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

Part 4: The Functional Safety File (FSF)

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.

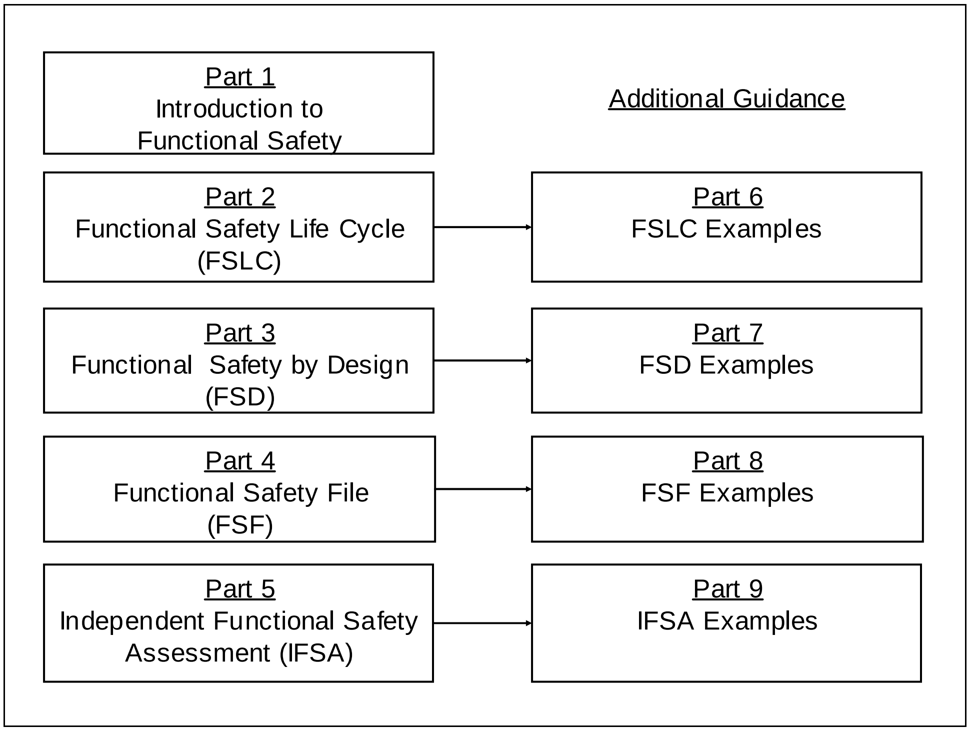
Part 1
Introduction to Functional Safety
Additional Guidance
Part 2
Functional Safety Life Cycle (FSLC)
Part 6
FSLC Examples
Part 3
Functional Safety by Design (FSD)
Part 7
FSD Examples
Part 4
Functional Safety File (FSF)
Part 8
FSF Examples
Part 5
Independent Functional Safety Assessment (IFSA)
Part 9
IFSA Examples

Figure 1 - The functional safety report series.

Report Scopes

Part 1: Introduction to Functional Safety

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

Part 2: The Functional Safety Life Cycle (FSLC)

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

Part 3: Functional Safety by Design (FSD)

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

Part 4: Functional Safety File (FSF)

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

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

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

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

Part 5: Independent Functional Safety Assessment (IFSA)

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

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

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

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

- Part 6 – Additional Guidance: Functional Safety Life Cycle Examples are used to develop the Scope of the Project Plan. The scope guides Project Functional Safety by Design (FSD) Compliance and Project Documentation.
- Part 7 – Additional Guidance: Functional Safety by Design Examples drives Project Design for Safety Compliance, which then becomes part of the Project Documentation.
- Part 8 – Additional Guidance: Functional Safety File Examples help to complete the Project Documentation, to enable a third party assessment.

