Functional Safety for Programmable Electronics Used in PPE: Best Practice Recommendations

(In Nine Parts)

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

Prepared by Safety Requirements, Inc.

NIOSH Contract 200-2003-02355,

September 2007

TABLE OF CONTENTS

LIST OF TABLES

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.

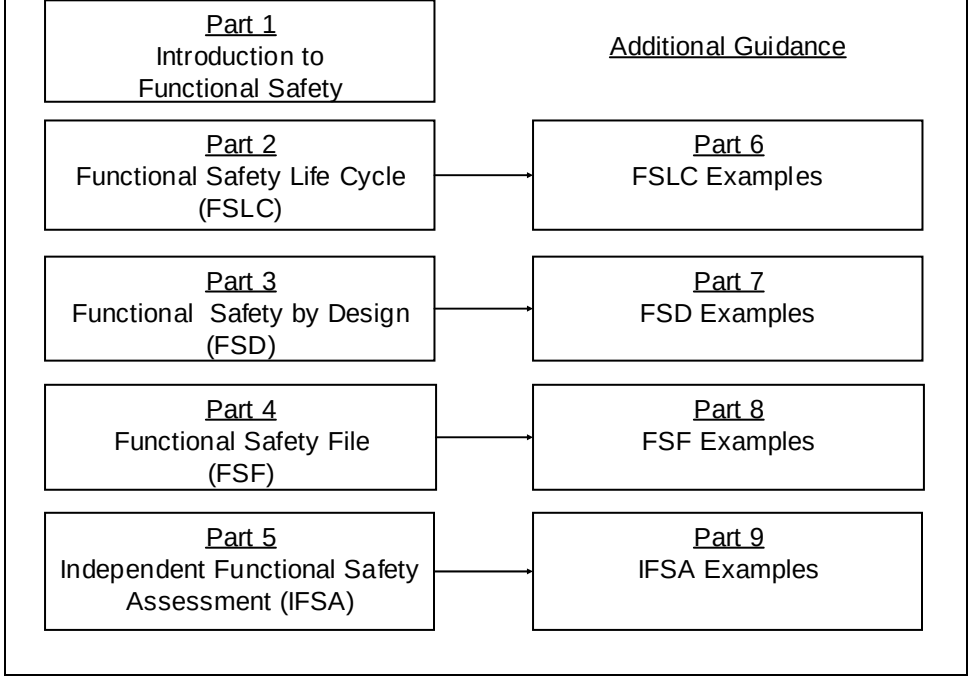

Figure 1 - The functional safety report series.

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

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.

Part 5: Independent Functional Safety Assessment (IFSA)

---

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

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

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.

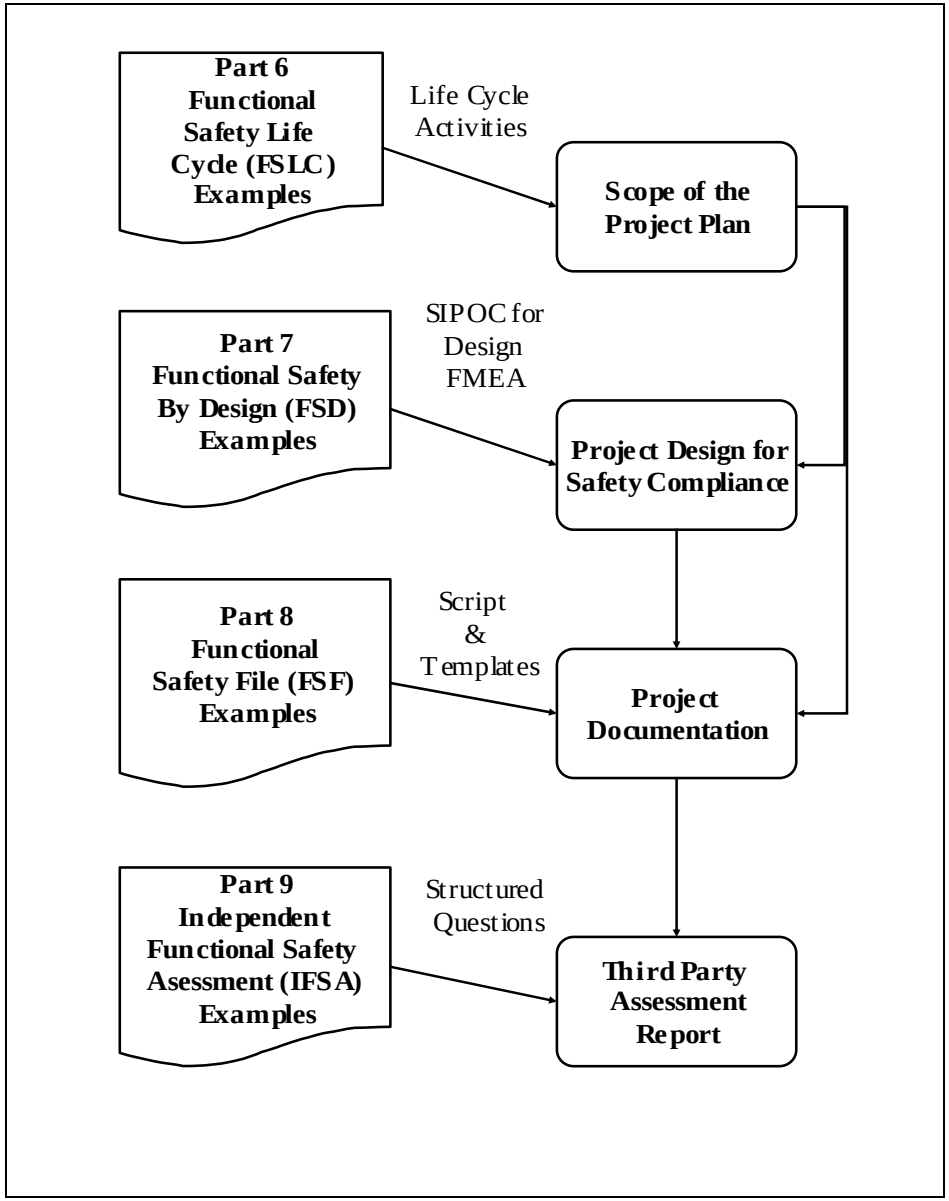

Figure 2 - Relationships among Parts 6, 7, 8, and 9

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

Part 7 bridges theory with practice for design activities by illustrating a Functional Safety

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

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 2 lists 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 3 provides an overview of

IC	Title / URL (http://)	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: Independent Functional Safety Assessment Examples is Part 9 in a nine-part series of recommendations addressing the functional safety of advanced PPE for first responders. As the companion document to Part 5 - it contains questions that may be used for reviewing Functional Safety File (FSF) documentation as part of a 3rd party safety assessment.

Part 9 provides information for use by life safety equipment manufacturers and users including component manufacturers, subassembly manufacturers, final equipment manufacturers, systems integrators, systems installers, 3rd party test laboratories, and life safety professionals.

1.0. INTRODUCTION

1.1. Report Scope

The report, Additional Guidance: Independent Functional Safety Assessment (IFSA) Questions is Part 9 in the nine-part series of recommendations addressing the functional safety of advanced personal protective equipment and systems (PPE) for first responders. As the companion document to Part 5, Part 9 provides example questions for assessing functional safety documentation.

The example questions may be used by manufacturers when preparing for 3rd party assessments and test laboratories conducting 3rd party assessments.

The questions are organized by the example documents identified in Part 8 Functional Safety File: Additional Examples. The questions are also cross-referenced to clauses in the NFPA 1800 Standard.

The organization of these documents is arbitrary. A manufacturer may choose to organize these documents differently based on their Quality Management System (QMS).

1.2. An Example Approach to Assessment

Manufacturers of PPE meet ISO 9001:2000 Quality Management System (QMS) Requirements. Meeting ISO 9001:2000 requires “documentation that enables communication of intent and consistency of action.”[4] The Functional Safety File (FSF) discussed in Parts 5 and 8 contain documentation that is part of the manufacturer’s QMS. These documents may be reviewed as part of an ISO 9001 audit to establish conformance to the QMS which includes practices for development of PPE.

Instead of repeating the ISO 9001 audit, an example approach to safety assessment is for the assessor to conduct a desk review of the Design Failure Modes and Effect

[4] ISO 9001:2000 Quality management systems – Requirements.Section 2.7.1 For further detail, see http://www.iso.org/iso/en/ISOOnline.frontpage. Date accessed October 31, 2006

documentation for functions that are critical to hazards and then to follow-up this review with functional tests in the test laboratory or at the manufacturer's facility.

1.3. Case Study: DKYS – Device that Keeps You Safety Requirements Inc.

Part 6 Additional Guidance: Functional Safety Life Cycle (FSLC) Examples describes 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. Responder Safety Inc. is using International Functional Safety Assessors, Inc. to review their Functional Safety File Documentation and test the DKYS equipment in accordance with the requirements in NFPA 1800. Responder Safety Inc. followed the best practices recommendations provided in Parts 4 and 8 of the NIOSH PPE Guidance. The names and events depicted in the case study are purely fictional. They do not identify any particular product, company or situation.

Table 3 provides a list of the DKYS FSF documents prepared by Responder Safety, Inc. and their supplier High Tech, Inc. The following subsections provide examples of assessment questions for each document in the FSF for DKYS. The results of the IFSA would be recorded in an IFSA report, an example of which was provided in Part 5.

