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

Part 5: The Independent Functional Safety Assessment (IFSA)

Prepared by Safety Requirements, Inc.

NIOSH Contract 200-2003-02355

September 2007

TABLE OF CONTENTS

LIST OF FIGURES

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.

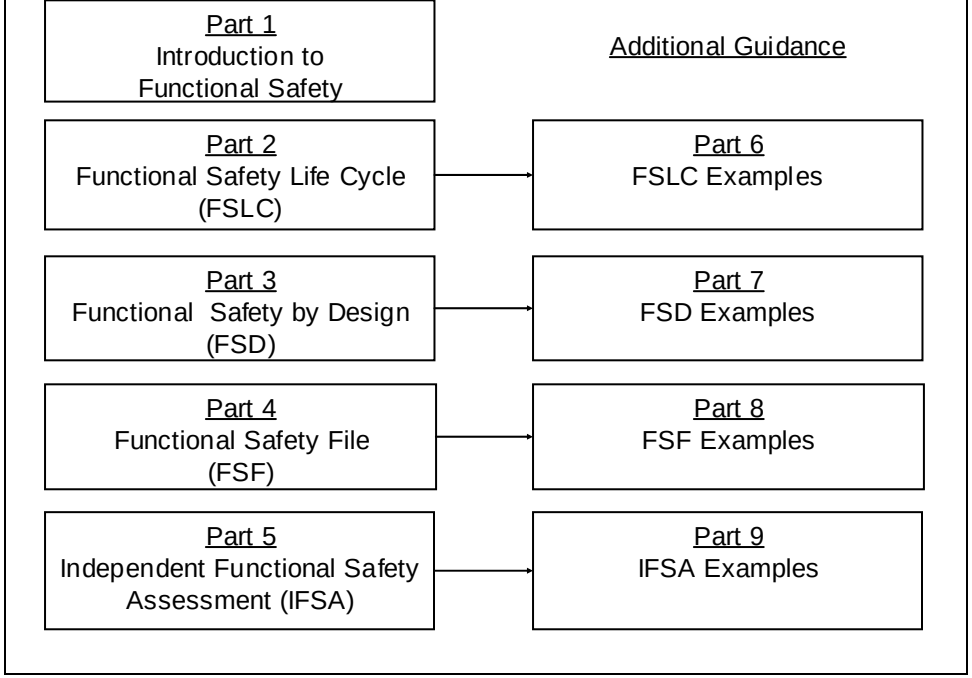


Figure 1 - The functional safety report series.

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.

---

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

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

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

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

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

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

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

Part 6 – Additional Guidance: Functional Safety Life Cycle Examples are used to develop the Scope of the Project Plan. The scope guides Project Functional Safety by Design (FSD) Compliance and Project Documentation.

Part 7 – Additional Guidance: Functional Safety by Design Examples drives Project Design for Safety Compliance, which then becomes part of the Project Documentation.

Part 8 – Additional Guidance: Functional Safety File Examples help to complete the Project Documentation, to enable a third party assessment.

Part 9 – Additional Guidance: Independent Functional Safety Audit Examples are employed in the development of the Third Party Assessment Report. Figure 2 overviews the relationships among Parts 6, 7, 8, and 9.

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

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

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.

