SANDIA REPORT
SAND2019-5764
Printed May 2019

Sandia National Laboratories

A Reliability Study on the ALERTUS Emergency Management Notification System

Alice B. Muna, Chris B. LaFleur

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Sandia National Laboratories conducted a reliability analysis on the Alertus mass notification system to determine if improvements need to be made to the system to increase reliability. The Alertus mass notification system for Building 803 was analyzed with a set number of components. The components, their associated failure modes and failure mode rates were inputted into a fault tree in the SAPHIRE software which calculated the reliability of the system to be 0.998269.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
EM	Emergency management
FTA	Fault Tree Analysis
GPON	Gigabit Passive Optical Network
ONT	Optical Network Terminal
PRA	Probabilistic Risk Assessment
RIAC	Reliability Information Analysis Center
Sandia	Sandia National Laboratories
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations

1. INTRODUCTION

The primary mission of the emergency management (EM) department at Sandia National Laboratories (Sandia) is to protect people, the environment, and information. This responsibility and associated actions are intended to meet the requirements of DOE Order 151.1D 160811 [1]. As part of this mission, the EM team is responsible for distributing protective action alerts whenever there is a perceived danger and protective actions are advised. These alerts consist of directed and quiet evacuations, shelter-in-place instructions, and lock-downs in case of an active shooter or hostile event. The workforce is alerted about events through different notification methods, one being building speakers and strobes. These speakers and strobes are activated through the Alertus system, which replaces the current Tone Alert Radio System (TARS) system.

1.1. Scope

This report documents a reliability study done on the Alertus mass notification system to determine if improvements need to be made to the system to increase reliability. The analysis is focused on the reliability of hardware sending the alert, but not whether or not the message is received. This report does not address the performance of the system to alert the members of the workforce via visual or audio signals. The objective of the DOE order is to alert the affected members of the workplace within 10 minutes of a confirmed event. The placement of notification appliances, and alternative channels of communications, is key to that notification but is not analyzed in this report. The analysis focuses on one building; however results can be extrapolated to other systems.

Assumptions used to document the project are documented here. The failure rates included in this analysis do not include failures due to improper design or installation. It is assumed that the design meets code requirements and all components were properly installed. An acceptance test is assumed to have been performed to identify failures in the "infant mortality" region of the reliability bathtub curve, shown in Figure 1-1. This analysis is not intended to capture "end-of-life" failures which are primarily due to long-term aging. Instead, this analysis captures failures in the statistical failure region of the bathtub curve where failures are random and consider to occur at a constant rate of failure. Generic reliability information was used due to lack of specific component failure data. This analysis could be refined if specific reliability information was provided by the manufacturers of the components. Finally, this analysis does not analyze the reliability of the building power system.

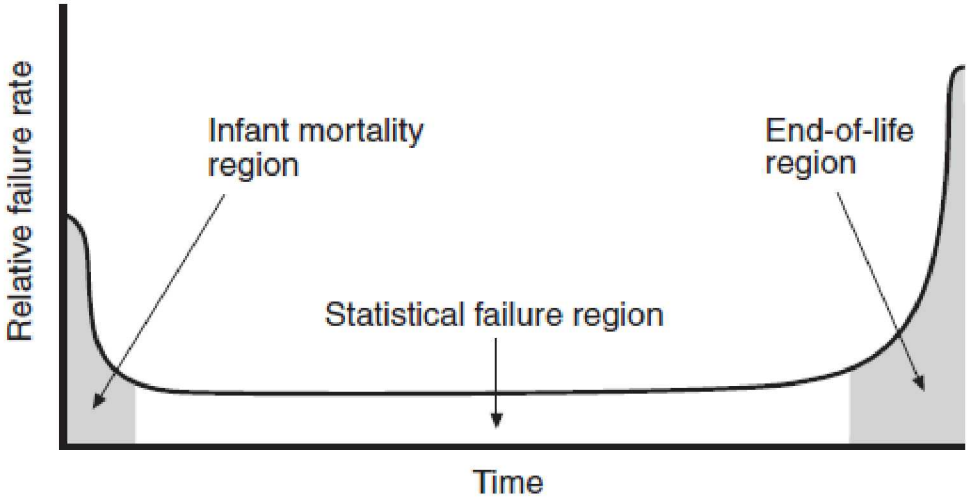

Figure 1-1. Reliability Bathtub Curve

2. METHODOLOGY

2.1. Reliability Fault Tree Analysis

Fault Tree Analysis (FTA) has been used for decades for reliability and safety analysis [2]. FTA is a *top-down* approach that logically traces the root causes of the undesired outcomes by identifying the necessary and sufficient conditions for their occurrence through systematic deductive inference. In doing so, FTA can relate combinations of individual component or device misbehaviors to undesired outcomes and rank these potential safety scenarios so that they can be prioritized for risk management. An FTA can be performed at varying levels of granularity, but for the purposes of this report we analyze failures of components and their impact to the overall system.