DKYS-1	Functional Safety Summary	Affirms and provides references to the salient safety information about the equipment functionality, intended use, and the manufacturer's responsibilities.	Version 1.5 25 Oct 2006	Responder Safety,
DKYS-2	Functional Safety Policy and Plans	Defines what activities will be conducted to meet product safety objectives.	Version 1.3 25 Oct 2006	Responder Safety.
DKYS-3	Product Manager Manual and Records	Defines steps in the functional safety life cycle to be considered by the product manager. Includes SIPOCs and references data records.	Version 1.6 25 October 2006	Responder Safety.
DKYS-4	Training Manual and Records	Identifies training requirements for the product team. Includes SIPOCs and references training records.	Version 1.9 25 Oct2006	Responder Safety.
DKYS-5	Product Requirements Specification	Specifies what the product will and will not do. The specification includes functional, safety, and performance requirements.	Version 1.12 25 Oct 2006	High Tech.
DKYS-6	Development Manual and Records	Includes SIPOCs for the development team and references records of development activities.	Version 1.4 25 Oct 2006	High Tech.
DKYS-7	Technical Review, Testing, Verification Manual and Records	Includes SIPOCs for the verification team to and references records of verification activities.	Version 1.7 25 Oct 2006	High Tech.
DKYS-8	Production Manual and Records	Includes SIPOCs for the production team and references records of development activities.	Version 1.3 25 Oct 2006	Responder Safety.
DKYS-9	Installation, Commissioning, and Validation Manual and Records	Includes SIPOCs for the validation team to and references records of validation activities.	Version 1.2 25 Oct 2006	Responder Safety.
DKYS-10	User Manual and Records	Includes instructions for the product user and references records of use activities.	Version 1.6 25 Oct 2006	High Tech.
DKYS-11	Distribution Manual and Records	Includes SIPOCs for distributing the product and references records of distribution activities.	Version 1.1 25 Oct 2006	Responder Safety.
DKYS-12	Maintenance and Repair Manual and Records	Includes SIPOCs for maintenance and repair of the product and references records of maintenance and repair activities.	Version 1.3 25 Oct 2006	High Tech.
DKYS-13	Management of Change Manual and Records	Includes SIPOCS for how change will be handled and references records of change activities.	Version 1.10 25 Oct 2006	Responder Safety.
DKYS-14	Decommissioning Manual and Records	Includes SIPOCS for product decommissioning and references records of decommissioning activities.	Version 1.2 25 Oct 2006	Responder Safety.
DKYS-15	Product Description	Describes the product function and intended use. Identifies any restrictions on use.	Version 1.7 25 Oct 2006	Responder Safety.
DKYS-16	Independent Functional Safety Assessment Report	Describes the approach to conducting the IFSA, the individuals involved, and records the findings.	Version 1.1 25 October 2006	Independent Functional Safety Assessors.

Table 3 - List of Functional Safety File Documents

2.0. IPSA QUESTIONS ORGANIZED BY DKYS FSF DOCUMENT AND NFPA 1800 REQUIREMENTS

2.1. Document #1- DKYS Functional Safety Summary

Table 4 provides an example questionnaire for inspecting Document #1 Functional Safety Summary. Document #1 affirms and provides references to the salient safety information about the equipment functionality, intended use, and the manufacturer's responsibilities. The Functional Safety Summary also defines the FSF and provides references to documents contained in the FSF.

Table 4 –Version1.0 Assessment Questions for Document #1 - DKYS Functional Safety Summary

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #1 - DKYS FUNCTIONAL SAFETY SUMMARY DOCUMENT	NFPA 1800 REQUIREMENT
1.0 Is there a Functional Safety File?	**4.2**
1.1 Is the purpose of the FSF specified?	6.3.4
1.1.1 Is the purpose as stated consistent with the NIOSH/NPPTL Best Practices Recommendations [5] for the FSF? (V*erify by assessing Document #2 Functional Safety Policy)*	6.3.4
1.2 Are the structure and contents of the FSF specified?	4.2
1.2.1 Are the contents as specified consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
1.3 Are the contents of the FSF available for assessment?	4.2
1.3.1 Do the contents of the FSF cover all safety information needed for assessment? (*Verify by assessing all documents in the FSF)*	6.3.4
1.4 Is there a signed statement which affirms that the FSF adequately and accurately documents the engineering of the system? *(Verify this by assessing all FSF documents.)*	4
2.0 Is there a Safety Policy that covers the development of electronics and software?	**6.3.4**

for DOCUMENT #1 - DKYS FUNCTIONAL SAFETY SUMMARY DOCUMENT	NFPA 1800 REQUIREMENT
2.1 Does the safety policy accurately and adequately cover the development of electronics and software? *(Verify by assessing Document #2 Functional Safety Policy)*	6.3.4
2.2 Is there a signed statement affirming that the safety policy has been followed?	4.2
3.0 Is there a description of FSLC activities for the project?	**6.3.4**
3.1 Does the description of the FSLC accurately and adequately cover the development of electronics and software? *(Verify by assessing Document #3 Product Manager Manual and Records.)*	6.3.4
3.1.1 Does the description comply with NIOSH/NPPTL best practice recommendations?	6.3.4
3.1.2 Does the description of the FSLC accurately and adequately cover the implemented practices? (*Verify by assessing all documents.)*	6.3.4
3.2 Is there a signed statement affirming that the FSLC has been followed?	4.2
4.0 Is there a description of the functionality of the equipment?	**6.3.4**
4.1 Does the description of the functionality of the equipment accurately and adequately describe the EQUIPMENT functions? *(Verify by assessing Document #5 Requirements Specification)*	6.3.4
4.2 Is there a description of the intended use of the equipment?	5
4.2.1 Does the statement of intended use accurately and adequately cover the intended uses of the equipment? *(Verify by assessing Document #5 Product Requirements Specification)*	5
4.3 Are Safety Claims specified for the equipment?	5
4.4 Do the safety claims accurately and adequately describe the EQUIPMENT? *(Verify by assessing Documents# 15- Product Description*)	5
4.5 Do the safety claims identify quantitative ranges for human, electronic, and electrical input and output to and from the EQUIPMENT? *(Verify by assessing Document #5- Product Requirements Specification.)*	5

for DOCUMENT #1 - DKYS FUNCTIONAL SAFETY SUMMARY DOCUMENT	NFPA 1800 REQUIREMENT
4.5.1 Have tests been conducted that validate the quantitative ranges identified for human, electronic, and electrical input and output to and from the EQUIPMENT? *(Verify by assessing Document #9- Installation, Commissioning, and Validation)*	6.3.4
4.6 Is there a Risk Categorization?	
4.7 If a RRF is claimed, has the RRF been validated? *(Verify by assessing Document #9- Installation, Commissioning, and Validation)*	6.3.4
4.8 Is there a signed statement affirming that the equipment functions, intended use, and safety claims as described are accurate and adequate?	4.2
5.0 Is there an As Built description of the equipment?	**4**
5.1 Does the as built description accurately and adequately describe the EQUIPMENT? *(Verify by assessing Document #15 Product Description)*	4
5.2 Is there a signed statement affirming that as built descriptions are accurate and adequate as specified and that the equipment is ready for calibration and use?	4.2
5.2.1 Does the signed statement identify conditions of use?	4, 5
5.2.2 Do the conditions of acceptability include rechecking operational diagnostics?	4, 5
6.0 Is there a signed statement which affirms that the FSF adequately and accurately documents the engineering of the system? *(Verify this by assessing all FSF documents.)*	**4**
7.0 Is there a signed statement which affirms that all identified hazards have been eliminated or that they are controlled to acceptable levels?	**4**

2.2. Document #2 –DKYS Functional Safety Policy

Table 5 provides an example questionnaire for inspecting Document #2 Functional Safety Policy and Plans. Document 2 defines what activities will be conducted to meet product safety objectives.

Table 5 - Version1.0 Assessment Questions for Document #2 - DKYS Functional Safety Policy and Plans

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #2 – DKYS FUNCTIONAL SAFETY POLICY DOCUMENT	NFPA 1800 REQUIREMENT
8.0 Is there a Safety Policy which identifies practices that must be followed when engineering functions using electronics and software technology?	**4**
8.1 Is the Safety Policy consistent with NIOSH/NPPTL Best Practices Recommendations?[6]	4
9.0 Does the safety policy identify governing regulations?	**4**
9.1 Does the safety policy establish best practices in accordance with governing regulations?	4
9.2 Is there a signed statement affirming that the governing regulations have been met?	4
10.0 Does the safety policy identify recognized standards that must be complied with?	**4**
10.1 Does the safety policy establish best practices in accordance with recognized standards?	4
10.2 Is there a signed statement affirming that the governing regulations have been met?	4
11.0 Were data from prior incidents considered when establishing the safety policy?	**4**
11.1 Were court records of accidents from using similar equipment consulted? http://pacer.psc.uscourts.gov	4
11.2 Were incident data from NIOSH Fire Fighter Fatality Investigation and Prevention Program http://www.cdc.gov/niosh/fire/implweb.html consulted when establishing the functional safety policy?	4
11.3 Were fire statistics and fire reports data from NFPA http://www.nfpa.org considered when establishing the safety policy and strategy?	4

for DOCUMENT #2 – DKYS FUNCTIONAL SAFETY POLICY DOCUMENT	NFPA 1800 REQUIREMENT
11.4 Were lessons learned from prior safety investigations and product recalls considered when establishing the functional safety policy?	4.7, 4.8
12.0 Is a standard for product life cycle activities specified or referenced?	**6.3.4**
12.1 Does the standard include FSLC activities?	6.3.4
12.1.1 Are the FSLC activities consistent with the NIOSH/NPPTL Best Practice Recommendations[7]?	6.3.4
12.2 Does the FSLC include risk identification, management, and control activities?	6.3.4
12.2.1 Is there a policy in place that documents how to identify, evaluate and measure risk?	6.3.4
12.2.2 Does the policy define what FSLC activities are to be carried out, based on the outcome of the risk identification, management, and control activities?	6.3.4

2.3. Document #3 – DKYS Product Manager Manual and Records

Table 6 provides an example questionnaire for inspecting Document #3 Product Manager Manual and Records. Document #3 defines steps in the FSLC to be considered by the product manager. The ASSESSMENT of the document includes examination of any referenced SIPOCs and data records.

