic Approach				
		CB2	Misuse					N/A
		CB3	Hazard Diagnostic Information					AND
			CC3	Olfactory Diagnostic Information				OR
				CD1	Timing			N/A
				CD2	Location			
				CD3	Sensory			
				CD4	Signal			
			CC4	Visual Diagnostic Information				AND
				CD5	System Behavior Information			OR
					CE1	Timing		N/A
					CE2	Location		
					CE3	Orientation		
					CE4	Sensory		
					CE5	Signal		
				CD6	Instrumentation Information			OR
					CE6	Timing		N/A
					CE7	Location		
					CE8	Orientation		
					CE9	Sensory		
					CE10	Signal		
			CC5	Audible Diagnostic Information				AND
				CD7	System Behavior Information			OR
					CE11	Timing		N/A
					CE12	Location		
					CE13	Sensory		
					CE14	Signal		
				CD8	Alarm Information			OR
					CE15	Timing		N/A
					CE16	Location		
					CE17	Sensory		
					CE18	Signal		
			CC6	Tactile Diagnostic Information				AND
				CD9	System Behavior Information			OR
					CE19	Timing		N/A
					CE20	Location		
					CE21	Orientation		
					CE22	Sensory		
					CE23	Signal		
				CD10	Control System Information			OR
					CE24	Timing		N/A
					CE25	Location		
					CE26	Orientation		
					CE27	Sensory		
					CE28	Signal		
		CB4	Actor Intellectual Function					OR
			CC7	Actor Mental Acuity				N/A
			CC8	Actor Attention				

The FTA corresponding to the Action pivotal event is presented in **Figure 22** and **Table 19**.

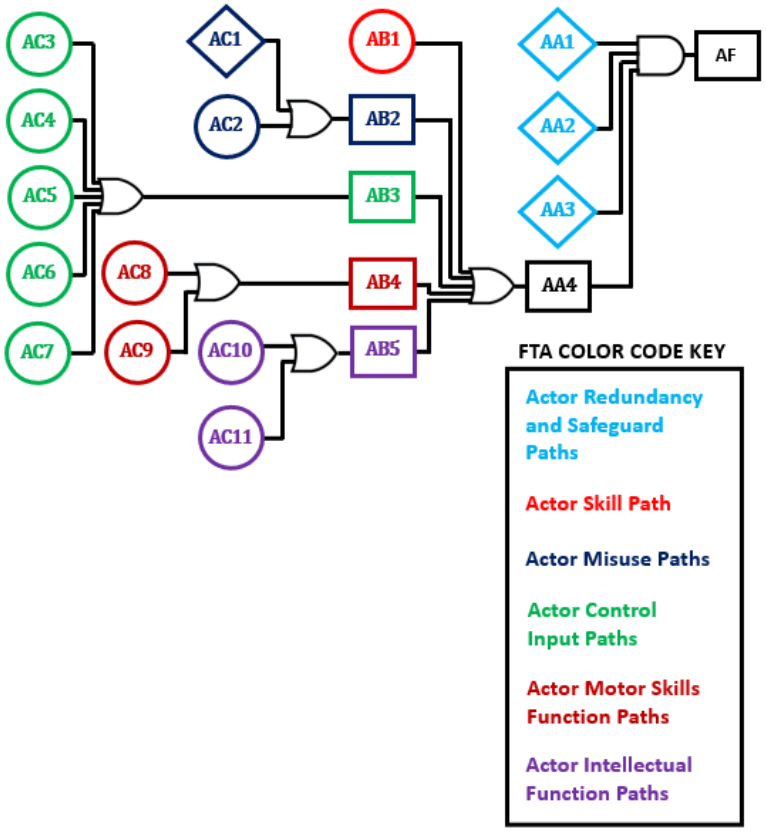


Figure 22: HFHM Action FTA Logic Network Used to Model the Probability of Fault for the Operator to be Unable to Correctly Apply Input Control to Correct the Hazard Behavior

Table 19: HFHM Action FTA Labels, Descriptions, and Logic Gate Types

ACTION PIVOTAL EVENT FTA NETWORK					
LABEL, EVENT DESCIPTION, AND LOGIC NETWORK GATE TYPE					
AF	Top Level Event				AND
	AA1	Redundant Actors			N/A
	AA2	Software Safeguards			
	AA3	Hardware Safeguards			
	AA4	Single Actor			OR
		AB1	Actor Skill		N/A
		AB2	Misuse		OR
			AC1	Intentional Misuse	N/A
			AC2	Malevolence	
		AB3	System Control Input		OR
			AC3	Timing	N/A
			AC4	Location	
			AC5	Orientation	
			AC6	Sensory	
			AC7	Control Interface	
		AB4	Actor Motor Skills Function		OR
			AC8	Gross Motor Skills	N/A
			AC9	Fine Motor Skills	
		AB5	Actor Intellectual Function		OR
			AC10	Actor Mental Acuity	N/A
			AC11	Actor Attention	

The FTA corresponding to the Feedback pivotal event is presented in **Figure 23** and **Table 20**.

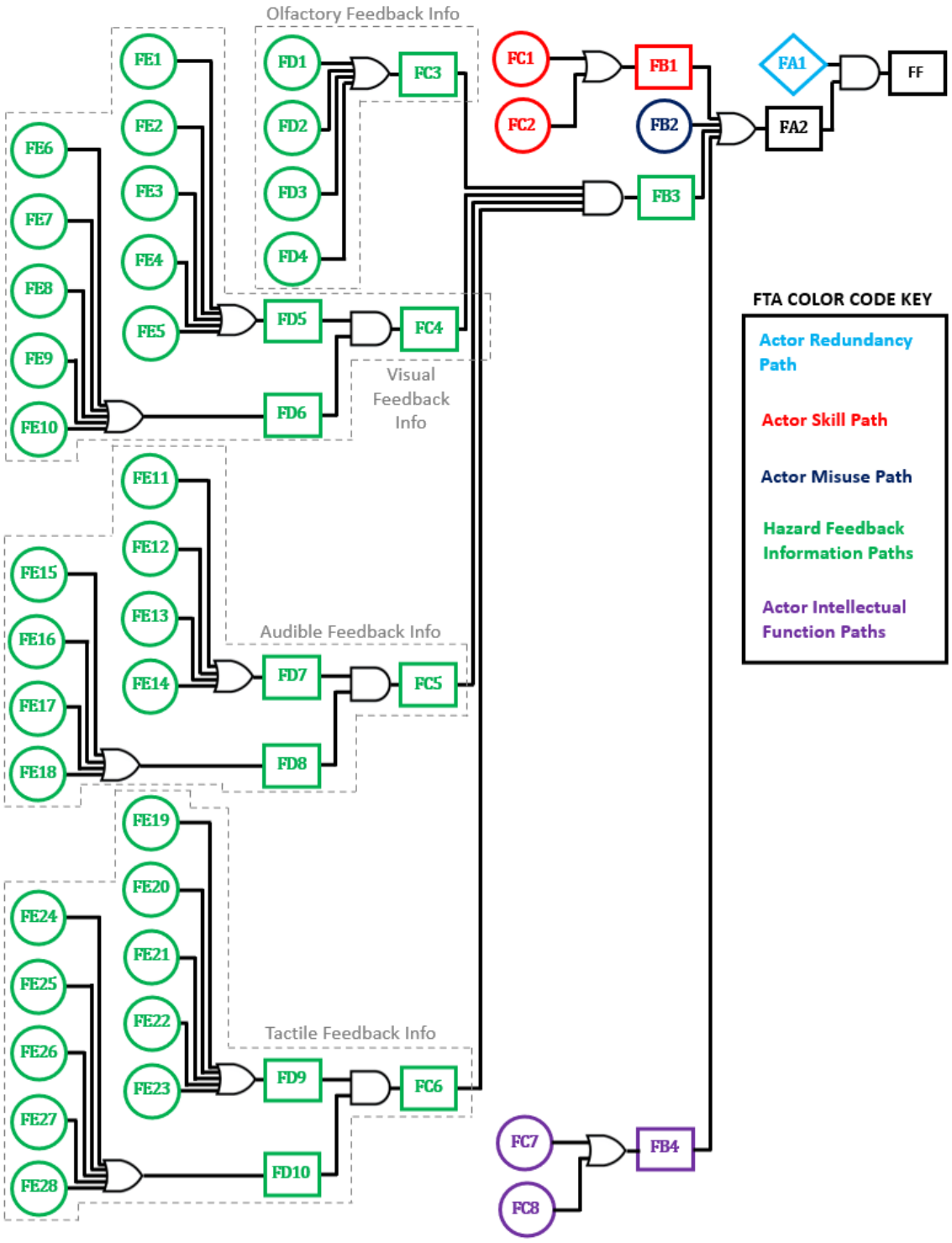


Figure 23: HFHM Feedback FTA Logic Network Used to Model the Probability of Fault for the Operator to be Unable to Receive and React Correctly to System Feedback Generated by Prior Input Control Action

Table 20: HFHM Feedback FTA Labels, Descriptions, and Logic Gate Types

FEEDBACK PIVOTAL EVENT FTA NETWORK										
LABEL, EVENT DESCIPTION, AND LOGIC NETWORK GATE TYPE										
FF	Top Level Event									AND
	FA1	Redunant Actors								N/A
	FA2	Single Actor								OR
		FB1	Actor Skill							OR
			FC1	Timing						N/A
			FC2	Feedback Interpretation						
		FB2	Misuse							N/A
		FB3	Hazard Feedback Information							AND
			FC3	Olfactory Feedback Information						OR
				FD1	Timing					N/A
				FD2	Location					
				FD3	Sensory					
				FD4	Signal					
			FC4	Visual Feedback Information						AND
				FD5	System Behavior Information					OR
					FE1	Timing				N/A
					FE2	Location				
					FE3	Orientation				
					FE4	Sensory				
					FE5	Signal				
				FD6	Instrumentation Information					OR
					FE6	Timing				N/A
					FE7	Location				
					FE8	Orientation				
					FE9	Sensory				
					FE10	Signal				
			FC5	Audible Feedback Information						AND
				FD7	System Behavior Information					OR
					FE11	Timing				N/A
					FE12	Location				
					FE13	Sensory				
					FE14	Signal				
				FD8	Alarm Information					OR
					FE15	Timing				N/A
					FE16	Location				
					FE17	Sensory				
					FE18	Signal				
			FC6	Tactile Feedback Information						AND
				FD9	System Behavior Information					OR
					FE19	Timing				N/A
					FE20	Location				
					FE21	Orientation				
					FE22	Sensory				
					FE23	Signal				
				FD10	Control System Information					OR
					FE24	Timing				N/A
					FE25	Location				
					FE26	Orientation				
					FE27	Sensory				
					FE28	Signal				
		FB4	Actor Intellectual Function							OR
			FC7	Actor Mental Acuity						N/A
			FC8	Actor Attention						

The four FTA logic networks are designed to calculate the associated probability of failure for the top-level event based on the fundamental HEP values and all intermediate probabilities calculated lower in the FTA logic network. The corresponding probability of success given for each top-level FTA is:

$$S = 1 - F \tag{5}$$

Where:

S = Top-Level Event Probability of Success
F = Top-Level Event Probability of Failure

Event Tree Analysis of Pivotal Events

Each pivotal event FTA is used to specify the corresponding probability of success and failure for an individual successive step in an Event Tree Analysis (ETA). The ETA then calculates the probability of success and failure for each sequential event. The logical basis of the ETA assumes that each pivotal event must proceed in order, without failure, for an ultimate successful outcome to occur [14]. In the case of the HFHM, all four events must successfully occur sequentially, in a specific order, for the HFTE to be resolved without an accident / mishap. If any individual pivotal event experiences a failure, then all subsequent events are null, and the HFTE has resulted in an accident / mishap. Per the ETA logic network, each individual contributing event is considered to be mutually exclusive in that any individual failure precludes success for all subsequent events. The logic network of the ETA is presented in **Figure 24**.

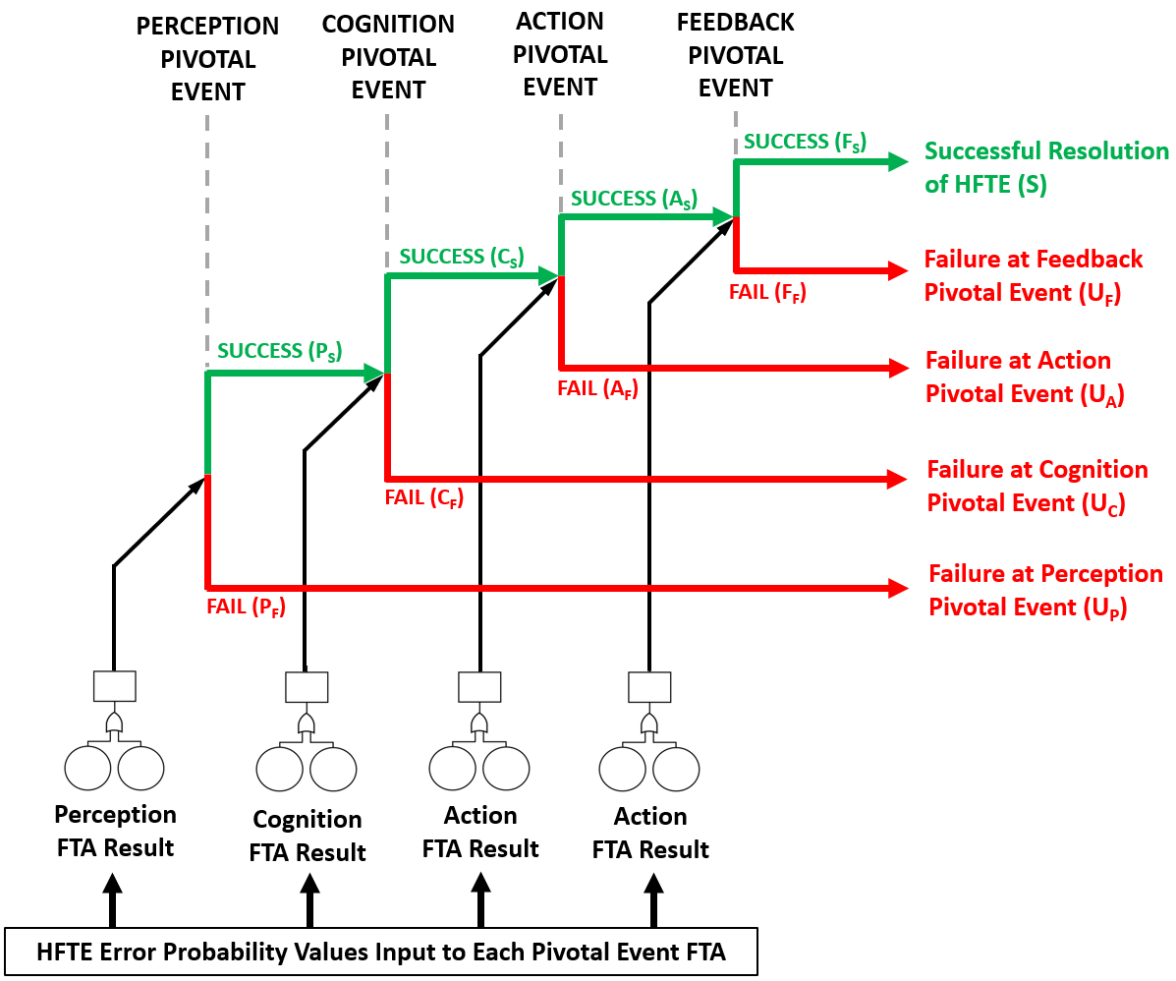


Figure 24: HFTE Sequential Processing Model ETA

The probability of a successful resolution of the HFTE due to human actor intervention, based on the ETA network, is:

$$S = (P_S)(C_S)(A_S)(F_S) \tag{6}$$

Where:

S = HFTE Probability of Success due to a Human Actor Intervention
P_S = Probability of Success of the Human Actor Perception Pivotal Event

C_S = Probability of Success of the Human Actor Cognition Pivotal Event
A_S = Probability of Success of the Human Actor Action Pivotal Event
F_S = Probability of Success of the Human Actor Feedback Pivotal Event

Conversely, the overall probability of an unsuccessful resolution to the HFTE due to human actor intervention, is determined using:

$$U = 1 - S \tag{7}$$

Where:

U = HFTE Probability of an Unsuccessful Human Actor Intervention
S = HFTE Probability of a Successful Human Actor Intervention

The probability of an unsuccessful resolution to the HFTE due to a failure of the human actor to receive and process feedback following a control action is:

$$U_F = (P_S)(C_S)(A_S)(F_F) \tag{8}$$

Where:

U_F = HFTE Probability of Failure due to Feedback Pivotal Event Failure
P_S = Probability of Success of the Human Actor Perception Pivotal Event
C_S = Probability of Success of the Human Actor Cognition Pivotal Event
A_S = Probability of Success of the Human Actor Action Pivotal Event

F_F = Probability of Failure of the Human Actor Feedback Pivotal Event

The probability of an unsuccessful resolution to the HFTE due to a failure of the human actor to correctly input control action following cognition is:

$$U_A = (P_S)(C_S)(A_F) \quad (9)$$

Where:

U_A = HFTE Probability of Failure due to Action Pivotal Event Failure
P_S = Probability of Success of the Human Actor Perception Pivotal Event
C_S = Probability of Success of the Human Actor Cognition Pivotal Event
A_F = Probability of Failure of the Human Actor Action Pivotal Event

The probability of an unsuccessful resolution to the HFTE due to a failure of the human actor to correctly input control action following cognition is:

$$U_C = (P_S)(C_F) \quad (10)$$

Where:

U_C = HFTE Probability of Failure due to Cognition Pivotal Event Failure
P_S = Probability of Success of the Human Actor Perception Pivotal Event
C_F = Probability of Failure of the Human Actor Cognition Pivotal Event

In addition to the equation cited above, note that the HFTE probability of failure due to the Perception pivotal event is equal to the probability of failure of the Perception event itself. Also note that the overall probability of an unsuccessful outcome to the HFTE (U) is equal to the sum of the other unsuccessful outcomes for each individual sequential pivotal event, or expressed mathematically as:

$$U = (U_P) + (U_C) + (U_A) + (U_F) \tag{11}$$

In summary, the HFHM model allows for users to model human error when considering overall system reliability. The characteristics of system design and the human actor within the system context are used to determine Performance Shaping Factors (PSFs) and their associated Human Error Probabilities (HEPs). The calculated HEP values are then used to calculate the basic event probabilities that are utilized at all entry level events of the four FTA networks. In cases where the human factors and system characteristics are considered to be standard and universally applicable, the HEP values can be derived from existing literature [16][1]. When certain PSF values are more specialized and standard values are not universally established or published, the HEP values can be based on an Expert Estimation / Expert Judgement approach [17]. For unique cases, where empirical data for specific operational scenarios has been derived, those HEP values can be specified directly in the HFHM. Once the individual HEPs are determined, and the respective pivotal events FTAs are calculated, an ETA is then used to

assemble the probabilities of the individual pivotal events, to calculate the overall probability of human error for the HFTE under consideration.

VERIFICATION & VALIDATION OF THE HUMAN FACTORS HAZARD MODEL

Referencing Research Question 1 (RQ1), the Human Factors Hazard Model (HFHM) is verified and validated using various methods. In support of Task 3 (T3), a direct comparison to an established Human Reliability Analysis (HRA) and an evaluation by industry and academic experts were performed. Also, a trade study of a hypothetical system design was evaluated to evaluate model performance against expected outcomes.

As noted above, to demonstrate the application of the HFHM, verification and validation of the model has been performed. Three different approaches are used to verify the performance of the HFHM and validate its utility with regards to system safety analysis, risk analysis, and reliability engineering. First, the HFHM is verified by performing a side-by-side comparison with a well-established and commonly utilized HRA technique, namely the Technique for Human Error Prediction (THERP). Second, the HFHM was evaluated by a group of Subject Matter Experts (SMEs) with particular knowledge in Systems Engineering as well as operations and facilities management. Lastly, the HFHM was evaluated using a trade study example with relevancy to a typical human factors hazard analysis.

HFHM Verification Using a THERP Comparison Analysis

Quantitative verification of the Human Factors Hazard Analysis (HFHM) analysis is supported via direct comparison of results accomplished using the Technique for Human Error-Rate Prediction (THERP). This technique is described in the literature as "Comparison to Other Models" [61]. To execute this approach, a baseline failure event was established incorporating

elements typical of a Human Factors Triggering Event (HFTE). The HFTE included an assumed hazard event, communication of system behavior to a human actor, cognitive processing by the actor to establish a corrective action response, control system input, and feedback resulting from control system input. A typical Human Reliability Analysis (HRA) event tree was established for the probability analysis per THERP methodology [13][16]. The event tree utilized to evaluate the baseline hazard event, as well as the subsequent permutations, using THERP is presented in **Figure 25**.

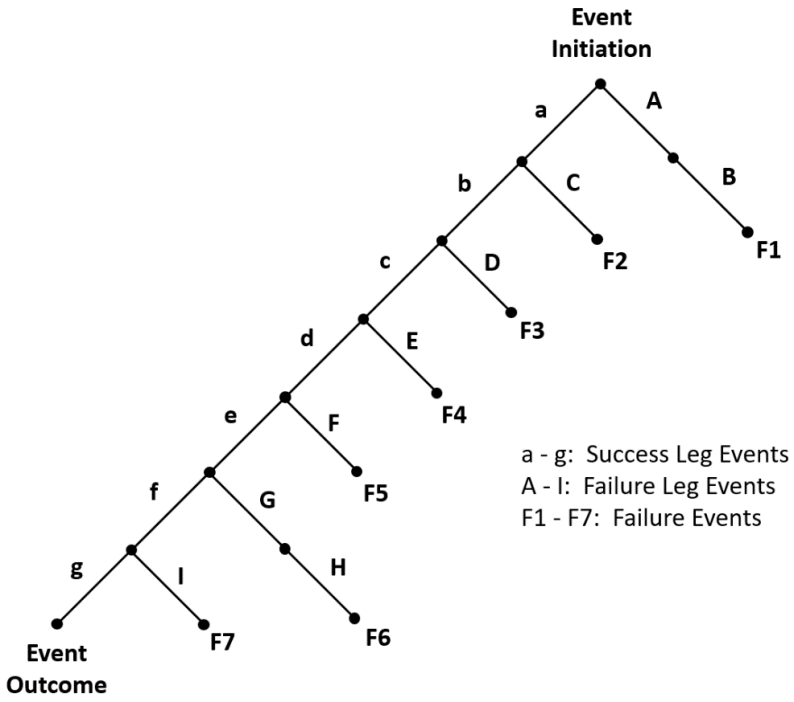


Figure 25: THERP Verification Model HRA Event Tree

For the specified event detailed in **Figure 25**, several opportunities for a failure related to human interaction with the system are detailed. The possible failure legs are labeled in the HRA

event tree as event A-I. Each failure leg represents an opportunity for the human actor interacting with the system, and attempting to avoid a mishap, are required to successfully receive a signal, process that signal, provide appropriate input action, and then interpret system feedback relevant to the control input rendered. The various human-system interactions that correspond to these possible failure legs are presented in **Table 21**.