Development of a FTA model starts by identifying the occurrence of a top event representing an undesirable outcome for a system or process. In this analysis, the undesirable income was determined to be the improper or out of specification functioning of any part of the Alertus system. This includes speakers and strobes. For example, if one speaker does not operate correctly, it constitutes an overall system failure.

A fault tree represents a logical structure through which component failure modes can be propagated from the bottom up through logic AND and OR gates to render a Boolean equation of all combinations of failures that cause the undesirable top-event to occur. The bottom level of the fault tree is comprised of features called 'basic events' which are specific failure modes that contribute to the occurrence of the top event. Each basic event is given either a point-value probability or a probability distribution based on its failure rate.

The fault tree solves this Boolean equation which represents all of the possible combinations of basic events that would lead to the top event. The result is that the fault tree can be used to quantify the failure probability of a system while also yielding qualitative insights regarding the design of a system.

2.2. SAPHIRE Software

The Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software was developed for the Office of Nuclear Regulatory Research at the U.S. Nuclear Regulatory Commission. SAPHIRE was developed to create and analyze probabilistic risk assessments (PRA) primarily for the nuclear power industry. SAPHIRE was used to construct the reliability fault tree and assign probability values to each of the component failure modes for this analysis. It was also used to solve the fault tree and produce cut sets. Additional information on the SAPHIRE can be found at https://saphire.inl.gov.

2.3. Description of Components

This reliability study is composed of analyzing reliability at the component level. The components included in this study are:

GPON Unit: The Gigabit Passive Optical Network (GPON) Optical Network Terminal (ONT) is a receptacle that passes the signal from the server to the Alertus Beacon unit.

Alertus Beacon: The Alertus Beacon is an audio-visual notification device that has a large text display informing building occupants of the emergency and instructs them how to respond. It also has a speaker and flashing strobes. The Alertus Beacon has a physical Ethernet connection to the

GPON unit which provides the emergency signals. The Alertus Beacon also connects to the Aletus Text to Speech Interface and strobes to send the signal to other locations throughout the building.

Alertus Text to Speech Interface: The Alertus Text to Speech Interface provides spoken voice output of message text to speakers throughout a building. The Text to Speech Interface receives the message via the Alertus Beacon, converts the message from text to speech, and sends the signal to speakers.

Speakers: Speakers are used to distribute the notification message to the building occupants. The speakers are provided by the contractor responsible for installation and in this instance, they are JBL Control 26CT (Ceiling) and JBL Control 25-1 (Wall) speakers.

Strobe: Strobes provide visual notification of an event to occupants. The speakers are provided by the contractor responsible for installation and in this instance, they are Edwards Signaling #48XBRMW120A.

2.4. Alertus FTA

This reliability study was conducted for Building 803, the Emergency Management Operations Building. This building was chosen because the Alertus system has already been installed so the as-built system information is available. Table 2-1 lists the number of components reviewed in this analysis.

Table 2-1. Number of components in Building 803 system

Component	803 System
GPON ONT unit	1
Alertus Beacon unit	1
Text to Speech Interface unit	1
Relay	1
Strobes	3
Speakers	3
Network component	1

The "network component" consists of the Sandia's hard-wired ethernet network which is connected to the GPON unit and enables it to send and receive signals from the emergency management command center. The "human error" component captures the failure mode where an electrician or other maintenance worker changes or cuts a wire to a component in the course of doing other work. If the system were to have continuous monitoring, the "human error" component can be removed.

Failure modes are the way each component can fail. A failure mode answers the question "How does the part fail?" This reliability study captures traditional failures of a component. For each component, credible failure modes were developed based on failure experience data collected in the Reliability Information Analysis Center (RIAC) Failure Mode Distribution and Non-Electric Parts Reliability Database [3, 4]. The RIAC is the U.S. Department of Defense's Center of Excellence in Reliability/Maintainability and Quality. The RIAC produces databases that contain failure mode and mechanism distribution data and failure data for a wide variety of electrical assemblies and electromechanical/mechanical parts and assemblies. Redundant cases for a given failure mode were

grouped together to simplify the analysis. The failure modes for each component are listed in Table 2-2.