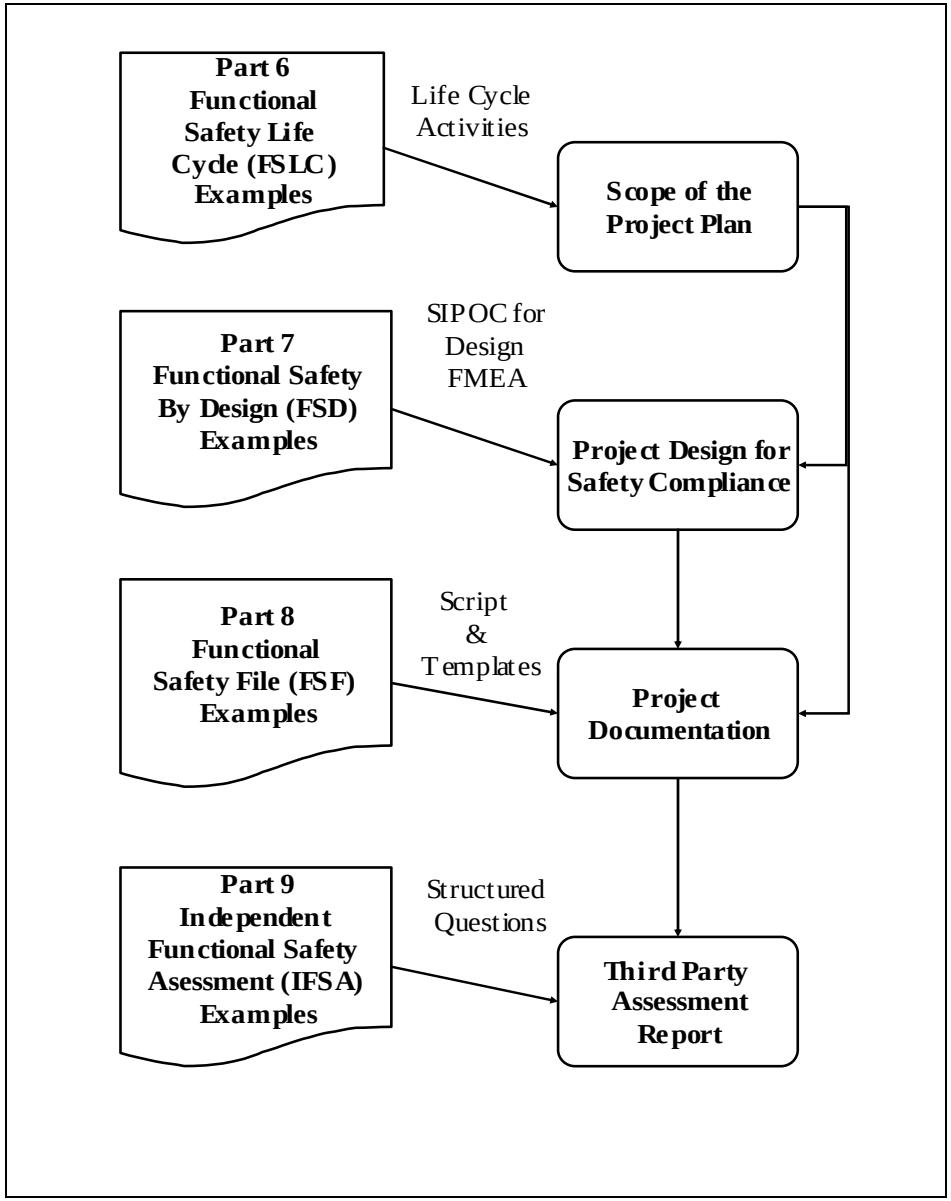


Figure 2 - Relationships among Parts 6, 7, 8, and 9

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
- Transmitting and receiving information about the site zone and the emergency

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 both standards.

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

Table 1 - Mining Industry Guidelines

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

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

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

Table 2 - Overview of ANSI UL 1988 and IEC 61508

ACKNOWLEDGEMENT

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

ABSTRACT

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

Advanced Personal Protective Equipment (PPE) incorporates 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.

This report, the Independent Functional Safety Assessment (IFSA), is the Part 5 in a nine-part series of recommendations addressing the functional safety of advanced Personal Protective Equipment (PPE) for emergency responders. Part 5 describes the scope, contents, and frequency of conducting IFSAs. The IFSA is an assessment of the documented evidence of the FSLC activities and FSD practices.

1.0. INTRODUCTION

1.1. Background

The PPE industry is using electronics and software technology to improve safety of emergency responders and to increase the likelihood of survival of victims. Electronics and software now provide protection, monitoring, and communication functions for emergency responders. Although use of electronics and software provides benefits, it also adds a level of complexity that, if not properly considered, may adversely affect worker safety.

Failure of functionality embedded in electronics and software may lead to new hazards or worsen existing ones. Electronics and software have unique failure modes that may be different from mechanical systems or hard-wired electronic systems. The situation led to the development of criteria for designing functional safety into the entire system from initial conceptualization to retirement.