Table 21: THERP Verification Model Failure Leg Event Descriptions

PROBABILITY TREE - FAILURE LEG	DESCRIPTION
A	Recognize Alarm
B	Recognize Indicator Lamp
C	Read Pressure Gage (Analog Meter)
D	Diagnose Hazard
E	Actuate Control (Push Button)
F	Actuate Control (Rotary Dial)
G	Recognize Alarm Shut-Off
H	Recognize Indicator Shut-Off
I	Cease Control Input

Several permutations of the baseline case were then established with various human and system factors, including actor stress levels, training and practice parameters, and instrumentation and control interface organization and ergonomics. Each human and system factor noted are used to establish PSFs that are then utilized to modify Human Error Probability (HEP) for the various permutations of the baseline analysis. As the human and system factors are adjusted in both analyses (THERP and HFHM), the resulting top-level probabilities of success and failure will adjust accordingly. A list of the various human and system factors that are present in the comparative study are presented in **Table 22**.

Table 22: Human and System Factors Used to Establish PSFs

PERFORMANCE SHAPING FACTOR (PSF)	DESCRIPTION
1	System Training w/ Hazard Practice
2	System Training w/o Hazard Practice
3	Instrumentation & Controls are Organized or Stereotyped
4	Instrumentation & Controls are not Organized or Stereotyped
5	Optimum Stress
6	Extremely High Stress

As a result of the variations applied to the baseline case, a total of eight operational scenarios are evaluated using THERP and compared with corresponding HFHM analyses. The analysis results for each permutation of the baseline model, utilizing the variable values are presented in **Table 23**.

Table 23: THERP and HFHM Analysis Results Comparison for All Design Study Cases

	PROBABILITY OF SUCCESS							
	PERFORMANCE SHAPING FACTOR (PSF) COMBINATIONS							
PROBABILITY TREE - SUCCESS LEG	1-3-5	1-3-6	1-4-5	1-4-6	2-3-5	2-3-6	2-4-5	2-4-6
a	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
b	0.997	0.997	0.970	0.970	0.997	0.997	0.970	0.970
c	0.999	0.990	0.999	0.990	0.990	0.900	0.990	0.900
d	1.000	1.000	0.995	0.995	1.000	0.995	0.995	0.995
e	0.999	0.999	0.990	0.990	0.999	0.999	0.990	0.990
f	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
g	0.999	0.990	0.999	0.990	0.990	0.900	0.990	0.900
THERP Probability of Success=	0.994	0.976	0.954	0.936	0.976	0.803	0.936	0.774
HFHM Probability of Success=	0.986	0.908	0.973	0.895	0.950	0.878	0.938	0.863
Agreement Between THERP & HFHM=	0.7%	7.5%	2.0%	4.6%	2.7%	9.4%	0.1%	11.5%
							Average Agreement Between Approaches=	4.8%

Good agreement between the solution calculated by THERP and the HFHM are demonstrated in this study. It can be argued that the HFHM solution to each particular scenario

is likely more accurate than the solution yielded by THERP in that each representative HFHM result accounts for more individual HEP values drawn from numerous human factors databases. A summary of the comparative trials detailed in **Table 23** above include:

- The average variability between the THERP and HFHM probability of success results, over the eight different trial cases, is 4.8%.
- The ranges of variability between the THERP and HFHM solutions are between a minimum of 0.1% and a maximum 11.5%, depending on the exact combinations of PSF employed in the analysis.

HFHM Evaluation Using a Design Study Example

An approach to validating the HFHM was via the evaluation of a design study for a manufacturing system that depends upon human intervention to operate successfully. This technique is described in the literature as "Parameter Variability" [61]. The manufacturing system selected for analysis is a hypothetical system that is representative of a system used to machine parts on centers. For the case evaluated, a forging work piece composed of a very high-cost aerospace alloy is assumed to be machined using a lathe. Typically, the work piece is turned on a rotational centerline, and material is removed using a shaped cutting insert. During the material removal, a lubricant / coolant is discharged onto the insert and work piece to remove machining debris as well as lubricate and cool the workpiece and tooling. Typically, the process being analyzed is very sensitive to spindle speeds, coolant flow rates, and cutting insert feed rates. If the part is turned too aggressively, it risks generation of an alpha case defect due to

surface heating, thus damaging the part beyond salvaging, and it would be scrapped at a very high cost to the company. The typical machining arrangement of the work piece in the CNC lathe is presented in **Figure 26**.

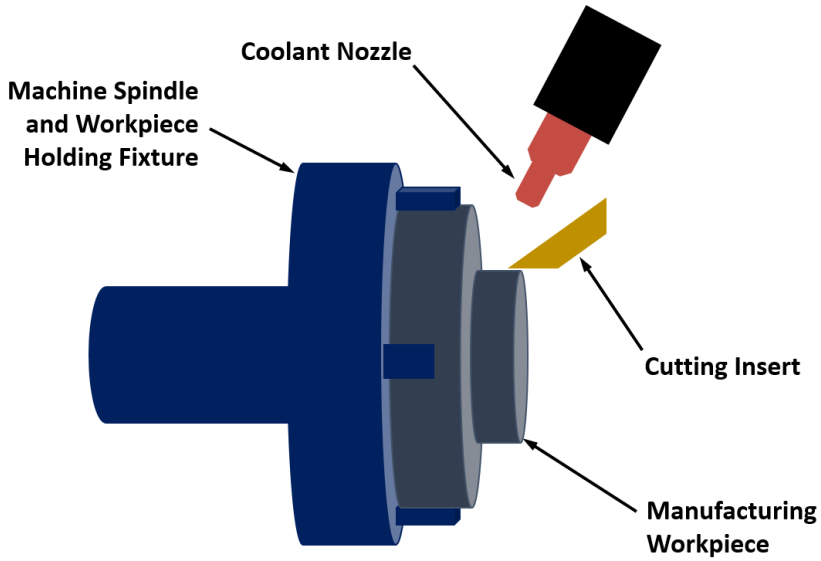


Figure 26: Typical Component Machining Arrangement

The design study being used to assist in the HFHM validation is regarding the operator (human actor) reaction to an unexpected low coolant flow issue. Therefore, the Human Factors Triggering Event (HFTE) is defined as during a normal machining operation, the system experiences a drop in coolant flow, that potentially endangers the component being manufactured. The low coolant flow can be the result of three different possible root causes. It could also be the result of any combination of these root causes. The low-rate root causes include:

- An obstruction in the flow path restricting the coolant flow
- Insufficient pump flow (pressure and / or pumping capacity)
- Low coolant level in reservoir

The manufacturing system design being analyzed includes the machining mechanism, coolant tank and pumping hardware, the control panel / user interface, and a human actor operator. The human actor and control panel provide input control to the machining mechanism and coolant management system. The control panel also provides instrumentation feedback to the actor regarding system performance and operational parameters. A schematic of the manufacturing system is presented in **Figure 27**.

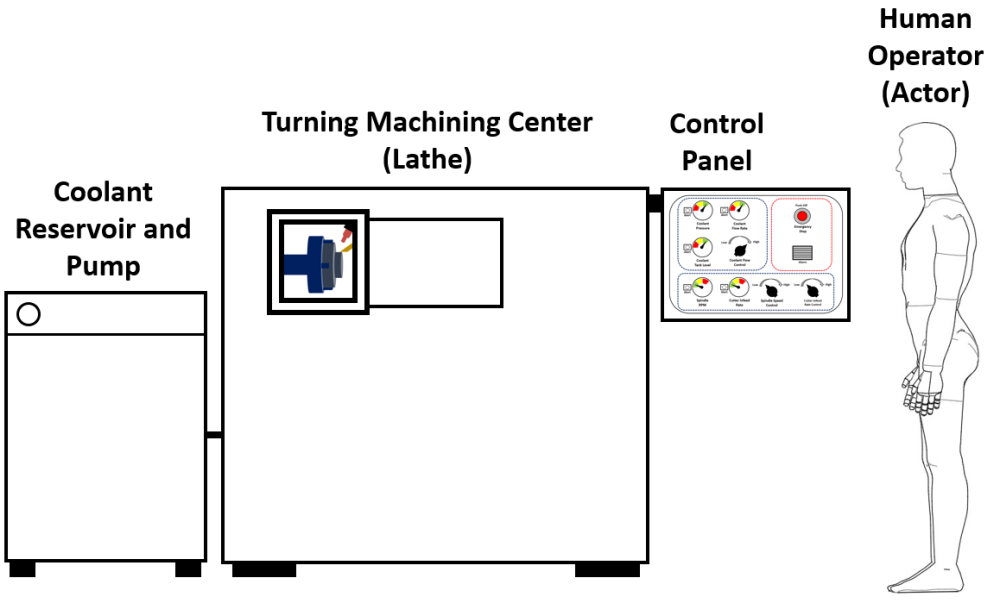


Figure 27: Design Study Manufacturing System Schematic

For the design study cases being evaluated, the coolant flow drops to an unacceptable level during operation, thus endangering the workpiece. The baseline case of the study is assumed to be the "worst-case" scenario, with two design updates performed to improve (lower) the Human Error Probability (HEP). For the baseline case, a trained and experienced actor is considered, however, the specific failure event is not practiced for, or simulated specifically. The actor is assumed to be moderately young (30 years old), not impaired, not fatigued, with optimal vision and hearing. The distraction and stress levels anticipated are considered to be moderate. The machining of the workpiece is not directly observable by the operator as no viewport is available for observation of the spindle, cutting insert, and coolant nozzle. The instrument and control interface are considered to be not organized by function nor are the instruments and input controls stereotyped for ease of interpretation and execution. The panel was not initially designed with good ergonomic principles or consideration of optimal human factors. In this configuration, instruments are not organized into logical or functional groups, and output information related to instrument displays are not oriented in a standardized or intuitive manner. Additionally, control interfaces do not follow established and consistent design protocols. In the baseline configuration, the instrumentation does not annunciate during the HFTE, nor does any audible alarm sound. An example of this type of instrumentation and control interface is presented in **Figure 28**. Note that the panel is difficult to read and interpret quickly. Instruments do not align in a coherent manner, and are not annotated for easy comprehension. Additionally, input controls actuate in non-standardized directions and often opposite the expected direction of travel of other related instruments. For example, the operator may turn the input control counter-clockwise to accelerate the spindle, but the associated rotational speed gage reads increasing speed with the needle rotating clockwise.

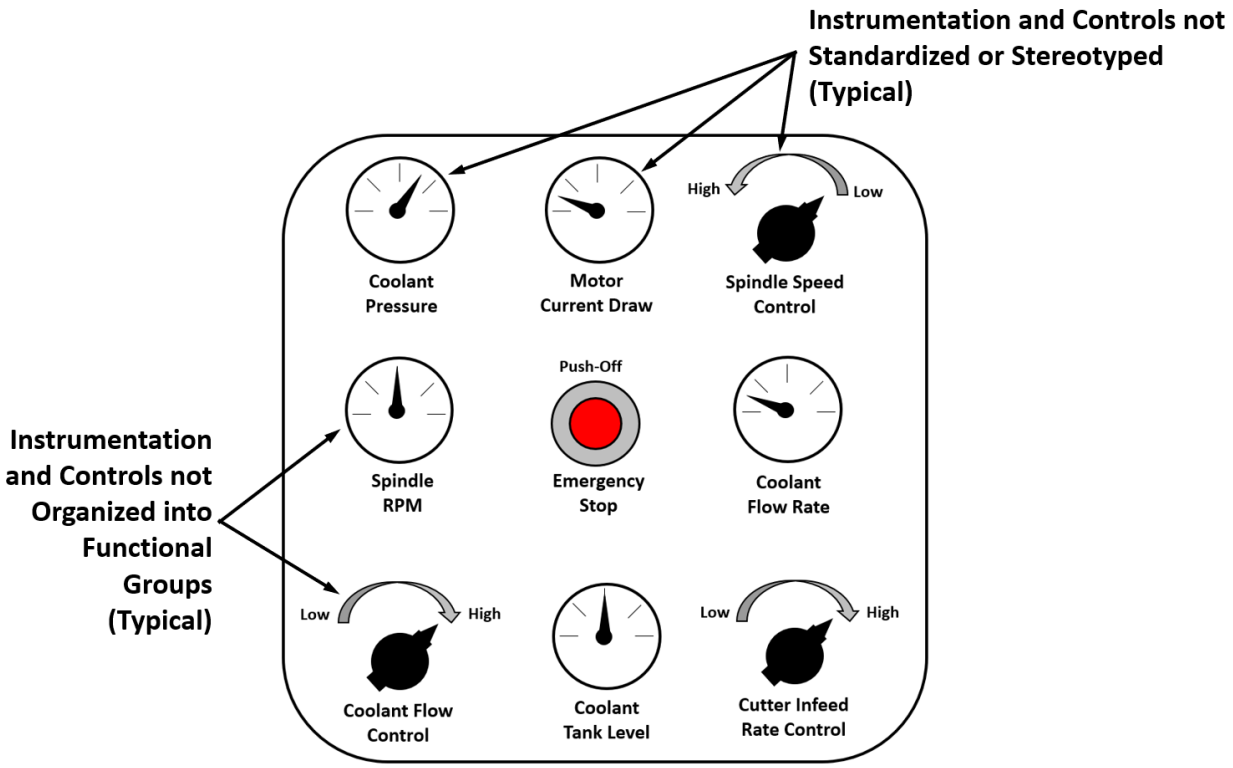


Figure 28: Unorganized and Non-Stereotyped Control Panel Example

In the first design update (Update 1), the distraction and stress levels are assumed to be reduced through procedural changes and training efforts. Additionally, a viewport is added for direct human actor observation of the workpiece manufacturing inside the manufacturing mechanism and the workspace is reorganized so that the manufacturing process and instrumentation can be monitored simultaneously. The control panel is redesigned such that it is clearly organized, labeled, and stereotyped with respect to instrumentation viewing and control input. In the new configuration, the instruments and controls are organized into functional groups, share a consistent readout and obvious marking scheme. The instruments and associated controls are stereotyped such that the readouts and control actuation directions are uniform and intuitive for a human actor to interpret. In addition to the organization and stereotyping of the

panel layout, the instruments are annunciated so that when measured values fall into an unacceptable range, an indicator illuminates to alert the actor. Additionally, an audible alarm is added to provide a signal to alert of errant system behavior. An example of the redesigned control panel with all instruments and control inputs organized and stereotyped is presented in **Figure 29**.

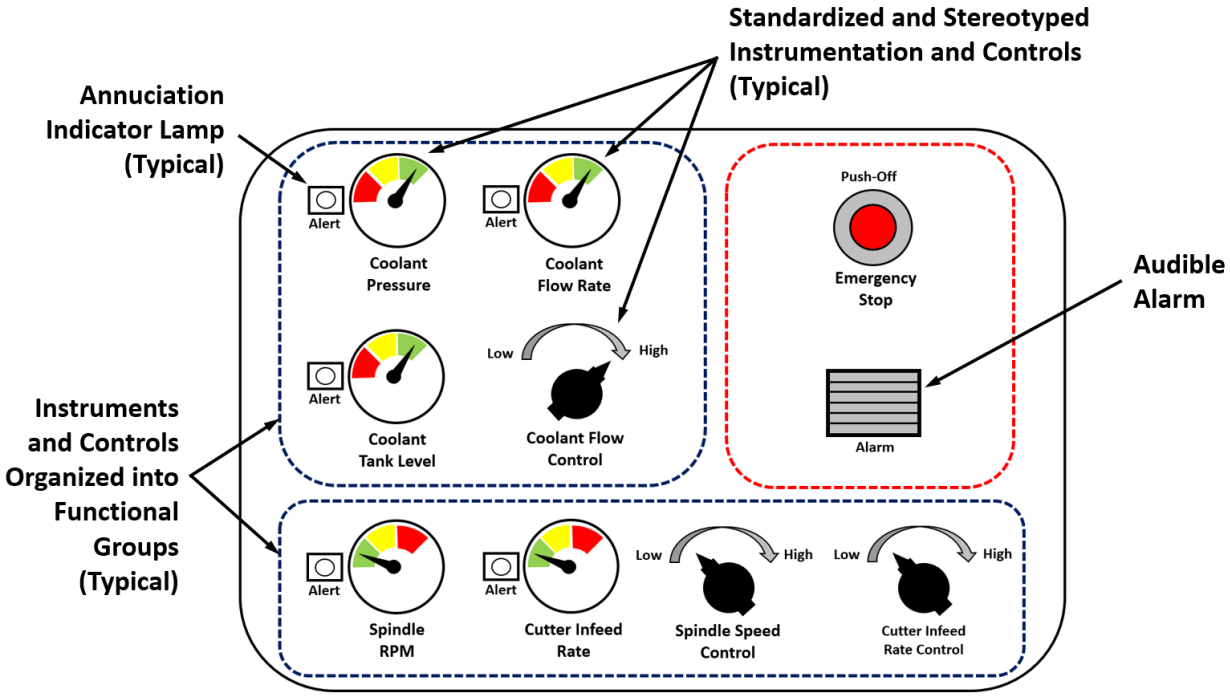


Figure 29: Organized and Stereotyped Control Panel Example

A second design iteration (Update 2) specifies that the loss of coolant flow fault be simulated and practiced by the operator such that their specific skill level increases with regards to recognizing and remediating the hazard event. The results of the baseline and two subsequent revisions (Update 1 and Update 2) reveal an improvement in the probability of success relative to

the human actor's reaction to the HFTE. For the conditions specified in the baseline case, an overall probability of success related to the human actor's response the low coolant flow fault is calculated by the HFHM to be 0.252 or 25.2%. Therefore, it is most likely that the hazard event will advance to become a mishap, and the workpiece will be damaged beyond recovery. A more detailed inspection of the HFHM result for the baseline case indicates that the Perception pivotal event only has a probability of success of 0.433 or 43.3% with the other three pivotal events (Cognition, Action, and Feedback) are all greater than 80%. This supports a conclusion that the signal indicating a low coolant flow is not effectively reaching the actor such that they can act upon that information and correct the unfolding HFTE. With the improvements specified for Update 1, the overall probability of success increases to 0.962 or 96.2%. It is also interesting to note, that for this configuration, all four pivotal event probabilities of success are in the 98-99% range. This indicates a significantly improved likelihood that the human actor will correctly respond to the loss of coolant flow fault. With the improvement specified for Update 2, the overall probability of success rises modestly to 0.979 or 97.9%. A summary of the design cases evaluated, with their respective probability calculations are presented in **Table 24**.

These results support the initial hypothesis that as design improvements are implemented, the HFHM will predict an overall positive trend in hazard reduction related to human-system interaction. It is important to note that the revisions made to the design and operational procedures to improve system safety will likely incur additional cost and potentially complicate the system, thus introducing other possible reliability concerns, etc. As such, for all system improvements specified, appropriate trade studies should be conducted to verify the net benefit of each revision. Note that the HFHM results only evaluate the issue from the perspective of a human actor's reaction to a hazard event.

Table 24: Validation Design Study Results

HFHM DEFINITION AND PSF INPUTS			HFHM OUTPUTS				
DESIGN CASE & DESCRIPTION	PERFORMANCE SHAPING FACTORS		PROBABILITIES OF SUCCESS				
Baseline Case			**PERCEPTION**	**COGNITION**	**ACTION**	**FEEDBACK**	**OVERALL**
Machining operation coolant flow failure with a required human operator intervention to avoid a mishap.	Moderately young actor (30 yrs)	→	0.433	0.814	0.853	0.839	0.252
	No Impairment						
	No appreciable fatigue						
	Normal actor visual acuity						
	Typical actor reaction time						
	Actor trained and experienced with system operations						
	Actor has no practice with specific HFTE behavior						
	Event occurs early in shift (1st hour of 8 total hours)						
	Instrumentation not organized or stereotyped						
	Instrumentation not annunciated for hazard alert						
	No audible alarm for hazard alert						
	Input controls not organized or stereotyped						
	No direct observation of machining operation by actor						
	Moderately high stress						
	Moderate distraction level						
	No adverse environmental conditions to inhibit actor response to HFTE						
	System operations are considred to be simple to understand						
Update 1			**PERCEPTION**	**COGNITION**	**ACTION**	**FEEDBACK**	**OVERALL**
All characteristics carried over from the Baseline Case with the noted revsions.	Instrumentation organized and stereotyped	→	0.988	0.997	0.980	0.997	0.962
	Annuciated indicators added for HFTE behavior						
	Audible alarm added for HFTE behavior						
	Input controls organized and stereotyped						
	Viewport added for direct actor observation of machining process						
	System organized for simultaneous viewing of process, instrumentation, and input control						
	Optimal stress level						
	Low distraction level						
Update 2			**PERCEPTION**	**COGNITION**	**ACTION**	**FEEDBACK**	**OVERALL**
All characteristics carried over from the Baseline Case with the noted revsions.	Consistent practice of HFTE response by actor	→	0.997	0.996	0.989	0.997	0.979

HFHM Validation from Industry Expert Feedback

Evaluation of the Human Factors Hazard Model (HFHM) was accomplished via independent testing, performance assessment, and feedback provided by a total of six Subject Matter Experts (SMEs) with professional positions. This approach is described in the literature as "Face Validity" [61]. The assessment team consisted of personnel representing systems engineers and systems engineering managers of a large, publicly traded defense and aerospace corporation, production and plant design managers of a mid-sized, privately owned aerospace products corporation, and a former facilities operations manager of a large public university and current faculty member of the Construction Management department at a public 4-year university.

