Functional Safety for Programmable Electronics Used in PPE: Best Practice Recommendations (In Nine Parts)

Part 7: Additional Guidance: Functional Safety by Design (FSD) Examples

Prepared by Safety Requirements, Inc.

NIOSH Contract 200-2003-02355,
September 2007

TABLE OF CONTENTS

TABLE OF CONTENTS I

LIST OF TABLES II

FOREWORD 4

BACKGROUND 4
THE REPORT SERIES 4
REPORT SCOPES 5
INTENDED USERS 10
RELEVANCE OF THE GUIDELINES 10
REFERENCE GUIDELINES AND STANDARDS 10

ACKNOWLEDGEMENT 13

ABSTRACT 14

1.0. INTRODUCTION 15

1.1. REPORT SCOPE 15
1.2. OVERVIEW OF FUNCTIONAL SAFETY ANALYSIS (FSA) PROCESS 16
1.3. CASE EXAMPLE: DEVICE THAT KEEPS YOU SAFE (DKYS) 19

2.0. JOB HAZARD ANALYSIS (JHA) 25

2.1. OVERVIEW OF JHA METHOD 25
2.2. JHA SUPPLIER-INPUT-PROCESS-CUSTOMER-OUTPUT (SIPOC) FORM (FORM FR-JHA-001 VERSION 1.0) 27
2.3. JHA PROCESS STEPS 29
2.4. JHA OUTPUT 31

3.0. HAZARD ANALYSIS (HA) 34

3.1. OVERVIEW OF THE HA METHOD 34
3.2. HA PROCESS STEPS 35
3.3. HA SIPOC FORM (FORM RS-HA-001 VERSION 1.0) 36
3.4. HA OUTPUT 41

4.0. DESIGN FAILURE MODE AND EFFECTS ANALYSIS (DFMEA) 44

4.1. OVERVIEW OF DFMEA METHOD 44
4.2. DFMEA SIPOC 46
4.3. DFMEA PROCESS STEPS 48
4.4. DFMEA OUTPUT 52

5.0. RISK ANALYSIS (RA) 54

5.1. OVERVIEW OF METHOD 54
5.2. RISK ANALYSIS SIPOC 60
5.3. RA PROCESS STEPS 62
5.4. RA OUTPUT 63

6.0. ABBREVIATIONS 64

7.0. GLOSSARY 66

APPENDIX 73

AUTODCP 73
EASY-FMEA 73
FMECA MODULE OF RELIABILITY WORKBENCH 74
FMEA-PRO 74
RELEX FMEA/FMECA 75
SABATON 75
XFMEA 75

LIST OF FIGURES

Figure 1 - The functional safety report series. 5
Figure 2 - Relationships among Parts 6, 7, 8, and 9 8
Figure 3 - Functional Safety Analysis (FSA) Process Steps 18
Figure 4 - Engineering Concept for DKYS Locator Subsystem 20
Figure 5 - Illustration of Interface Concept for Commander's PDA 22
Figure 6 – JHA Process Steps 28
Figure 7 – HA Process Steps 37
Figure 8 - DFMEA Process Steps 47
Figure 9 - Distribution of RPN Values 59
Figure 10 - RA Process Steps 61

LIST OF TABLES

Table 1 - Mining Industry Guidelines 11
Table 2 - Overview of ANSI UL 1988 and IEC 61508 12
Table 3 - High Tech's Updated Embedded System Engineering Process in support of NFPA 1800 Compliance 24
Table 4 - Primary Guidewords (Form RS-HA-001 Version 01) 35

Table 5 – Secondary Guidewords (Form RS-HA-002 Version 01) 39
Table 6 - Values of Severity (S) (from NFPA 1800 ESE) 49
Table 7 - Probability Values by Category 50
Table 8 - Detectability Criteria 51
Table 9 - Risk Category - RPN =1000 55
Table 10 - Risk Category - RPN =500 55
Table 11 - Risk Category - RPN = 250 55
Table 12 - Risk Category - RPN =125 55
Table 13 - Risk Category - RPN = 100 56
Table 14 - Risk Category - RPN = 50 56
Table 15 - Risk Category - RPN = 25 56
Table 16 - Risk Category - RPN =10 57
Table 17 - Risk Category - RPN = 5 57
Table 18 - Risk Category - RPN = 1 57
Table 19 - Frequency of RPN Values 58
Table 20- Example Acceptable RPN Values by Exposure Category 59
Table 21 – Possible Actions to Reduce RPN 62

FOREWORD

Background

Manufacturers of PPE use electronics and software technology to improve the safety of emergency responders and increase the likelihood of survival of victims. Electronics and software components embedded in PPE now provide protection, monitoring, and communication functions for emergency responders.

For example, innovative electronics and software engineers are accepting the challenge to design PPE that reduce reliance on audible communications. These products use radio and cellular frequencies to communicate digital information to the unit commander and among the various emergency responder agencies present on scene (i.e. police, fire, and rescue).

Innovators are also embedding electronics in turnout gear and taking advantage of newer materials. The result is more complex products including those that integrate products developed by different manufacturers. Although use of electronics and software provides benefits, the added complexity, if not properly considered, may adversely affect worker safety.

The Report Series

The report series contains best practice recommendations for the design and implementation of personal protection equipment and systems (PPE). The best practice recommendations apply to systems, protection layers, and devices using electronics and software embedded in or associated with PPE. The entire series provides information for use by life safety equipment manufacturers including component manufacturers, subassembly manufacturers, final equipment manufacturers, systems integrators, installers, and life safety professionals.

The reports in this series are printed as nine individual circulars. Figure 1depicts all nine titles in the series.

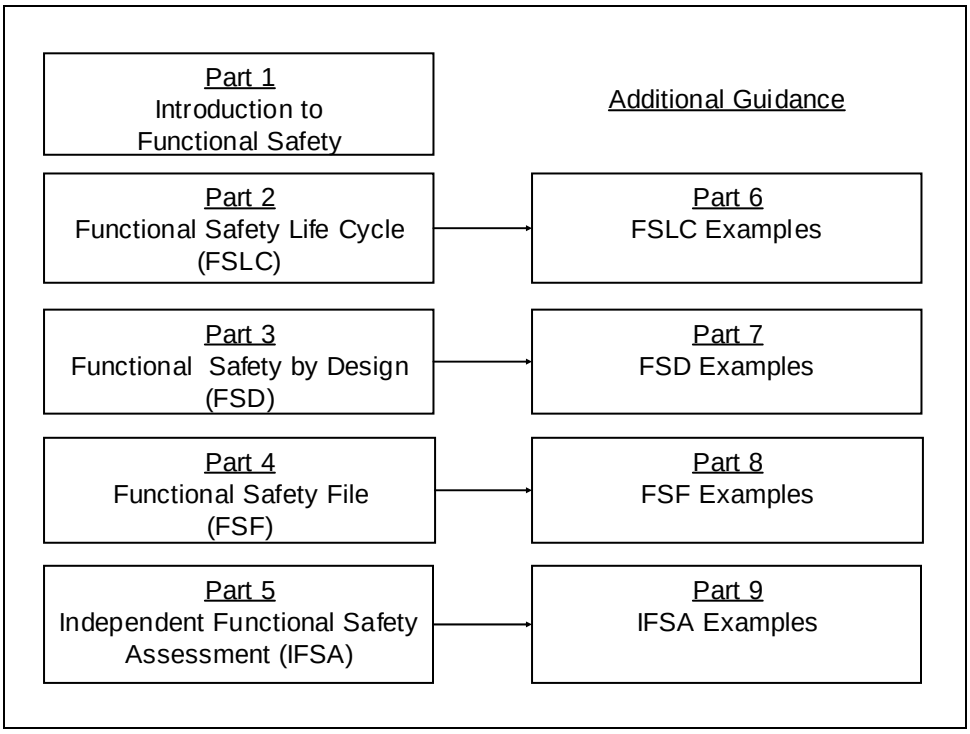


Figure 1 - The functional safety report series.

Report Scopes

Part 1: Introduction to Functional Safety

Part 1 is intended as an introductory report for the general protective equipment industry. The report provides an overview of functional safety concepts for advanced personal protective equipment and discusses the need to address them. The report also describes the practical benefits of implementing functional safety practices.

Part 2: The Functional Safety Life Cycle (FSLC)

Part 2 of the guidance recommends criteria for a Functional Safety Life Cycle. The use of a functional safety life cycle assures the consideration of safety during all phases of developing personal protection equipment and systems (PPE) from conceptualization to retirement, thus reducing the potential for hazards and injuries. The FSLC adds additional functional safety design activities to the equipment life cycle. FSD activities include identifying hazards due to functional failures, analyzing the risks of relying on electronics and software to provide functions, designing to eliminate or reduce hazards, and using this approach over the entire equipment life cycle. These activities start at the

equipment level and flow down to the assemblies, subsystems, and components.

Part 3: Functional Safety by Design (FSD)

Functional safety seeks to design safety into the equipment for all phases of its use. Electronics and software are components; therefore, design of these components must take into account the overall achievement of functional safety. Part 3, Functional Safety by Design (FSD) provides best practice design criteria for use by manufacturers of PPE. The Mining industry guidelines prepared by NIOSH, MSHA and the mining industry manufacturers and entitled Programmable Electronic Mining Systems: Best Practices Recommendations (in Nine Parts)[1] serves as a basis for these guidelines. The report also draws from the design criteria found in International Electro-technical Commission (IEC) Standard 61508 Functional Safety of E/EE/PE Safety Related Systems[2] and the American National Standards Institute(ANSI) by Underwriters Laboratories(UL) 1998 Standard for Safety – Software in Programmable Components[3].

Part 4: Functional Safety File (FSF)

Part 4, Functional Safety File (FSF), details best practices for safety documentation through the development of a document repository named the FSF. Capturing safety information in the FSF repository starts at the beginning of the FSLC and continues during the full life cycle of the system. The FSF provides the documented evidence of following FSLC and FSD guidance in the report series. In essence, it is a “proof of safety” that the system and its operation meet the appropriate safety requirements for the intended application.

---

1 NIOSH Mining Industry Circulars 9456, 9458, 9460, 9461, 9464, 9487, 9488 Programmable Electronic Mining Systems: Best Practices Recommendations, 2001-2002. For further detail, see http://www.cdc.gov/niosh/mining/pubs. Date accessed: October 31, 2006.

2 IEC 61508 Functional Safety of E/EE/PE Safety Related Systems. For further detail, see http://www.iec.ch/61508 . Date accessed October 31, 2006

3 ANSI UL 1998 Standard for Safety: Software in Programmable Components. For further detail, see http://www.ul.com/software/ansi.html . Date accessed October 31, 2006.

Part 5: Independent Functional Safety Assessment (IFSA)

Part 5, Independent Functional Safety Assessment (IFSA), describes the scope, contents, and frequency of conducting IFSAs. The IFSA is an assessment of the documented evidence of the FSLC activities and FSD practices.

Part 6, 7, 8 and 9: Functional Safety - Additional Guidance

The Additional Guidance Reports consists of Parts 6, 7, 8, and 9 of the report series, and provides additional detail, which will help users to apply the functional safety framework.

The Parts 6, 7, 8 and 9 guidance information reinforces the concepts, describes various methods and tools that can be used, and gives examples and references. The guidance reports are not intended to promote a single methodology or to be an exhaustive treatise of the subject material. They provide examples and references so that the user may intelligently choose and implement the appropriate approaches given the user's application as follows:

- Part 6 – Additional Guidance: Functional Safety Life Cycle Examples are used to develop the Scope of the Project Plan. The scope guides Project Functional Safety by Design (FSD) Compliance and Project Documentation.
- Part 7 – Additional Guidance: Functional Safety by Design Examples drives Project Design for Safety Compliance, which then becomes part of the Project Documentation.
- Part 8 – Additional Guidance: Functional Safety File Examples help to complete the Project Documentation, to enable a third party assessment.
- Part 9 – Additional Guidance: Independent Functional Safety Audit Examples are employed in the development of the Third Party Assessment Report. Figure 2 overviews the relationships among Parts 6, 7, 8, and 9.

Part 6– Additional Guidance: Functional Safety Life Cycle (FSLC) Examples

Many manufacturers are ISO 9001 compliant as a result of requirements in NFPA codes and standards, follow Six Sigma approaches, and are using the Department of Defense

(DoD) Software Engineering Institute (SEI) Capability Maturity Model (CMM) to improve life cycle practices. Part 6 provides a re-usable baseline FSLC Project Management Template (FSLC-PMT) that integrates these approaches. It also introduces the case example of DKYS, Device that Keeps You Safe to illustrate an FSLC. Appendix A of Part 6 is a general review of project management tools available to manage the FSLC activities.