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

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

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

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

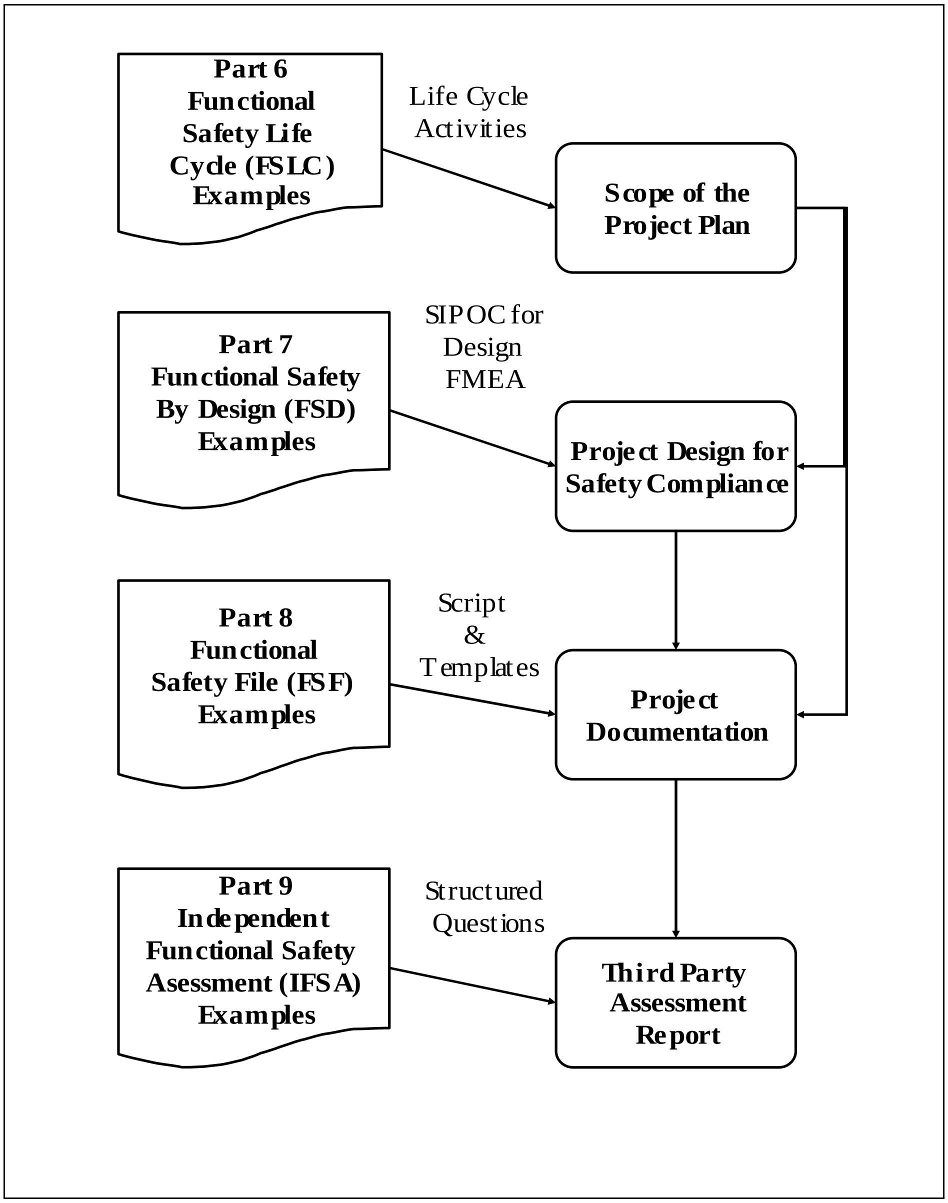

Figure 2 - Relationships among Parts 6, 7, 8, and 9

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

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

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

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

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

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

Intended Scope of Application

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

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

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

Intended Users

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

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

Relevance of the Guidelines

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

Reference Guidelines and Standards

Mining industry guidelines prepared by NIOSH, MSHA and the mining industry manufacturers and entitled *Programmable Electronic Mining Systems: Best Practices Recommendations (in Nine Parts)* serves as a basis for these guidelines. Table 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.