The three groups of SMEs utilized in this study were selected as a representative cross-section of prospective users of the HFHM across a range of industries and potential safety analysis scenarios. Each participant selected was a technical expert with current or prior management, operations, and design responsibility for system safety, including human factors considerations. They were considered authorities in their respective fields, with knowledge and experience related to safety evaluation relative to their products and employment responsibilities.

The first group of systems engineers and systems engineering managers represent a typical system lifecycle design team, with overall system safety responsibilities related to their engineering activities. These responsibilities include new system design and implementation, as well as sustaining engineering support related to very large and complex, legacy system designs, that have been deployed and maintained over several decades.

The second group of manufacturing management personnel identified as SMEs were selected due to their ongoing safety responsibility within a large and highly automated

manufacturing facility. Within this environment, there are many human interactions with electrical-mechanical-software based systems and sub-systems. Hence, engineering support personnel are required to continually assess system safety both in existing machining centers, as well as new systems being proposed for deployment to the shop floor.

The third SME, a Facilities Management and Construction Management (FM / CM) management professional and academic, was selected to evaluate possible application of the HFHM in an environment where members of the general public as well as operations and maintenance personnel may interact with systems that require comprehensive safety evaluations. FM / CM activities include many human interactions with industrial equipment, control systems, transportation systems, and maintenance activities. As noted by the SME selected for this study, safety and human factors considerations are continually taught and emphasized throughout an FM / CM degree program curriculum, as well as in industry based on-the-job training activities. Additionally, in professional practice, system safety analysis and human factors considerations has ongoing emphasis and focus in the best-practice management philosophy of FM and CM [62][63].

The HFHM software was presented and demonstrated to the SMEs. The SMEs were then requested to test the software's functionality in their applications of interest. Following their evaluation of the HFHM, the participants responded to a survey to identify their opinions on the function and fit for purpose of the HFHM model and software. Each respondent answered an online survey utilizing standard Likert scale responses. All of the questions were worded such that the most desirable answers were in the "Strongly Agree" and "Somewhat Agree" categories. To quantify the survey responses for analytical comparison, a point system was established corresponding to each possible user response. Integer values were assigned to each response

ranging from zero (least desirable response) to four (most desirable response), with two indicating a neutral opinion. A composite score for each survey question was then calculated. The survey questions, composite scores, and response commentary are presented in **Table 25**.

Table 25: SME Survey Responses on a Likert Scale with Zero (0) Corresponding to "Strongly Disagree", Two (2) Indicating Neutral, and Four (4) Corresponding to "Strongly Agree"

SURVEY QUESTION	COMPOSITE LIKERT SCORE (OUT OF 4.0)	COMMENTS
The Human Factors Hazard Model (HFHM) has an intuitive interface, it is well organized, and can be used efficiently with minimal training and practice.	3.3	Survey participants indicated general satisfaction with the software user interface and its overall usability.
The Human Factors Hazard Model (HFHM) can be utilized in a timely manner, and is able to generate a result in a timeframe useful to a safety analyst or engineer.	3.3	Survey participants generally found the HFHM approach can be utilized in an expedient manner, resulting in timely results.
The Human Factors Hazard Model (HFHM) is an effective tool for use in analysis related to human error probability within a system design, and would be useful in driving a standardized, uniform, and comparable approach to safety analysis.	3.8	Survey participants indicated a high level of confidence that the HFHM approach would be effective in standardizing human hazard response by making results comparable and uniform.
The Human Factors Hazard Model (HFHM) has a high degree of flexibility and can be used to analyze systems ranging from those that are very simple through those that are very complex.	3.7	Survey participants indicated a high level of confidence that the HFHM approach is sufficiently flexible that analyses ranging from simple systems to very complex systems can be evaluated.
The Human Factors Hazard Model (HFHM) will facilitate an efficient approach to design and trade studies as it relates to system safety analysis, and particularly, human factors within a system design.	3.3	Survey participants indicated a general level of confidence that the HFHM approach allows for an efficient approach to design and trade studies as they relate to human factors in system safety.
The Human Factors Hazard Model (HFHM) is useful in identifying potential safety oversights, as they relate to human factors, and can be used to help guide design activities to reduce risk associated with human actors being present in a system design.	3.7	Survey participants indicated a high level of confidence that the HFHM approach will act as a guide to system design activities related to risks associated with human factors.
The Human Factors Hazard Model (HFHM) has a high level of utility, and would improve my organization's ability to predict the hazards associated with human activity within a system, and reduce overall safety risk.	3.3	Survey participants indicate a general consensus that the HFHM approach is an improvement over their current approach to Human Reliability Analysis (HRA).

As noted in the table, the survey participants were posed with seven questions pertaining to their impressions and overall assessment of the HFHM and its functionality. The first question in the survey is regarding the software interface and general usability of the model. This question was intended to exclusively solicit user satisfaction (or dissatisfaction) with regards to the user friendliness of the program. This question was used to establish if follow-up inquiries were likely required to guide design of an improved user interface for future software versions. The other survey questions were intended to support the validation of the HFHM's ability to standardize, simplify, be flexible, timely to use, and provide an overall improvement, both in functionally, as well as in overall accuracy, to the current Human Reliability Analysis (HRA) techniques being employed by the user. As summarized in the table, all respondents indicated a high level of satisfaction and confidence in the HFHM and its ability to improve human factors safety analysis in system design.

In addition to standardized survey responses, general comments regarding their individual impressions of the model were also solicited from the survey participants. Relevant input from the survey comment section includes the following observations:

- Concerns about the complicated nature of the Human Factors (HF) and System Factors (SF) data entry. It was suggested that efforts be made to simplify this process and / or add possible AI features to anticipate user intent and pre-populate Performance Shaping Factor (PSF) information. As currently constructed, the HFHM has a significant amount of data to be evaluated in each analysis, and requires an exhaustive input of data. Suggestions were made to improve how the software handles or anticipates user intent.

- Concerns about the true scalability of the model, and how well it will adapt to very simple or very complex analyses.
- Concerns about possible misuse of the model to identify and exclude potential candidate workers based on the Human Factors (HF) data entered as part of the analysis.
- The possible inclusion of a master probability scaling factor so the model could be easily "tuned" in a universal fashion by analysists for specific applications and industries.

UNCERTAINTY ANALYSIS

As with all probabilistic analyses, statistical uncertainty is present in all Human Error Probability (HEP) determinations. Uncertainty within the Human Factors Hazard Model (HFHM) allows for a maximum possible (worst case), minimum possible (best case), and most likely (nominal) probability of failure for HEP calculations. Any of these three cases can be specified by the HFHM user in their initial analysis set-up. If required, the uncertainty can be revised to any of the three cases (worst, best, nominal) after an analysis to quickly perform a "what-if" analysis of model output. As illustrated in **Figure 30**, based on user selection of best case, worst case, or most likely case, the entire series of HEPs will be calculated, and the probabilities will be reported accordingly in the HFHM. As recommended in the Technique for Human Error-Rate Prediction (THERP) [16], uncertainty in the HEP calculations is accomplished by using a basic Error Factor (EF), that is applied to the nominal (most likely) HEP value. Using the baseline most likely HEP, the maximum possible probability of failure is calculated using:

$$P_{max} = P_{nom}(EF) \quad (12)$$

Where:

P_{max} = *Maximum Event Probability*
P_{nom} = *Nominal Event Probability*
EF = *Contributing Event Probability of Failure*

Using an identical Error Factor, the minimum possible probability of failure is calculated using:

$$P_{min} = \frac{P_{nom}}{(EF)} \quad (13)$$

Where:

P_{min} = *Minimum Event Probability*
P_{nom} = *Nominal Event Probability*
EF = *Contributing Event Probability of Failure*

The Error Factors used to establish uncertainty in the model are specified by the user in one of three ways: first, when published HEP data is utilized by the program the associated Error Factor is also selected from that source data. If a probability is selected from the standard Expert Estimation values, a corresponding standard Error Factor is automatically selected for the HEP value used. For user specified entries, in addition to the HEP value entered, the analyst is also required to provide an associated Error Factor to use in the uncertainty calculation. The

HFHM analyst selects which extreme case is desired to be calculated (best or worst) and equations (12) and (13) are used to establish HEP values throughout the model, otherwise the original HEP value is utilized in the model for the most likely case.

To illustrate the functionality of the HFHM with respect to the error factors assigned to each HEP value, the uncertainty analysis of the manufacturing operation design study detailed above is evaluated. Specifically, the results of the Update 2 case of said design study are presented in **Table 26**.

Table 26: HFHM Manufacturing Operation Design Study Example – Update 2 Uncertainty Analysis Results

	PERCEPTION	COGNITION	ACTION	FEEDBACK	OVERALL
MAXIMUM PROBABILITY OF SUCCESS (BEST CASE)	1.000	1.000	0.999	1.000	0.999
NOMINAL PROBABILITY OF SUCCESS (MOST LIKELY CASE)	0.997	0.996	0.989	0.997	0.979
MINIMUM PROBABILITY OF SUCCESS (WORST CASE)	0.969	0.966	0.894	0.966	0.808

As noted in **Table 26** above, the predicted maximum probability of success (best case), nominal probability of success (most likely case), and minimum probability of success (worst case) are reported for each of the four pivotal events, namely: Perception, Cognition, Action, and Feedback. Additionally, the overall probability of success is report for each case. In this particular example, the average, or most likely probability of success for the human actor and specific Human Factors Triggering Event (HFTE), is calculated to be approximately 97.9%.

However, per the prescribed error factors, the probability of success may be as high as 99.9% (best case) and as low as 80.8% (worst case).

THE AUTOMATED HUMAN FACTORS HAZARD MODEL

Referencing Research Question 1 (RQ1) the Human Factors Hazard Model (HFHM) is intended to be a practical and simple to use analytical tool. In support of Task 4 (T4), the model is established in an established commercial software suite, and is intended to have utility in most engineering environments, with near universal application in human factors and system safety analysis.

A large number of calculations are required to establish the Performance Shaping Factors (PSFs) and associated Human Error Probability (HEP) values that feed into the individual Fault Tree Analysis (FTA) models. Additionally, the associated quantity of calculations required to establish all intermediate and top-level probabilities in the FTA and ETA networks are also voluminous. Several thousand individual calculations are required to complete any single design iteration of the HFHM. Performing these calculations manually would require a large amount of time, and would likely be prone to errors if done manually. Therefore, it was determined that the HFHM must rely on a computational platform to efficiently produce results.

The Human Factors Hazard Model Analytical Platform

The Human Factors Hazard Model (HFHM) is intended to be automated using a commercially available software package. Microsoft Excel, the spreadsheet software that is included as part of the standard MS Office software suite, has been selected to be used as the analytical foundation of the HFHM model. This decision was made for several reasons: first, MS Excel is commonly available on the vast majority of computers worldwide, second, most users are familiar with and have operational experience with the basic functionality of the

software, third, the software has the programming and computational capabilities required to perform the required calculations of the HFHM, and fourth, the software has an intuitive, user friendly interface, and can present information in a logical and easy to understand format. The structure and functional flow of the HFHM within the spreadsheet software is presented in **Figure 30**.

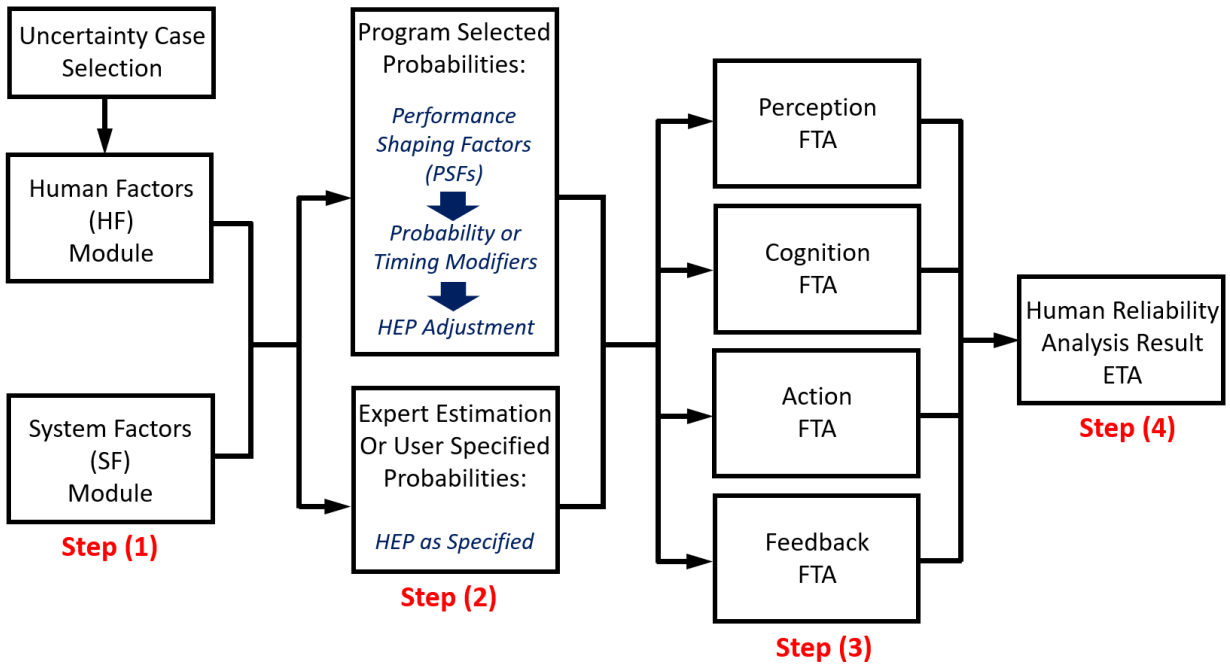


Figure 30: HFHM Software Functional Flow Diagram

As illustrated in **Figure 30**, step (1) includes the primary user interface where information specific to the human factors being analyzed, as well as characteristics of the system design that are entered into the program. The information specified at this step is typically derived from three possible sources. These include:

- Source material (literature derived values from established HRA methods or documented human behavior databases).
- Expert Estimation values based on standardized value of HEP.
- User defined values as determined by the specific hazard scenario circumstances, experimentally derived data, or custom determined human error probabilities.

For program selected probabilities that pull HEP data from published sources, Step (2) includes the algorithms that utilize the human factor (HF) and system factor (SF) data to define the relevant PSF's used to modify the various HEP's that are then passed to the FTAs of the four pivotal events. As previously discussed, the PSF modifying factors used to adjust baseline HEP values are defined in equations (1) and (2) above. If Expert Estimation or user specified probabilities are specified in Step (1), then the HEP data flows directly into Step (3) without modification. Step (3) includes all four FTAs used to predict the likelihood of failure due to the corresponding pivotal events, namely: Perception, Cognition, Action, and Feedback. The probabilities calculated in the FTAs of Step (3), are then passed to the Event Tree Analysis (ETA) in Step (4) to establish the overall probability of success (and failure) attributable to the human actor's response the hazard event.

As with all probabilistic analyses, statistical uncertainty is present in all HEP determinations. Uncertainty within the Human Factors Hazard Model (HFHM) allows for a maximum possible (worst case), minimum possible (best case), and most likely (nominal) probability of failure for Human Error Probability (HEP) calculations. Any of these three cases can be specified by the HFHM user in their initial analysis specification. As noted above, subsequent iterations of a given analysis can be quickly switched between all three uncertainty

scenarios for an efficient way to evaluate the variation due to Error Factors applied to the HEP values. As illustrated in **Figure 30**, based on user selection of best case, worst case, or most likely case, the entire series of HEP will be calculated and the probabilities will be reported accordingly in the HFHM.

The HFHM / MS Excel User Interface

The Human Factors Hazard Model relies upon the standard user interface present in MS Excel. However, numerous customizations and improvements have been made to streamline and simplify the specification of human and system factors as well as user interaction with other analytical features of the model. Additional functionality has been added to the model such that, if desired, the user can customize individual event probabilities within the four pivotal event Fault Tree Analysis (FTA) modules. The various data communication and productivity features present in the user interface of the HFHM include:

- "Fly-out" help features, including definitions and instructions for each PSF entry associated with the human factors and system features modules.
- Where applicable, three separate modes of PSF specification, including:
    - PSF from published HEP sources.
    - User specified HEP per the embedded Expert Estimation HEP scale values provided in the HFHM.
    - Custom HEP data as specified by the user. This data can be based on a more refined Expert Estimate activity, specialized knowledge of the particular PSF, or derived from empirical data if available.

- “Radio-button” customization of each pivotal event FTA, such that the user can intervene at any basic, intermediate, or top-level event with specific HEP data, superseding any automatically calculated hazard event probabilities.
- Graphical layout of the FTA and Event Tree Analysis (ETA) processes for user friendliness in troubleshooting analyses.
- Embedded pictorial FTA flow charts for user quick reference during analysis evaluation.

A detailed summary of the HFHM MS Excel user interface is available for reference in **APPENDIX B**.

APPLICATION OF THE HUMAN FACTORS HAZARD MODEL WITHIN CONVENTIONAL HAZARD ANALYSIS TECHNIQUES

Referencing Research Question 2 (RQ2), the proposed Human Factors Hazard Model (HFHM) is intended to improve established system safety Hazard Analysis Techniques (HATs). In support of Tasks 1 and 2 (T1 and T2), a strategy for implementation of the HFHM within existing HATs is proposed with reference to expected outcomes by accounting more thoroughly and accurately for human factors within system safety.

Most of the academic research in the field of human factors engineering being cited in this work was developed and documented over the past several decades. The initial research, dating back approximately to the 1960's and 1970's, was where the first extensive efforts were made to establish human performance baselines with respect to engineered systems [14]. Human actors within complex systems and system contexts such as nuclear powerplants, defense related systems, space systems etc. were the original sources of inspiration for determining and documenting human reliability, and how it relates to system safety. The human factors assessments originally developed for these industries are finding their way into other system design activities. Although the primary research focus of this current effort was intended to provide a new approach to Human Reliability Analysis (HRA) via the HFHM, a related investigation addresses the application of the HFHM results within established Hazard Analysis Techniques (HATs). This effort is to better coordinate and integrate system safety analysis that includes all areas of concern with regards to reliability and risk assessment within lifecycle management. The HFHM is intended to be a standardized and near universal analysis technique

that can implemented in classic hazard analysis with simplicity, providing a consistent approach to the evaluation of role human actors within a system context.

The proposed HFHM has direct application within some of the established HATs that have been in use for many decades in system safety analysis [14]. By including HFHM results within the system safety analyses performed using the traditional methods, a better understanding of system risk due to human factors can be determined. Any HAT that allows for the inclusion of human factors considerations, and particularly is used to evaluate the likelihood or probability of occurrence of a failure related to human interaction within system operations is a potential candidate for inclusion of the HFHM results. The analysis characteristics of common HATs and possible HFHM application are presented below in **Table 27**. Specific HATs that are identified as potentially compatible with HFHM results are highlighted in yellow.

Table 27: Common Hazard Analysis Techniques

HAZARD ANALYSIS TECHNIQUE (HAT)	HAZARD ANALYSIS TYPE	INDUCTIVE (I) DEDUCTIVE (D)	QUALITATIVE (L) QUANTITATIVE (N)	HAZARD ANALYSIS BASED ON LIKELIHOOD OF OCCURRENCE	APPLICATION USING HFHM RESULTS
FHA	PD,SD	I	L	Y	Y
PHL	CD	I,D	L	N	N
PHA	PD	I,D	L	Y	Y
SSHA	DD	I,D	L	Y	Y
SHA	SD	I,D	L	Y	Y
O&SHA	OD	I,D	L	Y	Y
HHA	HD	I,D	L	Y	N
RHA	RD	N/A	L	N	N
EHA	DD	I,D	L	Y	N
FTA	SD	D	L,N	Y	Y
FMEA	DD	I	L,N	Y	Y
FMECA	DD	I	L,N	Y	Y
HAZOP	PD	I	L	Y	Y
ETA	SD	D	L,N	Y	Y
CCA	SD,DD	D	L,N	Y	Y
CCFA	SD,DD	D	L	Y	Y
SwHA	SD	I,D	L	N	N
PHA	DD	I,D	L,N	Y	Y
THA	OD	I,D	L,N	Y	Y
FHA	DD	I,D	L,N	Y	Y
SCA	SD,DD	I,D	L,N	N	N
MA	SD,DD	D	L,N	Y	Y
PNA	SD,DD	D	L,N	Y	Y
BA	SD	I	L	Y	N
BPA	DD	D	L	Y	N
MORT	SD,DD	D	L,N	N	N
JHA	OD	I,D	L,N	Y	Y
THA	SD	I,D	L,N	Y	Y
SoSHA	SD	I,D	L,N	Y	Y

As identified in the table above, the probability of an accident occurring due to the results calculated using the HFHM can be directly applied in many HATs as the guiding factor in the Initial Mishap Risk Index (IMRI), Final Mishap Risk Index (FMRI), or other Risk categories as defined in each specific HAT. In the scope of this research project, two different HATs with possible HFHM application have been identified and selected for a detailed analysis and proposed approach for integration. Based on the author's professional experience, the most

commonly used HATs are the Failure Mode and Effects Analysis (FMEA) / Failure Mode, Effects and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA) methods. Therefore, these two methods have been evaluated, with strategies identified for integration of the HFHM results into the larger hazard analysis approach.

Fault Tree Analysis Applications for HFHM Integration

In the case of a Fault Tree Analysis (FTA), the probability of an accident can be determined using the results of Human Factors Hazard Model (HFHM) as one of the basic triggering events, as noted in the larger probability logic network. Each individual HFHM result for a specific Human Factors Triggering Event (HFTE) will be included as an entry-level element in the fault tree structure, and the combined probability of failure (or reliability) can be calculated directly. Due to the fact that an FTA accounts for the joint probabilities of different events within a logical organization, representing the interplay of various system components, multiple HFHM results can be evaluated and included in the larger sub-system or system analysis. To illustrate this concept, an example FTA showing the inclusion of the HFHM results is illustrated in **Figure 31**.