Table 6 - Version1.0 Assessment Questions for Document #3- DKYS Product Manager Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #3 - DKYS PRODUCT MANAGEMER MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
13.0 Is there a Product Manager Manual and Records?	**6.3.4**
14.0 Is there a SIPOC for the project manager to follow?	**6.3.4**
14.1 Are the activities specified in the SIPOC consistent with the NIOSH/NPPTL Best Practice Recommendations[8]?	6.3.4
14.1.1 Does the SIPOC identify records to be completed?	6.3.4
14.1.1.1. Does the SIPOC specify formats for these records?	6.3.4
14.1.1.2. Does the SIPOC specify when these records will be completed?	6.3.4
14.1.1.3. Does the SIPOC specify how the records will be maintained?	6.3.4
14.2 Is the scope of the FSLC consistent with the manufacturer's practices? (For example, a manufacturer may or may not have responsibility for installation commissioning, training, maintenance, and de-commissioning FSLC activities).	6.3.4
14.3 Does the Project Manager manual specify project monitoring and controlling activities?	6.3.4
14.3.1 Are the project monitoring and controlling activities and milestones consistent with the NIOSH/NPPTL Best Practice Recommendations?	6.3.4

for DOCUMENT #3 - DKYS PRODUCT MANAGEMER MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
14.3.2 Are there monitoring and controlling milestones?	6.3.4
14.3.3 Is the individual responsible for signing off on each milestone specified?	6.3.4
14.3.4 Are there records that indicate project monitoring and controlling activities and milestones have been followed?	6.3.4
15.0 Is there a description of the relationships and lines of communication set up between organizational functions that may impact or have responsibility for tasks with safety implications?	**6.3.4**
15.1.1 Are there records that indicate that the lines of communication have been followed?	6.3.4
15.1.2 Does the manual reference the applicable safety policy?	6.3.4
15.1.3 Are there records that the safety policy has been communicated to the development team?	6.3.4
16.0 Is there a specification of the minimum qualifications requirements for human resources involved in the product activities?	6.3.4
16.1 Is the specification consistent with the recommendations in the NIOSH/NPPTL Best Practices Recommendations guidance?	6.3.4
16.2 Are there records showing that the human resources involved met the criteria in the qualifications summary? *(Verify by assessing Document #4).*	6.3.4
17.0 Is a specification of the level of authority the human resources have in implementing the tasks necessary to complete the project?	**6.3.4**
17.1 Are verification and validation activities assigned to resources independent of the design activities?	6.3.4
17.2 Are there records showing that the level of authority has been adhered to?	6.3.4
17.3 Is a description of the mechanisms by which concerns can be brought to light by project personnel recorded?	6.3.4
18.0 Is there a SIPOC for placing documentation in the FSF?	**6.3.4**
18.1 Are procedures for placing a summary of the functional safety policy in the FSF described?	6.3.4
18.2 Are procedures for placing a description of the FSLC used for the project in the FSF described?	6.3.4
18.3 Are procedures for placing the criteria and rationale for selecting project staff in the FSF described?	6.3.4

for DOCUMENT #3 - DKYS PRODUCT MANAGEMER MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
18.4 Are procedures for placing all project specific plans in the FSF described?	6.3.4
18.5 Are procedures for placing all project development documents in the FSF described?	6.3.4
18.6 Are procedures for placing all user documents in the FSF described?	6.3.4
18.7 Are procedures for placing all operation documents in the FSF described?	6.3.4
18.8 Are procedures for placing all maintenance documents in the FSF described?	6.3.4
18.9 Are procedures for placing the results of the IFSAs in the FSF described?	6.3.4
19.0 Are there procedures for controlling access to the files in the FSF?	**6.3.4**
20.0 Are there procedures for reviewing the sufficiency and accuracy of the FSF at the monitoring and controlling milestones?	**6.3.4**
20.1 Do these procedures define criteria that must be met before proceeding to the next phase?	6.3.4
21.0 Is there a description of the FSLC techniques and tools used?	**6.3.4**
21.1 Are the FSLC techniques and tools appropriate to the life cycle objective?	6.3.4
21.2 Are the FSLC techniques and tools used consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
22.0 Is there a list of hazards that could occur during development of the equipment?	**6.3.4**
22.1 Are mitigation methods for all hazards in the list identified?	6.3.4
22.2 Are there records indicating that the hazards have been mitigated?	6.3.4

2.4. Document #4 – DKYS Training Manual and Records

Table 7 provides an example questionnaire for inspecting Document #4 – Training Manual and Records. Document #4 identifies training requirements for the product team. It includes a SIPOCs and references training records. Training requirements for users of the equipment is specified in the Document # 10.

Table 7 - Version1.0 Assessment Questions for Document#4 – DKYS Training Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #4- DKYS TRAINING MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
23.0 Are there a training manual and records?	**6.3.4**
23.1 Is there a SIPOC for establishing the competency of human resources for the project, including subcontractors, involved in FSLC activities?	6.3.4
23.1.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations[9]?	6.3.4
23.1.2 Are there records that the SIPOC has been followed?	6.3.4
23.1.3 Does the SIPOC identify records to be completed?	6.3.4
23.1.3.1. Does the SIPOC specify formats for these records?	6.3.4
23.1.3.2. Does the SIPOC specify when these records will be completed?	6.3.4
23.1.3.3. Does the SIPOC specify how the records will be maintained?	6.3.4
23.2 **Are training requirements specified for all project participants?**	**6.3.4**
23.2.1 Are the training requirements specified for all project participants (i.e., managers, engineers, manufacturers, and maintainers of the equipment?)	6.3.4
23.2.2 Are there signed records identifying training content, dates, and participants qualifying project participants?	6.3.4

2.5. Document #5 - DKYS Product Requirements Specification

Table 8 provides an example questionnaire for assessing Document #5 Product Requirements Specification. Document #5 specifies what the product will and will not do. The specification includes functional, safety, and performance requirements.

Table 8 - Version1.0 Assessment Questions for Document#5 – DKYS Product Requirements Specification

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #5 – DKYS REQUIREMENTS SPECIFICATION DOCUMENT	NFPA 1800 REQUIREMENT
24.0 Is there a written Product Requirements Specification?	**6.3.1, 6.3.2**
24.1 Does the specification define the functional safety and performance requirements that address the potential for failures due to design or systematic phenomena?	6.3.2
24.2 Does the specification define the functional safety and performance requirements that address the potential for failures due to random phenomena?	6.3.2
25.0 Are the equipment functions adequately and accurately described?	**6.3.1**
25.1 Does the specification identify individual functions of the equipment?	6.3.1
25.1.1 Are there any functions included in the equipment that are not described?	6.3.1
25.1.2 Are there any functions not included in the equipment that are described?	6.3.1
25.2 Does the specification identify if the function is a safety-critical function?	6.3.1
25.3 Does the specification identify if the function is a safety-related function?	6.3.1
25.4 Does the specification identify if the function is not related to safety?	6.3.1
25.5 Is there a description of the relationship between safety and other functional elements of the system?	6.3.4
26.0 Is a safety function defined for each hazard?	6.3.1
26.1 Is the safety function described with all parameters and there acceptable values identified for all operating modes specified?	6.3.1
26.2 Are all states (default, nominal, and risk (off-nominal)) of each safety function specified for all operating modes?	6.3.1

for DOCUMENT #5 – DKYS REQUIREMENTS SPECIFICATION DOCUMENT	NFPA 1800 REQUIREMENT
26.3 Are all constraints associated with the use of each safety function specified?	6.3.1
26.4 Are all events or combinations of events that trigger operating mode changes or safety function execution specified?	6.3.1
26.5 Are the risk reduction requirements specified for each safety function?	6.3.1
26.5.1 Are these requirements consistent with accepted standards?	6.3.1
26.5.2 Are these requirements consistent with established data?	6.3.1
26.5.3 Is adequate rationale provided?	6.3.1
26.5.3.1. Does the rationale for risk reduction claims include references to historical or other data used to support the risk reduction claim?	6.3.1
26.5.3.2. Are the performance requirements and constraints (e.g., range, rate, response time) of each safety function specified?	6.3.1
27.0 Are the interface requirements (i.e. human, electronics, software) for the equipment specified?	6.3.1
27.1 Does the specification identify quantitative ranges for human, electronic, and electrical interfaces to and from the equipment?	6.3.1
27.1.1 Does the specification identify units of measure for these ranges?	6.3.1
27.2 Are operating requirements specified?	6.3.1
27.3 Are calibration requirements specified?	6.3.1
27.4 Are diagnostic requirements specified?	6.3.1
27.5 Are testing requirements specified?	6.3.1
27.6 Are maintenance requirements specified?	6.3.1
27.7 If data logging is included does the log file reside in non-volatile memory?	6.1.4
27.7.1 Is it capable of logging a minimum of 2000 events?	6.1.4.2
27.7.2 Is it downloadable by the end user?	6.1.4.1
27.7.3 Does it log a date and time stamp for when device was turned on?	6.1.4
27.7.4 Does it log a date and time stamp for when the device	6.1.4

for DOCUMENT #5 – DKYS REQUIREMENTS SPECIFICATION DOCUMENT	NFPA 1800 REQUIREMENT
27.7.5 Does it log a date and time stamp for low power supply warning?	6.1.4
27.7.6 Does it log a date and time stamp for when device was turned off?	6.1.4
28.0 Is there a description of the relationship between the safety functions and other functions of the equipment?	**6.3.1**
28.1 Do the specifications identify if the function is a safety-critical function?	6.3.1
28.2 Do the specifications identify if the function is a safety-related function?	6.3.1
28.3 Do the specifications identify if the function is not related to safety?	6.3.1

2.6. Document #6 – DKYS Development Manual and Records

2.6.1. Table 9 provides an example questionnaire for inspecting #6 Development Manual and Records. Document #6 includes a SIPOC for the development team and references records of development activities.