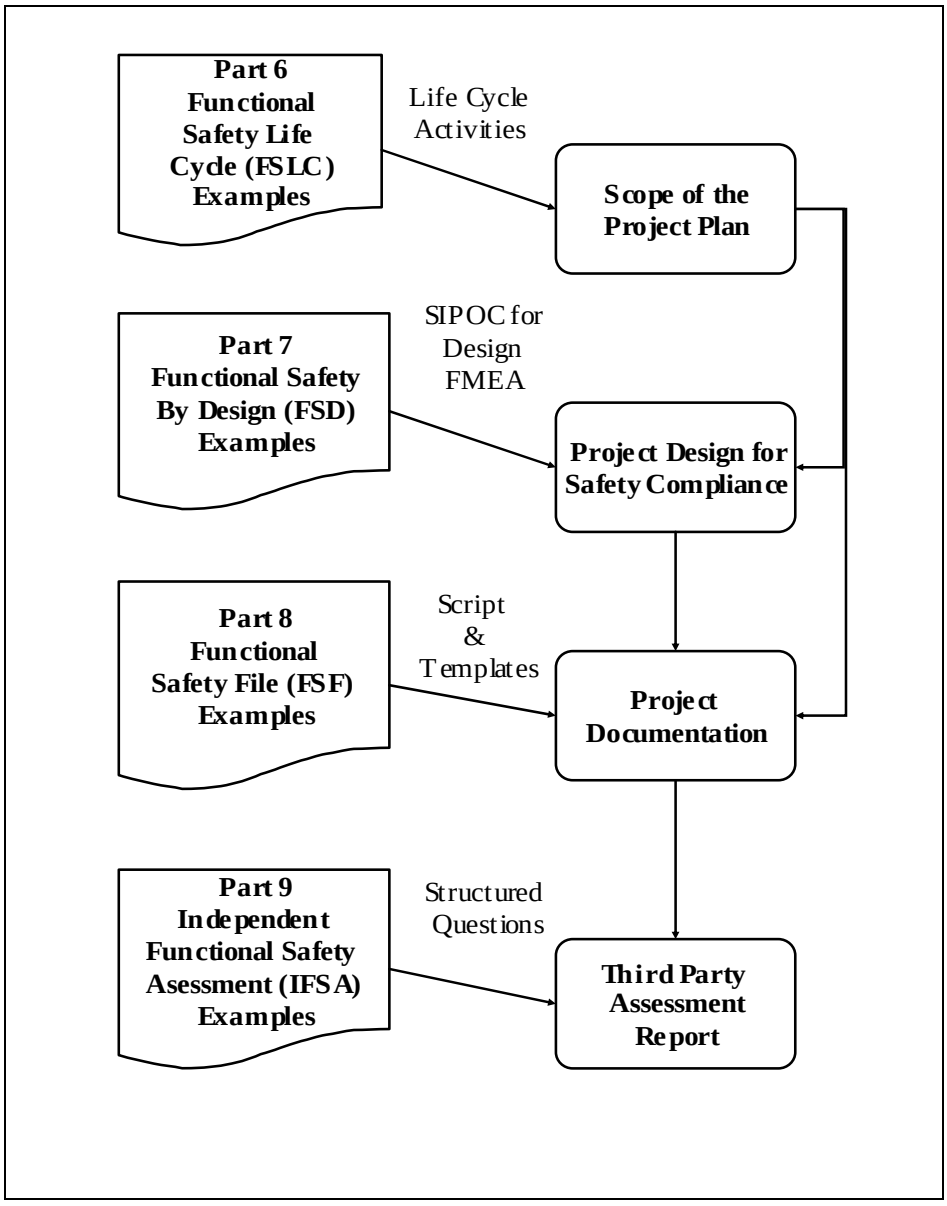


Figure 2 - Relationships among Parts 6, 7, 8, and 9

Part 7 – Additional Guidance: Functional Safety by Design (FSD) Examples

Part 7 bridges theory with practice for design activities by illustrating a Functional Safety Analysis (FSA) for person locator functions embedded in the DKYS components. The illustration addresses the conduct of a Job Hazard Analysis (JHA), a Hazard Analysis (HA), a Design Failure Modes and Effects Analysis (Design FMEA), and a Risk Analysis (RA). The report also references tools for conducting a Design FMEA.

Part 8 – Additional Guidance: Functional Safety File (FSF) Examples

Part 8 – Additional Guidance: Functional Safety File (FSF) Examples provides a prototype FSF Document Management System (DMS). Screen shots from the DMS define how a FSF may be organized and accessed. The prototype FSF-DMS supports preparation and management of FSF documents that would be submitted for an IFSA. The FSF-DMS uses the hypothetical next generation electronic safety equipment product, code-named DKYS, for Device that Keeps You Safe for illustration. Saros Inc's PDF Director System was used for rapid prototyping of the FSF-DMS. Appendix A provides information on PDF Director and other potential tools for DMS development.

Part 9 – Additional Guidance: Independent Functional Safety Assessment (IFSA) Examples

Part 9 – Additional Guidance: Independent Functional Safety Assessment Examples provides an approach to conducting an IFSA and an example audit questionnaire. The approach involves inspecting FSF documents using the questionnaire.

Intended Scope of Application

Systems, protection layers, and devices using electronics and software embedded in or associated with a PPE are within the intended scope of application. These provide

- Sensing and measuring biological, chemical and environmental characteristics of the site zone
- Providing auditory, vibration, visual, and sensory cues to an emergency responder
- Sensing and measuring physiological parameters about the emergency responder

- Identifying the location of the emergency responder
- Transmitting and receiving information about the site zone and the emergency responder
- Integrating and displaying safety information about site zones

Intended Users

The guidance is intended for use by life safety professionals and equipment manufacturers including:

- Manufacturers of components, subassemblies, and assemblies
- Final equipment manufacturers
- Systems integrators and installers
- Standards developers
- Equipment purchasers/users

Relevance of the Guidelines

- These recommendations do not supersede federal or state laws and regulations or recognized consensus standards.
- These recommendations are not equipment or application-specific.
- These recommendations do not serve as a compliance document.

Reference Guidelines and Standards

Mining industry guidelines prepared by NIOSH, MSHA and the mining industry manufacturers and entitled *Programmable Electronic Mining Systems: Best Practices Recommendations (in Nine Parts)* serves as a basis for these guidelines. Table 1 - Mining Industry Guidelineslists the published documents that form part of the mining industry guidelines. These documents can be found at http://www.cdc.gov/niosh/mining/topics/topicpage23.htm .

The mining guidelines are based on the requirements in existing standards—two of which are particularly applicable to PPE. These standards are the *ANSI UL 1998,*

Standard for Safety: Software in Programmable Components and IEC 61508, Functional Safety: E/EE/PE Safety-Related Systems. Table 1 provides an overview of both standards.

IC	Title	Authors	Year
9456	Part 1: 1.0 Introduction	John J. Sammarco, Thomas J. Fisher, Jeffrey H. Welsh, and Michael J. Pazuchanics	April 2001
9458	Part 2: 2.1 System Safety	Thomas J. Fisher and John J. Sammarco	April 2001
9460	Part 3: 2.2 Software Safety	Edward F. Fries, Thomas J. Fisher, and Christopher C. Jobes, Ph.D.	April 2001
9461	Part 4: 3.0 Safety File	Gary L. Mowrey, Thomas J. Fisher, John J. Sammarco, and Edward F. Fries	May 2002
9464	Part 5: Independent Functional Safety Assessment.	John J. Sammarco and Edward F. Fries	May 2002

Table 1 - Mining Industry Guidelines

STANDARD	ANSI UL 1998	IEC 61508
Title	Standard for Safety: Software in Programmable Components	Functional Safety: E/EE/PE Safety-Related Systems
Convened	1988	Early eighties

Approach	• Components
	• Embedded electronics and software
	  • Integrated safety controls
	  • Risk reduction based on coverage of identified hazards
	  • Equipment safety requirements
		• Components and systems
		• Networked
		• Separately instrumented safety systems
		• Risk reduction based on safety integrity level requirements
		• Equipment safety requirements

Standards Development Organization	Underwriters Laboratories (UL)	IEC SC 65A Working Group 9 and 10
Publication Date	First Edition: 1994 ANSI Second Edition: 1998	1998–2000
Where to obtain	http://www.comm-2000.com	http://www.iec.ch
Relevant URLs	http://www.ul.com/software/ http://www.ul.com/software/ansi.html	http://www.iec.ch/61508
Applications	UL 325, UL 353, UL 372, UL 1699, UL 1740, UL 2231, UL 61496	IEC 61511, IEC 62061, IEC 61496, IEC 61800-5

Table 2 - Overview of ANSI UL 1988 and IEC 61508

ACKNOWLEDGEMENT

In 1999, at the request of Congress, the National Institute for Occupational Safety and Health (NIOSH) established the National Personal Protective Technology Laboratory (NPPTL). The NPPTL provides leadership in the prevention and reduction of occupational disease, injury, and death for those workers who rely on personal protective technologies. Additional information about NPPTL can be found at http://www.cdc.gov/niosh/npptl and in NIOSH Publication 2003-127, National Personal Protective Technology Laboratory or by contacting Mr. Tim Rehak, the Project Officer at (412) 386-6866.

ABSTRACT

Emergency responders risk their lives to save the lives of others. It is a priority to provide them with the best equipment and the best guidance to minimize their exposure to hazards.

Advanced Personal Protection Equipment (PPE) incorporate product-ready technology in electrical, electronic, and programmable electronics. Use of newer materials, software, and wireless communications reduce safety risks. Experience has shown though, that these personal protective technologies may fail in ways not previously anticipated. Therefore, guidance for their use and integration is necessary.

The report, Additional Guidance: Functional Safety by Design (FSD) Examples is Part 7 in a nine-part series of recommendations addressing the functional safety of advanced personal protective equipment and systems (PPE) for emergency responders. As the companion document to Part 3 - it contains an example Functional Safety Analysis process. The process applies to early life cycle definition of PPE requirements as prior studies have identified requirements errors as a primary root cause of equipment field failures.

Part 7 provides information for use by life safety equipment manufacturers and users including component manufacturers, subassembly manufacturers, final equipment manufacturers, systems integrators, systems installers and life safety professionals.

1.0. INTRODUCTION

1.1. Report Scope

The report, Additional-Guidance: Functional Safety by Design (FSD) Examples is Part 7 in the nine-part series of recommendations addressing the functional safety of advanced Personal Protective Equipment (PPE) for emergency responders. As the companion document to Part 3, Part 7 bridges theory to practice by illustrating a best practices example for a Functional Safety Analysis (FSA) of PPE using electronics and software components.

The illustration provides one approach for complying with requirements in Section 6.4 Systems Design Approach and Criteria in the proposed NFPA 1800, Standard on Electronic Safety Equipment for Emergency Services[4]. The example FSA process addresses Requirements 6.4.1 and 6.4.2 in the NFPA 1800 standard.

The FSA process applies to early life cycle definition of PPE requirements. Multiple studies have identified requirements errors as a major source of field problems with equipment[5] . These problems may result in potential mishaps and they become more and more costly to correct as equipment development progresses.

The FSA process example described in this report provides a structured and formal approach which works well when projects are large (e.g. more than ten project members) and when two or three companies may be involved. The formalism shown may introduce unnecessary overhead for smaller, less complex projects. Some of the formalism may be eliminated for smaller projects if the objectives of all steps shown are met.

---

[4] NFPA 1800, Standard on Electronic Safety Equipment for Emergency Services, National Fire Protection Association, Boston, Mass., 2006. http://www.nfpa.org .

[5] Functional Safety for Programmable Electronics Used in PPE: Best Practice Recommendations (In Nine Parts), Part 1: Introduction to Functional Safety, National Institute for Occupational Safety and Health (NIOSH), National Personal Protective Technology Laboratory. Draft 2004.

1.2. Overview of Functional Safety Analysis (FSA) Process

1.2.1. Process Steps

The Functional Safety Analysis (FSA) process has four primary sub-processes. These sub-processes provide for analysis and traceability from emergency responder tasks to equipment designed to reduce the risk of hazards associated with job tasks. **Error! Reference source not found.** provides an overview of the FSA Process Steps.

The FSA process begins with the Job Hazard Analysis (JHA) conducted by the emergency responder organization. The JHA identifies hazards present during the execution of job tasks. The emergency responder organization identifies an initial version of requirements for equipment to protect against those hazards that are identified. Section 2.0 describes example steps for conducting a JHA.

Using the JHA and the initial requirements as input, the equipment manufacturer develops a Hazard Analysis (HA) for the equipment and uses this to produce a second version of requirements. The HA clarifies and augments the initial requirements specification. Section 3.0 describes example steps for conducting an HA.

The second version of requirements becomes the starting point for equipment design. As the equipment is designed, potential failure modes are identified and addressed as part of an iterative Design Failure Modes and Effects Analysis or Design FMEA. The Design FMEA clarifies and augments the second version of the requirements specification leading to a third version. Section 4.0 describes example steps for conducting a DFMEA.

The Design FMEA culminates when risks are minimized to an acceptable level as determined by the risk analysis (RA) for the equipment. A fourth or final version of the requirement specification is produced to ensure consistency between what is being required and user expectations.

Section 5.0 describes example steps for conducting a RA.. A quasi-quantitative measure, the RPN is computed as part of the RA . A target value for the RPN is specified in advance to achieve a consistent stopping point for all PPE depending on the environment of use.

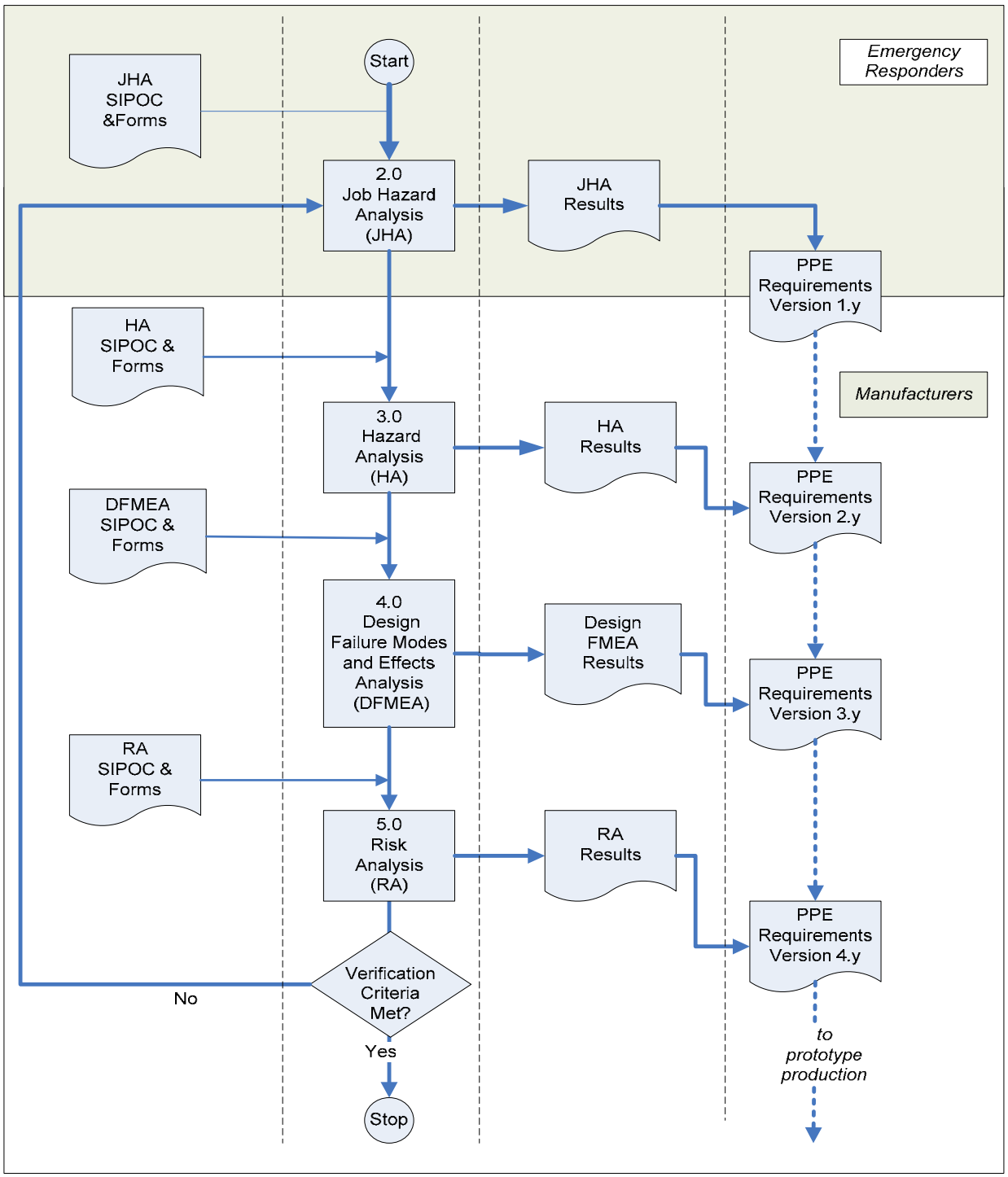
1.2.2. Process Stakeholders

The equipment manufacturer is the primary stakeholder for the FSA process. If the solution involves integrating PPE across different manufacturers, then the System Integrator is the primary stakeholder. Although the JHA is conducted by the emergency responder, it is important for the equipment manufacturer and the system integrator to consider the JHA and to learn how the equipment will be used. The manufacturer cannot anticipate all the ways in which equipment can be used or misused. The FSA steps provide both a specification of intended uses and evaluation of fitness for those intended uses. An emergency responder may develop a use for the equipment that is not part of its existing specification. An example of this situation might be attaching an accessory to the PPE in the field. It is recommended that the emergency responder revisit the JHA step and contact the manufacturer.