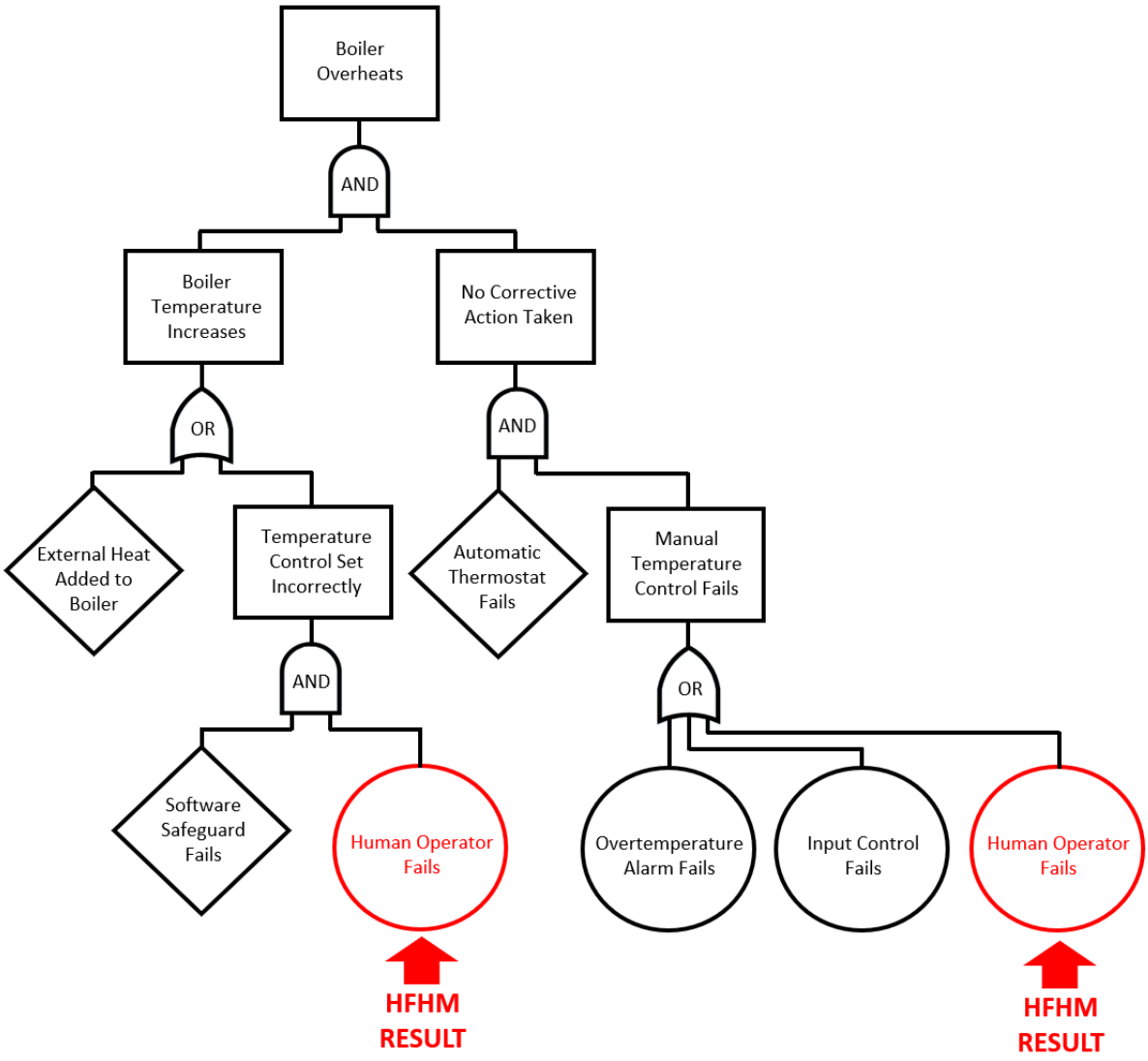


Figure 31: Example FTA (Boiler Over Temperature Event)

As illustrated in the FTA, the specific hazard event being evaluated is the undesired, and potentially hazardous overheating of a boiler in a system design. The hazard event top-level undesired outcome is the result of two simultaneous intermediate events, these being excessive heat being added to the boiler, and a failure of a required corrective action. As identified and noted in the FTA, both of these individual intermediate events have contributing human factors considerations. The contribution of the human actor to the hazard scenario could be ignored with

the FTA only considering the software-electrical-mechanical components identified. However, inclusion of the HFHM results, with an accurate accounting of the human factors contribution to the hazard event, will result in a much more accurate risk assessment.

In summary, any location in the FTA logic network, where human interaction with a system design can result in an accident / mishap, the HFHM results may be used to represent basic event probability in that FTA failure path. Subsequent analysis of the FTA can also include such diagnostic efforts as cut-set and path-set decomposition of the logic network [14]. A cut-set analysis is used to establish a group of initiators (basic events) that may include the human actor, which if all occur simultaneously, will result in a failure at the top-level within the logic network. The minimal cut-set represents the least group of initiators, which if they all occur, result in top-level failure. Additional quantitative analysis of the cut-set results can be used to detect high vulnerability combinations and single-point failures within the FTA logic. Conversely, a path-set analysis is used to establish a group of initiators which if none occur, the entire FTA logic network is guaranteed to not suffer a top-level failure. Therefore, a thorough FTA model, including all relevant human factors probabilities as calculated by the HFHM can be used to mitigate or eliminate potential hazards attributable to human behavior from the system design. This approach will also identify possible human actor related single-point failures which would be candidates for the implementation of system design redundancies or other safeguards.

Failure Mode and Effects Analysis Applications for HFHM Integration

In the case of the Failure Mode and Effects Analysis and the very closely related Failure Mode Effects and Criticality Analysis (FMEA / FMECA) approach to hazard analysis, the probability of failure due to a human actor interacting with the system can be directly accounted

for as part of the Risk Priority Number (RPN) calculated and tracked in the analysis worksheet. The RPN is composed of three different factors, which are defined as:

- Severity (S), which corresponds to the seriousness of a mishap should it occur. Typically, a score of 1 would correspond to a mishap that is considered minor, where a score of 10 would correspond to a mishap that has catastrophic consequences.
- Occurrence (O), which corresponds to the likelihood that a particular mishap will occur. Typically, a score of 1 would indicate that the event is very unlikely to occur and a score of 10 would indicate the probability of occurrence is very high.
- Detection (D), which corresponds to the likelihood that a particular mishap will be detected prior to it occurring and contributing to accident. Typically, a score of 1 would indicate that the hazard will typically be detected before it can occur, where a score of 10 would indicate that there is very little chance the hazard can be detected prior to it contributing to an accident / mishap.

Based on the three factors described above, the RPN calculation is of the form:

$$RPN = (S)(O)(D) \tag{14}$$

Where:

RPN = *Risk Priority Number*
S = *Hazard Severity*
O = *Hazard Occurrence*
D = *Hazard Detectability*

A follow-on calculation that is of use in the safety analysis related to FMEA / FMECA is the Criticality Number (CN) which is used to quantify only the effects of the Severity (S) and Occurrence (O). The Detectability (D) is not considered in determination of the CN such that it identifies the relative seriousness of the hazard regardless of whether it is detected or not prior to the accident / mishap. The CN calculation is of the form:

$$CN = (S)(O) \tag{15}$$

Where:

CN = *Criticality Number*
S = *Hazard Severity*
O = *Hazard Occurrence*

Failure probabilities related to Human Error Probability (HEP), as calculated by the Human Factors Hazard Model (HFHM), are accounted for in the FMEA / FMECA analysis. An example of an FMEA analysis related to the example Fault Tree Analysis (FTA) detailed in **Figure 31** is presented in **Table 28**.

Table 28: Example FMEA (Boiler Over Temperature Event)

Potential Failure Mode	Potential Failure Cause	Potential Effect(s) of Failure	Severity (S)	Occurrence (O)	Detection (D)	RPN (SxOxD)
External heat added to the boiler.	Improper ventilation or cooling of boiler room environment.	Boiler temperature increases above tolerance limits.	6	2	2	24
Software safeguards fail to stop high temperature set point.	Programming error in control system.	Boiler temperature increases above tolerance limits.	6	2	2	24
Operator specifies an incorrect temperature setting.	Human operator keypad entry mistake or lack of understanding of temperature setting requirements.	Boiler temperature increases above tolerance limits.	6	1	2	12
Thermostat fails to detect overtemp and command a cool-down.	Thermostat functional malfunction.	Corrective action not taken with regards to boiler temperature increase.	10	2	2	40
Overtemp alarm does not alert operator.	Defective alarm or sensor.	Operator is not alerted to take corrective action.	8	1	2	16
Manual temperature control does not initiate a boiler cool-down cycle.	Input control malfunction.	Corrective action not taken with regards to boiler temperature increase.	10	2	2	40
Operator fails to initiate manual control of boiler cool-down cycle.	Human error due to distraction or lack of understanding of an over-temperature scenario.	Corrective action not taken with regards to boiler temperature increase.	10	4	4	160

As highlighted in yellow in **Table 28**, two individual failure modes are identified as having direct correlation to Human Reliability Analysis (HRA). All three RPN factors will rely upon the HFHM result to provide guiding information. Potential mishap Severity (S) and Detection (D) may be inferred from the HFHM result. However, the Occurrence (O) factor, as

noted by the arrows in **Table 28**, will have direct numerical correlation to the risk of mishap associated with the HFHM result. The correlation of the Occurrence (O) factor to an actual probability of failure as determined by the HFHM is determined with an equivalency to a ranking. An example of a typical risk ranking matrix for use in conjunction with the FMEA / FMECA is presented in **Table 29**.

Table 29: Typical FMEA Risk Ranking Scores

SEVERITY (S)		
EFFECT	**CRITERIA (SEVERITY OF EFFECT)**	**RANKING**
Hazardous - Without Warning	Very high severity ranking when a potential failure mode affects safe system operation and/or involves non-compliance with governmental regulations without any warning.	10
Hazardous - With Warning	Very high severity ranking when a potential failure mode affects safe system operation and/or involves non-compliance with governmental regulations with a warning.	9
Very High	System / Sub-System / Component inoperatble with loss of primary function.	8
High	System / Sub-System / Component operable, but performance levels are severly compromised.	7
Moderate	System/ Sub-System / Component operable but performance is signficantly reduced.	6
Low	System/ Sub-System / Component operable but performance is noticably impacted. Defect is sure to be noticed.	5
Very Low	System/ Sub-System / Component operable but performance is marginally impacted. Defect is likely noticed.	4
Minor	System/ Sub-System / Component operable but performance is minorly impacted. Defect likely noticed by average operator.	3
Very Minor	System/ Sub-System / Component operable and performance is nearly optimal. Defect likely noticed by exerienced and/or discriminating operator.	2
None	No adverse effect.	1

OCCURRENCE (O)		
PROBABILITY OF FAILURE	**POSSIBLE FAILURE RATES**	**RANKING**
Very High - Inevitable	≥ 1 in 2	10
	1 in 3	9
High - Repeated	1 in 8	8
	1 in 20	7
Moderate - Occasional Failures	1 in 80	6
	1 in 400	5
	1 in 2,000	4
Low - Relatively	1 in 15,000	3
	1 in 150,000	2
Remote - Failure Is Unlikely	≤ 1 in 1,500,000	1

DETECTION (D)		
DETECTION	**LIKELIHOOD OF DETECTION**	**RANKING**
Absolute Uncertainty	Issue will most likely not be detected at the design, manufacturing, inspection, assembly, or operation level.	10
Very Remote	Very remote chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	9
Remote	Remote chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	8
Very Low	Very low chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	7
Low	Low chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	6
Moderate	Moderate chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	5
Moderately High	Moderately high chance issue will be detected at the design, manufacturing, inspection, assembly, or operational level.	4
High	High chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	3
Very High	Very high chance issue will be detected at the design, manufacturing, inspection, assembly, or operation level.	2
Almost Certain	Issue will most likely be detected at the design, manufacturing, inspection, assembly, or operation level.	1

The risk scoring system noted in **Table 29** is adapted from an RPN index developed by General Motors [6]. Note that the risk rankings with equivalent definitions and assigned

probabilities are somewhat arbitrary, and would be specifically defined by an analyst or organization with unique knowledge of the system and human factors characteristics.

HFHM Integration using Other HAT Approaches

As noted above, results of the Human Factors Hazard Model (HFHM) are integrated within established Hazard Analysis Techniques (HATs), to determine failure risk associated with system operation. Specific examples include HFHM integration within Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis / Failure Mode Effects and Criticality Analysis (FMEA / FMECA), where hazard risk associated with a Human Factors Triggering Event (HFTE) is accounted for in the larger risk analysis of the system design. However, as identified in **Table 27**, several other commonly utilized Hazard Analysis Techniques (HATs) are amenable to integration of Human Reliability Analysis (HRA), and more specifically application of the Human Factors Hazard Analysis (HFHM). A short summary of the features of the HAT that would indicate its ideal compatibility with the HFHM results include the following:

- System or sub-system level analysis.
- By default, human factors are considered in the HAT, or the analysis has the ability to easily include human factors in the analysis process without significant modifications to the basic approach.
- Ability to integrate quantified risk into the overall safety assessment.
- Ability to apply probability of failure into a ranking or other actionable directive to guide lifecycle design activities.

Note that these criteria are a guideline for HAT integration of the HFHM. Each application of the HFHM into HAT is case specific, and there is not a universal guide for the integration of HRA into classic hazard analysis.

INTEGRATION OF THE HUMAN FACTORS HAZARD MODEL WITHIN MODEL-BASED SYSTEMS ENGINEERING

Referencing Research Question 3 (RQ3), application of the Human Factors Hazard Model (HFHM) within Model-Based Systems Engineering (MBSE) has additional advantages beyond its application in system safety analysis and inclusion in various traditional Hazard Analysis Techniques (HATs). In support of Task 1 (T1), emerging modeling extensions to the Systems Modeling Language (SysML) are becoming available for general use in the Systems Engineering field. Additionally, as part of this study, standard Unified Modeling Language (UML) profiles, with application relative to the incorporation of the HFHM, have been identified and adapted as part of this research effort. In support of Task 2 (T2), a general approach for implementation of the HFHM into SysML has been developed and verified. In support of Task 3 and 4 (T3 and T4), the unique HFHM profiles developed in SysML are intended to be stereotypes that are easily reused and are linked directly into requirements management approaches consistent with MBSE.

Model-Based Systems Engineering (MBSE) is a Systems Engineering (SE) paradigm that formalizes the use of models throughout the systems engineering lifecycle. The literature asserts various advantages in the application of MBSE in system lifecycle architecting and design activities. Unlike the document-based approach to systems engineering, MBSE establishes an integrated and coherent virtual model, with clear and unambiguous representation of the system context and design [31][33][59]. MBSE is the recommended approach to lifecycle management as proposed by the International Council on Systems Engineering (INCOSE), as well as a growing number of government entities and industry partners [57].

MBSE paradigms require more focus on a single, shared model, which exists as the one version of the system configuration and design, and must represent all relevant aspects of the system [32][33]. For systems that include human factors and safety requirements, MBSE approaches must include models of human factors and system safety, in keeping with the 'model-centric' philosophy of MBSE [57].

Human capabilities and their implications for design, deployment, operation, and maintenance of systems are under researched in systems engineering in general, and in MBSE in particular [58][60]. Currently, a limited number of techniques and tools exist to effectively and efficiently implement comprehensive Human Reliability (HRA) within system-wide safety analyses, and no widely cited or standardized methods exist within the structure of Model-Based Systems Engineering (MBSE). Efforts are currently underway to develop standardized software tools to effectively integrate and manage system reliability and safety analysis within MBSE. Beginning in 2016, the Object Management Group (OMG), which is an international software standards consortium, has been working to establish a common approach to modeling reliability within the system safety domain. These efforts include standardized tools for use in developing Fault Tree Analysis (FTA) as well as Failure Mode and Effects Analysis (FMEA) within SysML. Other reliability and safety methods being explored for integration include Hazard and Risk Analysis (HARA), Goal Structured Notation (GSN), and System Theoretic Process Analysis (STPA). The current family of analytical tools are being produced by the commercial software company No Magic. As a result of these current development efforts, a new reliability modeling standard is being developed, and is in a pre-release beta configuration for user evaluation. This standard is called Risk Analysis and Assessment Modeling Language (RAAML). This new RAAML standard provides functional libraries in the Unified Modelling Language (UML) for

use in conjunction with the System Modeling Language (SysML) extension [28][29][30]. So, although the integration of reliability engineering into modern modeling languages is nascent, the connection of HRA to the modern tools of systems engineering has not been demonstrated to date.

Based on this understanding of the field, this work proposes to implement a Human Factors Hazard Model (HFHM) within SysML. The HFHM uses a quantitative approach to HRA to estimate the probability of an accident due to a human actor's interaction with system operations [9]. This new approach implements aspects of the HFHM within profiles provided by RAAML, and develops and demonstrates a unique profile within SysML for the modeling of human reliability in systems engineering applications.

Implementation of the Human Factors Hazard Model into SysML

This section describes the implementation of the HFHM within SysML, with the goal of enabling the accuracy, efficiency, reusability, and completeness that are the hallmarks of SysML-enabled MBSE processes. The HFHM is constructed using add-on profile libraries that are part of the recently developed Risk Analysis and Assessment Modeling Language (RAAML) extension. RAAML includes the essential modeling standards related to commonly applied Hazard Analysis Techniques (HATs) including FTA. The SysML model developed for the HFHM was designed for reuse such that any new analysis can directly implement all stereotypes documented here. The reliability model developed in SysML models all four individual pivotal event FTAs (Perception, Cognition, Action, Feedback), and shares the respective failure probabilities with the subsequent ETA where the top-level event probability of success and failure are documented. A schematic illustrating the basic structure and flow of information

within the SysML model, specifically as it relates to reliability and safety engineering, is presented in **Figure 32**.

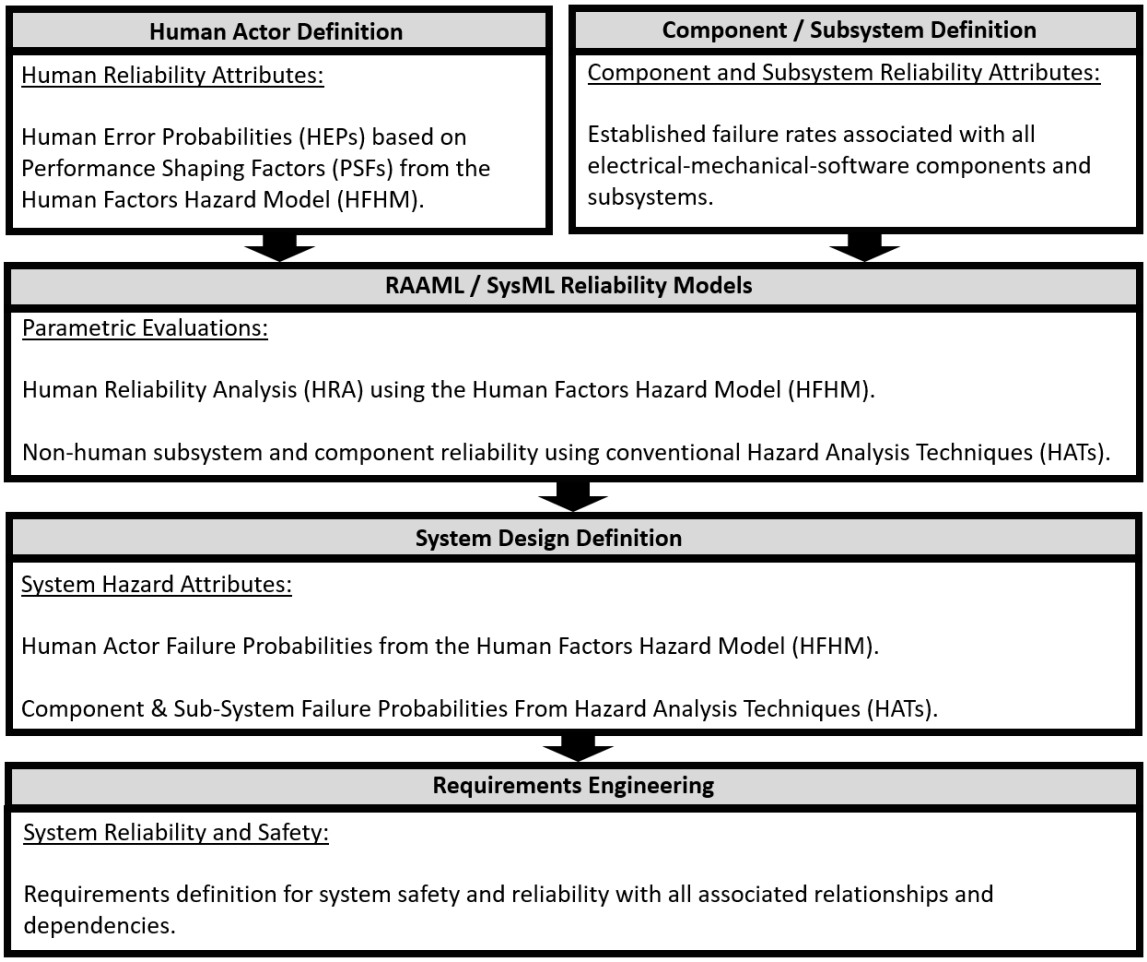


Figure 32 – Reliability and Safety Engineering Data Flow within the SysML Model

As implemented here, Performance Shaping Factors (PSFs) and Human Error Probabilities (HEPs) are calculated in the MS Excel software. These HEP values are output in a format that can be directly read into instance tables within the SysML model. Each pivotal event (Perception, Cognition, Action, and Feedback) has its own individual table that represents the

instance / implementation of that event, and provides basic event probabilities into the FTA which is implemented in RAAML. The values determined for each pivotal event are then evaluated in an ETA which is implemented as a separate and unique profile within SysML. This output of the ETA determines the likelihood of failure at the perception, cognition, action, and feedback steps, as well as the likelihood of top-level success (or failure) for the human actor. The HFHM / MBSE interface was developed using the Cameo Systems Modeler.