Table 2-2. Failure Modes of System Components

	Relay	GPON ONT	Alertus Beacon	Text to Speech	Strobe	Speaker	Network
Failure Modes	Out of Specification	Improper Output	Improper Output	Improper Output	Degraded Operation	Degraded Operation	System Off-Line
	High Contact Resistance	Fail to Operate	Fail to Operate	Fail to Operate	Out of Specification	Out of Specification	
	Seal Failure	Intermittent	Intermittent	Intermittent	No Operation	No Operation	
	Degraded Operation	Leakage	Leakage	Leakage			
	Short	Out of Specification	Out of Specification	Out of Specification			
	No Operation						

2.5. Determining failure probabilities for failure modes

Each of the components within the fault tree is required to have a failure rate probability. In an ideal reliability study, there would be component reliability data from the manufacturer or site-specific data. Attempts were made to find manufacturer-supplied reliability component data for the speaker, strobe, Alertus components, relays and the GPON ONT but no specific data was available. Therefore, generic data for a component type was used when specific information was not available.

2.5.1. RIAC Component Analysis

Each system component was given a failure rate, based on a specified RIAC component listed in Table 2-3. The failure rate was defined as the number of failures per million hours, shown in Equation 1:

$$\lambda_p(per\ million\ hrs) = \frac{Number\ of\ failures}{Total\ hours\ (million)} \qquad \text{Eqn. 1}$$

In the case where no failures were reported in the database, a Bayesian methodology is used to calculate the failure rate. In the analysis conducted, the speaker was the only component to not have any failures for the time reported. In this instance, the Jeffrey's prior: 0.5 failures (half of an event) was used as the number of failures in the rate calculation.

Failure modes were also selected based on a RIAC component's failure modes, also shown in Table 2-3. In a couple of instances, the failure mode component was not the same component used for the failure rate. The RIAC database also listed failure mode probabilities for each failure mode. These failure mode probabilities were multiplied by the failure rate to obtain a failure mode rate which was inputted into the SAPHIRE software as a point value. This is shown in Equation 2:

$$\lambda = \alpha\lambda_p \qquad \text{Eqn. 2}$$

where λ_p is the failure rate (for all failure modes) for a specific component and α is the failure mode probability, which is the fraction of component failures corresponding to the failure mode. A closeup showing the failure modes and associated failure mode rates is illustrated in Figure 2-1.

Table 2-3. Failure Rates and Modes for Components

Component	RIAC Component for Failure Rate	Failure Rate	RIAC Component for Failure Modes	Failure Mode	Failure Mode Probability	Failure Mode Rate
Relay	Relay	8.02E-08	Relay	Out of Specification	0.274	2.20E-08
				High Contact Resistance	0.254	2.03E-08
				Seal Failure	0.148	1.19E-08
				Degraded Operation	0.121	9.73E-09
				Shorted	0.118	9.44E-09
				No Operation	0.085	6.81E-09
GPON ONT	Electrical Component	9.44E-06	Electrical Component	Improper Output	0.789	7.45E-06
				Fail to Operate	0.053	5.00E-07
				Intermittent	0.053	5.00E-07
				Leakage	0.053	5.00E-07
				Out of Specification	0.053	5.00E-07
Alertus Beacon	Electrical Component	9.44E-06	Electrical Component	Improper Output	0.789	7.45E-06
				Fail to Operate	0.053	5.00E-07
				Intermittent	0.053	5.00E-07
				Leakage	0.053	5.00E-07
				Out of Specification	0.053	5.00E-07
Text to Speech	Electrical Component	9.44E-06	Electrical Component	Improper Output	0.789	7.45E-06
				Fail to Operate	0.053	5.00E-07
				Intermittent	0.053	5.00E-07
				Leakage	0.053	5.00E-07
				Out of Specification	0.053	5.00E-07
Strobe	Alarm	1.07E-05	Alarm Annunciator	Degraded Operation	0.353	3.78E-06
				Out of Specification	0.353	3.78E-06
				No Operation	0.294	3.15E-06
Speaker	Speaker	1.4512E-08	Alarm Annunciator	Degraded Operation	0.353	5.12E-09
				Out of Specification	0.353	5.12E-09
				No Operation	0.294	4.27E-09