1.2.3. Fitness for Intended Use

Involving the customer in discussions about hazards, requirements, and failure modes may seem time consuming. These discussions, however, provide much clarification of what is actually needed by the emergency responder to successfully accomplish job tasks. Hardware and software designers of embedded functions need to be able to clarify the impact of the design decisions that they may make when designing electronics and writing software code. It is important to involve the hardware and software designers in early stakeholder meetings where requirements are discussed and clarified**.**

Figure 3 - Functional Safety Analysis (FSA) Process Steps



1.3. Case Example: Device that Keeps You Safe (DKYS)

1.3.1. Background

The report Part 6 - Additional Guidance: Functional Safety Life Cycle Examples[6] described a garment, a dickey; that is easily donned, lies flat against the wearer's body, and is held down by the weight of turnout gear. The garment, developed by Responder Safety, Inc. is code-named DKYS, for Device that Keeps You Safe. The dickey provides equipment warnings to the user, active Radio Frequency Identifier (active RFID) tags, and biological measurements, motion detection, communications, and data recording functionality.

Part 7 focuses on the DKYS function which provides the locations of emergency responders to the unit commander.

1.3.2. Overview of DKYS Emergency Responder Locator Functional Requirements

Responder Safety, Inc has contracted with High Tech, Inc. to design the locator functionality. An initial concept definition meeting between Responder Safety, Inc, and High Tech, Inc. yielded the drawing shown in Figure 4. The DKYS locator system will automatically provide location information of the emergency responder to the unit commander.

The automatic communication will require an active Radio Frequency Identification (RFID) tag embedded in the DKYS. At least one emergency vehicle sent to a disaster scene would have a system that can be deployed to track the status and location of emergency responders. The laptop, one location sensor, and tag setup transmitter will be setup on or adjacent to the vehicle. At least two other portable location sensors would be setup around the scene to provide enough position data to triangulate the emergency responder's locations. In the event of inclement weather, the laptop and tag setup transmitter will be setup in a vehicle (e.g. a mobile command center or a fire chief's vehicle) and the sensors setup with appropriate cover. The commander would

[6] Functional Safety for Programmable Electronics Used in PPE: Best Practice Recommendations (In Nine Parts), Part 6 - Additional Guidance: Functional Safety Life Cycle Examples, National Institute for Occupational Safety and Health (NIOSH), National Personal Protective Technology Laboratory(NPPTL). Draft 2006.

have a Personal Digital Assistant (PDA) that is wirelessly connected to the laptop to allow free movement at the scene.

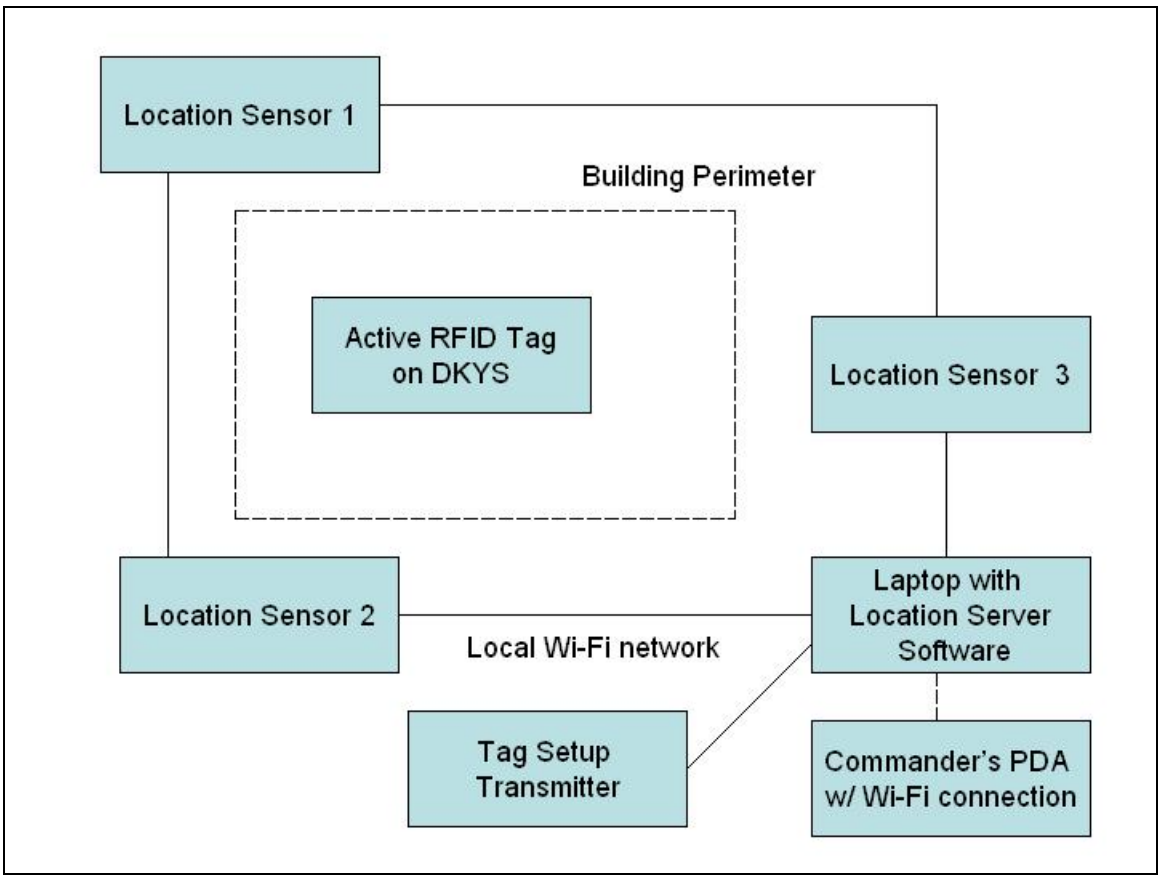


Figure 4 - Engineering Concept for DKYS Locator Subsystem

The Active RFID Tag device attached to the DKYS provides identification and location information of the emergency responder. The active RFID tag "blinks" an RF transmission at pre-programmed rates from 5 seconds and up. The location sensors receive these blinks and uses Differential Time of Arrival (DTOA) algorithms to determine the location of the tag. Accuracy of the determined location is normally 2 to 3 meters. High Tech, Inc. is working with the tag manufacturer to improve this accuracy to 1 meter. Read ranges are published as 1000 meters outside to 300 meters inside and locate ranges of 300 meters outside and 100 meters inside. Standard operating frequency is 2.4GHz. Information being transmitted includes id and biometric data.

Location Sensors are connected to a laptop server via standard wired Ethernet cables

or an 802.11b-compliant wireless LAN. The location sensors receive the tag transmissions and forward the information to the dedicated laptop server. The location sensors are established at the perimeter of the incident site to allow for the triangulation of the emergency responder's positions.

The Location Server Software Station performs location calculations, database functions and systems management. The unit commander can view the emergency responder id and location data locally at the dedicated laptop or through his or her PDA. There may be more than one location server station. The number of stations will depend on the size, complexity, and the number of vehicles at the emergency scene.

Controlled from the laptop, the Tag Setup Transmitter transmits id information to the tag should a replacement tag be required on the scene. A job hazard control task requires that tags be pre-configured offsite.

The Unit Commander's PDA displays a emergency responder id, location information, and emergency responder status information. Figure 5 illustrates the view that the commander can access both from the laptop and PDA.

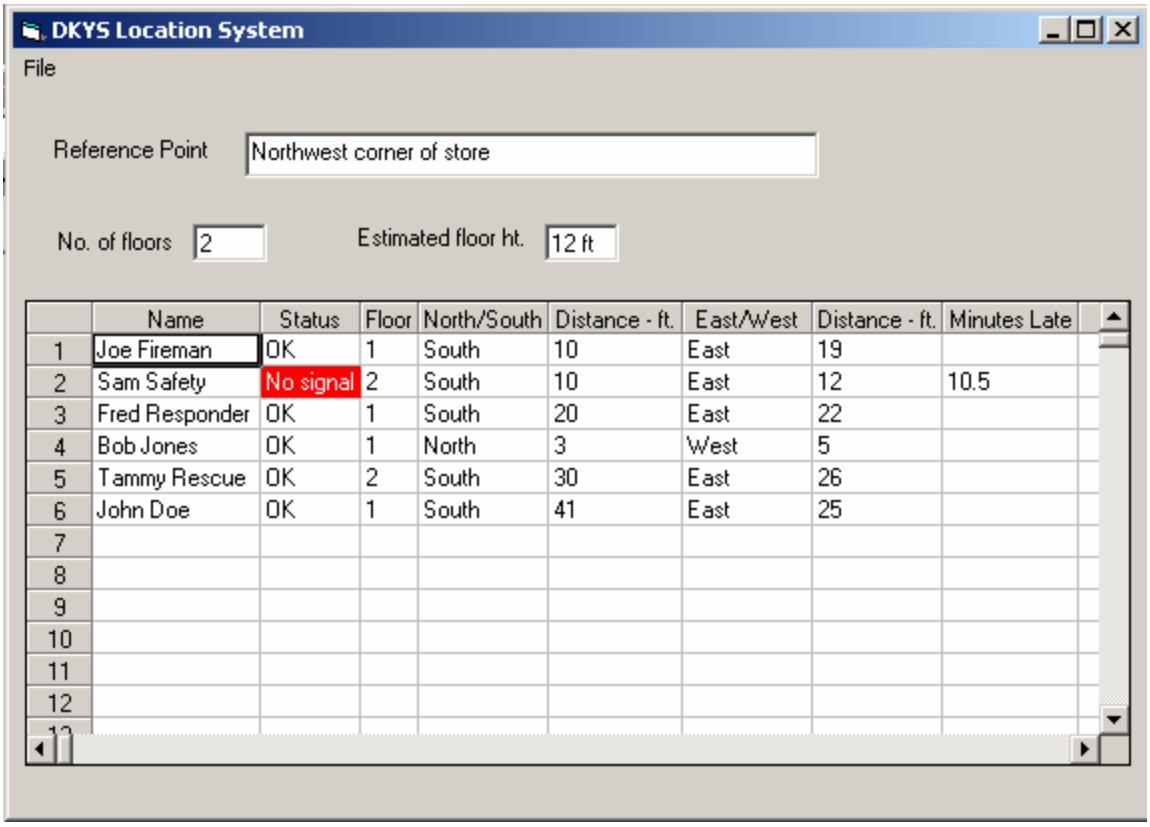


Figure 5 - Illustration of Interface Concept for Commander's PDA

Based on the discussions during the initial concept meeting - Responder Safety Inc. has requested that High Tech Inc. develop the locator electronics and software embedded in the DKYS product. Previously, High Tech submitted their embedded system prototype development process (See Section 3.2 of Part 6.), Responder Safety has requested that High Tech Inc. expand their practices by adding early life cycle safety verification activities. These activities will support Responder Safety's third party certification of DKYS with the requirements of NFPA ESE 1800 Section 6.4. Specifically, Responder Safety has requested that High Tech:

- Work with Responder Safety to obtain prospective customer input from a Job Hazard Analysis (JHA)
- Conduct a Hazard Analysis (HA) for the DKYS locator subsystem functionality
- Conduct Design Failure Mode and Analysis (DFMEA) activities as an integral part of their verification activities

- Prepare a quasi-quantitative Risk Analysis (RA)

1.3.3. High Tech Inc's Updated Embedded System Engineering Process

High Tech Inc. reviewed the proposed NFPA 1800 Standard[7] and updated their embedded system engineering process for compliance to Section 6.4. Table 3 illustrates the changes made to High Tech's process.

Note: High Tech has made these System Engineering Process changes for the DKYS project since it is a larger, more complex project. High Tech, Inc will continue to follow a simpler ad hoc process when conducting smaller innovative projects in the R&D laboratory which prototype ideas. For those prototypes that are commercialized, High Tech Inc. uses retrospective validation for testing and documentation.

[7] NFPA 1800, Standard on Electronic Safety Equipment for Emergency Services, National Fire Protection Association, Boston, Mass., 2006. http://www.nfpa.org.