Construction of Fault Tree Analysis Logic Networks using the Unified Modeling Language Profile Library

To develop the Fault Tree Analysis (FTA), an events catalog is modeled as a SysML Block Definition Diagram (BDD). By reusing and applying appropriate stereotypes from the Unified Modeling Language (UML) profile library, series events are categorized. The parent event categories are specified as basic events, intermediate events, and top-level events which represent the four pivotal events. These parent events correspond to the representative events as established in the Fault Tree Analysis (FTA) logic networks specified in the Human Factors Hazard Model (HFHM). The characteristics of these parent events are inherited across the series of events, using a generalization relationship, such that reusability and repeatability are facilitated. The basic model structure related to the catalog of events is presented in **Figure 33**.

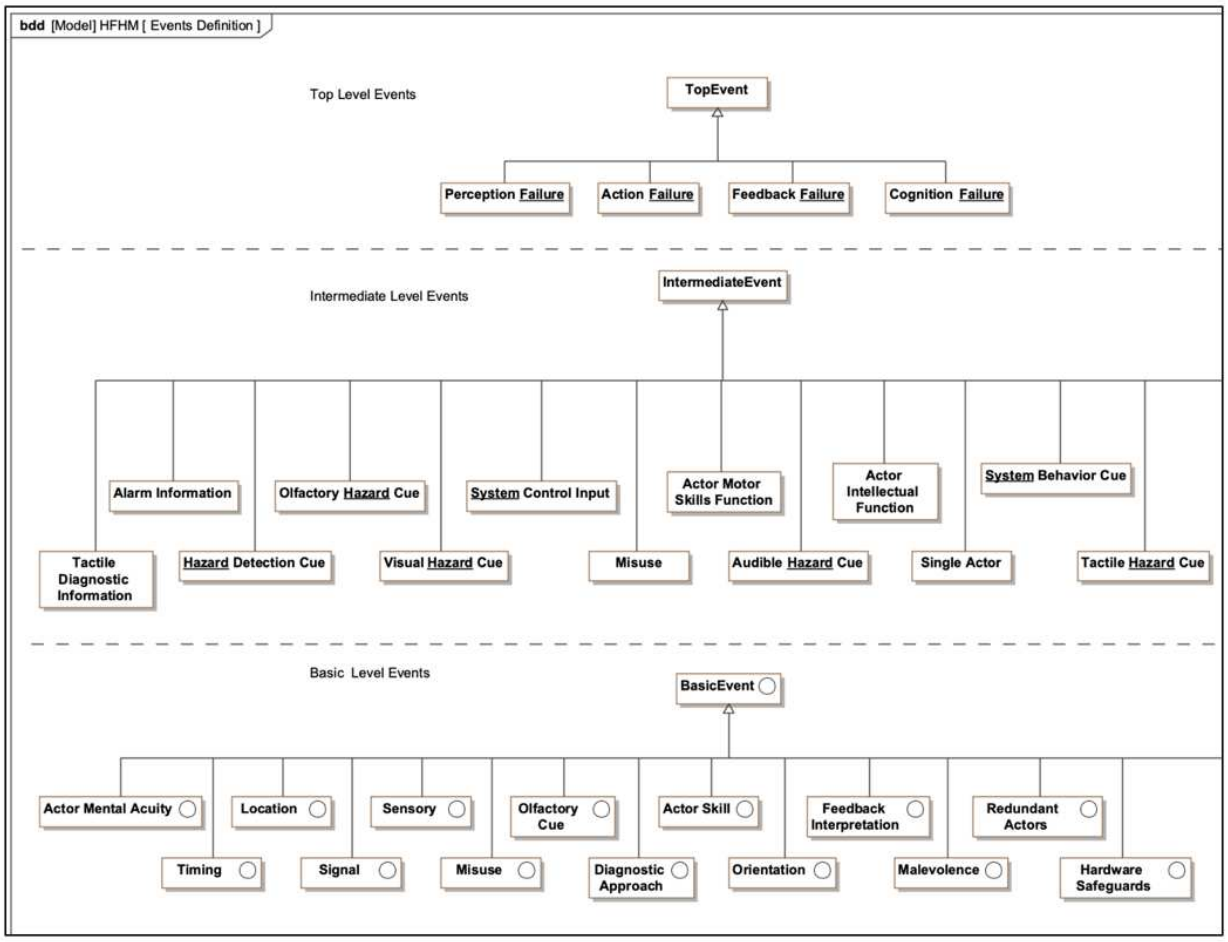


Figure 33 - Block Definition Diagram of the Catalog of Events for the HFHM

The top-level pivotal events, as defined in their associated FTA network, are modeled as blocks in a SysML BDD. The associated probability characteristics of each FTA is inherited from the respective <<FTATree>> stereotype [28][29]. The specific model structure associated with the <<FTATree>> stereotype is presented in **Figure 34**. Note that all four HFHM pivotal event FTAs utilize this stereotype to establish their basic, intermediate, and top-level event definition and structure. Each part includes probabilities associated with basic and intermediate events, and relevant logic gates (AND/OR), which provide the required logical relationships necessary to perform calculations within each FTA. This stereotype definition provides a

"black-box" modeling experience, as all relevant FTA structure can be selected, implemented, and reused by the system engineer / modeler, without concern as to the detailed model structure and function required to establish the respective pivotal events in a system safety analysis.

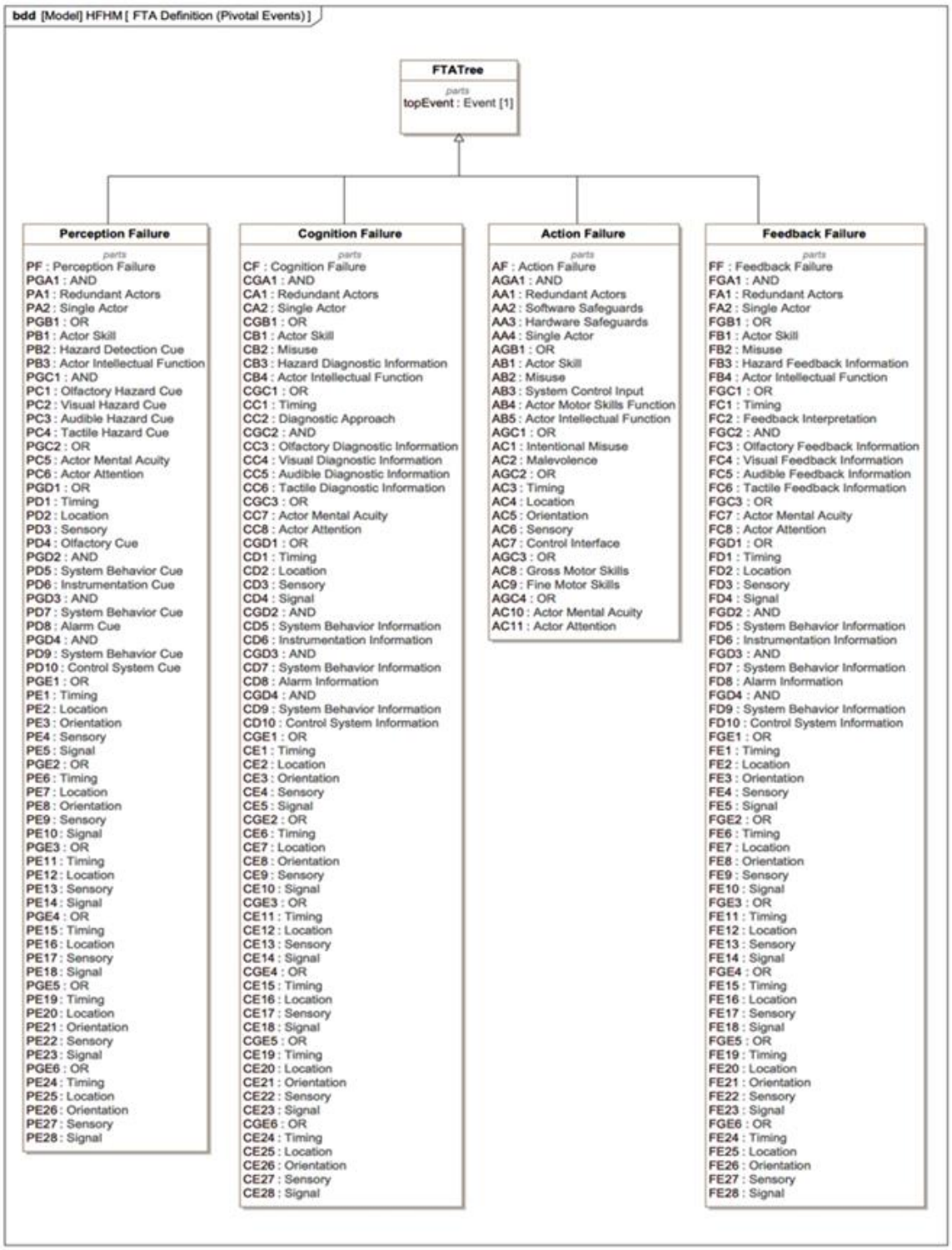


Figure 34 - <<FTATree>> Stereotype with Indentured Top-Level Pivotal Event Parts

The <<FTATree>> stereotype includes the required analytical model for each of the pivotal event FTA logic networks (Perception, Cognition, Action, and Feedback). An Internal Block Diagram (IBD) in SysML is used to establish the analytical relationship between each basic event, intermediate event, and top-level event, including all relevant logic gates in the model structure. The IBD represents the interconnections and interactions between all events and logic gates representing the FTA. The IBD related to the Action pivotal event is presented in **Figure 35**, which is the SysML equivalent of the FTA diagram presented in **Figure 22**. Although not shown, the three other pivotal event FTAs (Perception, Cognition, and Feedback) use an identical approach with a similar IBD to specify them within SysML.

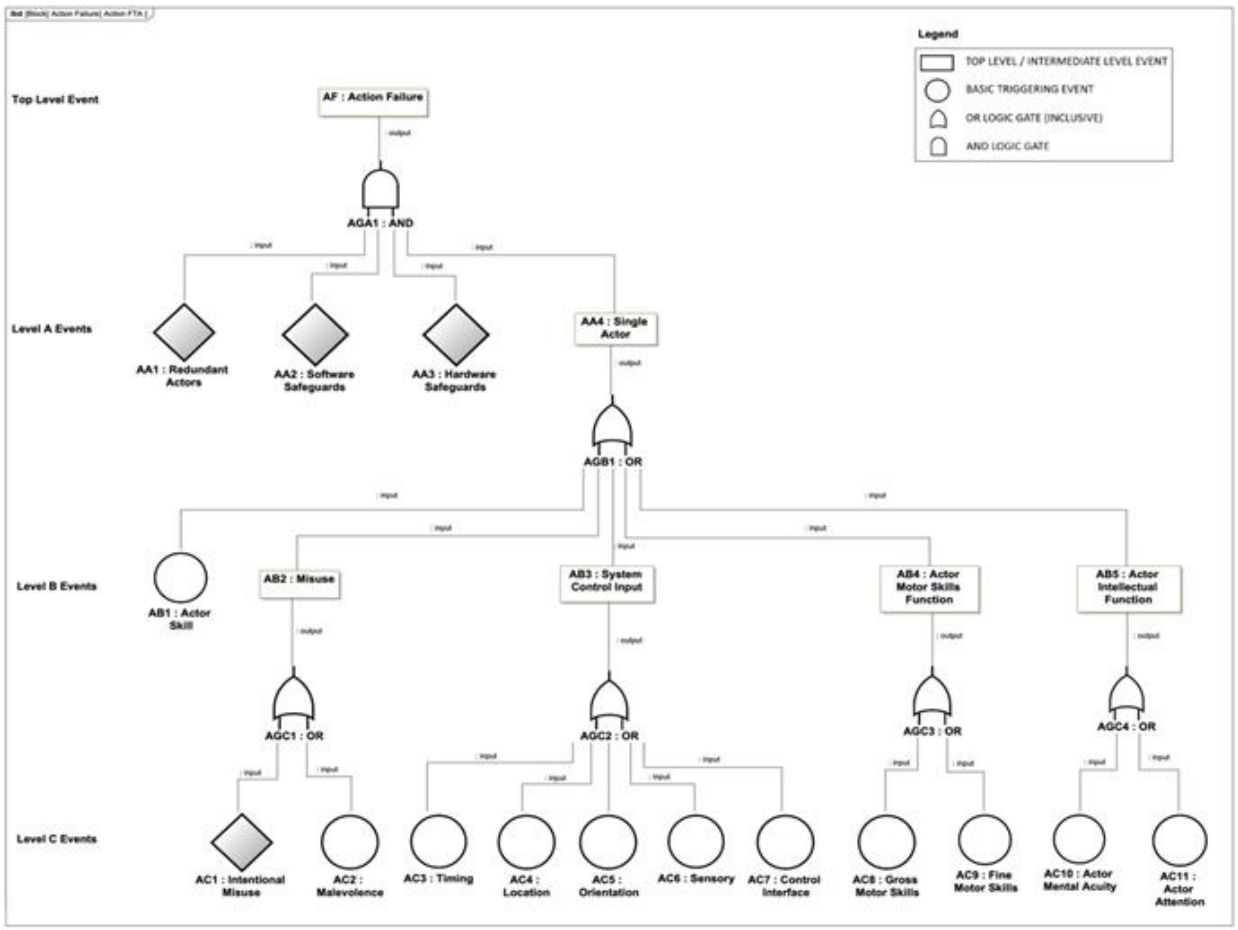


Figure 35 – SysML Action Pivotal Event Fault Tree

The mathematical basis that governs the AND / OR logic gates within the FTA network is defined by constraint blocks within the SysML model. Each constraint block receives an input from a source, which provides the lower-level probability of failure from a basic or intermediate event. The corresponding output of the same constraint block provides the calculated combined probability to the target block, which is the next higher intermediate or top-level event. The "AND" logic gate constraint block structure is presented in **Figure 36** and the "Inclusive-OR" logic gate constraint block structure is presented in **Figure 37**.

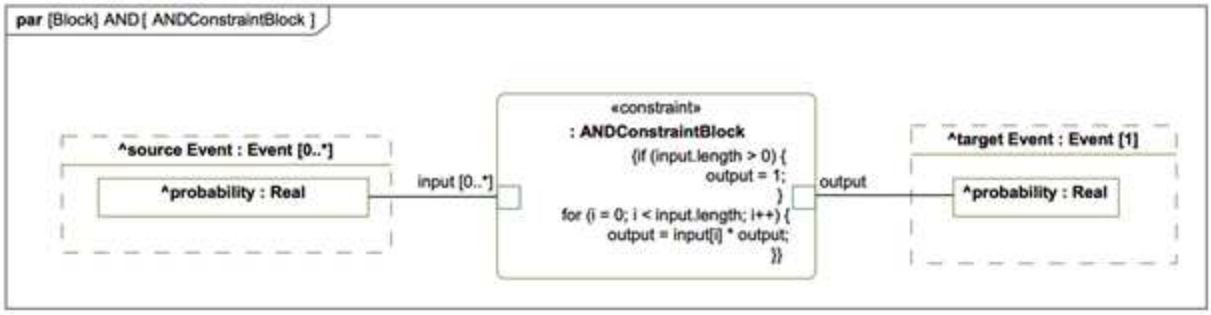


Figure 36 – Mathematical Basis for the AND Logic Gate (Constraint Block Structure)

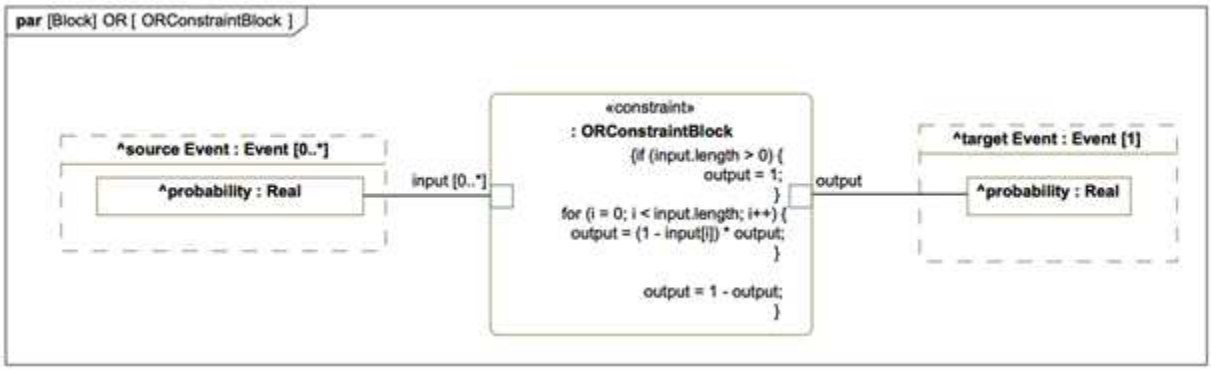


Figure 37 – Mathematical Basis for the Inclusive OR Logic Gate (Constraint Block Structure)

The probability of failure for each top-level event, in their respective FTA, is evaluated recursively beginning with the basic events at the entry level of the FTA logic network. The individual basic event failure probabilities are exported from SysML as instances, which are stored in associated instance tables. An example of an instance table corresponding to the Action pivotal event FTA as illustrated in **Figure 36** is presented in **Figure 38**. All other pivotal event FTAs have similar instance tables associated with them.

Criteria

Classifier: ısicEvent, IntermediateEvent, TopEvent ... Scope (optional): Action Failure

#	Name	probability : Real
1	AF	0.125
2	AA1	0.5
3	AA2	0.5
4	AA3	0.5
5	AA4	1
6	AB1	0.5
7	AB2	0.75
8	AB3	0.938
9	AB4	0.75
10	AB5	0.75
11	AC1	0.5
12	AC2	0.5
13	AC3	0.5
14	AC4	0.5
15	AC5	0.5
16	AC6	0.5
17	AC7	0.5
18	AC8	0.5
19	AC9	0.5
20	AC10	0.5
21	AC11	0.5

Figure 38 – Instance Table for Action Pivotal Event (Including Sample Input and Calculated Probabilities of Failure for all Events)

The default values for the probability of failure associated with each basic event are typed for these instances as shown in **Figure 39**. The same approach is repeated to represent the executed results of all FTAs associated with the other three pivotal events to establish the input values for all basic events.

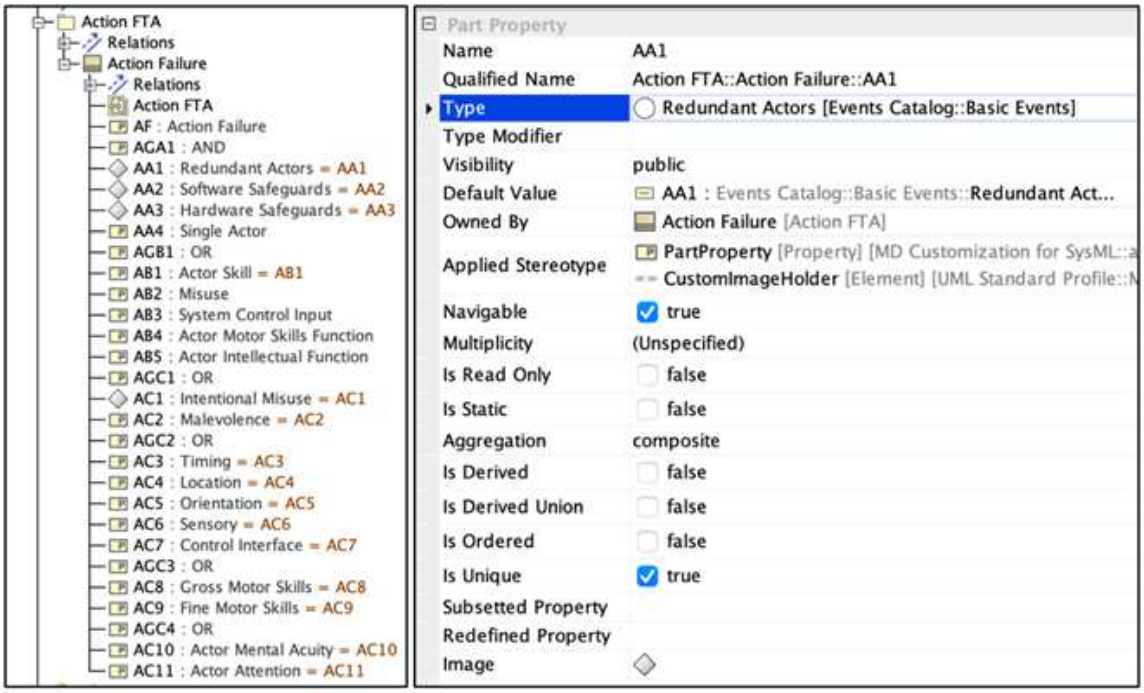


Figure 39 – Definition of Default Values for Basic Events by Instance

The result of these activities is an executable SysML model of the four pivotal event FTAs. When the modeler can input the conditions of the operation of the human actor, the SysML HFHM model FTAs output the probabilities of failure for each of the four pivotal events.

Construction of the Event Tree Analysis Logic Network using the Unified Modeling Language

With the pivotal event probabilities defined, the Human Factors Hazard Model (HFHM) uses an Event Tree Analysis (ETA) to model the successive probability of each pivotal event occurring in the order defined in **Figure 14**. The result of this ETA is an evaluation of the probability of the human actor successfully resolving the hazard event. ETA functionality was developed using default SysML libraries.

To model the ETA, a Block Definition Diagram (BDD) is created, composed of individual constraint blocks. Each constraint block is characterized using expressions and parameters used to calculate the probability of success and failure for each individual pivotal event, and the likelihood of a final successful outcome. The constraint blocks, as defined, can be reused as constraint properties typed with the appropriate blocks. The BDD representing the ETA is presented in **Figure 40**.