Functional safety seeks to design safety into the equipment for all phases of its use. Software is a sub-system; therefore, software safety is part of functional safety.

Part 5, Independent Functional Safety Assessment (IFSA), describes the scope, contents, and frequency of conducting IFSAs. The IFSA is an assessment of the documented evidence of the FSLC activities and FSD practices. It recommends best practices for the conduct of IFSAs. The IFSA determines the completeness and suitability of the functional safety activities, evidence, and justifications. A professional in the field of systems safety, who is independent of the project or project phase, conducts the IFSA. The recommended degree of independence is associated with the risk reduction factor (RRF) for the PPE.

1.2. Scope of IFSA

An independent functional safety assessment (IFSA) provides an independent examination of the safety policy/strategy, staff qualifications, and the functional safety life cycle (FSLC) practices. (See Figure 3 and Table 3.) It is conducted by consulting

the functional safety file (FSF) and through interviews with project staff. Project staff includes designers, manufacturers, assemblers, testers and users as appropriate.

The conduct of IFSAs supports the following safety objectives:

- Planned FSLC practices are suitable and effective for achieving the specified risk reduction objectives
- Actual FSLC practices adhere to the planned FSLC practices
- PPE design conforms to product safety design requirements

The conduct of IFSAs benefits both the manufacturer and the user in that potential problems are often detected early, thus allowing corrections to be made more effectively and efficiently.