<table>
<tr><th>Gate</th><th colspan="4">Definition</th><th>FSA Activity</th></tr>
<tr><td>0</td><td colspan="4">Project Go/No Go</td><td>Review Job Hazard Analysis</td></tr>
<tr><td>1</td><td colspan="4">Preliminary Requirements Stability/Design Readiness Review</td><td>Job Hazard Analysis Version 1.y
Hazard Analysis Version 1.y
Design FMEA Version 1.y
Risk Analysis Version 1.y
ESE Requirements Version 1.y</td></tr>
<tr><td rowspan="6">2</td><td colspan="4">Requirements Stability/Design Readiness Review[8]</td><td rowspan="6">Job Hazard Analysis Version 2.y
Hazard Analysis Version 2.y
ESE Requirements Version 2.y
Design FMEA Version 2.y
Risk Analysis Version 2.y
ESE Requirements Version 2.y</td></tr>
<tr><td colspan="2">Hardware</td><td colspan="2">Software/Firmware</td></tr>
<tr><td>2A1</td><td>Review Requirements</td><td>2B1</td><td>Review Requirements</td></tr>
<tr><td>2A2</td><td>Perform Functional and Timing Simulations</td><td>2B2</td><td>Review Design</td></tr>
<tr><td>2A3</td><td>Review Hardware Logic Assembly</td><td>2B3</td><td>Review Software/ Firmware Logic</td></tr>
<tr><td>2A4</td><td>Review Tests</td><td>2B4</td><td>Review Tests</td></tr>
<tr><td rowspan="5">3</td><td colspan="4">Design/Prototype Readiness Review</td><td rowspan="5">Job Hazard Analysis Version 3.y
Hazard Analysis Version 3.y
Design FMEA Version 3.y
Risk Analysis Version 3.y
ESE Requirements Version 3.y</td></tr>
<tr><td>3A</td><td colspan="3">Load Embedded Software/Firmware onto Control Hardware</td></tr>
<tr><td>3B</td><td colspan="3">Run Simulated/Emulated Usage Tests</td></tr>
<tr><td>3C</td><td colspan="3">Integrate Embedded Control into Equipment</td></tr>
<tr><td>3D</td><td colspan="3">Run Usage Tests</td></tr>
<tr><td>4</td><td colspan="4">Prototype Completion/Production Readiness Review</td><td>Job Hazard Analysis Version 4y
Hazard Analysis Version 4.y
Design FMEA Version 4.y
Risk Analysis Version 4.y
ESE Requirements Version 4.y</td></tr>
</table>

Table 3 - High Tech's Updated Embedded System Engineering Process in support of NFPA 1800 Compliance

[8] There is frequent on-going communication between the hardware and software/firmware engineers. The requirements stability/design readiness review activities may be combined for small systems.

2.0. JOB HAZARD ANALYSIS (JHA)

2.1. Overview of JHA Method

Job Hazard Analysis or JHA is a method to identify occupational safety and health hazards for workers before they occur. A JHA:

1. Focuses on the duties of the emergency responder by defining the work tasks conducted by the emergency responder
2. Identifies the equipment used by the emergency responder when conducting the work tasks
3. Specifies the attributes of the hostile, fire and hostile non-fire environments

OSHA 3071[9] identifies practices for Job Hazard Analysis in general. NFPA 1500[10] defines requirements for Occupational Safety and Health Programs for Fire Departments.

An important output from the JHA is Version 1.y[11] of the ESE Requirements Specification. The version may take the form of a purchasing specification and is typically developed by considering input from multiple manufacturers.

A JHA addresses what could go wrong, what are the consequences, how could it arise, what are other contributing factors, and how likely is it that the hazard could occur. After identifying the hazards, the analysis proceeds with the identification of hazard control measures starting with engineering controls, continuing with administrative controls, and then the use of PPE. Engineering control measures include elimination, removal or containment of the hazard. Administrative controls involve written operating procedures,

[9] OSHA 3071 Job Hazard Analysis, U.S. Department of Occupational Safety and Health, 2002. http:/www.osha.gov

[10] NFPA 1500, Standard on Fire Department Occupational Safety and Health Program, 2007. http://www.nfpa.org

[11] The version notation follows that used in the software industry. Specifically Version x.y refers to a formal release of a version of the requirements specification. A change in the value of x denotes a major release and the value of y denotes a minor release. The selected values of x are sequential numbers starting with the number one. The values of y are sequential numbers starting with the number zero.

exposure time limits, use of alarms or warning signals, use of a buddy system, and training.

Whenever ESE is used as a hazard control method, JHA best practice involves an additional step to further qualify job hazards stemming from use of the equipment. Manufacturers of PPE conduct this further analysis which is identified in this report as a Hazard Analysis (HA).

2.2. JHA Supplier-Input-Process-Customer-Output (SIPOC) Form (Form FR-JHA-001 Version 1.0)

<table>
<tr><th colspan="5">Form FR-JHA-001 Version 1.0</th></tr>
<tr><th colspan="5">Objective: Identify Emergency Responder job tasks which may become hazardous when Electronic Safety Equipment (ESE) fails to function in accordance with safety requirements</th></tr>
<tr><th>Supplier(s)</th><th>Input(s)</th><th>JHA Process</th><th>Output(s)</th><th>Customers</th></tr>
<tr><td>First Responder Safety Lead/Team</td><td>• Accident data
• List of Jobs
• Identification of Environment/ Criticality</td><td rowspan="3">See Figure 6.</td><td rowspan="2">• List of Hazardous Jobs (See 2.4.1)
• Job Hazard Analysis (See 2.4.2)
• Requirements Specification Version 1.0 (See 2.4.3)</td><td rowspan="2">• Equipment Design Team
• Equipment Design Verification Team</td></tr>
<tr><td>Safety Verification Lead/Team</td><td>• NFPA 1500
• OSHA 3071</td></tr>
<tr><td colspan="2"><u>Enablers</u>
• List of hazardous jobs
• List of job duties for hazardous jobs
• Training documents and records for hazardous jobs</td><td><u>Action Item List for Process/Enabler Changes:</u>
• Updated list of hazardous jobs
• Updated job duties for hazardous jobs
• Updated JHA process steps</td><td>• Process/ Enabler Owners</td></tr>
<tr><td colspan="5">Prepared by: Date: Page ___ of ___</td></tr>
</table>

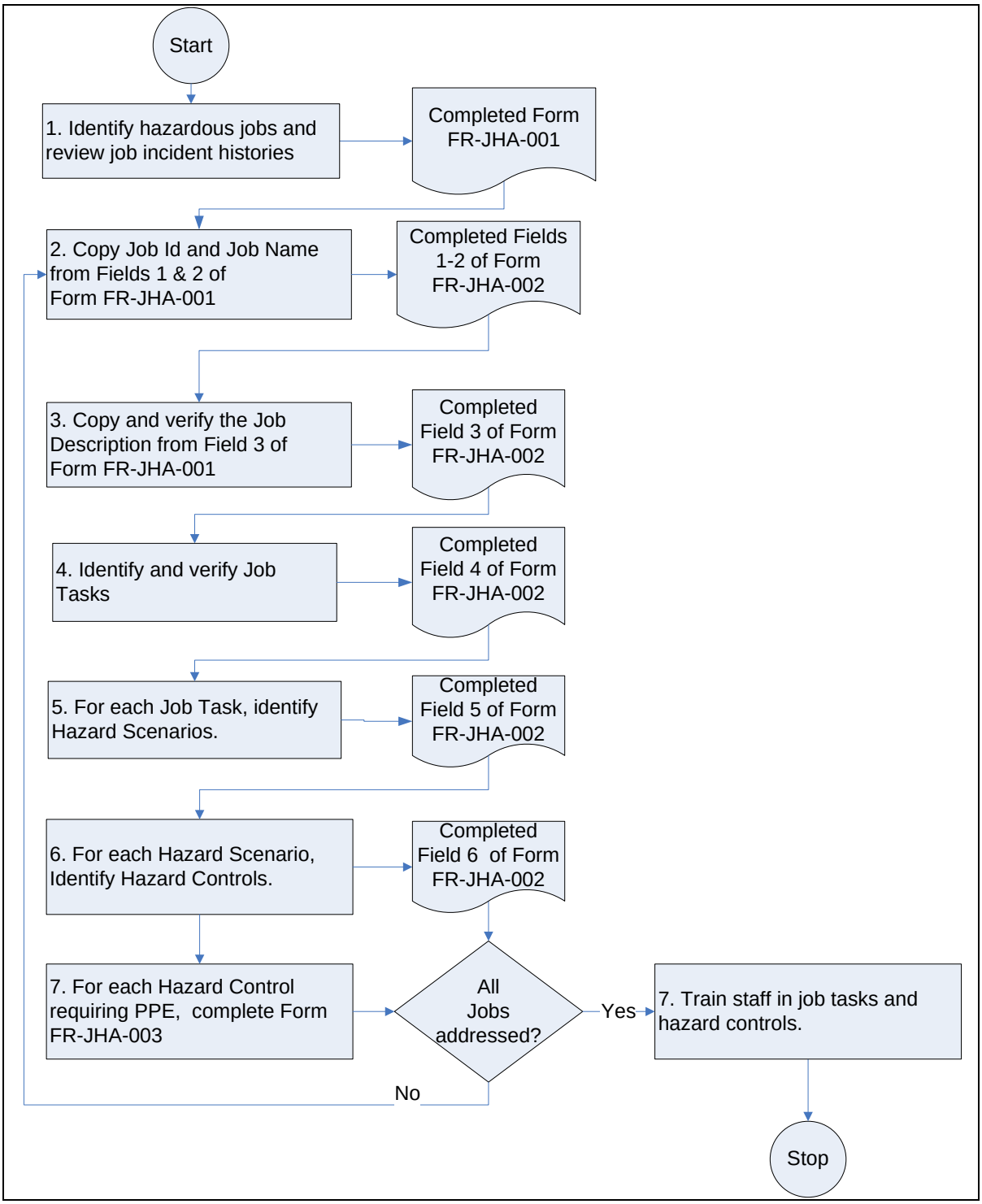


Figure 6 – JHA Process Steps

2.3. JHA Process Steps

2.3.1. Step 1- Identify and Review Hazardous Jobs and PPE Effectiveness

The JHA begins with completion of Form FR-JHA-001. The form lists the hazardous jobs that are new, have changed, or have not been previously studied. Job identification involves systematically describing the job objectives including a precise specification of the environment (hostile fire and hostile non-fire) which the emergency responder is operating within. A critical review of detailed incident reports, equipment problems, and hazard control studies and data can provide unique insights into how best to accomplish the job and minimize hazards. When PPE is relied on for hazard control, gauging the effectiveness of the PPE in the job environment becomes important.

2.3.2. Step 2 - Assign a Job Identifier

Once the jobs to be studied are identified, a unique identifier can be assigned. The identifier may be a standard job classification number and work item. The identifier and Job Name are recorded on Form FR-JHA-002 in Fields 1 and 2. There may be two job identifiers one for when the PPE is used in a hostile environment and one for when the PPE is used in a non-hostile environment.

2.3.3. Step 3 – Copy and Verify the Job Description

Step 3 carries forward the job description from Field 3 of Form FR-JHA-001 to Field 3 of Form FR-JHA-002. Verifying the job description against the job actually conducted makes certain that the appropriate jobs are studied as part of the JHA. The verification may be conducted as part of Step 1 instead. (See Section 2.3.1)

2.3.4. Step 4 – Identify and Verify Job Tasks

Step 4 identifies the job tasks for the job under review for hazard analysis. Here again, verification that these are the tasks conducted as a part of the job makes certain that the appropriate tasks are studied as part of the JHA. Additionally, training documents associated with the job and job tasks are identified and reviewed during this step if they have not been reviewed already during previous steps.

2.3.5. Step 5 – Identify Hazard Scenarios for each Job Task

Step 5 identifies hazard scenarios for each job task. It involves reviewing hazards

associated with similar job tasks, holding brainstorming sessions addressing “what if” scenarios, and reviewing research studies and accident data. Once the hazard scenarios are identified, the analyst may conduct a root cause analysis to assist them in determining if the hazard scenario can be eliminated at its root.

2.3.6. Step 6 - Identify Hazard Controls for each Hazard Scenario

Hazard controls for each hazard scenario are identified during Step 6. Hazard controls may involve avoiding the hazard by eliminating the job or changing the job task so that the hazard is removed or avoided, thus reducing the attendant risks. Whenever ESE is proposed as PPE to control hazards, consider training in proper care and maintenance, pre-op checkout, procedures for handling sensitivities, and user-friendly interfaces as important hazard control tasks.

2.3.7. Step 7 – Specify Requirements for PPE

Step 7 is an added JHA step that is important for communicating equipment needs between emergency responders and manufacturers of PPE. Using ESE for PPE amplifies the importance of Step 7 due to the failure modes of electronics technology. More clearly specified requirements yield more effective PPE for reducing job hazards. Here, the JHA analysts writes functional requirements that precisely specify what the expectations of the equipment are, what the parameters of the environments that the equipment is used in, proper handling and storage when not in use, and how to maintain equipment. As a part of communicating equipment needs, consider requesting that third party certification of ESE to the requirements stated in NFPA 1800.

2.4. JHA Output

2.4.1. List of Hazardous Jobs (Form FR-JHA-001 Version 1.0)

Form FR-JHA -001 Version 1.0				
LIST OF HAZARDOUS JOBS				
1 **Job Id**	**2** **Job Name:**	**3** **Job Description**	**4** **Reference(s)**	**5** **Notes**
001	***Unit Commander I***	***Assigns tasks and accounts for Fire Fighters while deployed in a hostile fire or hostile, non-fire environment.***	• ***HR Spec 001 Unit Commander*** • ***Attached Memo on PASS***	***JHA being revisited as a result of Fire Chief memorandum on potential for PASS device failures due to high temperatures. Chief Phoenix has requested that all ESE used for PPE be reviewed.***
Prepared by:			**Date:**	**Page ___ of ___**

2.4.2. Job Hazard Analysis (Form FR-JHA-002 Version 1.0)

Form FR-JHA -002 Version 1.0	
JOB HAZARD ANALYSIS	
1 Job Identifier: *001*	**2. Job Name: *Unit Commander I***
3 Job Description: ***Assigns tasks and accounts for Fire Fighters while deployed in a hostile fire or hostile, non-fire environment.***	
4 Job Tasks: ***Task 101 – Maintain up to date log of fire fighters deployed, approximate location, and status.***	
5 Job Hazard:	**6 Hazard Controls:**
***Unit Commander within hostile environment gets knocked out by falling timber*.**	**Unit Commander stays on perimeter of hostile environment and uses automated system to locate fire fighters**
Paper log gets destroyed by fire, wetness or blows away.	**Paper log replaced with Personal Digital Assistant**
Prepared by: ___*Joe Lead*_____Date: _____1/10/2007_____ Page ___ of ___	

2.4.3. Requirements Specification Version1.0 (Form FR-JHA-003 Version 1.0)

Form FR-JHA-003 Version 1.0			
Description: ***Personal Locator System to be used by emergency responders and unit commander to locate all deployed responders.***			
Top-Level Requirement Ref. No.	**Top Level Requirement**	**Sub-Level Requirement Ref. No.**	**Sub-level Requirements**
1	*Identify and locate all deployed emergency responders to unit commander.*	*1.1*	*Display identifier and location data on unit commander PDA or Laptop.*
		1.1.1	*Identifier must be unique in that no two operational emergency responders can have duplicate identifiers.*
		1.1.2	*Identifier must be visible in all hostile fire and hostile non-fire environments.*
		1.1.3	*Location data must be accurate to +/- one meter.*
		1.1.4	*Location data must be updated at least once per minute.*
Prepared by: _____*Joe Lead*_____ Date:1/10/2007			**Page ___ of ___**

3.0. HAZARD ANALYSIS (HA)

3.1. Overview of the HA Method

The JHA provides input to the Hazard Analysis (HA) which addresses hazards resulting from the potential for failure of the PPE. HA is a team approach for identifying and analyzing hazards associated with the use of PPE. The team uses primary and secondary guidewords to identify hazards that may result when the PPE fails to perform its intended function.