Table 9 - Version1.0 Assessment Questions for Document#6 – DKYS Development Manual and Records

3rd PARTY ASSESSMENT QUESTIONS For DOCUMENT #6- DKYS DEVELOPMENT MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
29.0 Is there a Development Manual?	**6.3.4**
29.1 Does the Development Manual contain one or more SIPOCs for electronics and software developers to follow?	6.3.4
29.1.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations[10] [11]?	6.3.4
29.1.2 Does the SIPOC identify activities and tools used for electronics and software development, including metrics, to be collected and applicable standards?	6.3.4
29.1.3 Does SIPOC define when development and coding activities take place?	6.3.4
29.1.4 Does the SIPOC define who conducts the development and coding?	6.3.4
29.1.5 Are there records that the SIPOC has been followed?	6.3.4
29.1.6 Does the SIPOC identify records to be completed?	6.3.4
29.1.6.1. Does the SIPOC specify formats for these records?	6.3.4
29.1.6.2. Does the SIPOC specify when these records will be completed?	6.3.4
29.1.6.3. Does the SIPOC specify how the records will be maintained?	6.3.4
29.1.6.4. Does the SIPOC specify what records will be retained for the FSF?	6.3.4
30.0 Is there a SIPOC for specifying requirements?	**6.3.4**
30.1.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations[12]?	6.3.4

[10] NIOSH/NPPTL Best Practice Recommendations, Draft Part 4, Section 3.2.3.

[11] NIOSH/NPPTL Best Practices Recommendations. Draft Part 3.

For DOCUMENT #6- DKYS DEVELOPMENT MANUAL AND RECORDS	REQUIREMENT
30.1.2 Does the SIPOC address how the functional safety requirements will be established?	6.1.2
30.1.3 Does the SIPOC address when the functional safety requirements will be specified?	6.1.2
30.1.4 Does the SIPOC identify records to be completed?	6.3.4
30.1.4.1. Does the SIPOC specify formats for these records?	6.3.4
30.1.4.2. Does the SIPOC specify when these records will be completed?	6.3.4
30.1.4.3. Does the SIPOC specify how the records will be maintained?	6.3.4
30.1.4.4. Does the SIPOC specify what records will be retained for the FSF?	6.3.4
30.1.5 Are there records that the SIPOC has been followed?	6.3.4
31.0 Is there a SIPOC addressing how the design will be accomplished?	**6.1.2**
31.1.1 Is there a list of design for safety principles to be followed?	6.1.2
31.1.2 Do the design activities specify fault-tolerant electronics design and defensive programming techniques including design logic that prevents, detects, and resolves non-terminating and non-deterministic states and error states including but not limited to undefined branch conditions, zero division, and underflow and overflow?	6.1.2
31.1.3 Do the design activities specify fault-tolerant electronics design and defensive programming techniques including user review and validation?	6.1.2
31.1.4 Does the SIPOC include design objectives for reducing risk to the emergency services personnel to a level as low as is reasonably practical?	6.1.2
31.1.5 Do the design objectives cover risks that could be caused by inaccurate reporting of information?	6.1.3
31.1.6 Is there a record (e.g. design review meeting minutes, design simulation results) indicating that these design for safety principles have been followed? *(See also Document #7 Verification)*	6.3.4
31.2 Is there a list of human factors principles to be adhered to?	6.4.2.7
31.2.1 Is there a record indicating that these human factors principles have been adhered to?	6.3.4
32.0 Does the SIPOC address how the coding will be accomplished?	**6.3.4**
32.1 Are there requirements for in-line code documentation?	6.3.4

For DOCUMENT #6- DKYS DEVELOPMENT MANUAL AND RECORDS	REQUIREMENT
32.2 Are there requirements for use of safe coding constructs?	6.3.4
32.3 Are there requirements for the use of pre and post assertions and exception handling?	6.3.4
32.3.1 Do these requirements include that the assertion and exception handling put the equipment in a fail-safe mode?	6.3.4
32.4 Are there requirements for code readability (i.e. module scope, size, and structure)?	6.3.4
32.5 Are there requirements for module and variable naming?	6.3.4
32.6 Are there records that the coding conventions have been followed *(See also Document #7 Verification)*?	6.3.4
33.0 Is there a SIPOC addressing project communications?	6.3.4
33.1 Does the SIPOC address communication and interaction with all activities conducted by the verification, validation, and management of change teams?	6.3.4
33.2 Does the SIPOC define when and who from the development team participates in verification, validation, and management of change activities?	6.3.4
33.3 Does the SIPOC define when and how the participation will occur?	6.3.4
33.4 Does the SIPOC define how action items from the verification, validation, and management of change teams will be resolved?	6.3.4
34.0 Does the design include diagnostic logic to detect and handle electronic hardware failures?	**6.4.2.7**
35.0 Does the design/coding include logic to detect and handle software execution errors?	**6.4.2.7**
36.0 Does the design/coding include logic that monitors the timing and sequencing of function execution?	**6.4.2.7**
37.0 Does the design/coding physically or functionally separate safety-critical and non-critical functions to reduce the potential for interface and execution failures?	**6.4.2.7**
38.0 Does the software code/firmware contain in-line code documentation that explains or references the author; last revision date; location of mathematical, I/O and other utilities used; variable naming conventions used, and assumptions?	**6.4.2.7**
38.1.1 Have the use of goto's been avoided?	6.4.2.7
38.1.2 Do looping constructs consistently adhere to coding conventions?	6.4.2.7
38.1.3 Do the electronics and software initialize to a	6.4.2.7

For DOCUMENT #6- DKYS DEVELOPMENT MANUAL AND RECORDS		REQUIREMENT
39.0	**Does the design/coding provide for error detection and correction of random errors in data transmitted across communication interfaces?**	**6.4.2.7**
40.0	**Does the design/coding provide for detection of inconsistencies in data representation (i.e. measurement units, binary representation, and order) across communication interfaces?**	**6.4.2.7**
41.0	**Do the design activities address fault-tolerant electronics design and defensive programming techniques including user review and validation?**	**6.4.2.7**
42.0	**Is there a secure, access controlled configuration management tool used for design and coding?**	**6.4.2.7**
42.1	Are there records that this tool is used to produce, control and archive the build files for the identified development milestones?	6.4.2.7
43.0	**Is there a unique checksum associated with the software build/version number for the identified development milestones?**	6.4.2.7
43.1	Has this checksum been verified?	6.4.2.7
44.0	**Are protocols for communicating among components described?**	**6.4.2.7**
45.0	**When using purchased electronics, software, and tools, is the name and version/revision identifier indicated?**	**6.4.2.7**
45.1	Is there information about a description of the purpose for which the electronics, software, or tool is being used?	6.4.2.7

2.7. Document #7- DKYS Verification Manual and Records

Table 10 provides an example questionnaire for inspecting Document #7 Technical Review, Testing, and Verification Manual and Records. Document #7 includes SIPOCs for the verification team to and references records of verification activities.