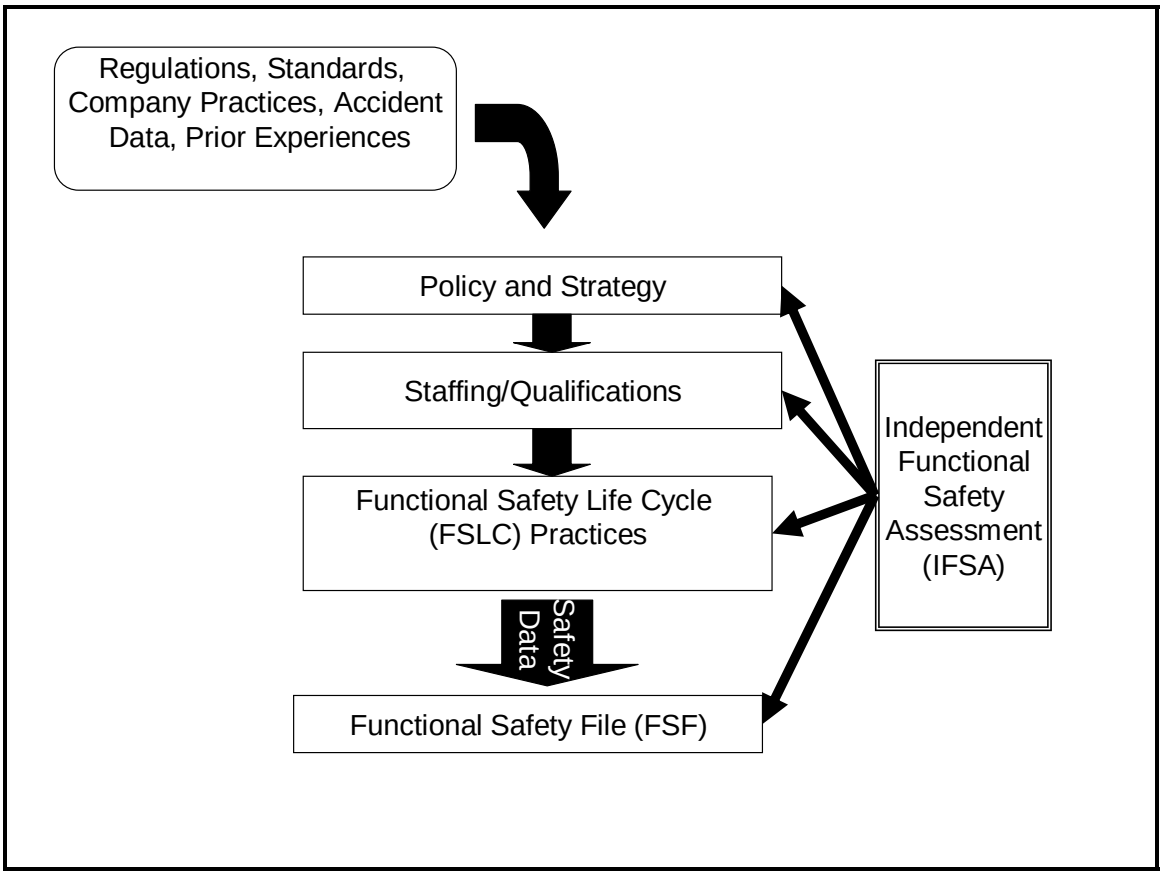


Figure 3 - Functional Safety Life Cycle Activities

Phase	Activity	Objectives	FSF Documentation
I. Plan		Develop a project plan that addresses the entire life cycle including planning, development and use activities, management of change activities, and the documentation of safety.	Functional Safety Summary Project Plans e.g. Project Management Plan, Electronics and Software Development Plan, Installation, Commissioning, and Training Plan, and Operation, Maintenance, and Decommissioning Plan, Management of Change Plan
II. Development and Use – Define the Safety Requirements	II.1 Define Scope	Define the conceptual equipment design, component and equipment interfaces and the overall functionality of the PPE.	Updated Functional Safety Summary Updated Project Plans Functional Safety Requirements Specification Product Description
	II.2 Hazard and Risk Analysis	Identify hazards, analyze event sequences leading to hazardous events and determine risks associated with these events.	
	II.3 Specify Requirements	Identify safety functions and specify design and performance requirements associated with these safety functions.	
	II.4 Design and Manufacture	Design and manufacture the equipment to meet the required specifications.	Updated Functional Safety Summary Updated Project Plans Updated Functional Safety Requirements Specification Updated Product Description

Phase	Activity	Objectives	FSF Documentation
	II.5 Review, Test, and Verify	Conduct design for safety reviews, test and verification activities for electronics and software components, subsystems, and systems.	Updated Functional Safety Summary Updated Project Plans Updated Functional Safety Requirements Specification Updated Product Description Review, testing, and verification activities and results
	II.6 Install, Commission, and Train	Install and commission the PPE properly and safely. Train the users and maintainers of the system.	Updated installation and commissioning plan Records of installation and commissioning activities and results Records of training activities and results e.g. schedules, topics covered, and qualification data
	II.7 Validate	Validate that the installation meets the equipment or systems requirements during commissioning and throughout operation and maintenance.	Updated project plans Updated project description Records of validation activities and results
II. Development and Use – Operation and Maintenance	II.8 Operate, Maintain, and Decommission	Properly operate and maintain the equipment or system for continuing functional safety.	Updated project plans Operation and maintenance manuals and records Records of decommissioning activities and results

Phase	Activity	Objectives	FSF Documentation
III. Prepare Safety Documentation		Prepare safety documentation throughout the functional safety life cycle.	See Rows I, II, and IV of this table
IV. Manage Change		Make all modifications in accordance with the management of change plan.	All updated project planning, development, use, operation, and maintenance documents important to functional safety demonstration Updated project description Configuration Identification Information History file Updated safety file Updated results of IFSA

Table 3 – Functional Safety Life Cycle Activities

Manufacturer participation in follow-up assessments depends on their organizational charter.

For example, a manufacturer of a heart rate sensor component sells the component to a systems integrator. The systems integrator uses the heart rate sensor along with other components to develop a standardized control subsystem that provides physiological measurement functions. The systems -integrator sells this control subsystem to emergency responder electronic garment manufacturers and to health care monitor manufacturers. Engineers at the electronic garment manufacturers add a remote communication subsystem to the control subsystem.

In this situation, the component and subsystem manufacturers are typically involved in the periodic follow-up assessments undertaken by the garment manufacturers when 1) the garment manufacturer requires it as part of their supplier assessment practices or 2) the follow-up assessment identifies a risk associated with the garment manufacturer's use of the component or subsystem. In the latter case, the extent of the component or subsystem manufacturer involvement in the follow-up assessment, if any, depends on the garment manufacturer's functional safety practices.