The report, Functional Safety File (FSF), is the fourth document in a nine-part series of recommendations addressing the functional safety of advanced personal protective equipment (PPE) for emergency responders. The FSF provides the documented evidence of following *Part 2 - The Functional Safety Life Cycle Safety* and *Part 3 - Functional Safety by Design*.

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 4 details best practices for safety documentation. The report also recommends the practice of retaining safety documentation in a centralized, secure location or a Functional Safety File (FSF). The FSF details the degree of safety, gives the supporting evidence, and identifies limitations for the system and its operation. In essence, it is a “proof of safety” that the system and its operation meet the appropriate safety requirements for the intended application.

1.2. What is a Functional Safety File or FSF?

The FSF provides the documented evidence of following Part 2 Life Cycle Safety and Part 3 Safety by Design. Establishing the FSF starts with the beginning of the safety life cycle or when system modification commences, is maintained during the full life cycle of the system, and provides administrative support for the safety program of the full system. Although an FSF assists in proving functional safety to an external reviewer, it also provides administrative and technical data that is useful to product managers, developers, and safety engineers.The Functional Safety File (FSF) consists of documentation that identifies and addresses safety issues. This written documentation is constructed as the activities associated with each development life cycle phase are performed. The safety file is an organized, traceable set of documentation that demonstrates the degree of safety, gives the supporting evidence, and identifies limitations for the system and its operation. In essence, it is a “proof of safety” that the system and its operation meet the appropriate safety requirements for the intended application.

A good definition of a “safety file” is given by Bishop and Bloomfield.[4]

> *A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.*

[4] Bishop P, Bloomfield R [1998]. A methodology for safety case development. In: Anderson T, ed. Proceedings of the Sixth Safety-Critical Systems Symposium (Birmingham, U.K.). New York: Springer-Verlag, pp. 194-203.

“Technical file”, “safety case”, “safety argument”, “safety assessment report”, or “safety justification” are other names in use for a safety file.

The safety file specifies safety claims, summarizes both quantitative and qualitative supporting evidence, and communicates any limitations on installation and operation. It includes written documentation and supporting engineering data that demonstrate—

- Satisfaction of specific safety requirements of the system
- Justification of engineering and management approaches to safety issues
- Conformance to recognized standards

The safety file is the summary of the rationale as to why the system is safe to deploy. The safety file evolves to summarize, before deployment of the system, the evidence for the conclusion that the system is safe to deploy. Early versions of the safety file record planned activities, as well as those completed, and justify increasing confidence in the safety of the system. Ideally, a preliminary safety file should be developed simultaneously with the design process, thereby keeping the design within a reasonable safety envelope. By integrating the safety file development into the design process, any unsuitable designs and associated costs are thereby avoided or at least minimized.

Although an FSF assists in demonstrating functional safety to an external reviewer, it also provides administrative and technical data that is useful to product managers, developers, and safety engineers. It contains a reference library of safety data about the product using existing product safety documentation throughout the Functional Safety Life Cycle (FSLC). The FSF is an organized collection of safety-related documents that provide a demonstrable, convincing, and valid suite of arguments that the system is adequately safe for a given life safety application. The safety file can be held on paper or electronic media.

Lastly, the FSF conveys the confidence that designers and purchasers have in the safety of the system. It provides evidence that, although an event may occur that was not foreseen or considered when the system was designed, all reasonably determinable safety-related concerns were considered and dealt with in accordance with best practices. This may provide an important legal defense.

1.3. Creating and Populating the Functional Safety File (FSF)

In creating the safety file, consider covering all PPE components and the interrelationships, and providing a system level view. It is important to:

- Specify the types of documents that are necessary for a safety file
- Specify how those documents relate to the other components of the PPE
- Specify the process by which the FSF is developed

Preparation of safety documentation starts during planning of a new product or a product modification. Thus, it is important to create the FSF during planning by defining the structure and content of the FSF. Consider starting the FSF at project inception by constructing a preliminary FSF. Then, as the design becomes developed, incrementally modify the FSF to evolve simultaneously with the design before the PPE is used in the field. By including supporting information from other sources, such as prior field experience of the PPE portions from an existing safety file might be usable for inclusion or reference.