Table 10 - Version1.0 Assessment Questions for Document#7 – DKYS Verification Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
46.0 Is there Verification Manual?	**6.3.4**
46.1 Does the manual contain one or more SIPOCs for electronics and software verifiers to follow?	6.3.4
46.2 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations[13]?	6.3.4
46.3 Do the SIPOCs identify activities and tools used for electronics and software verification, including metrics, to be collected and applicable standards?	6.3.4
46.4 Does SIPOC define when verification activities take place?	6.3.4
46.5 Does the SIPOC define who conducts the verification activities?	6.3.4
46.6 Does the SIPOC require that the individual conducting the verification activities cannot be the developer for the equipment functions to be verified?	6.3.4
46.7 Does the SIPOC identify records to be completed?	6.3.4
46.7.1 Does the SIPOC specify formats for these records?	6.3.4
46.7.2 Does the SIPOC specify when these records will be completed?	6.3.4
46.7.3 Does the SIPOC specify how the records will be maintained?	6.3.4
46.7.4 Does the SIPOC specify what records will be retained for the FSF?	6.3.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
47.0 Is there a SIPOC for Hazard Analysis activities?	**6.3.4**
47.1 Does SIPOC define when Hazard Analysis activities take place?	6.3.4
47.2 Does the SIPOC define who conducts the Hazard Analysis?	6.3.4
47.3 Does the SIPOC identify the classification of hazards as by risk category (i.e. hostile fire environment, hostile non-fire environment)?	6.3
48.0 Is there a hazard analysis record (i.e. a hazard log) that the Hazard Analysis SIPOC has been followed?	**6.3**
48.1.1 Does the record identify Environmental Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.2 Does the record identify Thermal Hazards that that could render the equipment unusable	6.4.1.1
48.1.3 Does the record identify Chemical Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.4 Does the record identify Biological Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.5 Does the record identify Electrical Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.6 Does the record identify Radiation Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.7 Does the record identify Person Position Hazards that could compromise the equipment functionality including rendering it unusable?	6.4.1.1
48.1.8 Does the record identify Person Equipment that could occur to the user of the equipment as a result of equipment failure??	6.4.1.1
48.1.9 Does the record identify Erroneous Information Hazards that could lead to undue exposure of the user of the equipment to hazards as a result of the equipment providing erroneous data?	6.4.1.1
48.1.10 Does the record (i.e. a hazard log) showing coverage of all hazards identified and traceability between hazards identified and safety functions	6.3.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
49.0 Is there a SIPOC for Risk Categorization activities?	**6.3.4**
49.1.1 Do the risk categorization activities take into account the intended use and the possible, expected, or likely exposures to which the device could be exposed?	6.2, 6.4.2.9
49.1.2 Do the risk categorization activities take into account the criticality for the device's electronics to perform for the safety of the emergency services personnel following exposure?	6.2, 6.4.2.9
49.1.3 Does the risk categorization use the category designations of hostile fire and hostile non-fire?	6.2, 6.4.2.9
50.0 Are there records that the Risk Categorization SIPOC has been followed?	**6.3.4**
51.0 Is there a SIPOC for on-going and iterative DFMEA process to reduce risk of failure by demonstrating acceptable risk reduction for all hazards identified?	**6.3.4, 6.4.2**
51.1 Does the SIPOC define when DFMEA activities take place?	6.3.4
51.2 Does the SIPOC define who conducts the DFMEA activities?	6.3.4
51.3 Does the SIPOC identify how results will be communicated among the FMEA team and other project teams?	6.3.4
51.4 Does the SIPOC specify how the appropriate outputs from the FMEA activities go back to the equipment design team, the design verification team, and the process/enabler owners?	6.3.4
52.0 Are there records that the FMEA SIPOC has been followed (usually completed FMEA tables)?	**6.3.4**
52.1 Do the FMEA tables address all functions identified by the Hazard Analysis?	6.4.2
52.2 Is there a FMEA table for each functional requirement?	6.4.2
52.3 Do the FMEA tables address all parts identified by the Safety Requirements Allocation?	6.4.2
52.3.1 Does the FMEA table identify all assemblies for the equipment to function?	6.4.2
52.3.2 Does the FMEA table identify all, subassemblies for the equipment to function?	6.4.2
52.3.3 Does the FMEA table identify all components necessary for the equipment to function?	6.4.2

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
52.3.4 Does the FMEA table identify all interfaces to communications devices associated with the equipment?	6.4.2
52.3.5 Does the FMEA table identify all internal and external power sources required for the equipment to function as intended?	6.4.2
52.4 Is there a completed FMEA table for each function/assembly, subassembly and component?	6.4.2
52.5 Do the FMEA tables identify failure modes for each function?	6.4.2
52.5.1.1. Do the failure modes addressed include, at a minimum, errors that can be introduced during all life cycle phases conducted by the manufacturer? Examples of errors to be considered include: • Inadequacies in the logic that implements the safety functionality (e.g. the way an underlying circuit is designed or a firmware/software program that has a unit conversion error thus output is set to low), • Fabrication errors (e.g. the material is cured incorrectly, a process step is missed), • Errors due to inadequacies in implementing functional changes (e.g. side effects of change not qualified, microprocessor model change causes new failure mode, FMEA not updated for change).	6.4.2.1
52.5.1.2. Does the failure modes addressed include failure modes induced by interference from outside sources?	6.4.2.4
52.5.1.3. Does the failure modes addressed include failure modes induced by electromagnetic emissions?	6.4.2.4
52.5.1.4. Does the failure modes addressed include failure modes induced by temperature extremes?	6.4.2.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS		NFPA 1800 REQUIREMENT
52.5.1.5.	Does the failure modes addressed include failure modes induced by humidity, moisture, and water exposure?	6.4.2.4
52.5.1.6.	Does the failure modes addressed include failure modes induced by heat and flame exposure?	6.4.2.4
52.5.1.7.	Does the failure modes addressed include failure modes induced by Chemicals?	6.4.2.4
52.5.1.8.	Does the failure modes addressed include failure modes induced by dust and debris?	6.4.2.4
52.5.1.9.	Does the failure modes addressed include failure modes induced by extreme impacts that can corrupt electronically maintained data and instruction processing?	6.4.2.4
52.5.1.10.	Does the failure modes addressed include failure modes induced by systematic failures including coding errors, syntax errors, endless loops, and timing errors?	6.4.2.4
52.5.1.11.	Does the failure modes addressed include failure modes induced by power-up initialization?	6.4.2.4
52.5.1.12.	Does the failure modes addressed include failure modes induced by power loss & transients?	6.4.2.4
52.5.1.13.	Does the failure modes addressed include failure modes induced by user interface?	6.4.2.4
52.5.1.14.	Does the failure modes addressed include failure modes induced by electronic interfaces?	6.4.2.4
52.5.1.15.	Does the failure modes addressed include failure modes induced by mode transitions?	6.4.2.4
52.5.1.16.	Does the failure modes addressed include failure modes induced by branch conditions division by zero, underflow and overflow?	6.4.2.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS		NFPA 1800 REQUIREMENT
52.5.1.17.	Does the failure modes addressed include failure modes induced by memory usage and addressing conflicts?	6.4.2.4
52.5.1.18.	Does the failure modes addressed include failure modes induced by failure in a supervisory section?	6.4.2.4
52.5.1.19.	Does the failure modes addressed include failure modes induced by software failure?	6.4.2.4
52.5.1.20.	Does the failure modes addressed include failure modes induced by timing deadlines, including real-time deadlines and timing requirements for interrupt services?	6.4.2.4
52.5.1.21.	Does the failure modes addressed include failure modes induced by scheduling constraints including task priorities?	6.4.2.4
52.5.1.22.	Does the failure modes addressed include failure modes induced by required processing resources (i.e. memory size, type of memory, and processor speed)?	6.4.2.4
52.5.1.23.	Does the failure modes addressed include failure modes induced by constraints on resource allocations (e.g. amount of memory, processor speed)?	6.4.2.4
52.5.1.24.	Does the failure modes addressed include failure modes induced by sensitivity of electronic performance to changes in safety parameter values and resource allocations?	6.4.2.4
52.5.1.25.	Does the failure modes addressed include failure modes induced by throughput (e.g. operating systems performance overhead, fault detection and recovery overhead, resource contention, locality of memory, tasks prioritization, and memory addressing schemes)?	6.4.2.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
52.5.2 Does the FMEA records identification of failure effects (conditions) for each function as a process step?	6.4.2.5
52.5.2.1. Are the following failure effects (conditions) considered: No no part of intended function is achieved More functional output is more than required Less functional output is less than required As well as all design intent but with additional results Part of only some of the function is achieved Reverse the logical opposite of the intention Early function occurs early relatively to clock time Late function occurs late relative to clock time Before function occurs before it should in sequence of operations After function occurs after it should in sequence of operations	6.4.2.5
52.5.3 Do the FMEA activities address ranking of failure modes and effects using a valid measure of importance, such as RPN? As a process step	6.4.2.6
52.5.3.1. For the RPNs claimed, are the manufacturer's review, test, and verification records consistent with that required for an RPN level?	6.4.2.6
52.5.3.2. Does the completed FMEA table show consideration of RPN?	6.4.2.6
52.5.4 Are there records showing that the FMEA has been updated at specified milestones?	6.3.4
52.5.5 Have all action items associated with the FMEA been closed out?	6.3.4
53.0 Is there a SIPOC for Design Review activities?	**6.3.4**
53.1.1 Does SIPOC define when design review activities take place?	6.3.4
53.1.2 Does the SIPOC define who participates in the	6.3.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
53.1.3 Do the design review activities meet accepted standards for design review?	6.3.4
54.0 Are there records of design reviews? i.e. meeting minutes, records showing action requests, and which verify completion of the action requests.	**6.3.4**
55.0 Is there a SIPOC for Code Review activities?	**6.3.4**
55.1.1 Does SIPOC define when code review activities take place?	6.3.4
55.1.2 Does the SIPOC define who participates in the code review activities?	6.3.4
55.1.3 Do the code review activities meet accepted standards for code review?	6.3.4
56.0 Are there records of code reviews? i.e. meeting minutes, records showing action requests, and which verify completion of the action requests.	**6.3.4**
57.0 Is there a SIPOC for electronics and software testing activities?	**6.3.4**
57.1 Does the SIPOC specify test objectives, test strategy, test procedures, format and recording of test results?	6.3.4
57.2 Does the SIPOC address how pass/fail will be determined?	6.3.4
58.0 Are there records of testing?	**6.3.4**
58.1 Are test levels recorded (e.g. software unit, module, and component, hardware design, electronic board (h/w and s/w integration), subassembly, assembly, assembly with accessory?)	6.3.4
58.1.1 Is the level of testing required for a specific category designation recorded?	6.3.4
58.2 Are test instructions and tools used for testing recorded?	6.3.4
58.3 Are there test records of pass/fail criteria outcomes?	6.3.4
58.4 Is test coverage of each function whose failure could involve a risk recorded (i.e. are the appropriate FMEA entries recorded?)	6.3.4
58.5 Are there records of tests that exercise fail-safe and fail-operational logic bringing the product to a risk addressed state been recorded?	6.3.4
58.6 Are there records of tests demonstrating that the scheduling requirements are met been recorded?	6.3.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1850 REQUIREMENT
58.7 Are there records of tests verifying that the safety functions meet the safety operating constraints?	6.3.4
58.7.1 Are there records of tests verifying the integrity of the separations between safety-related and non safety-related functions? (Separation is applied when a product provides core safety functions and other non-safety functions. This question may not be applicable for all EQUIPMENT because all functions may be safety-related.)	6.3.4
58.7.1.1. Has test data verifying that partition violations, caused by data handling errors, do not occur been recorded?	6.3.4
58.7.1.2. Has test data verifying that partition violations, caused by control errors, do not occur been recorded?	6.3.4
58.7.1.3. Has test data verifying that partition violations, caused by timing errors, do not occur been recorded?	6.3.4
58.7.1.4. Has test data verifying that partition violations, caused by misuse of resources, do not occur been recorded?	6.3.4
58.7.1.5. Is the consistency in the test data and control flows across interfaces verified and recorded?	6.3.4
58.7.2 Are there test records showing that the electronics and software only perform intended functions and do not provide output that may compromise safety recorded?	6.3.4
58.7.3 Are there test records of stress tests which verify that the software responds in accordance with the functional safety requirements listed?	6.3.4
58.7.4 Are there test records that confirm the safety requirements, including confirmation of operating modes and transition, such as startup, shutdown, reset, Manual(s), remote, semiautomatic, automatic, monitor, standby, emergency, and stuck/jammed (abnormal)?	6.3.4
58.8 Are there test records that confirm the safety requirements, including confirmation of operating modes and transition, such as startup, shutdown, reset, remote, semiautomatic, automatic, monitor, standby, emergency,	6.3.4