The following members make up the HA team:

- a moderator
- the equipment designer
- component designers
- electronics and software engineers
- emergency responders who use and maintain the equipment

The HA method is typically conducted at key milestones in the FSLC, including:

- during the conceptual design of the PPE,
- during prototype development
- when the prototype is complete and ready for production
- as part of the management of change process

Conducting a hazard analysis during the early conceptual stages of equipment design is sometimes referred to as a Preliminary Hazard Analysis or PHA. The use of the term preliminary connotes that the hazard analysis is not final and must be updated as the prototype is developed.

HA activities typically result in changes to requirements. Version 2.y of the requirements specification incorporates these changes. Proprietary information considered during the HA is marked as proprietary. Non-disclosure agreements may need to be signed by all

parties participating in the HA.

3.2. HA Process Steps

3.2.1. Step 1: Select Primary Hazard Analysis Guidewords

Table 4 provides a list of primary guidewords[12] to be used during the hazard analysis. Since the analysis focuses on PPE functions provided through the use of electronics and software technology, the analysis uses the term “Person-Equipment” for the primary guideword. Person-Equipment Hazards are hazards that are created by the clothing and equipment that the emergency responder wears. The type of hazard includes hazards that may result from failure of the PPE to perform part or all of its intended function.

Form RS-HA-001 Version 1.0			
	Hazard Ref. No.	**Hazard Guidewords**	**Description**
Primary	P-001	Person-Equipment Hazards	• Hazards to one or more emergency responders that are created by the failure of the electronics and software based PPE to perform part or all of its intended function.
Prepared by:		**Date:**	**Page of**

Table 4 - Primary Guidewords (Form RS-HA-001 Version 01)

3.2.2. Step 2- Select Secondary Hazard Analysis Guidewords

The secondary guidewords address hazards that the emergency responder is exposed to that could impact the functioning of the electronics and software based PPE. The guidewords were selected because the PPE electronics and software may exhibit failure modes when these hazards are present. Table 5 provides a list of secondary guidewords.

[12] The primary and secondary guidewords are an adaptation of the hazard types identified in Homeland Emergency Response Operational and Equipment Systems. Task 1. A Review of Modern Fire Service Hazards and Protection Needs.. Presented to: NIOSH/NPPTL. Presented by: Occupational Health and Safety Division, International Association of Fire Fighters.. 13 October 2003.

3.3. HA SIPOC Form (Form RS-HA-001 Version 1.0)

<table>
<tr><th colspan="5">Form RS-HA-001 Version 01</th></tr>
<tr><th colspan="5">Objective: Develop PPE Requirements from Hazard Analysis</th></tr>
<tr><th>Supplier(s)</th><th>Input(s)</th><th>Hazard Analysis Process Steps</th><th>Output(s)</th><th>Customers</th></tr>
<tr><td>Equipment Design Lead/Team</td><td>• List of PPE Requirements(See Section 2.4.3)
• List of Hazard Analysis Guidewords (See Table 4 and Table 5)
• JHA Requirements Specification</td><td rowspan="3">See
Figure 7.</td><td rowspan="2">• Completed Hazard analysis Table (See Section 3.4.1)
• Updated List of Requirements (See Section 1.1.1)
• Hazards to Requirements Map (See Section 3.4.3)</td><td rowspan="2">• Equipment Design Team
• Design Verification Team</td></tr>
<tr><td>Safety Verification Lead/Team</td><td>• NFPA ESE 1800 Section 6.4 Requirements</td></tr>
<tr><td colspan="2"><u>Enablers</u>
• List of Equipment Functions
• List of Hazard Analysis Guidewords
• Hazard Analysis Form</td><td><u>Action Item List for Process/Enabler Changes:</u>
• Updated List of Hazard Analysis Guidewords, as appropriate (See Table 4 and Table 5)
• Updated Hazard Analysis Process (See Section 3.2)</td><td>• Process/ Enabler Owners</td></tr>
<tr><td colspan="5">Prepared by: Date: Page ___ of ___</td></tr>
</table>

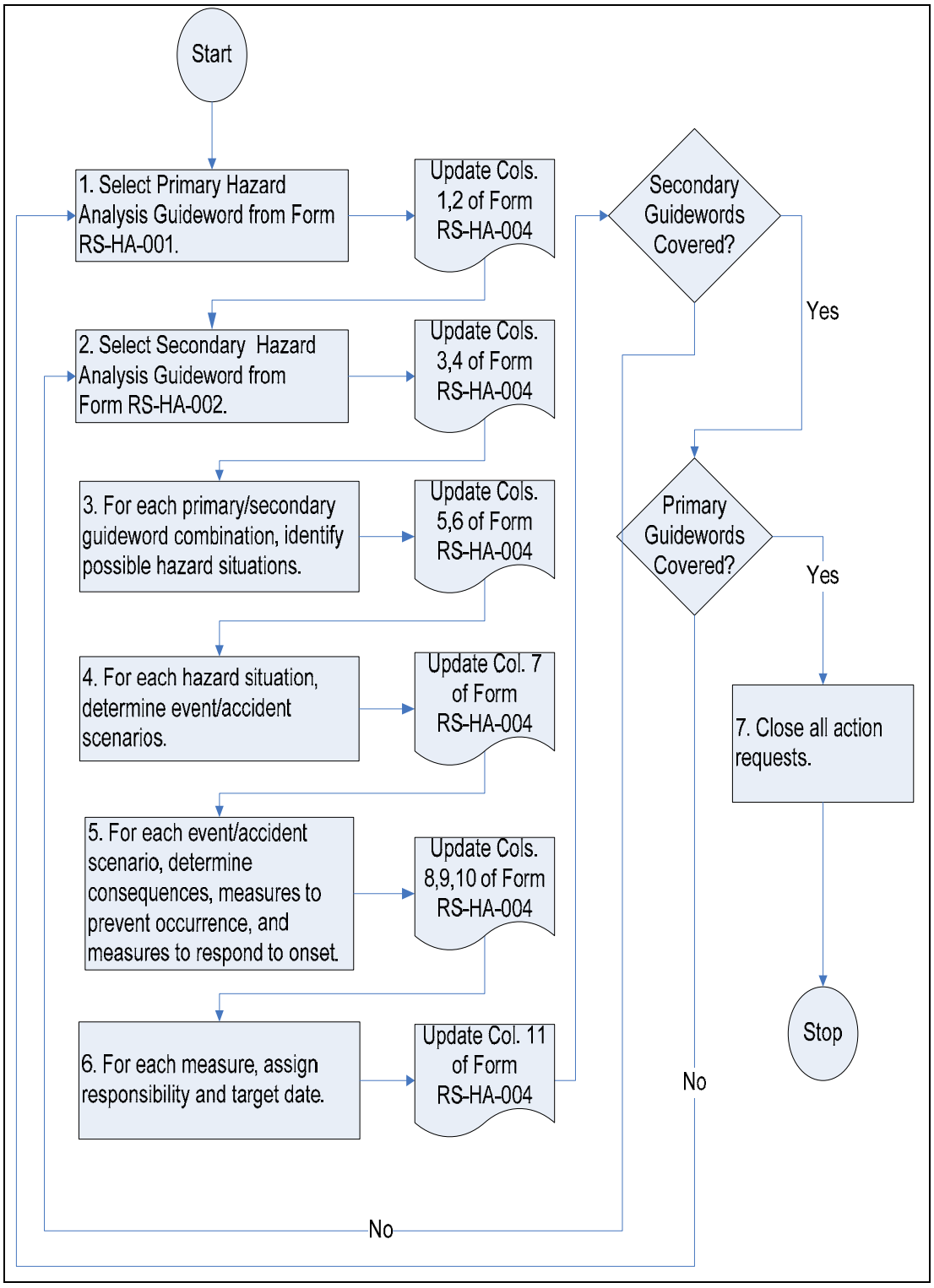


Figure 7 – HA Process Steps

Form RS-HA-002 Version 1.0			
	Hazard Ref. No.	**Hazard Guidewords**	**Description**
Secondary	S-001	Physical	Mechanical in nature or involving contact with an object that causes harm in some way (e.g. falling objects, flying debris, projectile/ballistic, abrasive rough surfaces, sharp edges, pointed objects, slippery surfaces, excessive vibration). For example, the RFID transmitter is dislodged from the emergency responder and then crushed by a falling object.
	S-002	Environmental	Environmental exposures encountered in the response environment: • High heat and humidity conditions (not extreme heat or thermal hazards) • Cold temperatures • Wetness • Electromagnetic Interference (EMI)/ Radio Frequency Interference (RFI) For example, the tag set up transmitter was left in the rain and has become non-operational.
	S-003	Thermal	Exposure to thermal energy from: • High heat sources (convective or radiant heat) • Flame impingement • Hot liquids and gases (hot water and steam) • Molten substances • Hot solids and surfaces For example, the electronics in the RFID tag melt.
	S-004	Chemical	Emergency responders encounter chemicals in a variety of different response activities, not just hazardous materials calls. The increasing presence of chemicals through industry and in households results in response environments, where chemicals are likely to be present. Each chemical poses different levels of hazards associated with its exposure. These hazards may include: • Toxicity (poisonous) • Corrosiveness • Irritation • Flammability • Reactivity (explosiveness or oxidation) For example, the location sensor is contaminated by a chemical spill and is no longer functioning.

Form RS-HA-002 Version 1.0			
	Hazard Ref. No.	**Hazard Guidewords**	**Description**
	S-005	Biological	Exposure to blood-borne pathogens, airborne pathogens, biological toxins, and biological allergens so that the equipment becomes contaminated. For example, the victim being rescued bleeds on the RFID tag. The victim is HIV positive.
	S-006	Electrical	Electricity may create three possible forms of hazards: • Exposure to electrical shock • Exposure to electrical arcs • Exposure to static electricity For example, there is a raging thunder storm and a key location sensor has been struck by lightening.
	S-007	Radiation	Radiation hazards are classified as either: • Ionizing radiation or • Non-ionizing radiation For example, a spill of radio active material contaminates the location sensor.
Prepared by: **Date:** **Page ___ of ___**			

Table 5 – Secondary Guidewords (Form RS-HA-002 Version 01)

3.3.1. Step 3 – Identify Possible Hazard Situations

The team identifies a hazardous situation that the PPE will aid in protecting the emergency responder.

3.3.2. Step 4 – Determine Hazardous Events and Consequences

The situation is further refined by identifying and considering events that could lead to the hazardous situation. Once the events are identified, the consequences are noted.

3.3.3. Step 5 - Determine Measures

Identify methods to prevent and/or to respond to the onset of the scenario.

3.3.4. Step 6 – Assign Responsibility and Target Date

Further action may be required to further assess the hazardous situation, determine event/accident scenarios or identify measures. In Step 6, the action is defined and responsibility assigned. Typical action items include clarifying requirements, adding requirements, and research to determine acceptable values of parameters in requirements.

3.3.5. Step 7 – Close all Action Requests.

Once the hazard analysis table is considered complete, closing all action requests becomes important.

Usually a quality assurance staff member takes ownership of the task because it involves checking for consistency between the required action and the action taken and noting any deviations. At times it also involves communicating with management to achieve closure on some tasks.

Of importance is making sure that the requirements have been updated and associated with hazards. This may be accomplished using Form RS-FSA-001 Hazards to Requirements Mapping shown in Section 3.4.3.

3.4. HA Output

3.4.1. Hazard Analysis Table

Form RS-HA-003 Version 01 Hazard Analysis Table

1 PRIMARY REF. NO. P001			2 PRIMARY GUIDEWORD : Person-Equipment		3 SECONDARY REF. NO. S002	4 SECONDARY GUIDEWORD: Environmental	
5 Hazard Ref No.	**6 Hazardous Situation**	**7 Event Ref. No**	**8 Hazardous Event**	**9 Consequences**	**10 Measures to Prevent Occurrence**	**11 Measures to Respond to the Onset of the Scenario**	**12 Action (what, who, by when)**
001	*Location of emergency responder unknown*	*001*	*Locator System electronic components exposed to high heat*	*Unit Commander is no longer able to locate emergency responders*	*Thermally insulate electronics to pass NFPA 1800 tests*	• *Add requirement for unit command function to displays loss of location information within 1 minute* • *Identify and implement fault tolerance algorithm to maximize locatability*	*Add DKYS Locator system design and verification requirements* *JRC 1/30/2007*
		002	*Locator System provides incorrect location for responder id*	*Unit Commander mis-deploys emergency responders*	*Require software code verification and testing as per NFPA 1800 Section 6*		
		003	*Locator System electronic components exposed to wetness*	*Unit Commander cannot locate emergency responders*	*Encapsulate in leak proof material. See NFPA 1800 Section 7*		
Prepared by:				**Date:**		**Page ___ of ___**	

3.4.2. Updated Requirements Specification (Form FR-JHA-003 Version 1.0)

FORM: FR-JHA-003 Version 1.0			
1 Description: ***Personal Locator System to be used by fire fighters and unit commander to locate all deployed responders.***			
2 **Top-Level Requirement Ref. No.**	**3** **Top Level Requirement**	**4** **Sub-Level Requirement Ref. No.**	**5** **Sub-level Requirements**
1	***Identify and locate all fire fighters to unit commander.***	***1.1***	***Display identifier and location data on unit commander personal digital assistant or laptop.***
		1.1.1	***Identifier must be unique in that no two operational emergency responders can have duplicate identifiers.***
		1.1.2	***Identifier must be visible in all hostile fire and hostile non-fire environments.***
		1.1.3	***Location data must be accurate to +/- one meter.***
		1.1.4	***Location data must be updated at least once per minute.***
		1.1.5	***Unit command function displays loss of location information within 1 minute***
		1.1.6	***Electronics must be thermally insulated .(See NFPA 1800 Section 7)***
		1.1.7	***Electronics must be leak proof . (See NFPA 1800 Section 7)***
		1.1.8	***Location system must be tolerant of x location sensor failures and y transmitter failures***
Prepared by: _____*Joe Lead*_____Date:1/10/2007 Page __1_ of 99			

Form RS-FSA-001 Version 01			
Hazard Ref. No	**Hazard Scenario Description**	**Top-Level Requirement Ref. No.**	**Top Level Requirement**
001	***Location of emergency responder unknown***	***1***	***Identify and locate all fire fighters to unit commander.***
Prepared by: _____*Joe Lead*_____Date:1/10/2007			**Page ___ of ___**

4.0. DESIGN FAILURE MODE AND EFFECTS ANALYSIS (DFMEA)

4.1. Overview of DFMEA Method

Existing NFPA standards require conducting a Failure Modes and Effects Analysis (FMEA) to address electrical and mechanical failures that could lead to a hazard.[13] The FMEA method may be extended to address the random and systematic failures for PPE. These failures result from inadequacies in the design of the electronics and software in the embedded control. The extension is referred to as DFMEA for Design Failure Modes and Effects Analysis. Although developed independently, the DFMEA process shown is very similar to that described in the Electronics Association Document titled *Potential Failure Modes and Effects Analysis*[14].