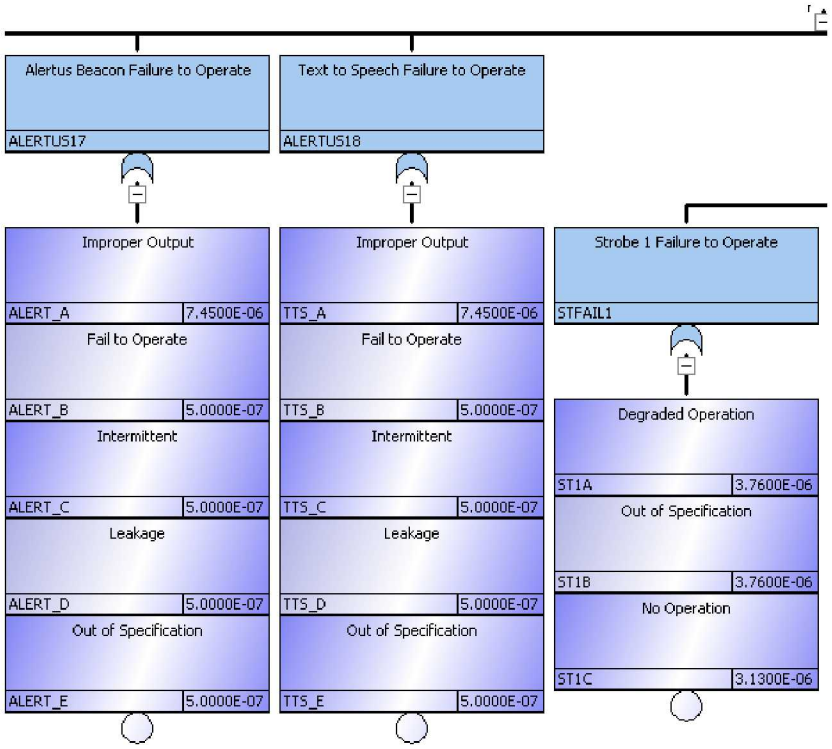

Figure 2-1. Closeup of a Portion of the Fault Tree

2.5.2. Network Analysis

The network itself is required to send signals from emergency management to the GPON ONT unit. The only failure mode in this scenario is that the network is not operating and the system is off-line. Sandia maintains its own metrics on system downtime and these were used to create an average system downtime. For the purposes of this report, the failure rate for the network is 6.71E-04.

2.5.3. Human Component

The failure mode of a maintenance worker accidentally cutting an incorrect wire was important to incorporate as the system is not currently designed to be addressable. However, there is no easy number to draw from for this human-caused failure. In the nuclear community, the failure rate of an average performance is assumed to be 1E-3, or error 1/1000 times [5]. This value was used to calculate an initial result and will be included in the sensitivity analysis to address uncertainty associated with this parameter. Placing the wires in conduit would also decrease this rate.

3. RESULTS

3.1. Fault Tree

The components, their associated failure modes and failure mode rates were inputted into a fault tree in the SAPHIRE software, illustrated in Figure 3-1. The fault tree is comprised of only OR gates, meaning that if any component were to fail it would constitute a system failure. In Boolean logic, all the failure mode rates would be multiplied in order to determine the system reliability. The reliability value for the Alertus system based on the analysis is 0.998269.