for DOCUMENT # -7 DKYS VERIFICATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
58.9 Is there a requirement to test traceability record?	6.3.4
58.10 Does the requirement to test traceability records cover all requirements specified in the *Document #5 Product Requirements Specification?*	6.3.4
58.11 Do the records provided verify the electronics and software functions as required?	6.3.4
59.0 Is there a verification summary record?	6.3.4
59.1 Does the summary include measures, techniques, and procedures used for confirming that equipment functions conform to requirements?	6.3.4
59.2 Does the summary record include a description of the facilities, equipment/tools which were used?	6.3.4
59.3 Does the summary record list those who conducted the verification, validation, and testing listed and the dates of testing?	6.3.4
59.4 Does the summary record specify the objectives for each level of testing recorded?	6.3.4
59.5 Does the summary record reference work instructions at each level of testing recorded?	6.3.4
59.6 Does the summary record reference test cases with objective pass/fail criteria for each test conducted?	6.3.4

2.8. Document #8 – DKYS Production Manual and Records

Table 11 provides an example questionnaire for inspecting Document #8 Production Manual and Records. Document #8 includes SIPOCs for the production team and references records of development activities.

Table 11 - Version1.0 Assessment Questions for Document #8 – DKYS Production Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #8 DKYS - PRODUCTION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
60.0 Is there a Production Manual?	**6.3.4**
60.1 Does the Production manual contain one or more SIPOCs for electronics and software verification activities during production?	6.3.4
60.1.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
60.1.2 Does the SIPOC identify activities and tools used for electronics and software verification during production, including metrics, to be collected and applicable standards?	6.3.4
60.1.3 Does SIPOC define when verification activities take place?	6.3.4
60.1.4 Does the SIPOC define who conducts the verification activities?	6.3.4
60.1.5 Does the SIPOC identify records to be completed?	6.3.4
60.1.5.1. Does the SIPOC specify formats for these records?	6.3.4
60.1.5.2. Does the SIPOC specify when these records will be completed?	6.3.4
60.1.5.3. Does the SIPOC specify how the records will be maintained?	6.3.4
60.1.5.4. Does the SIPOC specify what records will be retained for the FSF?	6.3.4
61.0 Are there records that the Production SIPOC has been followed?	**6.3.4**
61.1 Does the production manual require a checksum verification of the software/firmware when loaded into memory?	6.3.4
61.1.1 Are there production records showing evidence of checksum verification?	6.3.4

2.9. Document #9 – DKYS Validation Manual(s) and Records

Table 12 provides an example questionnaire for inspecting Document #9 Validation Manual and Records. Document #9 includes SIPOCs for the validation team and references records of validation activities.

Table 12 - Version1.0 Assessment Questions for Document#9 - DKYS Installation, Commissioning, and Validation Manual and Record

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #9 – DKYS VALIDATION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
62.0 Does the DKYS Validation Manual contain one or more SIPOCs for verifying equipment before field use?	6.3.4
62.1.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
62.1.2 Does the SIPOC identify activities and tools used including metrics, to be collected and applicable standards?	6.3.4
62.1.3 Does SIPOC define when these activities take place?	6.3.4
62.1.4 Does the SIPOC define who conducts these activities?	6.3.4
62.1.5 Does the SIPOC identify records to be completed?	6.3.4
62.1.5.1. Does the SIPOC specify formats for these records?	6.3.4
62.1.5.2. Does the SIPOC specify when these records will be completed?	6.3.4
62.1.5.3. Does the SIPOC specify how the records will be maintained?	6.3.4
62.1.5.4. Does the SIPOC specify what records will be retained for the FSF?	6.3.4
63.0 Is there a list of hazards that could occur during validation of the equipment described?	6.3.4
63.1 Are safety precautions to be taken during installation and commissioning listed?	6.3.4
64.0 Are there records of that the SIPOC has been followed?	6.3.4
64.1 Are there records of use case or scenario testing?	6.3.4
64.2 Are there records of mode transition testing?	6.3.4

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #9 – DKYS VALIDATION MANUAL AND RECORDS		NFPA 1800 REQUIREMENT
64.3	Are there records of tests that validate the quantitative ranges identified for human, electronic, and electrical input and output to and from the EQUIPMENT?	6.3.4
64.4	Are there records of validation tools and equipment used during installation and commissioning?	6.3.4
64.5	Are there calibration records for validation tools and equipment?	6.3.4
64.6	Are there records validating the contents of the user manual?	6.3.4
65.0	**Is there a validation summary record?**	6.3.4
65.1	Does the summary record specify the objectives for validation?	6.3.4
65.2	Does the summary include measures, techniques, and procedures used for confirming that equipment functions conform to requirements?	6.3.4
65.3	Does the summary record include a description of the facilities, equipment/tools which were used?	6.3.4
65.4	Does the summary record list those who conducted the validation testing and the dates of testing?	6.3.4
65.5	Does the summary record reference work instructions for validation testing?	6.3.4

2.10. Document #10 – DKYS User Manual and Records

Table 13 provides an example questionnaire for inspecting Document #10 User Manual and Records. Document #10 includes instructions for the product user and references records of use activities.

Table 13 - Version1.0 Assessment Questions for Document #10 - DKYS User Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #10 - DKYS USER MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
66.0 Are the DKYS User Manual contents consistent with NIOSH/NPPTL Best Practice Recommendations[14]?	**6.3.4**
66.1 Are the acceptable configurations of the equipment identified?	6.3.4
66.1.1 Is there a unique checksum that the user of the equipment can use to verify that the configuration of software/firmware is acceptable?	6.3.4
66.2 Is there a statement of the Intended Use of the EQUIPMENT?	6.3.4
66.2.1 Is there an equipment label that the user of the equipment can use to verify the category designation?	6.3.4
66.3 Does the statement of intended use define Conditions of Use?	6.3.4
66.3.1 Does the statement of intended use define acceptable operating ranges?	6.3.4
66.3.2 Does the statement of intended use indicate restrictions and limitations on uses?	6.3.4
66.3.2.1. Are normal and abnormal operating ranges specified?	6.3.4
66.3.3 If the EQUIPMENT is intended to be used as a stand-alone device, is the stand-alone usage defined?	6.3.4
66.3.3.1. Does the stand-alone usage definition indicate what should not be connected to the EQUIPMENT?	6.3.4
66.3.4 If the equipment may be used with accessories, are the allowable accessories and their interfaces uniquely identified?	6.3.4

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #10 - DKYS USER MANUAL AND RECORDS	NFPA 1600 REQUIREMENT
66.3.5 If the equipment may be used with peripherals, are the allowable peripherals and their interfaces uniquely identified?	6.3.4
66.3.6 Are there detailed procedures on how to use the equipment?	6.3.4
66.3.6.1. Do the procedures include interfacing with the software and/or hardware?	6.3.4
66.3.6.2. Is there a list of hazards that could occur during use of the equipment?	6.3.4
67.0 Is there a reference to repair and maintenance requirements and activities?	6.3.4
68.0 Is there a procedure for reporting problems with using the equipment?	6.3.4

2.11. Document #11 – DKYS Distribution Manual(s) and Records

Table 14 provides an example questionnaire for inspecting Document #11. Document #11 includes SIPOCs for distributing the product and references records of distribution activities.