The Functional Safety Best Practices recommendations include a recommendation that the manufacturer have oversight activities addressing the safety and performance of components and subsystems. Some manufacturers choose to address this recommendation by using recognized components.

1.3. Types of Independent Functional Safety Assessments (IFSAs)

The number and types of the IFSAs depends on the equipment's functional scope, complexity and risk reduction objectives, prior experience of the project staff, and corporate management practices.

Four types of IFSAs are recommended as summarized below:

FSF conducted after the planning and safety requirements specification (Phase II-3 of the FSLC).

- Design IFSA—an IFSA of the design conducted after the design verification phase (Phase II-5 of the FSLC)
- Validation IFSA—an IFSA conducted after all validation activities are concluded and the PPE is ready to become operational (Phase II-7 of the FSLC)
- Periodic Follow-up IFSA—an IFSA conducted periodically after the PPE has been released and is in use (Phase II-8 of the FSLC)

When a manufacturer does not participate in a recommended FSLC activity, the activity may be omitted from the defined FSLC. Depending on the activity, this may result in foregoing the IFSA related to that activity.

> *Example 1:* A manufacturer of stand-alone or handheld equipment may not be involved with commissioning, field maintenance, or decommissioning activities. Therefore, commissioning, field maintenance, or decommissioning activities would not be a part of their FSLC. Additionally, the manufacturer would not be responsible for conducting follow-up IFSAs.
>
> *Example 2:* A manufacturer of an equipment component may not be involved in design and integration of equipment that uses their component. Therefore, the equipment component manufacturer would not be responsible for the validation activity of the FSLC. Additionally, the component manufacturer would not be responsible for conducting validation IFSAs.

Figure 4 - Example of IFSA Schedule for Electronic Firefighter Garment shows a hypothetical project schedule for developing a new firefighter instrumented sensor garment worn under turnout gear.

---

[4] The preliminary IFSA is optional though recommended for new technology PPES projects, project teams, and for higher risk life safety applications.