While the FSF is directed to the particular purpose of demonstrating functional safety achievement to an external reviewer, it is developed using existing product engineering information. The FSF draws from the documents produced during the management, planning, development and use, and maintenance activities. It is built incrementally by populating it throughout the entire Functional Safety Life Cycle (FSLC) for the product as shown in Figure 3.

Depending on the complexity of the system, the developer may decide to organize the safety file into several subsystem safety files, which in turn can be used in support of the top-level (main) safety file for the PPE as shown in Figure 4.[5]

Traceability is an important feature of the safety file. If the FSLC is followed and the safety file is appropriately populated with deliverables from each phase, one will be able to select a hazard and trace from the hazard/risk analyses, through specifications and safety function allocation, to design, verification, and implementation, and finally, see at

[5] The Functional Safety Life Cycle (FSLC) was described in Part 2 of this nine-part series

validation that the selected hazard was addressed, designed for, and resolved in an acceptable manner. When the concept of traceability is applied throughout a project, the cohesiveness of the safety file is greatly improved.

1.4. Benefits of having a Functional Safety File (FSF)

Without written safety documentation and supporting safety engineering data, it is extremely difficult and, in some cases, impossible to verify and validate that a PPE is adequately safe for its intended application. In some cases, a lack of data may make it difficult to investigate an incident adequately to determine if root causes and contributing factors were attributable to the electronics and software.

Thus, there are several important benefits in creating a safety file as follows:

- Reduces the overall system life cycle cost by considering safety problems at the beginning of the design
- Documents evidence of safety and rationale for safety approaches and decisions. This is important for subsequent changes so that changes do not undo or degrade the original degree of safety.
- Supports the equipment manufacturer in any accident investigations, liability, and/or litigation issues by demonstrating that the vendor has in fact done everything reasonably possible to make the system safe.
- Provides evidence of on-going compliance with other regulatory and/or guidance documents.
- Aids in future design of related systems. Most of the work will have already been accomplished for any additional modifications and/or enhancements to the system.