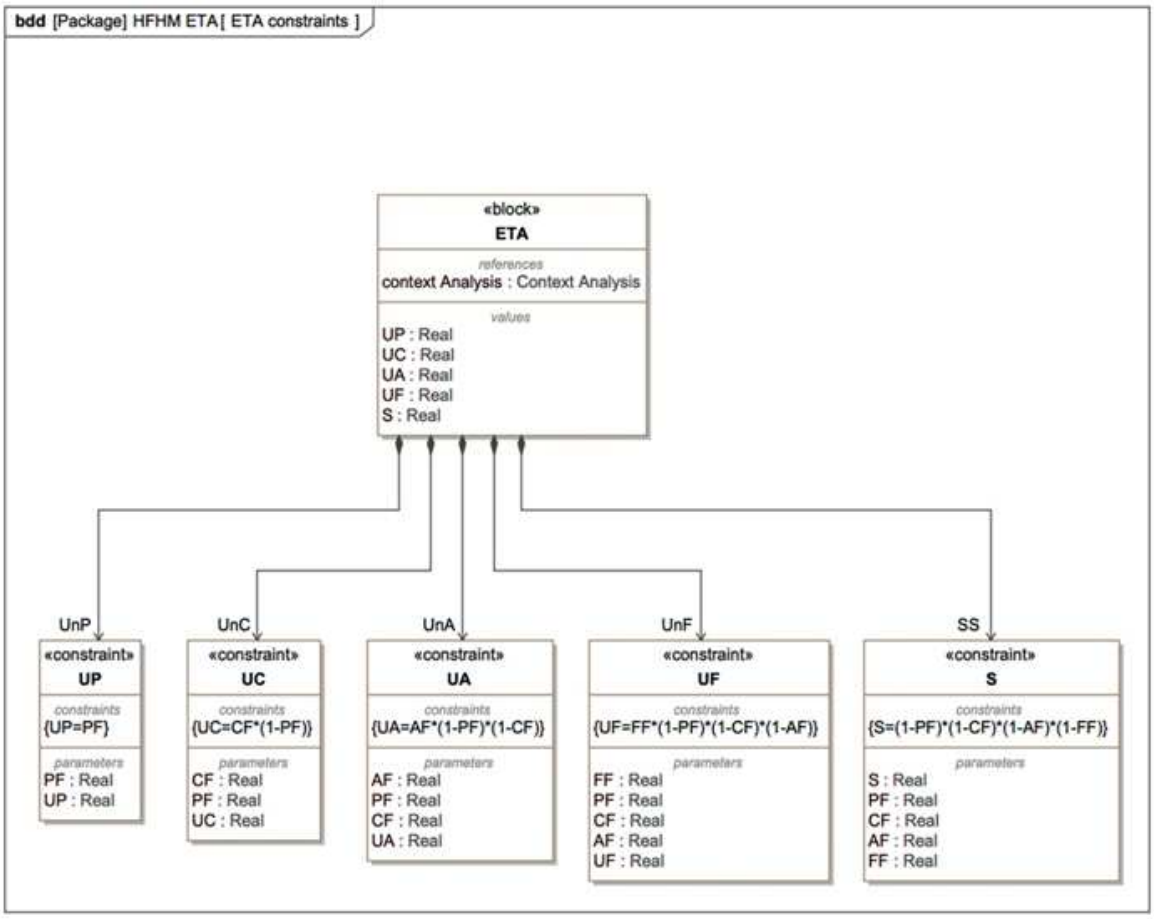


Figure 40 – BDD of Constraint Blocks for the ETA

In addition, an overarching context analysis block is created in a BDD to provide a basis for automating the execution of the FTAs and for integrating those results into the ETA. All four of the individual FTA blocks, representing each pivotal event, are composed within the context analysis as presented in **Figure 41**.

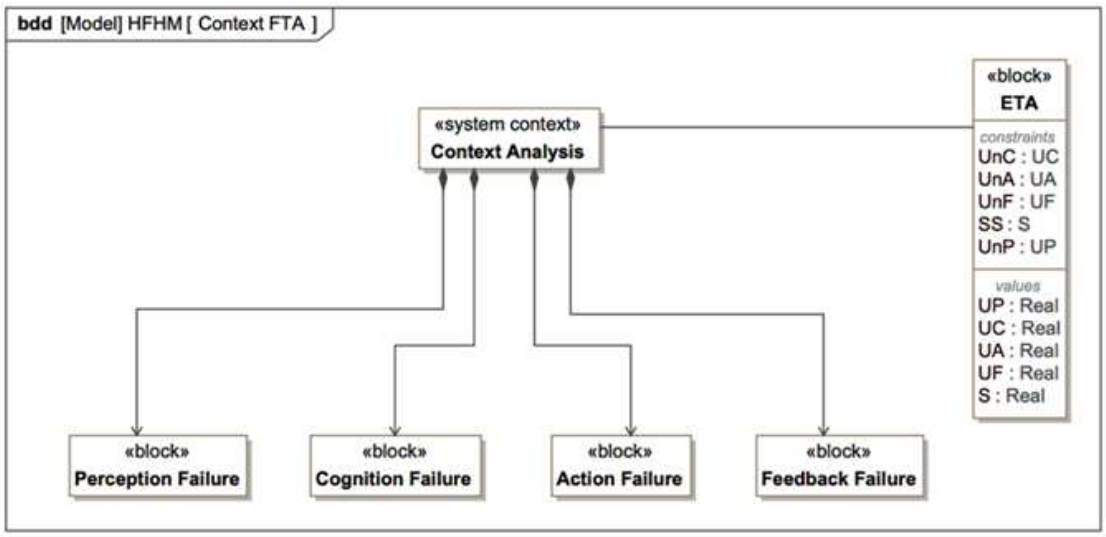


Figure 41 – FTA Blocks and ETA Block within the Context Analysis Block

The ETA itself is constructed in a SysML Parametric diagram, within the context analysis block. Constraints are reused as constraint properties, and the tree is per the logic network of the ETA. The FTA and ETA blocks that were composed within the context analysis, allows mapping of the FTA results (source) to the ETA Calculations (target). The values of probability of failure from the pivotal events are tied to their respective constraint parameters within the ETA using binding (equivalency) connectors. The ETA context analysis diagram is presented in **Figure 42**.

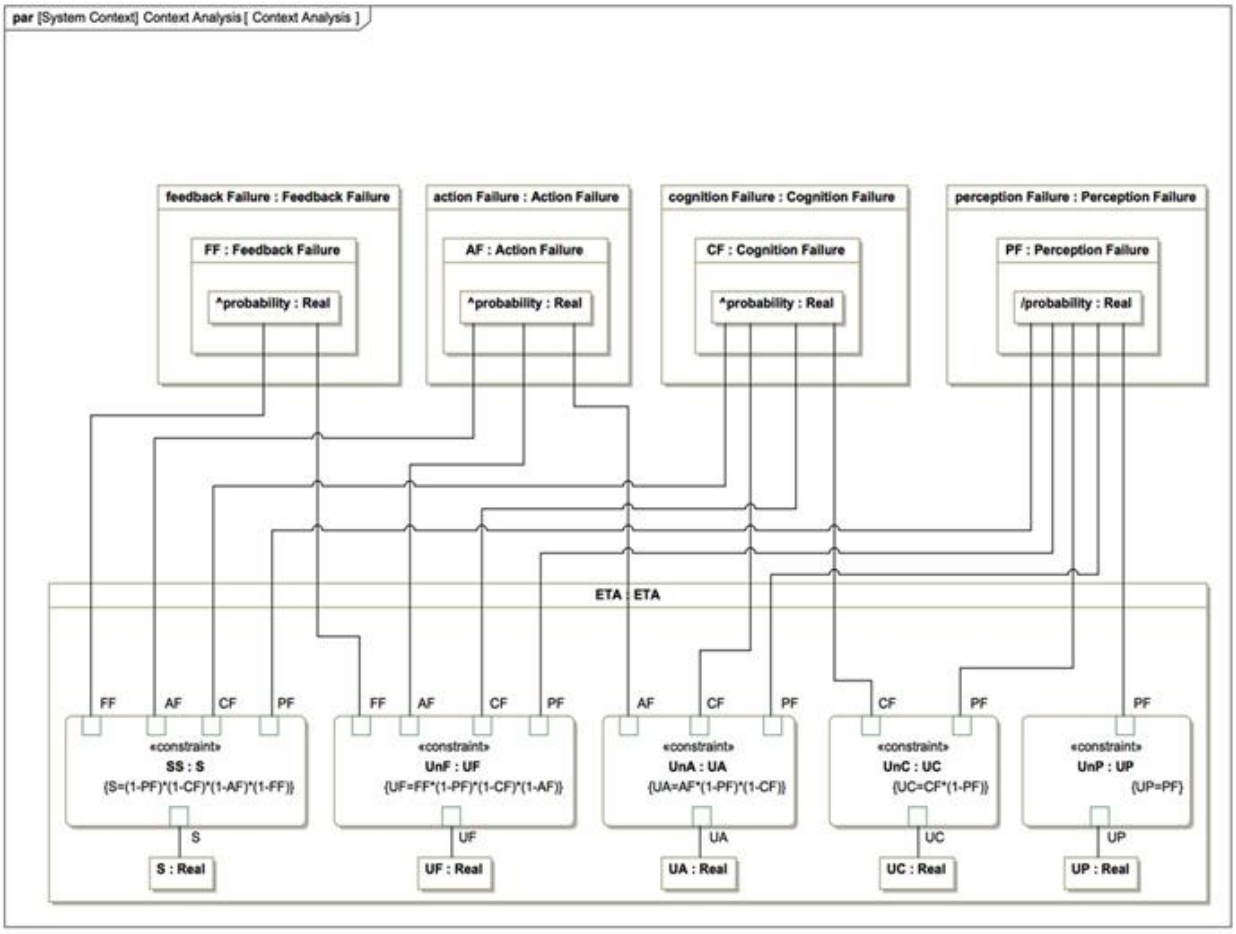


Figure 42 – ETA Structure in the Context Analysis

A simulation configuration is employed to automate the execution of all pivotal event FTAs and the top-level ETA. This is accomplished by executing the overarching context analysis block and compiling the results of the underlying analysis in an instance table for review by the analyst. The context block and instance table are presented in **Figure 43** and **Table 30** respectively.

Figure 43 – FTA / ETA Execution using the Simulation Configuration

Table 30 – FTA / ETA Results Summary Instance Table

#	Name	perception Failure.PF.probability : Real	cognition Failure.CF.prob : Real	action Failure.AF.prob : Real	feedback Failure.FF.prob : Real	ETA.UP : Real	ETA.UC : Real	ETA.UA : Real	ETA.UF : Real	ETA.S : Real
1	context Analysis	0.483	0.496	0.125	0.496	0.483	0.256	0.033	0.113	0.115

Requirements Engineering and Management within Model Based Systems Engineering

The Human Factors Triggering Event (HFTE) probabilities calculated using the Human Reliability Analysis (HRA) model developed using SysML, as described in this work, have utility with regards to Requirements Engineering within the lifecycle design. A direct parametric link between the human actor failure probabilities as well as other system reliability information

will improve the efficiency and accuracy of documenting, verifying, and validating the various risk and reliability requirements related to the system safety specifications. The HRA information can be used individually, as well as in combination with other Hazard Analysis Techniques (HATs), to determine predicted failure rates of the various system components. These results can then be parametrically linked to system requirements which are embedded within the system model architecture. This supports the underlying philosophies of Model-Based Systems Engineering (MBSE), namely a single unambiguous and unified model allowing generation of results and diagrams and documents representing the system design in a virtual format.

SysML Data Links to the Automated Human Factors Hazard Model

The automated Human Factors Hazard Model (HFHM) establishes an interface with the Fault Tree Analysis (FTA) / Event Tree Analysis (ETA) developed in the Systems Modeling Language (SysML). The Human Error Probability (HEP) values used to determine the failure probabilities associated with the various basic events present in each individual pivotal event FTA are tabulated in an instance table format for direct importation into the SysML model for use in hazard event simulation. As the HFHM accesses the various Performance Shaping Factors (PSFs), as specified by analyst, the individual HEP values are automatically calculated by the software. These HEP values are then used to populate the basic event data tables. An example of the export data instance tables formatted for SysML interface are presented in **Table 31**.

Table 31 – HFHM Instance Tables for SysML Utilizations

PERCEPTION			COGNITION			ACTION			FEEDBACK		
#	Name	probability: Real	#	Name	probability: Real	#	Name	probability: Real	#	Name	probability: Real
1	PF		1	CF		1	AF		1	FF	
2	PA1	1.00000000	2	CA1	1.00000000	2	AA1	1.00000000	2	FA1	1.00000000
3	PA2		3	CA2		3	AA2	1.00000000	3	FA2	
4	PB1	1.00000000	4	CB1		4	AA3	1.00000000	4	FB1	
5	PB2		5	CB2	1.00000000	5	AA4		5	FB2	1.00000000
6	PB3		6	CB3		6	AB1	1.00000000	6	FB3	
7	PC1		7	CB4		7	AB2		7	FB4	
8	PC2		8	CC1	1.00000000	8	AB3		8	FC1	1.00000000
9	PC3		9	CC2	1.00000000	9	AB4		9	FC2	1.00000000
10	PC4		10	CC3		10	AB5		10	FC3	
11	PC5	1.00000000	11	CC4		11	AC1	1.00000000	11	FC4	
12	PC6	1.00000000	12	CC5		12	AC2	1.00000000	12	FC5	
13	PD1	1.00000000	13	CC6		13	AC3	1.00000000	13	FC6	
14	PD2	1.00000000	14	CC7	1.00000000	14	AC4	1.00000000	14	FC7	1.00000000
15	PD3	1.00000000	15	CC8	1.00000000	15	AC5	1.00000000	15	FC8	1.00000000
16	PD4	1.00000000	16	CD1	1.00000000	16	AC6	1.00000000	16	FD1	1.00000000
17	PD5		17	CD2	1.00000000	17	AC7	1.00000000	17	FD2	1.00000000
18	PD6		18	CD3	1.00000000	18	AC8	1.00000000	18	FD3	1.00000000
19	PD7		19	CD4	1.00000000	19	AC9	1.00000000	19	FD4	1.00000000
20	PD8		20	CD5		20	AC10	1.00000000	20	FD5	
21	PD9		21	CD6		21	AC11	1.00000000	21	FD6	
22	PD10		22	CD7					22	FD7	
23	PE1	1.00000000	23	CD8					23	FD8	
24	PE2	1.00000000	24	CD9					24	FD9	
25	PE3	1.00000000	25	CD10					25	FD10	
26	PE4	1.00000000	26	CE1	1.00000000				26	FE1	1.00000000
27	PE5	1.00000000	27	CE2	1.00000000				27	FE2	1.00000000
28	PE6	1.00000000	28	CE3	1.00000000				28	FE3	1.00000000
29	PE7	1.00000000	29	CE4	1.00000000				29	FE4	1.00000000
30	PE8	1.00000000	30	CE5	1.00000000				30	FE5	1.00000000
31	PE9	1.00000000	31	CE6	1.00000000				31	FE6	1.00000000
32	PE10	1.00000000	32	CE7	1.00000000				32	FE7	1.00000000
33	PE11	1.00000000	33	CE8	1.00000000				33	FE8	1.00000000
34	PE12	1.00000000	34	CE9	1.00000000				34	FE9	1.00000000
35	PE13	1.00000000	35	CE10	1.00000000				35	FE10	1.00000000
36	PE14	1.00000000	36	CE11	1.00000000				36	FE11	1.00000000
37	PE15	1.00000000	37	CE12	1.00000000				37	FE12	1.00000000
38	PE16	1.00000000	38	CE13	1.00000000				38	FE13	1.00000000
39	PE17	1.00000000	39	CE14	1.00000000				39	FE14	1.00000000
40	PE18	1.00000000	40	CE15	1.00000000				40	FE15	1.00000000
41	PE19	1.00000000	41	CE16	1.00000000				41	FE16	1.00000000
42	PE20	1.00000000	42	CE17	1.00000000				42	FE17	1.00000000
43	PE21	1.00000000	43	CE18	1.00000000				43	FE18	1.00000000
44	PE22	1.00000000	44	CE19	1.00000000				44	FE19	1.00000000
45	PE23	1.00000000	45	CE20	1.00000000				45	FE20	1.00000000
46	PE24	1.00000000	46	CE21	1.00000000				46	FE21	1.00000000
47	PE25	1.00000000	47	CE22	1.00000000				47	FE22	1.00000000
48	PE26	1.00000000	48	CE23	1.00000000				48	FE23	1.00000000
49	PE27	1.00000000	49	CE24	1.00000000				49	FE24	1.00000000
50	PE28	1.00000000	50	CE25	1.00000000				50	FE25	1.00000000
			51	CE26	1.00000000				51	FE26	1.00000000
			52	CE27	1.00000000				52	FE27	1.00000000
			53	CE28	1.00000000				53	FE28	1.00000000

SUMMARY AND CONCLUSIONS

The Human Factors Hazard Model (HFHM) was developed to improve the process of Human Reliability Analysis (HRA), with a particular interest of developing a system that is compatible with existing system safety Hazard Analysis Techniques (HATs). The objective of developing the new modeling approach for quantifying human error, as it relates to safety hazards, is to provide a general and standardized model for near universal application in Human Error Probability (HEP) prediction. The predictive model was developed and then verified against existing HRA approaches and methods. Additionally, the model was evaluated by several subject matter experts (SMEs) to evaluate its functionality and utility within a Systems Engineering (SE) environment as well as a high-volume manufacturing factory and a facilities management organization. A trade study evaluation was also performed to ascertain the flexibility, timeliness, and overall usefulness of the analytical model for predicting human hazard probabilities.

Research Question Task Outcome Summaries

In response to the research questions posed in this dissertation, a series of tasks were assigned. In answering these tasks, the outcome of each research question is established, with a final status related to the associated question. Detailed description of each task outcome are as follows:

RQ1-T1: Several Human Reliability Analysis (HRA) approaches were examined. The HRA technique most scrutinized in this study was the Technique for Human Error Rate Prediction (THERP). This approach is the most commonly cited human factors analysis method. Another method that is commonly applied is Expert Estimation, which has wide application in system safety analysis as well. Typically, each technique has been developed and has evolved with certain industries and applications in mind. Most techniques are quite detailed, and can be relatively complicated to implement in hazard analysis. As such, a significant amount of training and practice is required to master a given technique. Consequently, each technique can be time consuming and costly to employ in human factors analysis. For the reasons noted above, it was identified that a more universal and simplified approach to HRA that yields an accurate Human Error Probability (HEP) value would have value to system safety analysis and system lifecycle management.

RQ1-T2 and RQ1-T4: As described, a new Human Factors Hazard Model (HFHM) has been developed to answer the limitations of existing HRA techniques. The HFHM was developed such that it has as broad of application in HRA as possible. As noted, the fundamental functionality of the new model focusses on the determination of general human and system factors related to a specific operational hazard scenario within a system context. From the human and system values identified, Performance Shaping Factors (PSFs) are established to determine HEP values for use in the Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). The FTA / ETA models produce the intermediate probabilities required to calculate the top-level probability of failure associated with the defined Human Factors Triggering Event (FHTE) that will result in a mishap if no corrective action is implemented. The HFHM is standardized and automated within MS Excel such that with the revision of human and system factors, the

resulting PSFs, HEPs, and subsequent event probabilities, including the top-level probability of failure are instantly recalculated. As such, the HFHM expresses a high level of utility with regards to trade studies and sensitivity studies, being able to update designs as quickly as PSFs can be revised within the automated computational platform.

RQ1-T3: As a method to verify the HFHM result, a comparative study to THERP was performed. As described, a baseline case HFTE was established, with a total of eight permutations of the original analysis scenario, with the associated hazard analysis results. For each THERP result, and equivalent HFHM evaluation was performed. Comparison of the two analysis approaches indicated good agreement between the calculate results with an average agreement between models of approximately 4.8%. Additionally, an evaluation of the HFHM was performed with a hypothetical trade study. Results of the trade study indicate that the HFHM functions as intended, and yields realistic probability results and trends for a specified HFTE. For the trade study, an initial design is evaluated, and with subsequent design improvements accounted for. As expected, the overall probability of success related to the human response to the HFTE indicates a trend of improvement.

RQ2-T1 and RQ2-T2: As noted, an integration approach for the FHHM results into traditional Hazard Analysis Techniques (HATs), used in classic system safety analysis, is proposed. Numerous existing HAT approaches with possible HFHM compatibility are identified, with a more detailed integration technique developed and described for the FTA and Failure Mode and Effects Analysis / Failure Mode Effects and Criticality Analysis (FMEA / FMECA). For an example scenario involving a hazard event related to a boiler over-temperature event, integration of the HFHM result into both an FTA and FMEA/FMECA analysis is proposed. The application of the HFHM is shown to improve the HAT approach in two different ways. First, the error

probability due to human-system interaction is added directly to the analysis, such that the risk due to a human actor's activities within the system is accurately represented in the HAT method. Without an HFHM result, any accounting for human factors in the analysis would most likely be loosely estimated, or based upon a different HRA approach which may or may not have an optimized solution for the case at hand. Second, with the implementation of the HFHM into the HAT, an accurate accounting of the mishap probability specific to human actor interaction with the system is established in the overall analysis. Without the inclusion of the HFHM results, the classic HAT approaches would most likely not yield an accurate result. Without consideration of the risk associated with human activity within the system context, overall system safety analysis will not fully account for all possible risk.

RQ3-T1: An approach to reliability and risk analysis within Model-Based Systems Engineering (MBSE) is currently under development. The Risk Analysis and Assessment Modeling Language (RAAML), currently in development by the Object Management Group (OMF) provides a standardized approach to classic hazard analysis using commonly used HATs. Using a pre-release version of RAAML in conjunction with standard SysML libraries, a protocol for implementing the HFHM into MBSE has been developed. Using RAAML libraries as well as custom developed SysML constraint blocks, the FTA and ETA elements of the HFHM have been stereotyped and implemented into a functioning module capable of producing identical results as achieved using the base HFHM as originally automated. The activity to implement the HFHM within SysML has resulted in a unique application of an existing reliability profile as well as development of a new and novel approach to calculating and documenting HRA within MBSE.