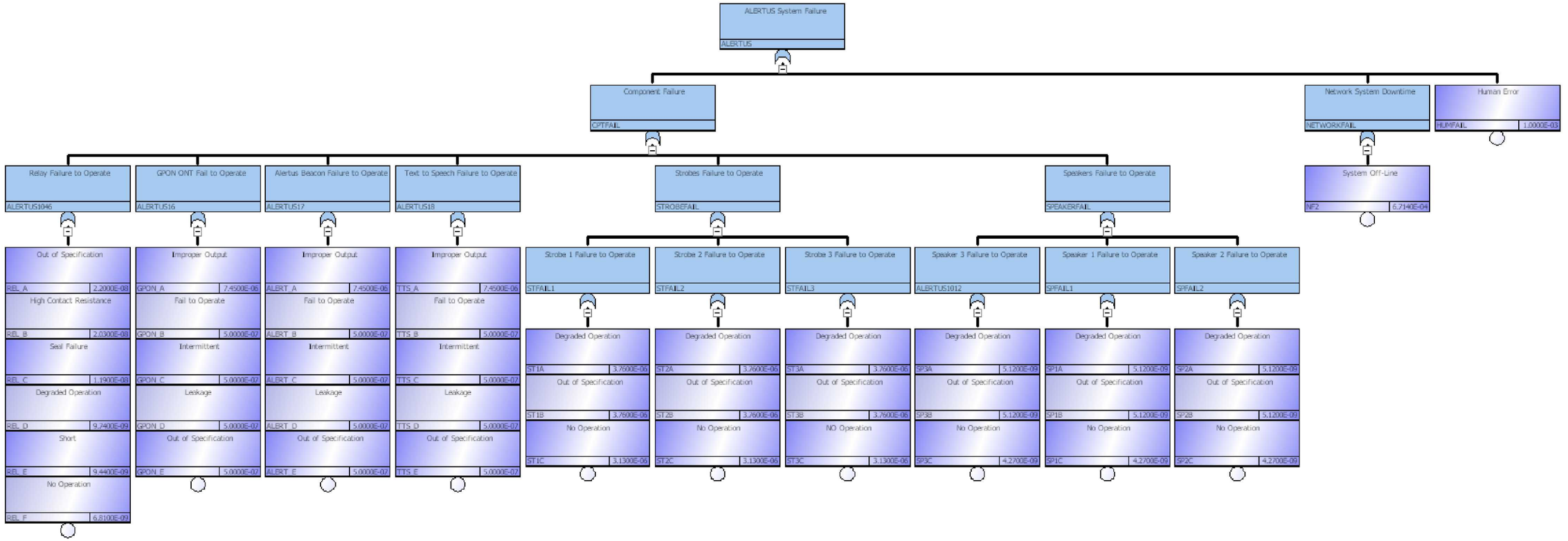

Figure 3-1. SAPHIRE Fault Tree for Alertus System

3.2. Human Error Sensitivity Analysis

The SAPHIRE software uses the probabilities of all the fault tree inputs and calculates a value based on the Boolean logic. The reliability value for the Alertus system based on the previously discussed inputs is 0.998269. The largest contributor to this value is the human error value as discussed in Section 2.5.3. Therefore, a sensitivity analysis was conducted to determine the reliability value if the system became addressable. Two alternate values were proposed for human error. The first scenario is for a non-addressable system but where the wiring is installed within conduit. Installing the wiring within conduit will better protect the wires from erroneous or unintentional cuts. A value for wires in conduits was found in the RIAC database and used to determine the probability for the conduit scenario. The second scenario analyzes a completely addressable system which would output an immediate error if a wire is cut, resulting in no human error component. The results of this are shown in Table 3-1.

Table 3-1. Human Error Sensitivity Analysis

	Human Error Probability	Fault Tree Probability
Non-Addressable, Wiring not in Conduit	1.00E-03	0.998269
Non-Addressable, Wiring in Conduit	4.05E-9	0.999268
Addressable	0	0.999269

3.3. Other Building Analysis

To compare the reliability of the 803 system, another much larger building was chosen for analysis. The building selected was building 880 whose number of components varied significantly from the Building 803 system, as shown in Table 3-2. Based on the updates to the number of components, the fault tree probability values were updated. These values demonstrate how varying the number of components changes the overall fault tree probability. Table 3-3 shows the fault tree probabilities for Buildings 803 and 880. The same sensitivity analysis for human error probability was performed for Building 880.

Table 3-2. Number of components in Buildings 803 and 880 systems

Component	803 System	880 System
GPON ONT unit	1	39
Alertus Beacon unit	1	39
Text to Speech Interface unit	1	39
Relay	1	39
Strobes	3	176
Speakers	3	176
Network component	1	1
Human Error	1	1

Table 3-3. Reliability values for Buildings 803 and 880

	Human Error Probability	Bldg. 803 Fault Tree Probability	Bldg. 880 Fault Tree Probability
Non-Addressable	1.00E-03	0.998269	0.995344
Non-Addressable, Wiring in Conduit	4.05E-9	0.999268	0.99634
Addressable	0	0.999269	0.99634

3.4. Next Steps

Appropriate next steps if the reliability results are not accepted involve conducting a detailed analysis based on manufacturer-provided reliability data instead of generic reliability information. Research to optimize the preventative maintenance testing of the system could identify failures in a timely manner.

REFERENCES

[1] *Comprehensive Emergency Management System*, 2016.

[2] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, "Fault Tree Handbook," U.S. Nuclear Regulatory Commission1981.

[3] Nonelectronic Parts Reliability Data Publication (NPRD-2016) [Online]. Available: https://www.quanterion.com/product/publications/nonelectronic-parts-reliability-data-publication-nprd-2016/

[4] Failure Mode Mechanism Distributions [Online]. Available: https://www.quanterion.com/product/tools/failure-mode-mechanism-distributions-fmd-2016/

[5] R. L. Boring, "Fifty Years of THERP and Human Reliability Analysis " presented at the Probabilistic Safety Assessment and Management (PSAM11), Helsinki, FInland, 2012. Available: https://inldigitallibrary.inl.gov/sites/sti/sti/5680968.pdf

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Alice Muna	8854	amuna@sandia.gov
Chris LaFleur	8854	aclafle@sandia.gov
Donald Lincoln	47371	dflinco@sandia.gov
Tomas Sanchez	4879	tmsanch@sandia.gov
Eugene McPeek	4876	emcpeek@sandia.gov
Technical Library	9536	libref@sandia.gov

This page left blank

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.