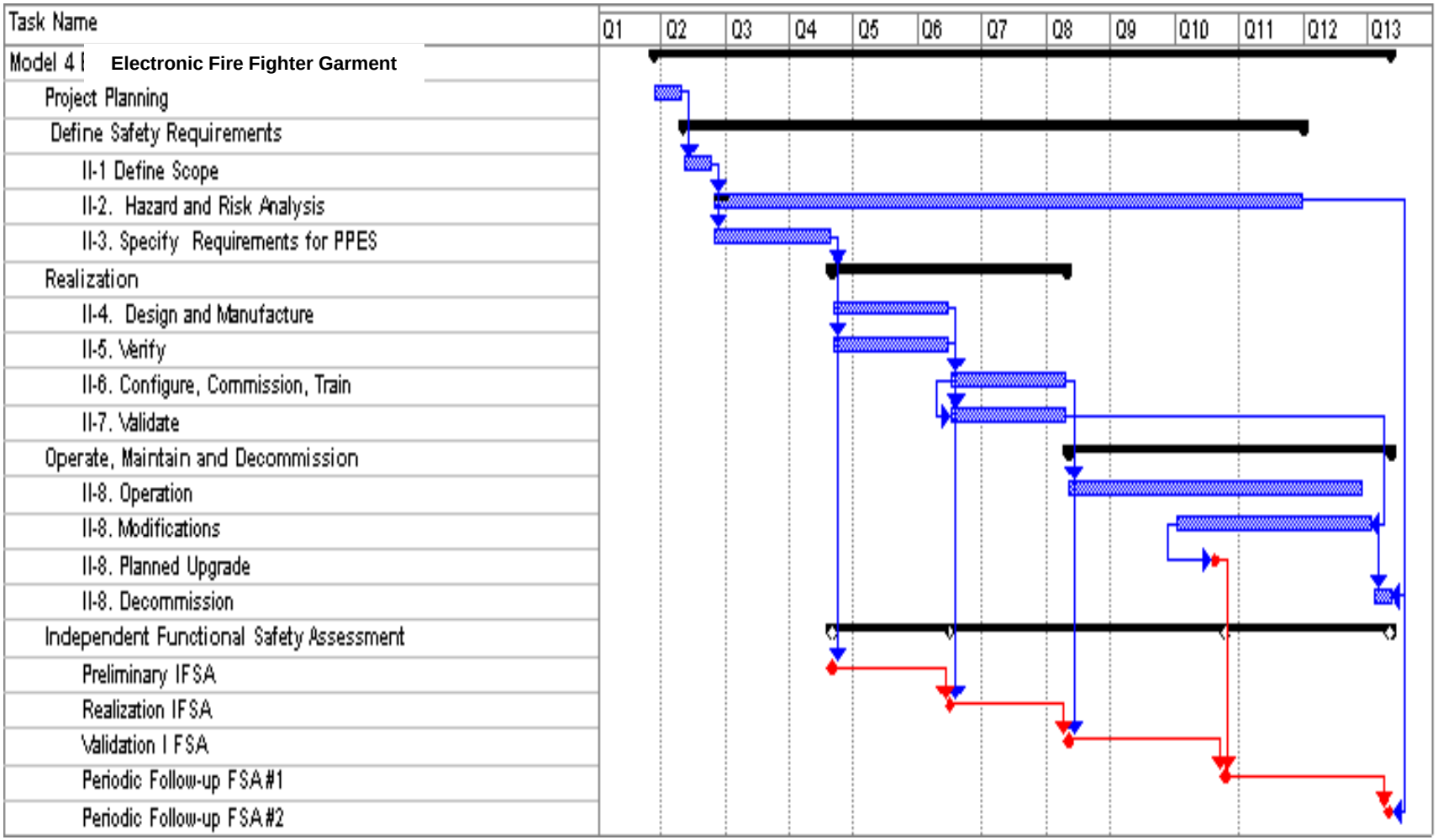
recommendations provided in Part 2. The type and frequency of IFSAs are planned at the start of the project. Because the product is new, uses advanced technology, is intended to be worn in both severe exposure that is potentially hazardous and non-hazardous fire environments, the company safety policy requires at a minimum:

- a Preliminary IFSA
- a Design IFSA
- a Validation IFSA
- one Periodic Followup IFSA per year.

The Preliminary IFSA will occur once all project plans are in place and the safety requirements specification is at a point where design could begin. The Design IFSA is planned for when the design is complete and there is a working prototype. The Validation IFSA is planned for the end of installation/commissioning and validation. Two Periodic Followup IFSAs are planned—one associated with a planned product upgrade and one associated with decommissioning the product.

Periodic Follow-ups are scheduled as needed to address risks associated with product changes and when the product is decommissioned. An annual follow-up is usually a minimum requirement even if no product changes have been made. In this situation, the follow-up assessment addresses the on-going implementation of the best practices.

Figure 4 - Example of IFSA Schedule for Electronic Firefighter Garment



The IFSA approach has common characteristics with the ISO 9001 Quality Management Systems, the Six Sigma, and the Software Process Assessment approaches as summarized in Section 1.6.

1.4. Degree of Independence of IFSAs

Table 1 recommends selecting the degree of independence of the assessor based on the risk reduction requirements for the intended use of the PPE. Regulatory requirements and company safety policy may require a greater degree of independence. Criteria useful in selecting the degree of independence include:

- Number of functions provided
- Complexity of the solution (e.g. number and criticality of functions provided)
- Prior use of the design
- Use of advanced technology
- User concerns
- Service history with similar devices

Degree of Independence	Risk Reduction Factor 1 (RRF1) *Severe Exposure Fire Environment and Potential for Fire*	Risk Reduction Factor 2 (RRF 2) *Hazardous or Potentially Hazardous Non-Fire Environment*	Risk Reduction Factor 3 (RRF3) *Non-hazardous, Non-fire environment*
Independent Person	Not Recommended	Not Recommended	Recommended
Independent Department	Not Recommended	Recommended	Highly Recommended
Independent Organization	Highly Recommended	Highly Recommended	---