RQ3-T2 and RQ3-T4: In these tasks, an MBSE approach to hazard analysis has been developed and tested. The PSFs as calculated within the HFHM interface can be ported to the stereotyped SysML model via four different instance tables established for the primary pivotal events as defined in the hazard model. HEP values calculated by the HFHM are recorded in instance tables for Perception, Cognition, Action, and Feedback. The instance tables are then read into the SysML model. The respective HEP values are then utilized by the stereotyped FTA / ETA functionality to produce the top-level probabilities of success and failure as related to human actor interaction within the system during a HFTE. The code was developed using the RAAML extension as well as unique development of functionality within SysML. The HFHM approach implemented within SysML is standardized, and can be easily reused throughout various system model architectures.

RQ3-T3: System safety analysis results generated within the MBSE architecture related to the HFHM integration can be directly linked to the Requirements Domain within SysML. Using constraint blocks within the Parametric Domain of SysML, relevant requirements information can be communicated and managed throughout the system model as defined in SysML. As characteristics relative to the human actor are revised and updated within the MBSE architecture, the associated requirements will update accordingly and communicate relevant lifecycle design information. Due to the parametric nature of MBSE, as HFHM result update, the respective requirements engineering will reflect all relevant revisions.

Research Project Conclusions

A Human Factors Hazard Model (HFHM) approach to human factors related safety analysis has been developed, verified against a widely utilized Human Reliability Analysis

(HRA), and evaluated by several Subject Matter Experts (SMEs) with regards to its utility and application in system lifecycle design. Additionally, an integration method, with stereotyped libraries have been developed in SysML for direct application within Model-Based Systems Engineering (MBSE). As an extension of the direct link within MBSE, Human Reliability Analysis (HRA) results generated by the HFHM can be directly coupled to engineering requirements management, as it relates to reliability of the system design. Based on the outcome of this research project, an improved approach to human factors engineering, and particularly the assessment of risk associated with human actors within a system lifecycle design has been established.

Future Research and HFHM Development Activities

Several areas have been identified for future research and development related to the Human Factors Hazard Model (HFHM). Specific research-based tasks have been identified for continued verification and validation of the current model. These include:

- Further verification of the HFHM through expanded correlation of fundamental Human Error Probabilities (HEPs) and Performance Shaping Factors (PSFs) to values incorporated in the model database. This would be accomplished through an expanded literature evaluation as well as developing specific human performance experiments to verify baseline HEP and PSF values currently established within the model.
- Further verification of the HFHM through direct correlation to hazard simulations

designed to assess overall model performance. This includes a design of experiments incorporating simulations of various hazard scenarios with a range of human actors exhibiting different training, experience, intellectual, and physiological characteristics. Simulation results would compare HFHM results to actual demonstrated human performance. This effort would contribute to a greater understanding of the top-level accuracy and limitations of the model. Additionally, a better understanding and documentation of error factors related to HEP would be cataloged.

- Expanded research into the incorporation of the HFHM results into additional commonly cited Hazard Analysis Techniques (HATs). This includes a systematic evaluation of existing HATs with regards to their compatibility to the HFHM technique, and the development of specific strategies to integrate HFHM results into individual HAT approaches.

- Additional field testing of the HFHM, using a larger and more diverse population of Subject Matter Experts (SMEs), to gain additional insight into model strengths and potential weaknesses with regards to Human Reliability Analysis (HRA).

In addition to research-based validation and verification activities, areas for future software development and functional improvements related to the current HFHM model have been identified. These include:

- Improvement of the data interpolation algorithms within the programming logic to

"smooth" certain values that use discrete steps versus a continuum of values to establish HEP and PSF assignments. This effort would support a finer resolution of probability predictions, thus improving model accuracy.

- Expanded integration of the HFHM within Model-Based Systems Engineering (MBSE), specifically within the Systems Modeling Language (SysML) and Risk Analysis and Assessment Modeling Language (RAAML) extension. This would include the expanded development of the current modeling stereotypes to include HEP and PSF functionality currently modeling the HFHM, as well as direct links to requirements engineering.

- Exploration of redevelopment of the HFHM into a stand-alone application that does not require an intermediate software tool such as MS Excel for operation. This would potentially allow for an improved user interface, enhanced user error trapping, improved user help features, and expanded presentation and documentation of simulation results.

REFERENCES

[1] K.R. Boff, J.E. Lincoln, *Engineering Data Compendium – Human Perception and Performance*, Harry G. Armstrong Aerospace Medical Research Laboratory: Wright-Patterson Air Force Base, 1988

[2] D.F. Hultsch, S.W.S. MacDonald, R.A. Dixon, *Variability in Reaction Time Performance of Younger and Older Adults*, Journal of Gerontology: Psychological Sciences, 2002

[3] R.L. Olson, R.J. Hanowski, J.S. Hickman, J. Bocanegra, *Driver Distraction in Commercial Vehicle Operations*, FMCSA-RRR-09-042, U.S. Department of Transportation, Federal Motor Carrier Safety Administration, 2009

[4] *New Data from Virginia Tech Transportation Institute Provides Insight into Cell Phone Use and Driving Distraction*, Virginia Tech Transportation Institute, 2009

[5] T.J. Kirsch, *An Analysis of the Crash Risk and Likelihood of Engaging in a Distraction While Driving Using Naturalistic, Time-Series Data*, Iowa State University, 2018

[6] *Potential Failure Mode and Effects Analysis (FMEA) – Reference Manual,* Chrysler Corporation, Ford Motor Company, General Motors Corporation, 1st Edition, 1995

[7] *Systems Engineering Handbook – A Guide for System Life Cycle Processes and Activities*, 4th Edition, INCOSE - Wiley, 2015

[8] *Guide for Writing Requirements*, INCOSE Document No. INCOSE-TP-2010-006-03, Version 3, 2019

[9] D.S. Birch, T.H. Bradley, *Development of a Human Factors Hazard Model Using HEP / FTA / ETA*, Wasatch Aerospace & Systems Engineering Conference (AIAA-INCOSE), 2021

[10] N. Siu, *Dynamic Accident Sequence Analysis in PRA: A Comment on 'Human Reliability Analysis – Where Shoudst Thou Turn?'*, Reliability Engineering & System Safety, Volume 29, Issue 3, 1990

[11] G. W. Hannaman, D.H. Worledge, *Some Developments in Human Reliability Analysis – Approaches and Tools*, Reliability Engineering & System Safety, Volume 22, Issus 1-4, 1988

[12] A. Spurgin, *Another View of the State of Human Reliability Analysis (HRA), Reliability Engineering & System Safety*, Volume 29, Issue 3, 1990

[13] N.A.A. Aziz, A. Fumoto, K. Suzuki, *Assessing Human Error During Collecting a Hydrocarbon Sample of the Chemical Plant Using THERP*, Journal of Fundamental and Applied Sciences, ISSN: 1112-9867, 2017

[14] C.L. Ericson II, *Hazard Analysis Techniques for System Safety*, 2nd Edition, Wiley, 2016

[15] D.I. Gertman, H.S. Blackman, *Human Reliability and Safety Analysis Data Handbook*, 3rd Edition, Wiley-Interscience, 1993

[16] A.D. Swain, H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, SAND80-0200, 1983

[17] M.K. Comer, D.A. Seaver, W.G. Stillwell, C.D. Gaddy, *Generating Human Reliability Estimates Using Expert Judgment*, NUREG/CR-3688 – SAND84-7115, VOL 1 & 2, 1984

[18] W.E. Vesely, F.F. Goldberg, N.H. Roberts, D.F. Haasl, *Fault Tree Handbook*, NUREG-0492, Systems and Reliability Research – Office of Nuclear Regulatory Research, United States Nuclear Regulatory Commission, 1981

[19] B.S. Dhillon, *Human Reliability with Human Factors*, Pergamon Press, 1986

[20] S.J. Guastello, *Human Factors Engineering and Ergonomics*, 2nd Edition, CRC Press, 1986

[21] M.V. Stringfellow, *Accident Analysis and Hazard Analysis for Human and Organizational Factors*, PhD Dissertation, Massachusetts Institute of Technology, 2010

[22] R.B. Shirley, C. Smidts, M.Li, A. Gupta, *Validating THERP: Assessing the Scope of a Full-Scale Validation of the Technique for Human Error Rate Prediction*, Annals of Nuclear Energy, Vol. 77, Ohio State University, 2014

[23] D.E. Embrey, P. Humphreys, E.A. Rosa, B. Kirwan, K. Rea, *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*, United States Nuclear Regulatory Commission – Human Factors and Safeguards Branch, Office of Nuclear Regulatory Research, Contract No. DE-AC02-76CH00016 Fin. No. A-3219, 1984

[24] *Aircraft Accident Report – Decent Below Visual Glidepath and Impact with Seawall – Asiana Airlines Flight 214*, NTSB/AAR-14/01, PB2014-105986, 2014

[25] *Department of Defense Standard Practice – System Safety*, MIL-STD-882E, Revision E, 2012

[26] M. Stamatelos, J. Caraballo, W. Vesely, J. Dugan, J. Fragola, J. Minarick, J. Ralsback, *Fault Tree Handbook with Aerospace Applications*, NASA Office of Safety and Mission Assurance, V 1.1, 2002

[27] A. Berres, K. Post, A. Armonas, M. Hecht, T. Juknevicius, D. Banham, *OMG RAAML Standard for Model-Based Fault Tree Analysis*, Object Management Group, 2021

[28] G. Biggs, K. Post, A. Armonas, N. Yakymets, T. Juknevicius, A. Berres, *OMG Standard for Integrating Safety and Reliability Analysis into MBSE: Concepts and Applications*, INCOSE International Symposium, Volume 29, Issue 1, 2019

[29] G. Biggs, T. Juknevicius, A. Armonas, K. Post, *Integrating Safety and Reliability Analysis into MBSE: Overview of the New Proposed OMG Standard*, INCOSE International Symposium, Volume 28, Issue 1, 2018

[30] A.H. de Andre Melani, G.F. de Souza, *Obtaining Fault Trees Through SysML Diagrams: A MBSE Approach for Reliability Analysis*, IEEE, 2020 Annual Reliability and Maintainability Symposium (RAMS)

[31] J.M. Borky, T.H. Bradley, *Effective Model-Based Systems Engineering*, Springer, 2019

[32] S. Friedenthal, A. Moore, R. Steiner, *A Practical Guide to SysML – The Systems Modeling Language*, MK/Elsevier, 2015

[33] L. Delligatti, *SysML Distilled: A Brief Guide to the Systems Modeling Language*, Addison-Wesley, 2014

[34] K. Pohl, *Requirements Engineering: Fundamentals, Principles, and Techniques*, Springer, 2010

[35] V.J. Gawron, *Human Performance and Situation Awareness Measures*, CRC Press, 2019

[36] V.J. Gawron, *Workload Measure*, CRC Press, 2019

[37] S. Hendrickson, M. St. Pierre, *HRA Database Review*, U.S. Department of Energy, Sandia National Laboratories, 2015

[38] R. Pearson, *Decibel Level of Common Sounds: Comparison Chart, Soundproof Expert Website*, 2020

[39] *The Human Hearing Range – What Can You Hear*, WIDEX Blog, WIDEX USA, Inc. 2016

[40] *Types of Color Blindness*, National Eye Institute, U.S. National Institutes of Health, U.S. Department of Health and Human Services, 2019

[41] E. Schlosser, *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*, Penguin Books, 2013

[42] *Effects of Blood Alcohol Content on Driving*, CDC Motor Vehicle Safety Info Sheet, Centers for Disease Control and Prevention, 2020

[43] *How Alcohol Impacts the Brain – What Alcohol Means for Your Health*, Northwestern Medicine, Northwestern University, 2021

[44] B. Uren, *How Alcohol Impairs Your Ability to Drive*, University of Michigan Health Blog, 2016

[45] *Drivers are Falling Asleep Behind the Wheel*, National Safety Council Web Information, 2021

[46] *Facts + Statistics: Drowsy Driving*, Insurance Information Institute Web Information, 2021

[47] *Pilot's Handbook of Aeronautical Knowledge*, Federal Aviation Administration, U.S. Department of Transportation, FAA-H-8083-25B, 2006

[48] *Final Report – Germanwings Accident at Prads-Haute-Bleone (Alps-de-Haute-Provence, France)*, Bureau d'Enquetes et d'Analyses pour la Securite de l'aviation Civile, 2016

[49] *Aircraft Accident Report – American Airlines Flight 191*, National Transportation Safety Board, NTSB-AAR-79-17, 1979

[50] *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*, National Highway Traffic Safety Administration, U.S. Department of Transportation, DOT HS 812 115, 2015

[51] M. Rauterberg, *Perception, Cognition, Action: An Action Theoretical Approach*, Systematica, Volume 14, Number 1, 1999

[52] D.W. Carruth, M.D. Thomas, B. Robbins, A. Morais, *Integrating Perception, Cognition, and Action for Digital Human Modeling*, Digital Human Modeling, Lecture Notes in Computer Science, Volume 4561, 2007

[53] J.P. Clements, *Three Mile Island Unit 2 – Case Study Overview*, NUREG, 2015

[54] G.J. Burkholder, K.A. Cox, L.M. Crawford, J.H. Hitchcock, *Research Design and Methods – An Applied Guide for the Scholar-Practitioner*, Sage Publications, 2020

[55] N.G. Leveson, *Engineering a Safer World*, MIT Press, 2011

[56] B.S. Blanchard, W.J. Fabrycky, *Systems Engineering and Analysis*, 5th Edition, Prentice Hall, 2011

[57] D.D. Walden, G.J. Roedler, K.J. Forsberg, R. D. Hamelin, T.M. Shortell, *INCOSE System Engineering Handbook – A Guide for System Life Cycle Processes and Activities*, INCOSE-TP-2003-002-04, 4th Edition, 20215

[58] A.M. Madni, *Integrating Humans with Software and Systems: Technical Challenges and a Research Agenda*, Systems Engineering - The Journal of the International Council on Systems Engineering, Volume 13, Issue 3, 2010

[59] P.J. Younse, J.E. Cameron, T.H. Bradley, *Comparative Analysis of a Model-Based Systems Engineering Approach to a Traditional Systems Engineering Approach for Architecting a Robotic Space System through Knowledge Categorization*, Systems Engineering. 2021;24:117-199

[60] M.E. Miller, J.M. McGuirl, M.F. Schneider, T.C. Ford, *Systems Modeling Language Extension to Support Modeling of Human-Agent Teams*, Systems Engineering. 2020;1-15

[61] *Systems Engineering Guide*, The MITRE Corporation, ISBN 978-0-0615-97442-2, 2014

[62] E.M. Wetzel, W.Y. Thabet, *Utilizing Six Sigma to Develop Standard Attributes for a Safety for Facilities Management (SFFM) Framework*, Safety Science, 2016

[63] E.M. Wetzel, J. Lucas, W.Y. Thabet, *The Utilization of an Asset Safety Identification Tool (ASIT) to Support Safety During Facilities Management*, ASCE International Workshop, 2017

APPENDIX A – GLOSSARY OF TERMS

Accident: An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on) [55]. See Below - This definition is synonymous with that of *Mishap* as proposed by Ericson [14].

Actor: A human being that interacts with a system as either a component of the system or in the system context.

Ergonomics: The study and science of how human beings interact with their surroundings and work in a particular environment. Often the emphasis and focus are to maximum human performance, minimize error, an minimize risk or injury.

Human Factors: The capabilities, characteristics, and constraints of human beings with respect to their interface with other humans, engineered systems, and environments. This may correspond to the anticipated response of a human to a stimulus, or performance of a human being relative to a specific task.

Human Factors Hazard Model (HFHM): The Human Reliability Analysis (HRA) model developed as part of this research project to provide a simplified, universal approach to determining the probability of success (or failure) related to a human reaction to a Human Factors Triggering Event (HFTE).

Human Factors Triggering Event (HFTE): Any interaction between a human actor within the system context and the system design that could result in an accident or mishap depending upon the human response to the system behavior.

Human Error Probability (HEP): The probability that a human actor will respond incorrectly to a hazard event, thus resulting in a mishap or accident.

Human Reliability Analysis (HRA): The analysis of human behavior with respect to the likelihood of performing a task, or series of tasks correctly.

Irrelevant Environment: The environment surrounding the system in which it exists and functions, but is not anticipated to have any interaction or bearing on system function [34]. This is the region of the system domain outside of the system context.

Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [14][25]. See Above - This definition is synonymous with that of *Accident* as proposed by Leveson [55].

Reliability: The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time [14].

Safety: Freedom from conditions that result in an accident. The ability for the system to exclude mishaps during a stated operation under stated conditions for a defined amount of time [14].

System: An assemblage or combination of functionality related elements or parts forming a unitary whole [56].

System Context: The part of a system environment that relevant to system operation and requirements [34]. Actors located within the system context can and will possibly interact and affect system function.

Validation: The method by which an engineering requirement is determined to meet the stated definition and is correct and agreed upon by all stakeholders [34].

Verification: The method by which the component, sub-system, or system functionality is determined to be correct and acceptable [34].