The DFMEA method provides a qualitative way to identify and rank PPE failure modes that could lead to product hazard. The DFMEA process scope considers safety functions that are implemented in electronics and software components. It applies to functions which are implemented using a variety of electronic materials (e.g. gallium arsenide, silicon on sapphire) and components (Field Programmable Gate Arrays (FPGAs), Microcontrollers) and different software languages (micro-assembly, C, C++, Ada). Since functions involve multiple components, the approach starts with function identification instead of component identification. This starting point differs from the starting point of a traditional product design FMEA.

Input to the DFMEA includes information from the prior Hazard Analysis List and functional specifications. This permits the DFMEA participants to consider impact of component PPE failure modes on other functions. For example, transition management software embedded in PPE equipment inadvertently locks the software execution in a periodic diagnostic mode the motion detection software function may not execute at all. Thus safety analysis issues related to functional and component interdependence are

[13] See for example, NFPA 1981 Standard on Open-Circuit Self-Contained Breathing Apparatus for Fire and Emergency Services.

[14] Potential Failure Modes and Effects Analysis, JEP 131A,, JEDEC Solid State Technology Association, Electronic Industries Alliance, May 2005.

considered. Additionally, the DFMEA supports verifying traceability of hazards from functional safety requirements → safety by design→ implementation → verification→ validation → use.

The DFMEA method may be integrated with FMEA methods for non-electronic components including all types of product materials. The benefit of integrating these methods would be to address failures that cross technology boundaries. Consider the example of providing thermal protection of the ESE using a new material to reduce the susceptibility of the electronics to high heat. Combining the FMEA of the new material with the DFMEA for the electronics, would result in a better qualification of the potential for failure of the ESE due to exposure to high temperatures.

4.2. DFMEA SIPOC

<table>
<tr><th colspan="5">Form RS-DFMEA-001 Version 01 DESIGN FMEA SIPOC</th></tr>
<tr><th colspan="5">1 Objective: Identify and address electronics and software failure modes and effects that could lead to a product hazard</th></tr>
<tr><th>2 Supplier(s)</th><th>3 Input(s)</th><th>4 DFMEA Process</th><th>5 Output(s)</th><th>Customers</th></tr>
<tr><td>Equipment Design Lead/Team</td><td>• List of Equipment Functions
• List of Equipment Components including peripherals/accessories
• Equipment Diagram showing assemblies, subassemblies, peripherals, components, and accessories
• Electronic Hardware components
• Electronic Schematic
• Block Diagram of PE Architecture
• Software/Firmware Flowchart or Process Diagram
• Software/Firmware Detailed Design/Module Calling Structure
• List of Included Software Libraries (utilities and macros)</td><td rowspan="3">See Figure 8.</td><td rowspan="2">• DFMEA Chart through RPN calculation
• Update all inputs as appropriate</td><td rowspan="2">• Equipment Design Team
• Design Verification Team</td></tr>
<tr><td>Safety Verification Lead/Team</td><td>• Completed Hazard analysis form
• Mapping of functional requirements to hazards
• NFPA ESE 1800 Section 6.4 Requirements</td></tr>
<tr><td colspan="2">Enablers
• DFMEA Process
• Part Identification checklist (PIC)
• Failure Mode Checklist (FMC)
• Failure Effect Checklist (FEC)
• Failure Severity Checklist (FSC)
• Risk Priority Number (RPN)Calculation</td><td>Action Item List for Process/Enabler Changes</td><td>Process/Enabler Owners</td></tr>
<tr><td colspan="2">Prepared by:</td><td>Date:</td><td colspan="2">Page ___ of ___</td></tr>
</table>

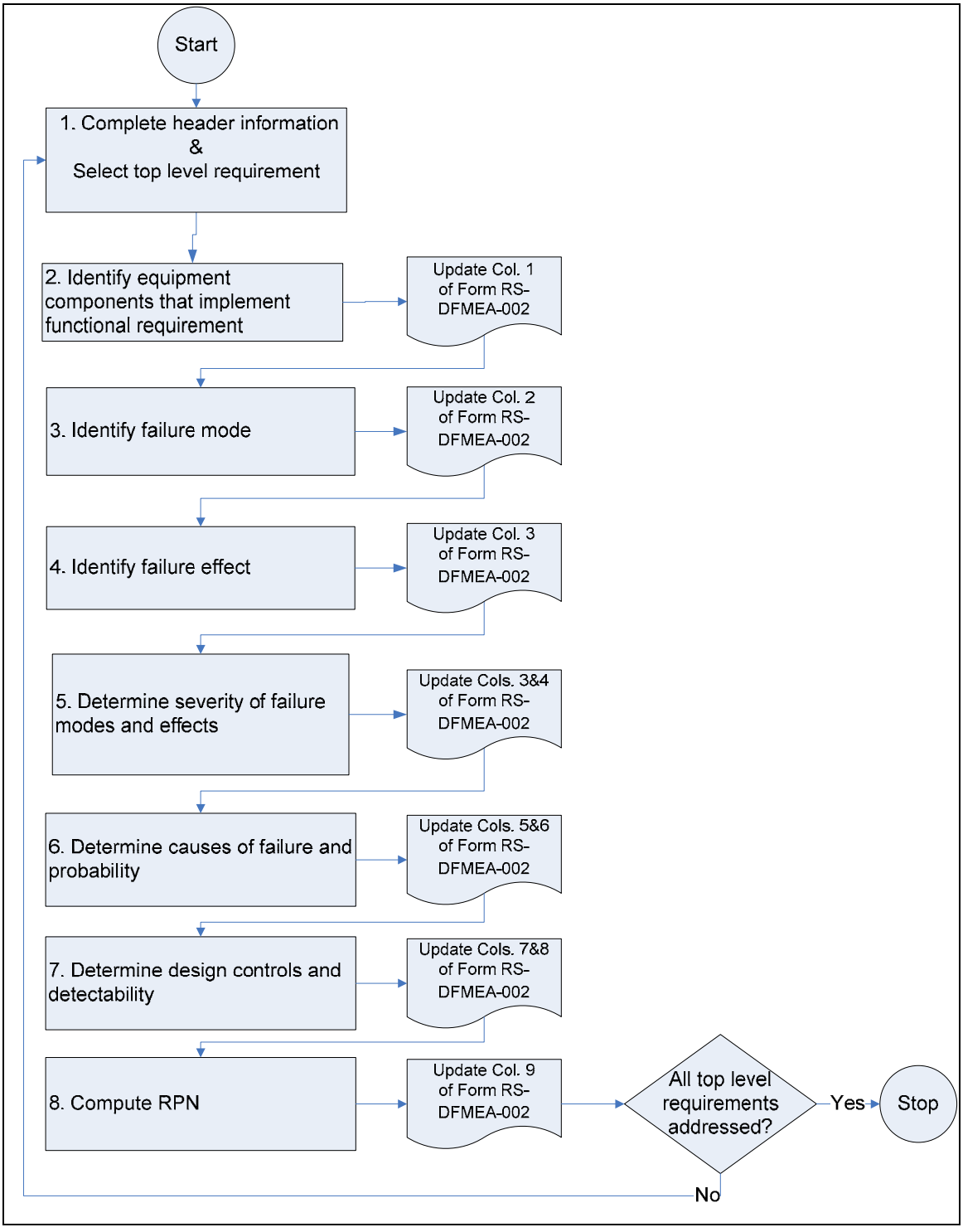


Figure 8 - DFMEA Process Steps

4.3. DFMEA Process Steps

4.3.1. Step 1 – Select Top Level Requirement

The DFMEA process begins with Step 1 by selecting a top level requirement from the Hazard to Requirements Mapping output from the HA. Record the top level requirement number and the requirement description on Form RS-DFMEA-002. (See Section 4.4.2)

4.3.2. Step 2 - Identify equipment components

Step 2 identifies all of the equipment components which implement the top level requirement. A component in this context is a critical part or subassembly that is either manufactured or purchased by the PPE manufacturer. List the components in Column 1 of Form RS-DFMEA-002.(See Section 4.4.2)

4.3.3. Step 3 - Specify failure mode for identified components.

For each component listed in Step 2, list potential failure modes in Column 2 of Form RS-DFMEA-002. A failure mode is any requirements, design, or implementation error that results in failure of the PPE to deliver part or all of its intended functionality.

4.3.4. Step 4 - Identify failure effects

For each component failure mode included in the second column, Step 4 identifies one or more failure effects that the identified failure mode would have on delivery of PPE functions. Include the failure effect in the third column. A failure effect is a deviation in function output value (e.g. value is too high, value is too low, value is wrong information) or timing (e.g. early, late, or not at all).

4.3.5. Step 5 - Determine Severity (S) of failure modes and effects

For each component failure mode and effect included in the third column of Form RS-DFMEA-002, record a value for the severity level in the fourth column. Base the value of the severity level, on the criteria provided in Table 6 - Values of Severity .

Severity (S)	Description	Value
Critical	A product hazard that judgment and experience indicate is likely to result in a condition immediately dangerous to life or health (IDLH) for individuals using or depending on the compliant product. If an IDLH condition occurs, the user will sustain, or will be likely to sustain, an injury of a severity that could result in loss of life, or result in significant bodily injury or loss of bodily function, either immediately or at some point in the future.	10
Major A	A product hazard, other than Critical, that is likely to result in failure to the degree that the compliant product does not provide any protection or reduces protection, and is not detectable to the user. The term “reduces protection” means the failure of specific protective design(s) or feature(s) that result in degradation of protection in advance of reasonable life expectancy to the point that continued use of the product is likely to cause physical harm to the user, or where continued degradation could lead to IDLH conditions.	10
Major B	A product hazard, other than Critical or Major A, that is likely to result in reduced protection, and is detectable to the user. The term “reduces protection” means the failure of specific protective design(s) or feature(s) that result in degradation of protection in advance of reasonable life expectancy to the point that continued use of the product is likely to cause physical harm to the user, or where continued degradation could lead to IDLH conditions.	5
Minor	A product hazard, other than Critical, Major A, or Major B, that is not likely to materially reduce the usability of the compliant product for its intended purpose, or a product hazard that is a departure from the established applicable standard and has little bearing on the effective use or operation of the compliant product for its intended purpose.	1

Table 6 - Values of Severity (S) (from NFPA 1800 ESE)

4.3.6. Step 6: Determine causes of failure and probability (P)

Step 6 lists the root causes of the failure for each potential failure mode and effect in Column 5 Form RS-DFMEA-002. There are a number of logical techniques for determining the root cause including:

- Cause and Effect Diagram – commonly called a fishbone diagram this technique works well in a group setting for coming to a consensus for the root cause.
- Fault Tree Analysis (FTA) – a top down approach for analyzing critical components.
- Software Fault Tree Analysis (SFTA) – FTA applied to software faults which result in failure modes that could lead to a hazard.
- Event Tree Analysis (ETA) - a logical, bottom-up graphical technique to determine outcomes from a single initiating hazardous event.

For each root cause, list the probability that the failure would occur using the categories in Table 7 in the 6th column of Form RS-DFMEA-002.

Category	Description	Probability
Frequent	The failure will occur often in the equipment life cycle	10
Occasional	The failure will occur at least once in the equipment life cycle	5
Improbable	So unlikely that it can be assumed that the failure will not occur in the equipment life cycle.	1

Table 7 - Probability Values by Category

4.3.7. Step 7: Determine Design Controls and Detectability (D)

For each likely cause of failure, Step 7 lists the design controls that will help assure that this failure can be detected. The design control is identified in Column 7 of Form RS-DFMEA-002. Determine the design controls based on the root cause using the analysis techniques described in Section 4.3.6. When causes are identified, discuss and document the design controls that will minimize the occurrence of the failure mode and effect and maximize its detectablity. For each design controls assign a detectability value based on Table 8 and include in Column 8 of the Form RS-DFMEA-002.

Category	Description	Value
Undetectable	There is no way to detect the occurrence of the failure mode and effect. Effective design controls are not in place.	10
Not Sure	The design controls in place may not always detect the failure mode and effect.	5
Detectable	The design controls in place will always detect the failure mode and effect.	1

Table 8 - Detectability Criteria

4.3.8. Step 8: Compute Risk Priority Number (RPN)

Step 8 computes a Risk Priority Number (RPN) based on the values of risk, probability, and detectability as follows:

RPN = S x P x D

The lower the value of the RPN indicates the lower the risk that a given failure will occur. The RPN value is the measure used as input to the Risk Analysis discussed in the next section. .