Table 14 - Version1.0 Assessment Questions for Document#11 - DKYS Distribution Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #11 – DKYS DISTRIBUTION MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
69.0 Does the DKYS Distribution Manual contain one or more SIPOCs for verifying equipment before field use?	**6.3.4**
69.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
69.2 Does the SIPOC identify activities and tools used including metrics, to be collected and applicable standards?	6.3.4
69.3 Does SIPOC define when these activities take place?	6.3.4
69.4 Does the SIPOC define who conducts these activities?	6.3.4
69.5 Does the SIPOC identify records to be completed?	6.3.4
69.5.1 Does the SIPOC specify formats for these records?	6.3.4
69.5.2 Does the SIPOC specify when these records will be completed?	6.3.4
69.5.3 Does the SIPOC specify how the records will be maintained?	6.3.4
69.5.4 Does the SIPOC specify what records will be retained for the FSF?	6.3.4
70.0 Does the distribution manual list documents to be distributed with the equipment?	6.3.4
70.1.1 Is User Manual listed?	6.3.4
70.1.2 Is a unique identifier for the user manual recorded in distribution records? (e.g. title, version number, date)	6.3.4
70.2 Has the user manual been validated? *(Assess by assessing Document #9)*	6.3.4

2.12. Document #12 – DKYS Maintenance and Repair Manual and Records

Table 15 provides an example questionnaire for inspecting Document #11 Maintenance and Repair Manual and Records. Document #12 includes SIPOCs for maintenance and repair of the product and references records of maintenance and repair activities. (See Part 4, Section 3.10) **See Part 4, Section 3.2.5)**

Table 15 - Version1.0 Assessment Questions for Document #12 - DKYS Maintenance and Repair Manual and Records

3rd PARTY INSPECTION QUESTIONS for DOCUMENT #12 – DKYS MAINTENANCE AND REPAIR MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
71.0 Does the DKYS Maintenance and Repair Manual contain one or more SIPOCs?	6.3.4
72.0 Does the SIPOC include calibration and diagnostic activities?	6.3.4
72.1 Are the activities carried out by the user, the manufacturer, or a repair center?	6.3.4
73.0 Are the procedures to prevent an unsafe state during operation and maintenance recorded?	6.3.4
74.0 Are circumstances and procedures for bypassing or overriding safety functions or interlocks described?	6.3.4
74.1 Are these circumstances and procedures justified?	6.3.4
74.2 Are they conducted by trained individuals under strict risk control protocols?	6.3.4
75.0 Does the plan include circumstances and procedures for restoring and verifying safety functions or interlocks after they have been bypassed or overridden?	6.3.4
76.0 Does the plan include calibration and diagnostic activities?	6.3.4
77.0 Is there a list of hazards that could occur during installation of the equipment?	6.3.4
78.0 Are there detailed instructions on how to maintain and repair the equipment?	6.3.4
78.1 Do these instructions include interfacing with the software and/or hardware?	6.3.4
79.0 Are there maintenance records?	6.3.4
79.1 Do the maintenance records include maintenance schedules?	6.3.4

for DOCUMENT #12 – DKYS MAINTENANCE AND REPAIR MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
79.2 Do the maintenance records include time of the maintenance?	6.3.4
79.3 Do the maintenance records include who conducted the test?	6.3.4
79.4 Do the maintenance records include results of the test?	6.3.4
79.5 Do the maintenance records include problem reports?	6.3.4
80.0 Do these records identify the unique configuration of the EQUIPMENT?	6.3.4
81.0 Are there written instructions for maintainers of the EQUIPMENT?	6.3.4
81.1 Do the maintenance instructions specify a calibration procedure?	6.3.4
81.2 Do the maintenance instructions specify the operation intervals for which the EQUIPMENT must be checked or calibrated according to the manufacturer's specifications?	6.3.4
81.3 Are other equipment that must be tested in combination with the EQUIPMENT specified?	6.3.4
81.4 Do the maintenance instructions specify the operation intervals for which the combined EQUIPMENT must be checked or calibrated according to the manufacturer's specifications?	6.3.4
82.0 Are there written instructions for maintainers of the EQUIPMENT?	6.3.4
83.0 Is there a description of repair activities within the plan?	6.3.4
84.0 Does the plan include calibration and diagnostic activities?	6.3.4
84.1 Are the activities carried out by the user, the manufacturer, or a repair center?	6.3.4
85.0 Are the procedures to prevent an unsafe state during operation and maintenance recorded?	6.3.4
86.0 Are circumstances and procedures for bypassing or overriding safety functions or interlocks described?	6.3.4
86.1 Are these circumstances and procedures justified?	6.3.4
86.2 Are they conducted by trained individuals under strict risk control protocols?	6.3.4
87.0 Are documentation guidelines for describing the proposed change outlined in the plan?	6.3.4
88.0 Is the definition of acceptable risk outlined within the plan?	6.3.4
89.0 Is a hazard log showing coverage of each hazard and	6.3.4

for DOCUMENT #12 – DKYS MAINTENANCE AND REPAIR MANUAL AND RECORDS		NFPA 1800 REQUIREMENT
	and verification results included?	
90.0	Are there guidelines addressing how to avoid the introduction of new hazards?	6.3.4
91.0	Is there a unique reference to the applicable version and configuration of the EQUIPMENT?	6.3.4
92.0	Are operating activities specified with respect to how changes will require modifying and repeating these activities?	6.3.4
93.0	Are calibration activities specified with respect to how changes will require modifying and repeating these activities?	6.3.4
94.0	Are diagnostic activities specified with respect to how changes will require modifying and repeating these activities?	6.3.4
95.0	Are testing activities specified with respect to how changes will require modifying and repeating these activities?	6.3.4
96.0	Are maintenance activities specified with respect to how changes will require modifying and repeating these activities?	6.3.4
97.0	Are training requirements included in the plan?	6.3.4
97.1	Is re-training needed when changes are made?	6.3.4
97.2	Are the types of training that will be required when changes are made identified?	6.3.4

2.13. Document # 13 – DKYS Management of Change Manual and Records

Table 16 provides an example questionnaire for inspecting Document #13 Management of Change Manual and Records. Document #13 includes SIPOCS for how change will be handled and references records of change activities.

Table 16 - Version1.0 Assessment Questions for Document #13 - DKYS Management of Change Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #13 – DKYS MANAGEMENT OF CHANGE MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
98.0 Does the DKYS Management of Change Manual contain one or more SIPOCs for verifying equipment before field use?	**6.3.4**
98.1 Are the SIPOCs consistent with NIOSH/NPPTL Best Practice Recommendations[15]?	6.3.4
98.2 Does the SIPOC identify activities and tools used including metrics, to be collected and applicable standards?	6.3.4
98.3 Does SIPOC define when these activities take place?	6.3.4
98.4 Does the SIPOC define who conducts these activities?	6.3.4
98.5 Does the SIPOC identify records to be completed?	6.3.4
98.5.1 Does the SIPOC specify formats for these records?	6.3.4
98.5.2 Does the SIPOC specify when these records will be completed?	6.3.4
98.5.3 Does the SIPOC specify how the records will be maintained?	6.3.4
98.5.4 Does the SIPOC specify what records will be retained for the FSF?	6.3.4
99.0 Does the SIPOC address how the configurable item to be changed will be handled?	**6.3.4**
99.1 Is the configurable item identification scheme specified?	6.3.4

[15] NIOSH NPPTL Best Practices Recommendations, Part 4, Section 3.2.6 and

for DOCUMENT #13 – DKYS MANAGEMENT OF CHANGE MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
99.2 Is there a description of how configurable items will be received?	6.3.4
99.3 Is there a description of how configurable items will be stored?	6.3.4
99.4 Is there a description of how configurable items will be handled or accessed?	6.3.4
99.5 Is there a description of how configurable items will be released after change?	6.3.4
100.0 Does the SIPOC detail the activities for maintaining baseline versions of a product?	**6.3.4**
101.0 Does the SIPOC describe the format for and the initiation, transmittal, review, implementation, tracking, and closure of change requests and discrepancy reports?	6.3.4
102.0 Are there records of Management of Change activities?	**6.3.4**
102.1 Are there records of configurable items?	6.3.4
102.1.1 Are the configurable items uniquely identified?	6.3.4
102.1.2 Are there records of receipt of configurable items?	6.3.4
102.1.3 Are there records of storage of configurable items?	6.3.4
102.1.4 Are there records of handling of configurable items?	6.3.4
102.1.5 Are there records of release of configurable items?	6.3.4
103.0 Are there records describing all changes made to the equipment since the last assessment?	**6.3.4**
103.1 Do the records identify the configurable item being changed?	6.3.4
103.2 Is there a unique identifier for tracking the change?	6.3.4
103.3 Do the records describe the reasons for the change?	6.3.4
103.4 Do the records describe the impact of the change on functional safety?	6.3.4
103.5 Do the records show authorization of the change before implementation?	6.3.4
103.6 Do the records show verification of the change for all changes?	6.3.4
103.7 Do the records show validation of the change for all changes?	4,5
103.8 Do the records show that the documentation affected by the change been updated? (e.g. changes in user manual or	6.3.4

for DOCUMENT #13 – DKYS MANAGEMENT OF CHANGE MANUAL AND RECORDS	NFPA 1600 REQUIREMENT
103.9 Do the records show closure of the change including sign off by the responsible individual?	6.3.4

2.14. Document #14 – DKYS End of Service Life Manual and Records

Table 17 provides an example questionnaire for inspecting Document #14 End of Service Life Manual and Records. Document #14 includes SIPOCS for product End of Service Life and references records of End of Service Life activities.