APPENDIX B – HUMAN FACTORS HAZARD MODEL FUNCTIONAL INTERFACE OVERVIEW

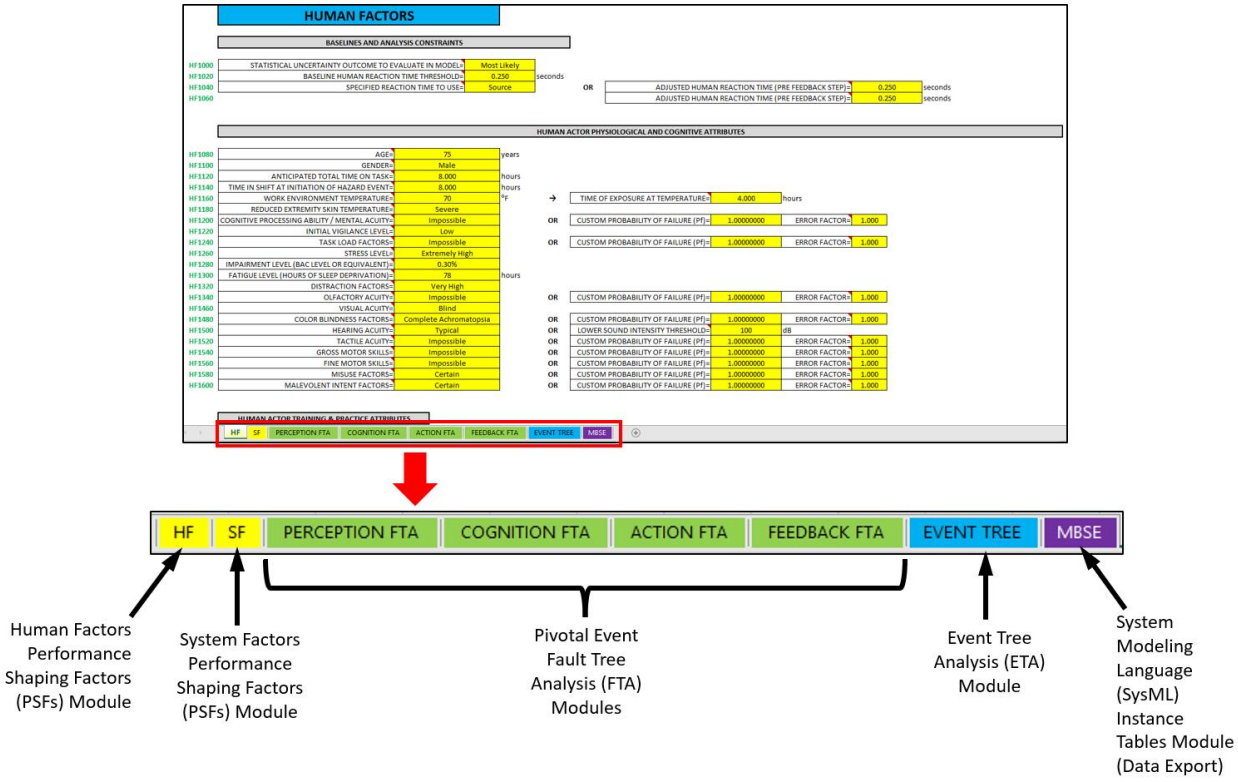


Figure B1 – Human Factors Hazard Model (HFHM) User Interface Details

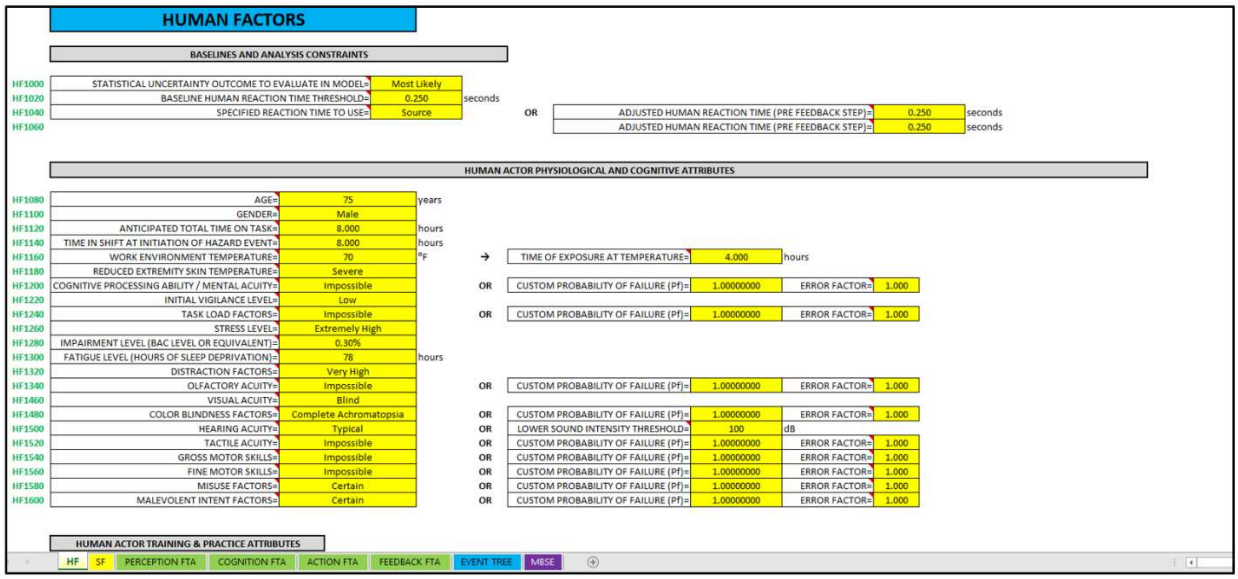


Figure B2 – Human Factors Module Interface

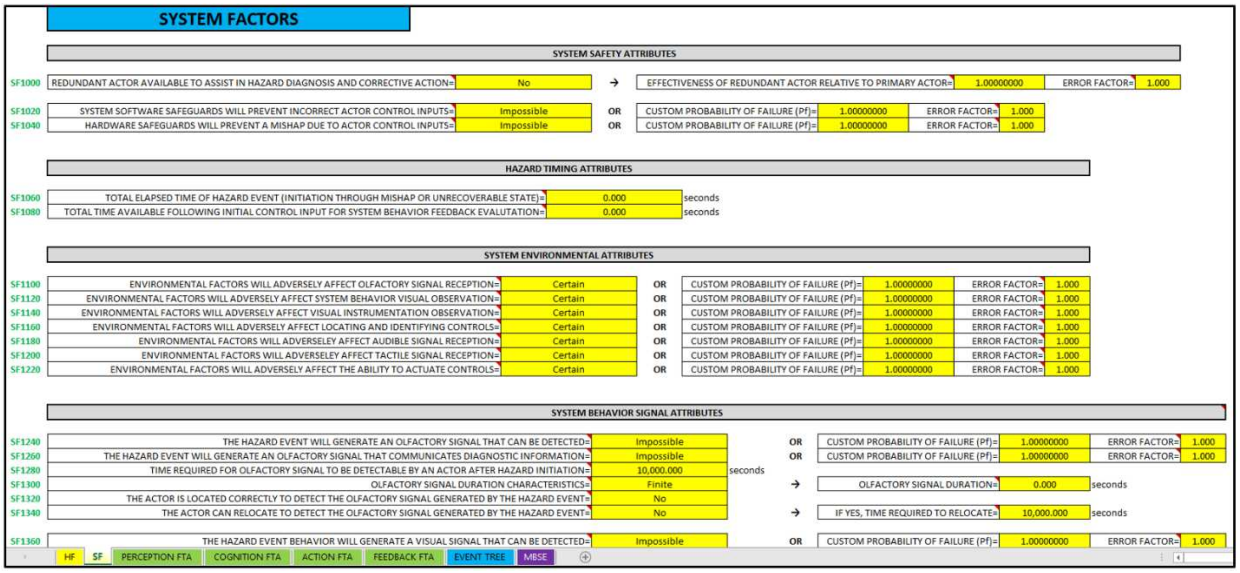


Figure B3 – System Factors Module Interface

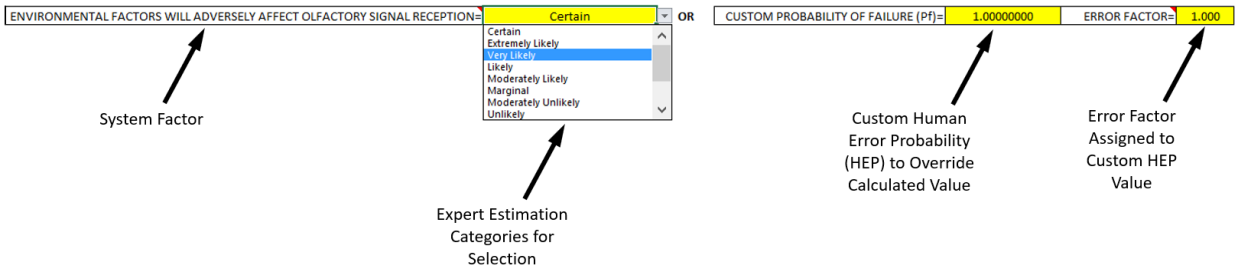


Figure B4 – User Interface for Performance Shaping Factor (PSF) Entry and User Specified Human Error Probability (HEP)Values

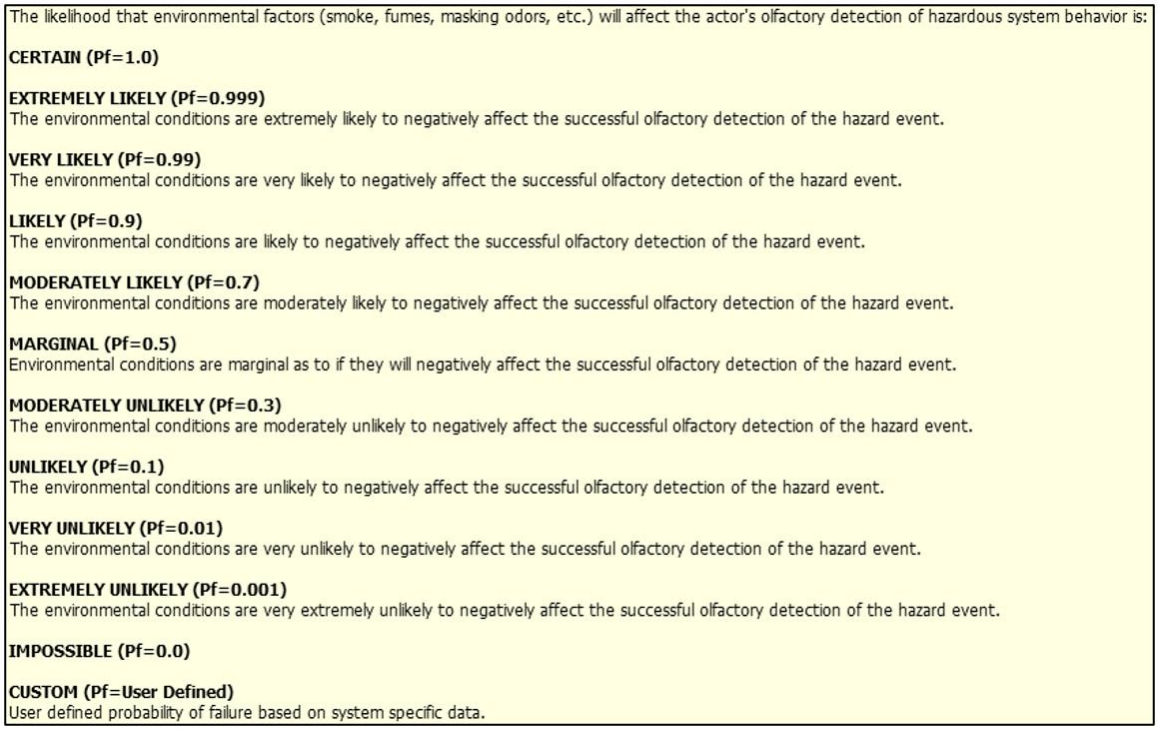


Figure B5 – Expert Estimation Classifications and Associated Probabilities of Failure (Fly-Out Hint Dialog Box)

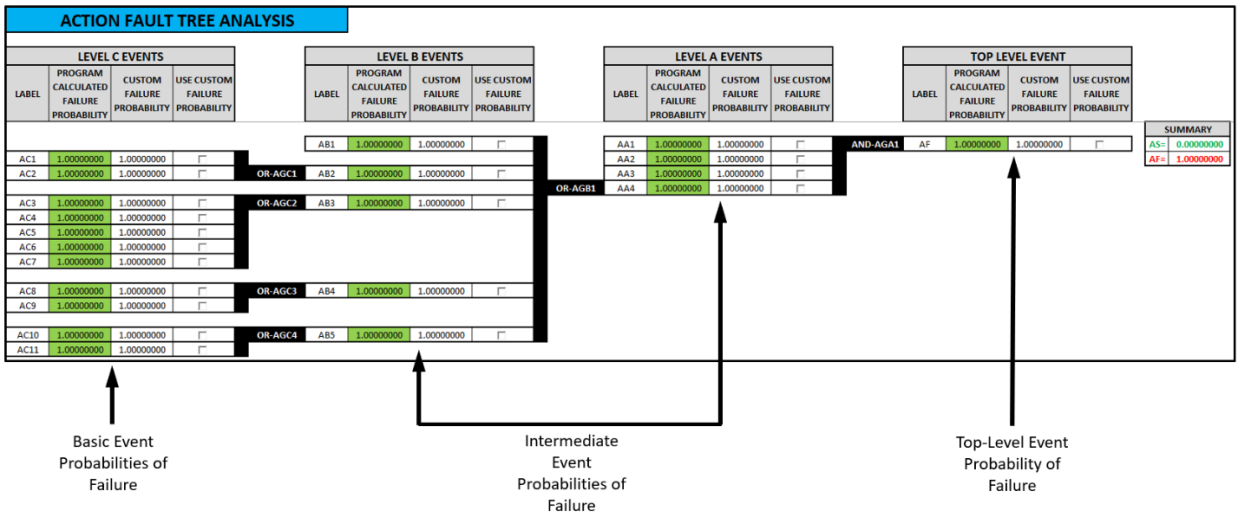


Figure B6 – Fault Tree Analysis (FTA) Module (Action Pivotal Event)

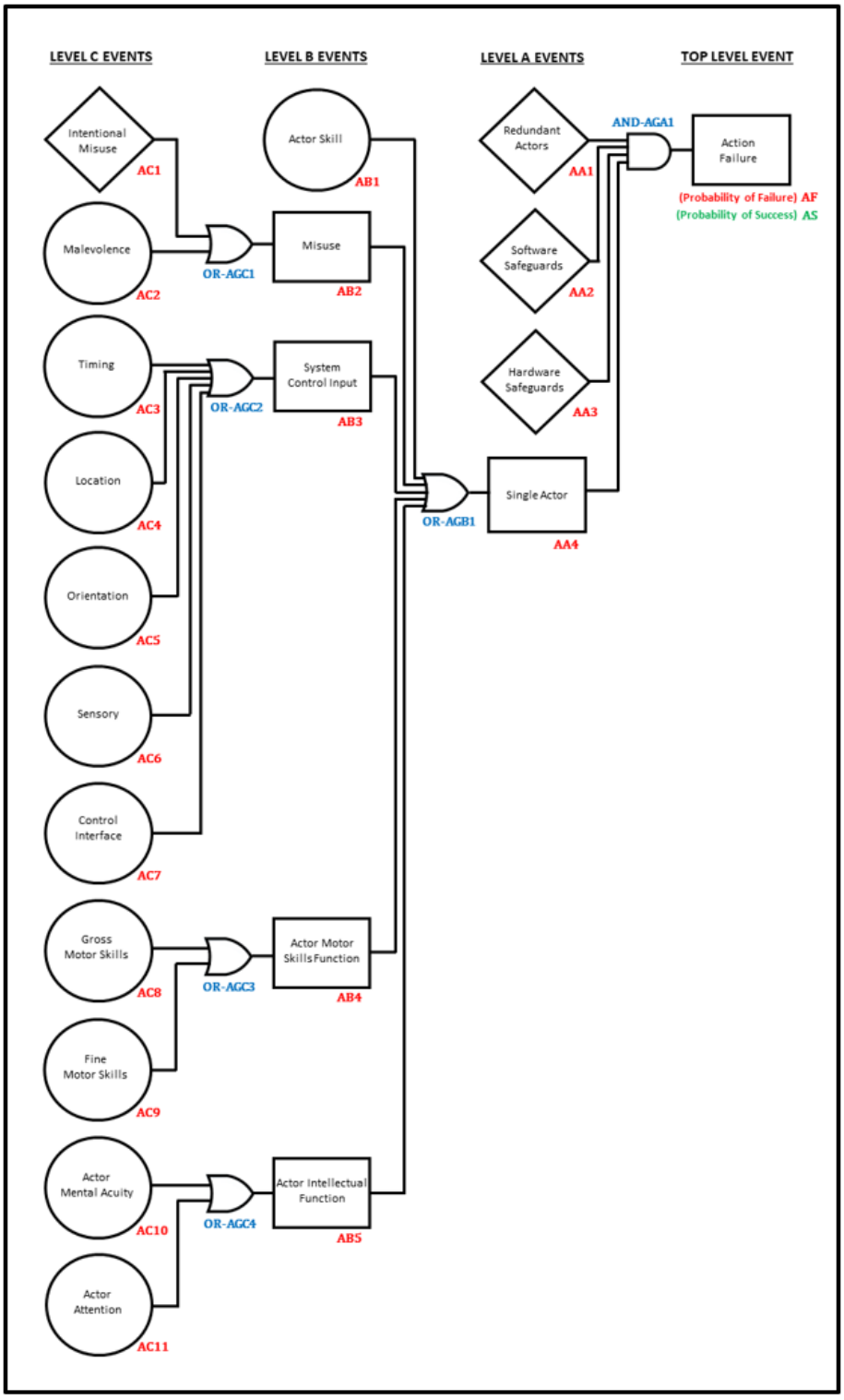


Figure B7 – Fault Tree Analysis (FTA) User Reference Graphic (Action Pivotal Event)

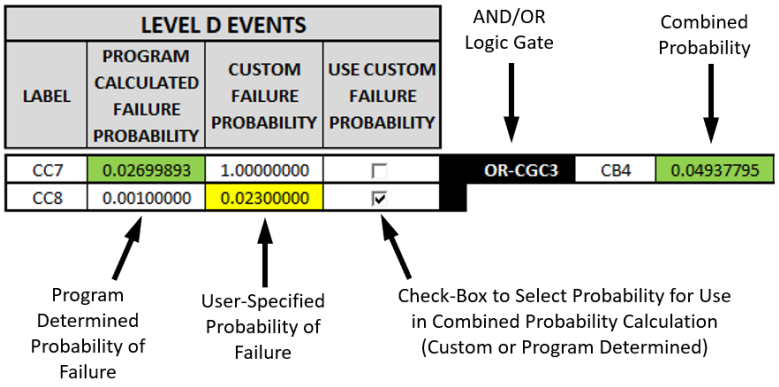


Figure B8 – Fault Tree Analysis (FTA) User Specified Data Input Details

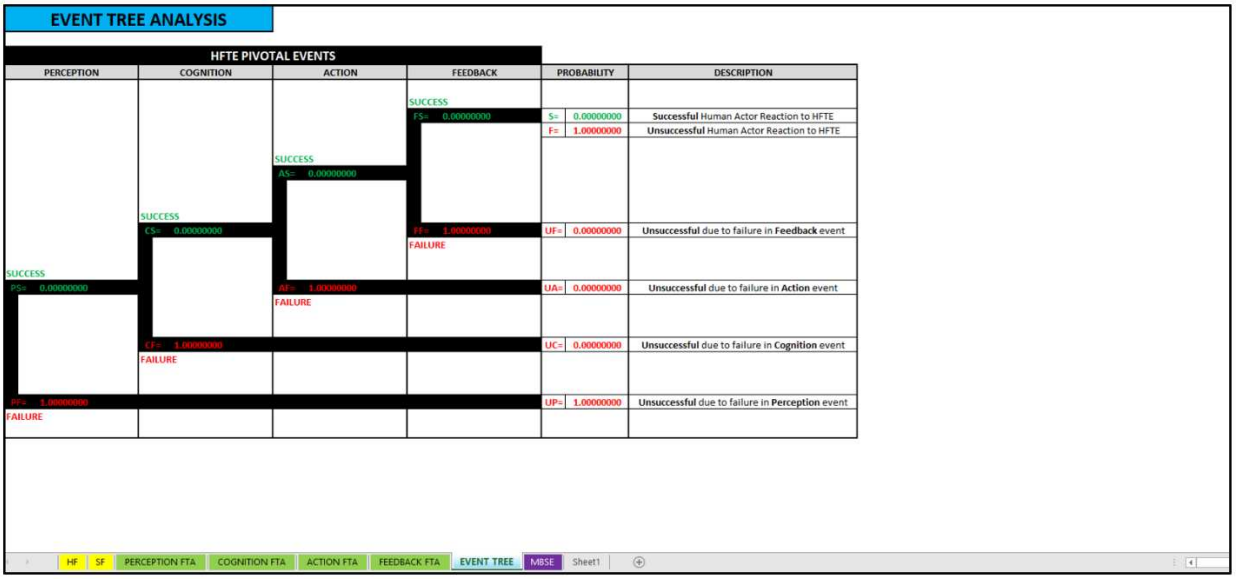
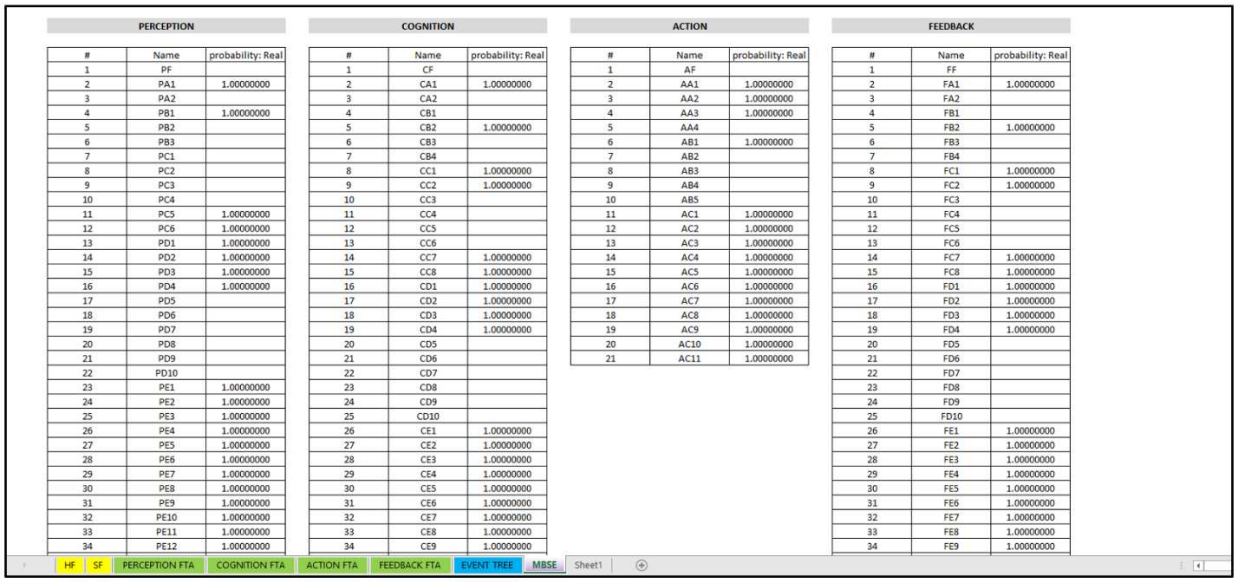


Figure B9 – Event Tree Analysis (ETA) Module



PERCEPTION

#	Name	probability: Real
1	PF	
2	PA1	1.00000000
3	PA2	
4	PB1	1.00000000
5	PB2	
6	PB3	
7	PC1	
8	PC2	
9	PC3	
10	PC4	
11	PC5	1.00000000
12	PC6	1.00000000
13	PD1	1.00000000
14	PD2	1.00000000
15	PD3	1.00000000
16	PD4	1.00000000
17	PD5	
18	PD6	
19	PD7	
20	PD8	
21	PD9	
22	PD10	
23	PE1	1.00000000
24	PE2	1.00000000
25	PE3	1.00000000
26	PE4	1.00000000
27	PE5	1.00000000
28	PE6	1.00000000
29	PE7	1.00000000
30	PE8	1.00000000
31	PE9	1.00000000
32	PE10	1.00000000
33	PE11	1.00000000
34	PE12	1.00000000

COGNITION

#	Name	probability: Real
1	CF	
2	CA1	1.00000000
3	CA2	
4	CB1	
5	CB2	1.00000000
6	CB3	
7	CB4	
8	CC1	1.00000000
9	CC2	1.00000000
10	CC3	
11	CC4	
12	CC5	
13	CC6	
14	CC7	1.00000000
15	CC8	1.00000000
16	CD1	1.00000000
17	CD2	1.00000000
18	CD3	1.00000000
19	CD4	1.00000000
20	CD5	
21	CD6	
22	CD7	
23	CD8	
24	CD9	
25	CD10	
26	CE1	1.00000000
27	CE2	1.00000000
28	CE3	1.00000000
29	CE4	1.00000000
30	CE5	1.00000000
31	CE6	1.00000000
32	CE7	1.00000000
33	CE8	1.00000000
34	CE9	1.00000000

ACTION

#	Name	probability: Real
1	AF	
2	AA1	1.00000000
3	AA2	1.00000000
4	AA3	1.00000000
5	AA4	
6	AB1	1.00000000
7	AB2	
8	AB3	
9	AB4	
10	AB5	
11	AC1	1.00000000
12	AC2	1.00000000
13	AC3	1.00000000
14	AC4	1.00000000
15	AC5	1.00000000
16	AC6	1.00000000
17	AC7	1.00000000
18	AC8	1.00000000
19	AC9	1.00000000
20	AC10	1.00000000
21	AC11	1.00000000

FEEDBACK

#	Name	probability: Real
1	FF	
2	FA1	1.00000000
3	FA2	
4	FB1	
5	FB2	1.00000000
6	FB3	
7	FB4	
8	FC1	1.00000000
9	FC2	1.00000000
10	FC3	
11	FC4	
12	FC5	
13	FC6	
14	FC7	1.00000000
15	FC8	1.00000000
16	FD1	1.00000000
17	FD2	1.00000000
18	FD3	1.00000000
19	FD4	1.00000000
20	FD5	
21	FD6	
22	FD7	
23	FD8	
24	FD9	
25	FD10	
26	FE1	1.00000000
27	FE2	1.00000000
28	FE3	1.00000000
29	FE4	1.00000000
30	FE5	1.00000000
31	FE6	1.00000000
32	FE7	1.00000000
33	FE8	1.00000000
34	FE9	1.00000000

Figure B10 – Model-Based Systems Engineering (MBSE) System Modeling Language (SysML) Instance Table Program Outputs