4.4.1. Partial List of DKYS Locator System Components and Technology

Product Name	DKYS Locator System	
Component Name	Included in DFMEA	Reason / Comment
DKYS Embedded active RFID tag	*Yes*	*Device is exposed to hazardous environment and critical function*
Location Sensor Hardware	*Yes*	*Device will be outside hazardous environment but is mission-critical*
Location Sensor Firmware	*Yes*	*Device will be outside hazardous environment but is mission-critical.*
Location Server Software	*Yes*	*Software that analyzes incoming location and ID data, organizes it, and provides it to PDA Display firmware*
Tag Setup Transmitter	*Yes*	*If fails, tags may be set up inaccurately*
Tag Setup Firmware	*Yes*	*If fails, tags may be set up inaccurately*
PDA Hardware	*Yes*	*Allows commander to get information sooner thus important it work.*
PDA Firmware/Software	*Yes*	*Allows commander to get information sooner thus important it work.*
Laptop Hardware		*Not provided by manufacturer and will be in conditioned environment.*
Laptop Software	*Yes*	*Mission-critical; laptop hardware must be identified*

4.4.2. DFMEA Output (Form RS-DFMEA-002) – Active RFID Tag Entry

Form RS-DFMEA-002 DESIGN FMEA

Req. No. *1*	***Identify all emergency responders to unit commander***				**Design Lead**		**RJO**			**Date *1/10/2007***				
					Participants		**RBC JSF**			**Sheet 1 Of 54**				
											Action Results			
Column 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Assembly, Sub-Assembly, Component, or Accessory	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity (s)	Potential Cause(s)/ Mechanism(s) of Failure	Probability (P)	Design Controls	Detectability (D)	Risk Priority Number (SxPxD)	Recommended Action(s)	Responsibility & Target Completion Date	ActionTaken	New Severity	New Probability	New Detectability	New RPN
Active RFID Tag	***Interference***	***Inaccurate or unreadable data***	***10***	***Electromagnetic***	***5***	***Increase power***	***1***	***50***	***Reduce EMI susceptibility***	***RBC 1-05-2007***	***Increased battery strength and power of signal requirements (See Req. 1.35)***	***10***	***1***	***1***	***10***
	Transmitter fails	***No data***	***10***	***Exposed to temperature conditions outside operating range***	***1***	***Improve robustness***	***1***	***10***	***Use transmitters with broader operating range***	***JSF 1-07-2007***	***Changed operating range requirement (See Req. 1.60)***	***10***	***1***	***1***	***10***
	Microprocessor memory fails	***No data***	***10***	***Physical damage due to water ingress***	***1***	***Protect from water ingress***	***1***	***10***	***Encapsulate microprocessor in ceramic***	***JSF 1-10=2007***	***Added requirement for ceramic encoating (See Req 1.299)***	***10***	***1***	***1***	***10***
Location Server Software	Software algorithm shows stale data when no RFID tags are active	Location data values arrive too late giving wrong information	10	Software bug inCOTS location software	1	Check bug list and provide proven in use criteria	1	10	Test for all known bugs Establish compliance with proven in use criteria	***RBC 1-10-2007***	Did comprehensive bug review and testing consistent with proven in use requirementns	10	1	1	10
Prepared by:					**Date:**						**Page ___ of ___**				

5.0. RISK ANALYSIS (RA)

5.1. Overview of Method

The DFMEA process includes a step for computing a measure identified as the Risk Priority Number or RPN. Higher RPN values imply higher risks. The Risk Analysis process provides the determination of whether the DFMEA process may be stopped because risk is reduced to ALARP. Achieving DFMEA completeness and consistency among ESE manufacturers suggests that a quantified value be provided for RPN. The value is the ALARP upper limit, specifically is the maximum value for which the risk would no longer be acceptable. The ALARP upper limit is a minimum requirement since risks could be reduced further to the ALARP lower limit.

Table 6, Table 7, and Table 8 provided candidate values for the risk factors of Severity (S), Probability (P), and Detectability (D) which when multiplied together provides the RPN value. The categories and values in these tables are arbitrary. The values chosen simplify decision making by avoiding values that are close together and therefore difficult to differentiate. The selected values also make multiplication easier. The example RPN values delineate only when ALARP is met and not met.

Using the candidate values for severity, probability, and detectability results in 10 possible values of RPN. Each value refers to categories of risk as shown in Table 9 thru Table 18 inclusive.

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
10	Critical, Major A	10	Frequent	10	Undetectable	1000

Table 9 - Risk Category - RPN =1000

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
5	Major b	10	Frequent	10	Undetectable	500
10	Critical, Major A	5	Occasional	10	Undetectable	500
10	Critical, Major A	10	Frequent	5	Not Sure	500

Table 10 - Risk Category - RPN =500

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
5	Major B	5	Occasional	10	Undetectable	250
5	Major B	10	Frequent	5	Not Sure	250
10	Critical, Major A	5	Occasional	5	Not Sure	250

Table 11 - Risk Category - RPN = 250

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
5	Major B	5	Occasional	5	Not Sure	125

Table 12 - Risk Category - RPN =125

Value	Category	Value	Category	Value	Category	Value
1	Minor	10	Frequent	10	Undetectable	100
10	Critical, Major A	1	Improbable	10	Undetectable	100
10	Critical, Major A	10	Frequent	1	Detectable	100

Table 13 - Risk Category - RPN = 100

Severity (S)		**Probability (P)**		**Detectability (D)**		**RPN**
Value	Category	Value	Category	Value	Category	Value
1	Minor	5	Occasional	10	Undetectable	50
5	Major B	1	Improbable	10	Undetectable	50
1	Minor	10	Frequent	5	Not Sure	50
10	Critical, Major A	1	Improbable	5	Not Sure	50
5	Major B	10	Frequent	1	Detectable	50
10	Critical, Major A	5	Occasional	1	Detectable	50

Table 14 - Risk Category - RPN = 50

Severity (S)		**Probability (P)**		**Detectability (D)**		**RPN**
Value	Category	Value	Category	Value	Category	Value
1	Minor	5	Occasional	5	Not Sure	25
5	Major B	1	Improbable	5	Not Sure	25
5	Major B	5	Occasional	1	Detectable	25

Table 15 - Risk Category - RPN = 25

Value	Category	Value	Category	Value	Category	Value
1	Minor	1	Improbable	10	Undetectable	10
1 10	Minor Critical, Major A	10 1	Frequent Improbable	1 1	Detectable Detectable	10 10

Table 16 - Risk Category - RPN =10

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
1	Minor	1	Improbable	5	Not Sure	5
1	Minor	5	Occasional	1	Detectable	5
5	Major B	1	Improbable	1	Detectable	5

Table 17 - Risk Category - RPN = 5

Severity (S)		Probability (P)		Detectability (D)		RPN
Value	Category	Value	Category	Value	Category	Value
1	Minor	1	Improbable	1	Detectable	1

Table 18 - Risk Category - RPN = 1

Note that the Risk Category of RPN = 10 reduces residual risk of failures to:

- Minor severity that are improbable and undetectable
- Minor severity that are frequent but detectable
- Critical or Major A severity that are improbable and detectable

The value of 10 thus seems reasonable for a more quantitative definition of an ALARP upper limit. Note also that a value of 10 or less also represents 26% of the possible

be reduced further to RPN=5 or RPN = 1.

RPN Value	Frequency	Percentage of values that are Equal to or Less than the value
1000	1	100%
500	3	96%
250	3	85%
125	1	74%
100	3	70%
50	6	59%
25	3	37%
10	3	26%
5	3	15%
1	1	4%
Total	27	

Table 19 - Frequency of RPN Values

Figure 9 and Table 19 - Frequency of RPN Valuesshow the distribution of values for RPN=1000 and below. Selecting a target value of RPN=10 or less leaves seven RPN values that are considered ALARP and do not have to be further reduced.

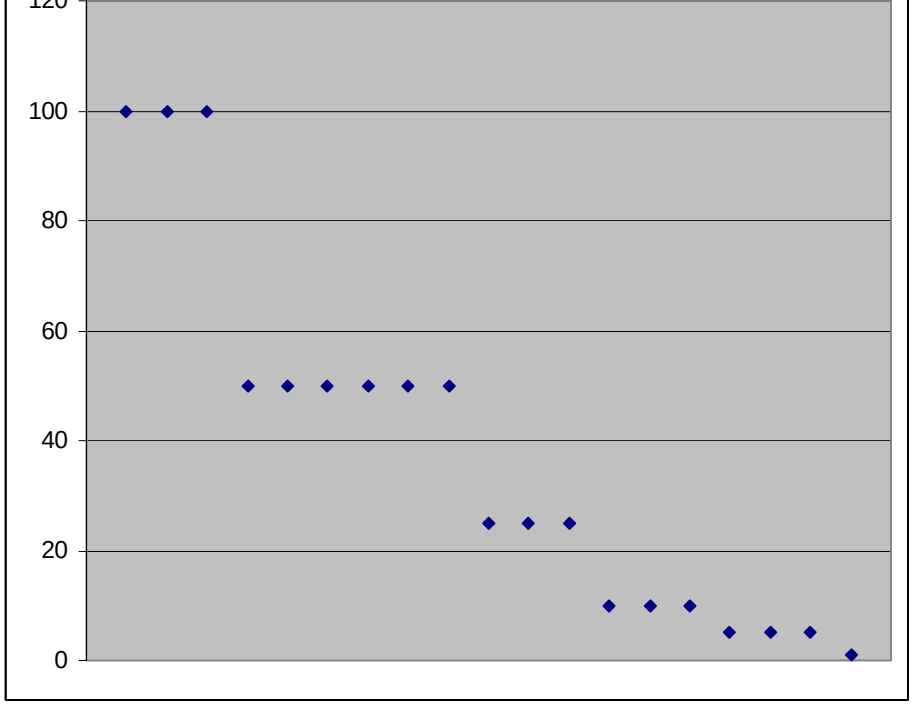


Figure 9 - Distribution of RPN Values

The following table maps the target ALARP upper limit of Risk Category of RPN=10 to exposure categories based on the environment of use of the PPE. The RPN values shown in Table 20- Example Acceptable RPN Values by Exposure Category represent a value above which actions need to be taken to further reduce the RPN.

Exposure Category	Acceptable RPN Value
Hostile, Fire	RPN<=10
Hostile, Non-Fire	RPN<=10

Table 20- Example Acceptable RPN Values by Exposure Category

.

5.2. Risk Analysis SIPOC

<table>
<tr><th colspan="5">Form RS-RA-001 Version 01</th></tr>
<tr><th colspan="5">Objective: Determine if risk requirements are met.</th></tr>
<tr><th>Supplier(s)</th><th>Input(s)</th><th>RA Process</th><th>Output(s)</th><th>Customers</th></tr>
<tr><td>Equipment Design Lead/Team</td><td>• DFMEA Chart through RPN calculation column
• RPN Criteria</td><td rowspan="3">See Figure 10 - RA Process Steps.</td><td rowspan="2">• Completed DFMEA Chart
• Completed Risk Analysis form</td><td rowspan="2">• Equipment Design Team
• Design Verification Team</td></tr>
<tr><td>Safety Verification Lead/Team</td><td>• Risk Class Specification
• NFPA ESE 1800 Section 6.4 Requirements</td></tr>
<tr><td colspan="2">Enablers
• Risk Analysis Process</td><td>Action Item List for Process/Enabler Changes</td><td>Process/Enabler Owners</td></tr>
<tr><td colspan="5">Prepared by: Date: Page ___ of ___</td></tr>
</table>

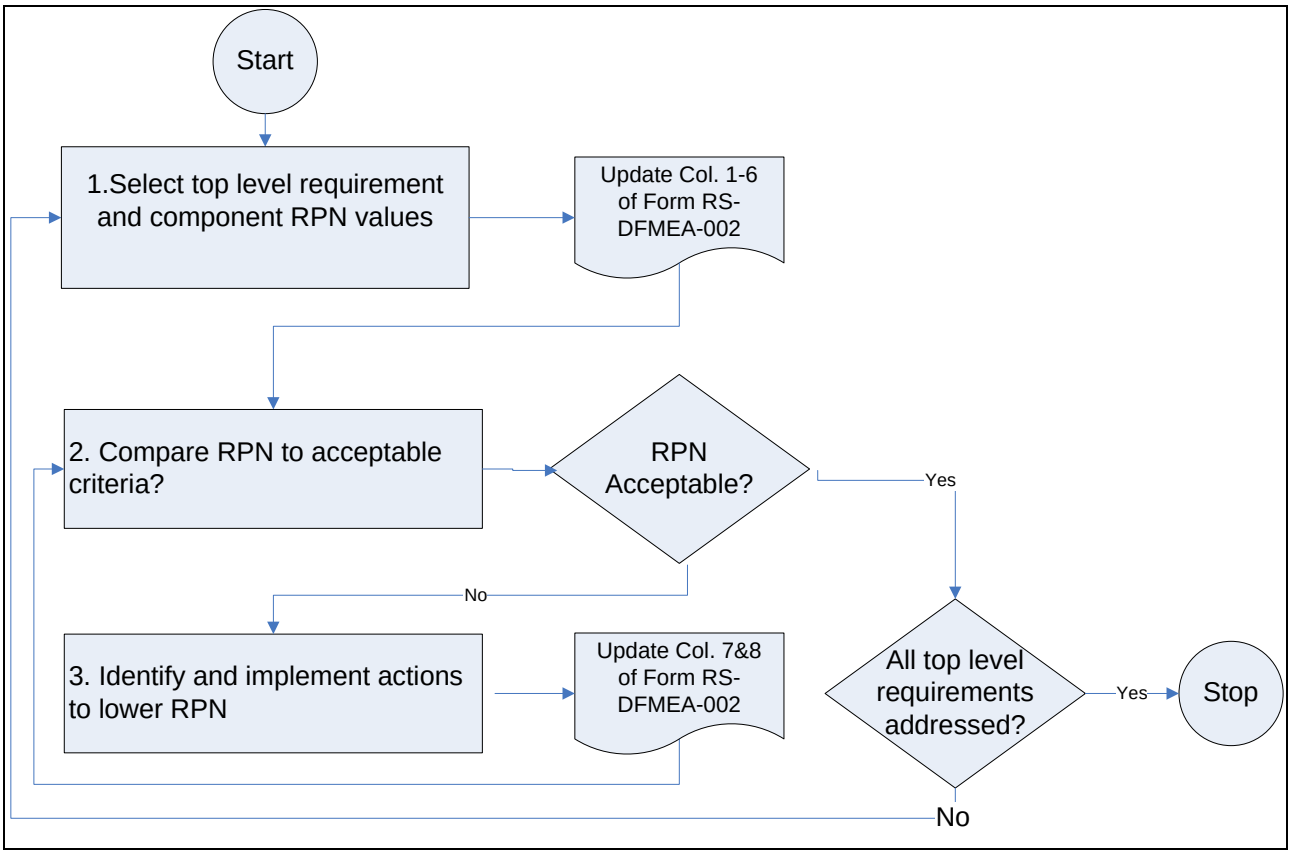


Figure 10 - RA Process Steps

5.3. RA Process Steps

5.3.1. Step 1 – Select Top Level Requirement and Component to Review

Step 1 involves selecting the top level requirement and the maximum RPN for each component identified by the DFMEA on Form RS-DFMEA-002 Version 1.0. For each component of each top level functional requirement analyzed, summarize findings in the Form RS-RA-002 Version 1 Columns 1 through 6. Step 2 – Compare Actual Value to Acceptable Value of RPN.

Compare Columns 5 and 6. If Column 6 is greater than Column 5, then proceed with Step 3.

5.3.2. Step 3 - Identify and implement actions to lower RPN value

If the RPN does not meet the criteria established in Column 5 - Acceptable RPN Value, identify and document actions taken to reduce the RPN to acceptable values. Actions that can be taken would include those identified in Table 21.

Factor	Possible Actions
Severity	Change the type of component, redesign the component
Probability	Modify / protect the component
Detectability	Add additional sensors

Table 21 – Possible Actions to Reduce RPN

Complete actions to assure all critical components have an RPN below the acceptable value. Summarize results in Columns 7 and 8 of Form RS-RA-002 Version 1.0.