Table 17 - Version1.0 Assessment Questions for Document #14 – DKYS End of Service Life Manual and Records

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #14 – DKYS END OF SERVICE LIFE MANUAL AND RECORDS	NFPA 1800 REQUIREMENT
104.0 Is there an End of Service Life Manual?	**6.3.4**
104.1 Does End of Service Life manual contain one or more SIPOCs for taking the equipment out of service?	6.3.4
104.1.1 Are the SIPOC(s) consistent with NIOSH/NPPTL Best Practice Recommendations?	6.3.4
104.1.2 Does the SIPOC identify End of Service Life activities and tools used including metrics, to be collected and applicable standards?	6.3.4
104.1.3 Does SIPOC define when End of Service Life activities take place?	6.3.4
104.1.4 Does the SIPOC define who conducts the End of Service Life activities?	6.3.4
104.1.5 Does the SIPOC identify records to be completed?	6.3.4
104.1.5.1. Does the SIPOC specify formats for these records?	6.3.4
104.1.5.2. Does the SIPOC specify when these records will be completed?	6.3.4
104.1.5.3. Does the SIPOC specify how the records will be maintained?	6.3.4
104.1.5.4. Does the SIPOC specify what records will be retained for the FSF?	6.3.4
105.0 Are there records of the End of Service Life activities?	**6.3.4**
105.1 Is the date and reason for end of service life recorded?	6.3.4
105.2 Is the unique configuration of the equipment recorded?	6.3.4
105.3 Are the End of Service Life tools and equipment used identified?	6.3.4
105.3.1 Are there calibration records for End of Service Life	6.3.4

for DOCUMENT #14 – DKYS END OF SERVICE LIFE MANUAL AND RECORDS		NFPA 1600 REQUIREMENT
105.4	Are there records established for closing down to an inactive, safe state, dismantling, removal, waste processing, and/or storage for possible reuse?	6.3.4

2.15. Document #15: DKYS Product Description

Table 18 provides an example questionnaire for inspecting Document #15 Product Description. Document#15 describes the product function and intended use. It also identifies any restrictions on use.

(See Part 4, Section 3.4)

Table 18 - Version1.0 Assessment Questions for Document #15 – DKYS Product Description

3rd PARTY ASSESSMENT QUESTIONS for DOCUMENT #4 – DKYS PRODUCT DESCRIPTION DOCUMENT	NFPA 1800 REQUIREMENT
106.0 Is there a description of equipment functionality?	5.2, 6.3.4
106.1 Are equipment functions listed?	5.2, 6.3.4
106.1.1 Are there any equipment functions available that are not listed?	5.2, 6.3.4
106.1.2 Are there any equipment functions not available that are listed?	5.2, 6.3.4
107.0 Is there an As Built description of the equipment?	5.2, 6.3.4
107.1 Does the as built description include name and model number?	5.2, 6.3.4
107.2 Does the as built description list all equipment parts including identifying information for each part?	5.2, 6.3.4
107.2.1 Are there parts in the equipment that are not listed as part of the as built description?	5.2, 6.3.4
107.2.2 Are there parts listed in the as built description that are not in the equipment?	5.2, 6.3.4
107.3 Are equipment accessories listed?	5.2, 6.3.4
107.3.1 Are there accessories to the equipment that are not listed?	5.2, 6.3.4
107.3.2 Are there accessories not listed that are for use with the equipment?	5.2, 6.3.4
107.4 Are equipment peripherals listed?	5.2, 6.3.4
107.4.1 Are there peripherals to the equipment that are not listed?	5.2, 6.3.4

for DOCUMENT #4 – DKYS PRODUCT DESCRIPTION DOCUMENT	NFPA 1800 REQUIREMENT
107.4.2 Are there peripherals not listed that are for use with the equipment?	5.2, 6.3.4
108.0 Is there an equipment diagram?	5.2, 6.3.4
108.1 Does the equipment diagram show electronic assemblies?	5.2, 6.3.4
108.1.1 Are there any electronic assemblies not shown in the equipment diagram that are present?	5.2, 6.3.4
108.1.2 Are there any electronic assemblies shown in the equipment diagram that are not present?	5.2, 6.3.4
108.2 Does the equipment diagram list all software/firmware components?	5.2, 6.3.4
108.2.1 Are there any software/firmware components not listed in the equipment diagram?	5.2, 6.3.4
108.3 Does the equipment diagram show accessories?	5.2, 6.3.4
108.3.1 Are there any accessories not shown in the equipment diagram that are present?	5.2, 6.3.4
108.3.2 Are there any accessories shown in the equipment diagram that are not present?	5.2, 6.3.4
108.4 Does the equipment diagram show electronic interfaces to the accessories?	5.2, 6.3.4
108.4.1 Are there any electronic interfaces not shown in the equipment diagram that are present?	5.2, 6.3.4
108.4.2 Are there any electronic interfaces shown in the equipment diagram that are not present?	5.2, 6.3.4
108.5 Does the equipment diagram list all software interfaces to the accessories?	5.2, 6.3.4
108.5.1 Are there any software interfaces not listed in the equipment diagram that are present?	5.2, 6.3.4
108.5.2 Are there any software interfaces listed in the equipment diagram that are not present?	5.2, 6.3.4
108.6 Does the equipment diagram show peripherals?	5.2, 6.3.4
108.6.1 Are there any peripherals not shown in the equipment diagram that are present?	5.2, 6.3.4
108.6.2 Are there any peripherals shown in the equipment diagram that are not present?	5.2, 6.3.4
108.7 Does the equipment diagram show all electronic interfaces to the peripherals?	5.2, 6.3.4
108.7.1 Are there any electronic interfaces not shown in the equipment diagram that are present?	5.2, 6.3.4

for DOCUMENT #4 – DKYS PRODUCT DESCRIPTION DOCUMENT	NFPA 1800 REQUIREMENT
108.7.2 Are there any electronic interfaces shown in the equipment diagram that are not present?	5.2, 6.3.4
108.8 Does the equipment diagram list all software interfaces to the peripherals?	5.2, 6.3.4
108.8.1 Are there any software interfaces not listed in the equipment diagram that are present?	5.2, 6.3.4
108.8.2 Are there any software interfaces listed in the equipment diagram that are not present?	5.2, 6.3.4
109.0 Is there a block diagram showing the electronic architecture for all electronic assemblies?	6.3.4
109.1 Does the block diagram show electronic subassemblies for all assemblies?	6.3.4
109.1.1 Are there any inconsistencies between electronic subassemblies shown and the parts identified in the parts list for the As Built description?	6.3.4
109.1.2 Does the block diagram show electronic components for all subassemblies?	6.3.4
109.1.3 Are there any inconsistencies between electronic components shown and the parts identified in the parts list for the As Built description?	6.3.4
109.2 Are there electrical schematics showing the power distribution for all electronic assemblies?	6.3.4
109.2.1 Have the power requirements been validated for the schematic?	6.3.4
110.0 Are there design descriptions for all software/firmware components?	6.3.4
110.1 Does the description include detailed design /module calling structures for the software/firmware?	6.3.4
110.1.1 Has the detailed design/module calling structures been verified? (Assess by reviewing Document #7)	6.3.4
110.2 Does the description include software/firmware flowchart or process diagrams?	6.3.4
110.2.1 Have the detailed flowcharts or process diagrams been verified? (Assess by reviewing Document #7)	6.3.4
110.3 Does the description list required software libraries (utilities and macros)?	6.3.4
110.3.1 Have the software libraries been verified or certified? (Assess by reviewing Document #7)	6.3.4

for DOCUMENT #4 – DKYS PRODUCT DESCRIPTION DOCUMENT	NFPA 1800 REQUIREMENT
111.0 Does the description provide data dictionaries or glossaries?	6.3.4
111.1.1 Have the data dictionaries or glossaries been verified? (Assess by reviewing Document #7)	6.3.4
111.2 Does the description list all interfaces to other software?	6.3.4
111.2.1 Have these interfaces been verified? (Assess by reviewing Document #7)	6.3.4
111.3 Does the description include all human interfaces?	5.2, 6.3.4
111.3.1 Have the human interfaces been validated? (Assess by reviewing Document #9)	6.3.4
111.4 Does the description include mode or state transition diagrams?	6.3.4
111.4.1 Have the mode or state transition diagrams been verified? (Assess by reviewing Document #7)	6.3.4
111.5 Does the description include memory maps to electronic storage locations?	6.3.4
111.5.1 Have the memory maps been verified (Assess by reviewing Document #7)	6.3.4

3.0. EXAMPLE DFMEA ASSESSMENT THREADS FOR DKYS

3.1. Assessment Objective

The objective of the assessment is to confirm the DFMEA documentation submitted for compliance to ESE 1800 requirement 6.3.4. The 3rd party reviewer focuses on the following questions:

52.0 Are there records that the DFMEA SIPOC has been followed (usually completed DFMEA tables)?

52.2. Is there a DFMEA table for each functional requirement?

52.5.1.10 Does the failure modes addressed include failure modes induced by systematic failures including coding errors, syntax errors, endless loops, and timing errors?

58.0 Are there records of testing?

3.2. Assessment Thread

The 3rd party reviewer selects Requirement No. 1 and its Sub-requirement 1.1.4 to assess. Requirement 1 addresses “the correct identification of all first responders to the unit commander”. Sub-requirement 1.1.4 states “Location data must be updated at least once per minute.”

The DFMEA prepared by the manufacturer indicates that the Location Server Software could fail with a potential failure mode of “Software algorithm shows stale data when no RFID tags are active. This results in a failure effect of the unit commander having the wrong location information for the deployed first responders. Since the Location Server Software is a Commercial Off the Shelf (COTS) Component, the manufacturer did not have access to the source code. They did check all known bugs at the time of testing and continue to monitor bug lists for components in fielded products. They also provided proven-in-use data. The reviewer checks the date of the bug lists, establishes that the proven-in-use criteria stated are acceptable, and reviews the verification

records for this function. Since this is an important function, the reviewer requests a laboratory test of the DKYS for the condition of “no active RFID tags.”[16]

[16] The functional test for degenerate conditions such as no active RFID tags may be specified in ESE 1800 or a future product standard for location identification and tracking equipment.

4.0 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

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

5.0. 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.