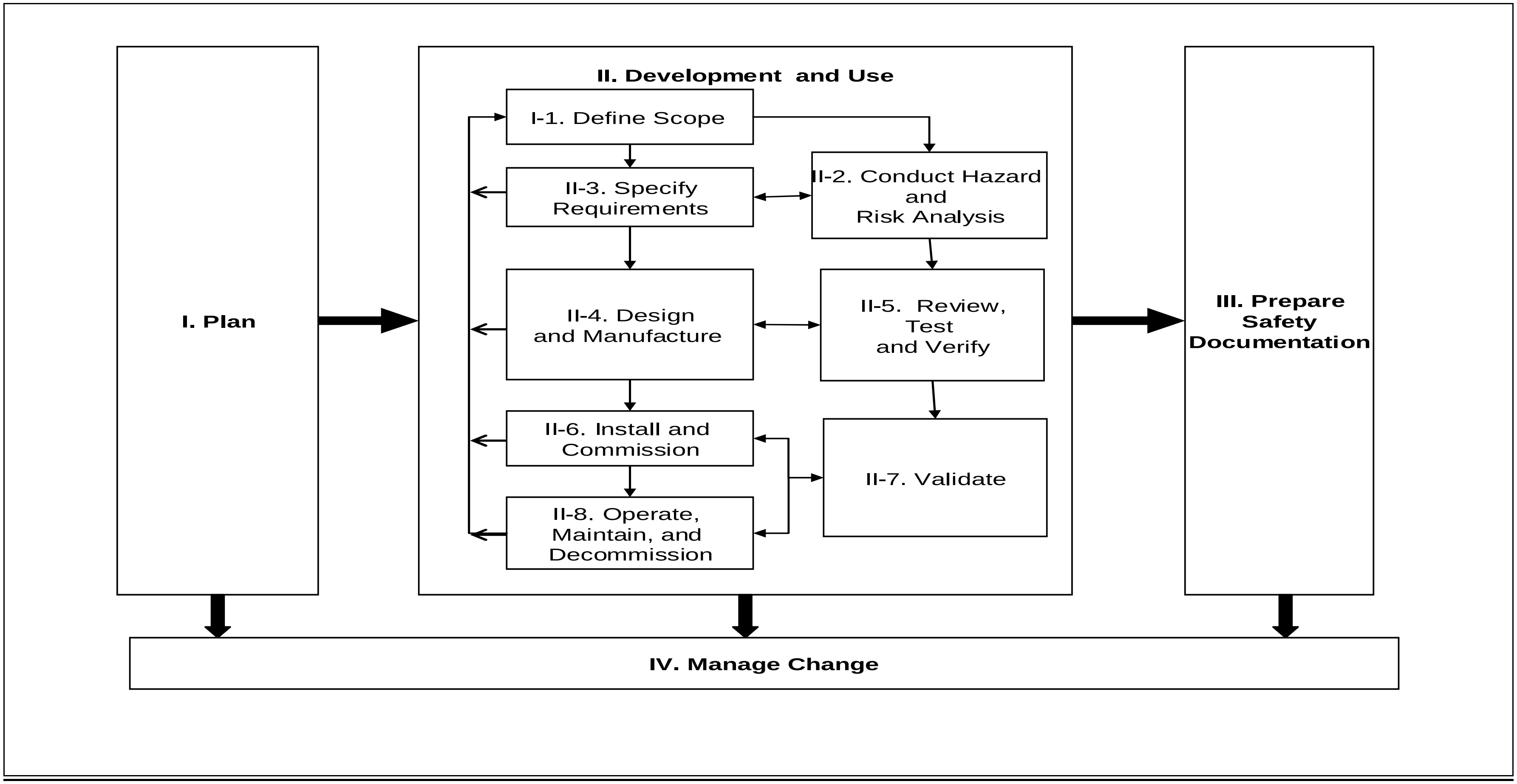
I. Plan
II. Development and Use
I-1. Define Scope
II-2. Conduct Hazard and Risk Analysis
II-3. Specify Requirements
II-4. Design and Manufacture
II-5. Review, Test and Verify
II-6. Install and Commission
II-7. Validate
II-8. Operate, Maintain, and Decommission
III. Prepare Safety Documentation
IV. Manage Change

Figure 3 – The Functional Safety Life Cycle.

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 – Objectives by FSLC Phase and Activity

- Captures the engineering process capability needed for staying in business in the future as the demand for more complex, more highly integrated automated systems increases.

2.0. STRUCTURE AND FORMAT FOR THE FSF

2.1. Objectives

2.1.1. Establish a structure that is easy to maintain and facilitates independent functional safety assessments (IFSAs).

2.2. Recommendations

2.2.1. Develop the structure and format of the FSF to be consistent with organizational safety practices. An example Functional Safety File Structure is shown in Figure 4.

2.2.2. Consider the use of hierarchy in organizing the FSF, e.g., there may be individual functional safety files for subsystems and components with a top-level FSF providing the summary for the complete PPE as shown in Figure .

NOTE: Such an organization may be practical when PPE are assembled from components and subsystems acquired from sources outside of the project. The supplier provides safety file documentation when they provide the subsystems and components.

2.2.3. Organize the FSF to facilitate traceability of safety functions across subsystems and components.

NOTE: Traceability is important to reaching closure for the identified hazards. Populating the FSF with deliverables from each phase permits selecting hazards and tracing them from the hazard/risk analyses, through specifications and safety function allocation, to design, verification[6]

2.2.4. Provide a revision history log for the FSF.

[6] See System Safety Program Plan, Notes 18 and 34.