Table 4 - Recommended Degree of Independence of the Assessor

1.5. IFSAs for Fielded PPE

When PPE are already in use in the field, the proven-in-use concept may justify a reduced scope and independence of assessments. Claiming proven-in-use requires supporting evidence of a safe service history that includes:

- Incidents and severity
- Problem reports of in-service problems that may have not resulted in an incident
- Exposure data
- Environmental conditions
- Random hardware failure data
- Systematic error data
- Usage
- Maintenance frequencies and rigor

- Management of change data

More detail on proven-in-use may be found in IEC 61508 Standard[5]. When making proven-in-use decisions for product repairs and upgrades it becomes important to avoid a rapid decision based on an already demonstrated safe service history. Given the manner in which electronics and software fail, a seemingly small change may result in a potential safety problem. To meet risk reduction requirements when upgrading or expanding existing product features, the PPE manufacturer selects a greater scope, frequency, and degree of independence of IFSA. The outcome of updating the hazard and risk analysis provides the basis for the decision rather than proven-in-use.

1.6. Relationship of IFSAs to Other Standards

1.6.1. ISO 9000:2000

Having quality management practices in place provides a baseline set of practices which support the achievement of quality products. Functional safety practices will overlap with quality management practices. IFSAs may be considered as part of ISO registration auditing requirements. However, the converse is not true ISO registration audits typically do not address all product safety practices.

1.6.2. Six Sigma

The six sigma approach involves designing to meet customer needs. For PPE, a customer need is to have equipment that reduces life safety risk. Thus practices that are six-sigma compliant will overlap with functional safety practices. For example, a practice that involves review of the equipment safety requirements specification with the user would be both six sigma compliant and functional-safety compliant.

[5] See IEC 61508 for more specifics on Proven-In-Use Criteria, Table 3 for where to obtain reference document.

2.0. PLANNING AN IFSA

2.1. Objectives

2.1.1. To create a plan for effective IFSAs consistent with regulatory requirements, the company safety policy, and NIOSH best practices recommendations

2.2. Recommendations

2.2.1. Establish the IFSA plan through a collaborative effort among the equipment manufacturer, integrator, maintainer, and user.

2.2.2. Accommodate incremental implementation of IFSAs carried out in parallel with the PPE development and use activities.

2.2.3. Determine the scope, timing, and frequency of conducting each of the four types of IFSAs.

- Preliminary IFSA
- Design IFSA
- Validation IFSA
- Periodic follow-up IFSA

2.2.4. Select the degree of independence of the assessor using Table 1.

2.2.5. Determine the extent that proven-in-use[6] service history will be used.

3.0. PRELIMINARY IFSAs

3.1. Objectives

3.1.1. Assess the safety policy, project plans, and preliminary FSF to reduce the potential for safety problems

[6] See IEC 61508 for more specifics on proven-in-use criteria.

3.1.2. Assess the selection of RRF requirements for an inappropriate RRF objective

3.1.3. Assess the education, training, experience and qualifications of involved persons in relation to their specific activities to minimize the potential for safety problems

3.2. Recommendations

3.2.1. Consider the contents of the FSF as the primary input with interviews of involved persons as a complement to obtaining information.

3.2.2. Consider assessing the following:

- Project plans for coverage of recommended FSLC practices and adherence to safety policy
- Declared RRF with respect to the planned PPE safety functions
- Contents of the FSF and documented procedures for further populating it. *(See Part 9 for an example assessment checklist).*
- Results of hazard and risk analyses for coverage and prioritization of identified hazards and sufficiency of the selected RRF
- Traceability of the safety requirements specification to the hazard and risk analysis
- Qualifications of the project team for engineering experience appropriate to the application, the technology, and the RRF

3.2.3. Document the results of the Preliminary IFSA in a report containing the following information:

- A description of the assessment's scope
- A very brief description of the system and its intended application
- Identification of the assessor(s) and their associated affiliations
- A listing of all documentation examined
- A listing of all reference material used for the assessment
- An itemized listing of assessment questions
- Outcome of each item assessed (e.g. *accepted, not applicable, action request)*

- All assessor notes associated with each item assessed *(e.g. rationale for why not applicable is checked)*
- Conduct the Preliminary IFSA on a per-PPE component basis for a given application.