5.4. RA Output

Form RS-RA-002 Version 1.0							
Risk Analysis Report for DKYS Model 1							
Col 1	2	3	4	5	6	7	8
Date	**Requirement Number**	**Component**	**Risk Class**	**Accept-able RPN Value**	**Highest RPN Value**	**Status**	**Action Request** *(who, what and when If criteria not met)*
2/28/2007	***1***	***Active RFID Tag***	***I***	***<10***	***25***	***In Process***	***Design team will meet 2/28/2007 to discuss needed actions***
3/15/2007	***1***	***Active RFID Tag***	***I***	***<10***	***5***	***Complete***	***Design team added shielding around the tag that minimized electromagnetic effects and added caution to users manual.***
Prepared by:		Date:		Page of			

6.0. ABBREVIATIONS

ABBREVIATION	DEFINITION
ALARP	As Low As Reasonably Practical
ANSI	American National Standards Institute
CMM	Capability Maturity Model
CTQ	Critical to Quality
DFMEA	Design Failure Modes and Effects Analysis
DKYS	Device that Keeps You Safe
DMS	Document Management System
EIA	Electronic Industries Alliance
EMI	Electromagnetic Interference
ESE	Electronic Safety Equipment
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
FSA	Functional Safety Analysis
FSD	Functional Safety by Design
FSF	Functional Safety File
FSLC	Functional Safety Life Cycle
FSLC-PMT	Functional Safety Life Cycle – Project Management Template
FTA	Fault Tree Analysis
HA	Hazard Analysis
HAZOP	Hazard and operability study
IAFF	International Association of Fire Fighters
IDLH	Immediately Dangerous to Life and Health
IFSA	Independent Functional Safety Assessment
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
JHA	Job Hazard Analysis
LOPA	Layer Of Protection Analysis

ABBREVIATION	DEFINITION
MOC	Management Of Change
MSHA	Mine Safety and Health Administration
NFPA	National Fire Protection Association
NIOSH	National Institute for Occupational Safety and Health
NPPTL	National Personal Protective Technology Laboratory
OSHA	Occupational Safety and Health Administration
PASS	Personal Alert Safety System
PDA	Personal Digital Assistant
PFD	Probability Of Failure On Demand
PHL	Preliminary Hazard List
PM	Project Manager
PPE	Personal Protection Equipment
QMS	Quality Management System
RA	Risk Analysis
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RPN	Risk Priority Number
RRF	Risk Reduction Factor
SEI	Software Engineering Institute
SFTA	Software Fault Tree Analysis
SIL	Safety Integrity Level
SLC	Safety Life Cycle
SIPOC	Supplier-Input-Process-Output-Customer
SLC	Safety Life Cycle

7.0. GLOSSARY

As low as reasonably practical (ALARP): A risk level associated with failure of the PPE that is considered acceptable because it is as low as reasonably practical.

Balanced Scorecard: Method for measuring organizational success by viewing the organization from customer, financial, internal business process, and learning and growth perspectives

Component: Any material, part, or subassembly used in the construction of PPE. Computer hardware and software are components of PPE.

Configurability: The ability to rapidly configure a PPE system to meet different life safety threats and to account for different user needs.

Compatibility: Requirements for the proper integration and operation of one device with the other elements in the PPE system.

Critical to Quality Tree: A six sigma method that uses a tree diagram for identifying important characteristics of a process or product that is critical to quality

Electronic Safety Equipment: Products that contain electronics embedded

in or associated with the product for use by emergency services personnel that provides

enhanced safety functions for emergency services personnel and victims during emergency incident operations (from NFPA 1800).

Failure modes and effects analysis (FMEA): This technique uses deductive logic to evaluate a system or process for safety hazards and to assess risk. It identifies the modes in which each element can fail and determines the effect on the system.

Functional Safety of ESE: ESE that operates safely for its intended functions.

Functional Safety Analysis: The process of identifying failures which lead to missed or inaccurate delivery of functions causing the potential for harm.

Functional safety by design (FSD): A system design approach that involves looking at the entire context of use for the equipment or system, identifying hazards, designing to eliminate or reduce hazards, and doing this over the entire life cycle for the PPE.

Functional safety file (FSF): Safety documents retained in a secure centralized location, which make the safety case for the project.

Functional safety life cycle (FSLC): All activities conducted in accordance with a functional safety approach to designing and building safety into the entire system from initial conceptualization to retirement.

Hazard: An environmental or physical condition that can cause injury to people, property, or the environment.

Hazard and operability study (HAZOP): This is a systematic, detailed method of group examination to identify hazards and their consequences. Specific guidewords are used to stimulate and organize the thought process. HAZOP [Ministry of Defense 1998] has been adapted specifically for systems using programmable electronic systems (PES).

Hazard Analysis: The process of identifying hazards and analyzing event sequences leading to hazards.

Hazard and risk analysis: The identification of hazards, the process of analyzing event sequences leading to hazardous events, and the determination of risks associated with these events. Risk analysis determines the risk reduction requirement for the equipment or system based on qualitative or quantitative approaches**.**

Hazard and risk analysis team: The group of first responders, electrical, electronics, computer hardware/software, manufacturing, and safety specialists responsible for the safety and integrity evaluation of PPE from its inception through its implementation and transfer to operations to meet corporate safety guidelines.

Hazard List: A list used to identify for tracking hazards throughout the FSLC. The list describes each hazard in terms of the event (s) that would lead to an accident scenario. When the hazard is identified during an accident analysis, the description of the hazard will also reference the accident scenario and consequences and measures that may be taken to avoid or prevent recurrence. The hazard list is used as input to the FMEA.

Human-computer interaction: The application of ergonomic principles to the design of human-computer interfaces.

Human-machine interface: The physical controls, input devices, information displays, or other media through which a human interacts with a machine in order to operate the machine.

Independent department: A department whose members are capable of conducting an IFSA. The department must be separate and distinct from the departments responsible for the activities and subject to Functional Safety Assessment or validation, taking place during the specific phase of the FSLC.

Independent functional safety assessment (IFSA): A systematic and independent examination of the work processes, design, development, testing, and safety file documentation for a product/machine/control system to determine compliance with applicable safety recommendations/standards/regulations.

Independent organization: An organization that is legally independent of the development organization whose members have the capability to conduct IFSAs. The organization member conducting the audit must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent person: A person who is capable of conducting an IFSA. The person must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent protection layer (IPL): Engineered safety features or protective systems or layers that typically involve design for safety in the equipment, administrative procedures, alarms, devices, and/or planned responses to protect against an imminent hazard. These responses may be either automated or initiated by human actions. Protection should be independent of other protection layers and should be user and hazard analysis team approved.

Internal assessment: Conducted by the manufacturer to determine that the design and development process continues to comply with the safety plans and the safety file procedures. A report is issued and reviewed by appropriate management personnel.

Interoperability: The ability of PPE equipment and systems to provide services to and accept services from other PPE equipment and systems and to use the services so exchanged to enable them to operate effectively together.

Layer of protection analysis (LOPA): An analysis that identifies risk reduction targets by evaluating selected risk scenarios.

Lean Manufacturing: Implementing steps to reduce waste during the manufacturing process. There are eight types of waste – defects, overproduction, waiting, unused talent, transportation, inventory, motion, and extra processing.

Maintainability: The ability to maintain a PPE with minimum maintenance and repair so that the PPE can remain in service with full operation.

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.

Periodic follow-up safety assessment: A systematic, independent, and periodic assessment which determines if the functional safety of the PPE is maintained.

Personal alert safety system (PASS): Devices that sense movement or lack of movement and that automatically activate an audible alarm signal to alert others in locating a first responder.

Personal protection equipment (PPE): Equipment and systems that provide the following life-safety protection functions:

- Protection against thermal, abrasion, puncture wounds, respiratory, vision, hearing and limited chemical and biological pathogen exposure hazards
- Monitoring of physiological, chemical, biological, and environmental parameters
- Communication among first responders and between first responders and victims

PPE functional requirements: Functions provided by the application including those functions required to meet NFPA equipment safety requirements.

PPE performance requirements: Timing and resource constraints imposed by the application including constraints needed for safety performance, such as delivering data

to the user within the time frame required.

Preliminary hazard analysis (PHA): This technique uses the results of PHL, lessons learned, system and component design data, safety design data, and malfunction data to identify potential hazard areas. In addition, its output includes ranking of hazards by severity and probability, operational constraints, recommended actions to eliminate or control the hazards, and perhaps additional safety requirements.

Preliminary hazard list (PHL): This is the first analysis performed in the system safety process and strives to identify critical system functions and broad system hazards. It uses historical safety data from similar systems and mishap/incident information hazard logs to guide the safety effort until more system-specific is developed.

Probability of failure on demand (PFD): A value that indicates the probability of a system failing to respond on demand. The average probability of a system failing to respond to a demand in a specified time interval is referred to as "PFD avg."

Project plan: A document that addresses the entire life cycle including development and use activities, management of change activities, and the documentation of safety. The project plan is updated throughout the life cycle.

Proven In Use: The component is considered reliable because it has been used in several products in the application over a period of time and reliability data is available for the component.

Random hardware failure: A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Rapid fire progression: A rapid rise in temperature that leads to an almost instantaneous combustion of materials over a larger area.

Record: Stating results achieved or providing evidence of activities performed.

Requirements Specification: A list of PPE requirements where each requirement is uniquely identified, traceable, and has safety performance criteria specified.

Retrospective Validation: Validation after the ESE has been fielded which is based on review of development documentation and testing and on field problem reports.

Risk analysis: Determination of the risk reduction requirement for the equipment or system based on qualitative or quantitative approaches.

Risk management summary: Details the risk management activities and summarizes the important risks identified and the means used to remove or mitigate them.

Risk reduction factor (RRF): Measure of the amount of risk reduced through implementation of safety equipment, training, and procedures. RRF is usually expressed as a reduction in the risk of loss of life.

Risk Priority Number (RPN): A number which establishes the priority for addressing the risk. RPN is computed based on severity, probability, and detectability. The higher the number obtained the higher the priority for addressing the potential failure.

Safety: Freedom from unacceptable risks.

Safety claims: A safety claim is a statement about a safety property of the PPE, its subsystems and components.

Safety integrity: The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period.

Safety Policy: A statement which describes in general the organizational commitment to safety and how safety issues will be addressed.

Safety statement: A succinct summary statement affirming the completeness

and accuracy of the FSF and the level of safety demonstrated for the PPE.

Safety life cycle (SLC): All activities conducted in accordance with a systems approach to designing and building safety into the entire system from initial conceptualization to retirement.

Scalability: The ability to scale up PPE to respond to threats, which cross jurisdictional boundaries.

Suppler Input Process Output Customer (SIPOC) Diagrams: Diagrams which show suppliers, the required input, the steps in a process, the output produced, and the customer of that output.

Systematic failure: A failure related to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors. Examples of systematic failures include design errors in interfaces and algorithms, logic/coding errors, looping and syntax errors, and data handling errors.

Traceability: Ability to trace the history, application or location of that which is under consideration.

Usability: Ease of use of the PPE. Usability is specified by stating performance requirements that define what users expect to accomplish.

Validation: Analysis, review, and test activities that establish that the PPE is built in accordance with the first responder needs. Did we build the right PPE?

Verification: Analysis, review and test activities that establish that the PPE is built in accordance with the PPE specifications. Did we build the PPE right?

Voice of the Customer (VOC): Six Sigma methods for collecting data on the desires and expectations of the customer. These methods include focus groups, surveys, websites, customer site visits, and interviews with distributors and/or retailers, current and lost customers.

APPENDIX

Below is a listing of seven FMEA design tools. These tools also assist with process FMEA, although the focus of this information is design-related FMEA. The tool descriptions were derived from the tool providers' literature and web sites.

AutoDCP

Customer Driven Systems

39555 Orchard Hill Place Suite 600

Novi, MI 48375

(248) 374-5050

E-mail: sales@cdssupport.com

http://www.customerdriven.com

Provides construction of industry standard quality documents including the Design FMEA, Process FMEA and Control Plan. Implements engineering changes, line-balancing and process reengineering efforts. Bridges the Design FMEA to the Process FMEA to Corrective Actions and back.

Easy-FMEA

Retriever Technology Ltd

P.O. BOX 3

Tenbury Wells

Worcs WR15 8XY

UK

Phone: +44-(0)-1584-781444

E-mail: sales@reetec.co.uk

http://www.reetec.co.uk

Prepares design and process failure modes and effects analysis (FMEA) documents

conforming to most industry standards including QS9000.

FMECA Module of Reliability Workbench

Isograph Inc.
4695 MacArthur Court
11th Floor
Newport Beach
CA 92660

Phone : (949) 798-6114

E-mail : sales@isographdirect.com
http://www.isograph.com

Provides the framework and reporting facilities to allow users to construct FMECAs to MIL-STD-1629A, BS 5760 Part 5, GJB 1391-92 and similar standards as well as customizing the FMECA to the user's own requirements. Design and Process FMEAs may be constructed and analyzed.

FMEA-Pro

Dyadem International Ltd
9050 Yonge Street
Suite 401
Richmond Hill
ON L4C 9S6
Canada
Phone: (905) 882-5055
Email: Sales: sales@dyadem.com
http://www.dyadem.com

A Failure Mode and Effects Analysis software solution intended to improve quality, productivity, and safety while providing a means for reviewing product and process designs and ensuring regulatory compliance Analyzes product designs and manufacturing processes, shortens study time,, and prevents failures from occurring.

Libraries and templates provide a knowledge base for the studies.

Relex FMEA/FMECA

Relex Software Corporation

540 Pellis Road
Greensburg, PA 15601
Phone: (724).836-8800
E-mail: info@relexsoftware.com

http://www.relexsoftware.com

Allows you to analyze the potential failure modes of your system and the resulting effects of those failures. Industries standards are supported. Support both Design and Process FMEAs.

Sabaton

Sydvest

Sluppenvegen 12E
N-7037 Trondheim
Norway

Phone: +47 73 84 41 00

E-mail: post@sydvest.com

http://www.sydvest.com

An analysis tool supporting FMEA (Failure Mode and Effects Analysis) and FMECA (Failure Mode, Effects and Criticality Analysis). Supports international standards such as ISO 9000, SAE J1739, SAE ARP5580, IEC 60812, BS 5760-5 or MIL-STD 1629.

Xfmea

ReliaSoft Plaza
115 South Sherwood Village Drive

Tucson, Arizona 85710

Phone: (520).886-0410

E-mail: Sales@ReliaSoft.com

http://www.reliasoft.com

Facilitates Failure Mode and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA) and provides data management and reporting capabilities.

Support for Major Industry Guidelines.