4.0. DESIGN IFSA

4.1. Objectives

4.1.1. Assess that the PPE "as designed and verified" has been constructed to maintain the specified RRF requirement

4.2. Recommendations

4.2.1. Consider the contents of the FSF as the primary input with interviews of involved persons as a complement to obtaining information.

4.2.2. Consider assessing the following for completeness:

- Contents of the FSF (See Appendix A for an example assessment checklist).
- Specified RRF(s) for the PPE function(s)
- Design verification procedures and records
- Management of change procedures and records
- Traceability of:
- safety requirements specification to the hazard and risk analysis results
- design to the safety requirements specification
- design verification results to the design, the safety requirements specification, and to the hazard and risk analysis results

4.2.3. Document the results of the Design IFSA in a report containing the following information:

- A description of the assessment's scope
- An updated description of the system, its design, and intended application

- Identification of the assessor(s) and their associated affiliations
- A listing of all documentation examined
- A listing of all reference material used for the assessment
- An itemized listing of assessment questions
- Outcome of each item assessed (e.g. *accepted, not applicable, action request)*
- All assessor notes associated with each item assessed *(e.g. rationale for why not applicable is checked)*

4.2.4. Conduct the Design IFSA on a per-PPE basis for a given application.

5.0. VALIDATION IFSA

5.1. Objectives

5.1.1. Assess that the PPE "as designed and validated" has been constructed to maintain the specified RRF requirement over the life cycle of the PPE..

5.2. Recommendations

5.2.1. Consider the contents of the FSF as the primary input with interviews of involved persons as a complement to obtaining information.

5.2.2. Consider assessing the following for completeness:

- Contents of the FSF *(See Appendix A for an example assessment checklist).*
- Specified RRF(s) for the PPE function(s)
- Validation procedures and records
- Management of change procedures and records
- Traceability of:
    - safety requirements to the hazard and risk analysis results
    - validation tests to the safety requirements specification

5.2.3. Document the results of the Validation IFSA in a report containing the following information:

- A description of the assessment's scope
- An updated description of the system, its design, and intended application
- Identification of the assessor(s) and their associated affiliations

- A listing of all documentation examined
- A listing of all reference material used for the assessment
- An itemized listing of assessment questions
- Outcome of each item assessed (e.g. *accepted, not applicable, action request)*
- All assessor notes associated with each item assessed *(e.g. rationale for why not applicable is checked)*

6.0. Periodic Follow-up IFSA

6.1. Objectives

6.1.1. Assess that the PPE "as operated, maintained, and decommissioned" maintains the specified RRF requirement.

6.2. Recommendations

6.2.1. Consider the contents of the FSF as the primary input with interviews of involved persons as a complement to obtaining information.

6.2.2. Consider assessing the following for completeness:

- Contents of the FSF (See Appendix A for an example assessment checklist).
- Specified RRF(s) for the PPE function(s)
- All FSLC procedures and records as appropriate
- Traceability of:
  - safety requirements to the hazard and risk analysis results
  - validation tests to the safety requirements specification

6.2.3. Document the results of the Follow-Up IFSA in a report containing the following information:

- A description of the assessment's scope
- An updated description of the system, its design, and intended application
- Identification of the assessor(s) and their associated affiliations
- A listing of all documentation examined

- A listing of all reference material used for the assessment
- An itemized listing of assessment questions
- Outcome of each item assessed (e.g. *accepted, not applicable, action request)*
- All assessor notes associated with each item assessed *(e.g. rationale for why not applicable is checked)*

7.0. SUMMARY

The guidance provides best practices recommendations for the number and types of IFSAs. Conducting IFSAs contributes to reducing the risk of field failures of equipment. They may be conducted by first, second, or third parties depending on the risk reduction objectives for the PPE. IFSAs audit the functional safety life cycle practices implemented for a PPE. They are easily integrated with existing practices that are ISO 9001 and/or six-sigma compliant.

8.0. 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

ABBREVIATION	DEFINITION
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

9.0. 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 emergency 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 emergency 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 emergency responders and between emergency 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 emergency 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.