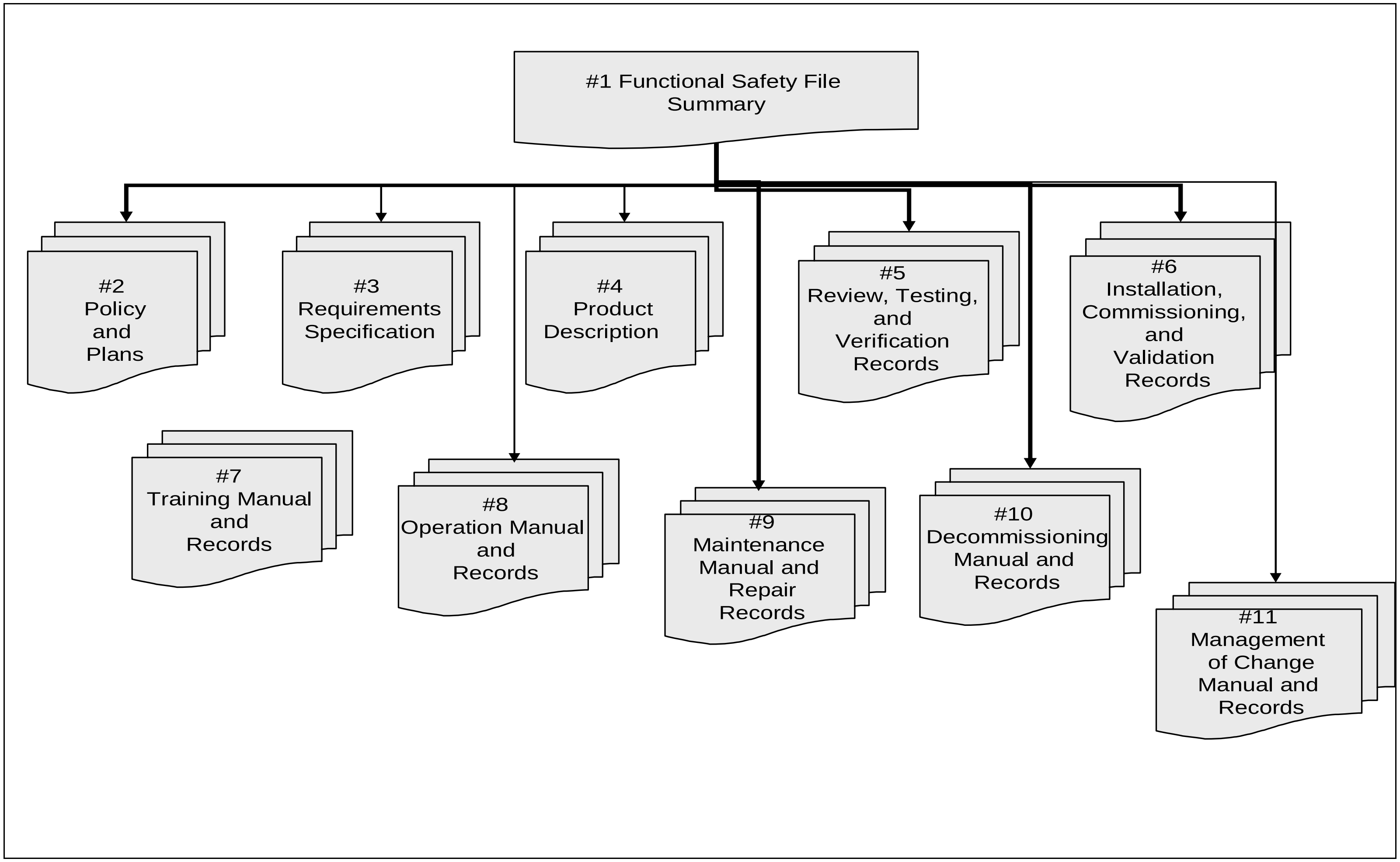
#1 Functional Safety File Summary
#2 Policy and Plans
#3 Requirements Specification
#4 Product Description
#5 Review, Testing, and Verification Records
#6 Installation, Commissioning, and Validation Records
#7 Training Manual and Records
#8 Operation Manual and Records
#9 Maintenance Manual and Repair Records
#10 Decommissioning Manual and Records
#11 Management of Change Manual and Records

Figure 4 - Example structure of a Functional Safety File

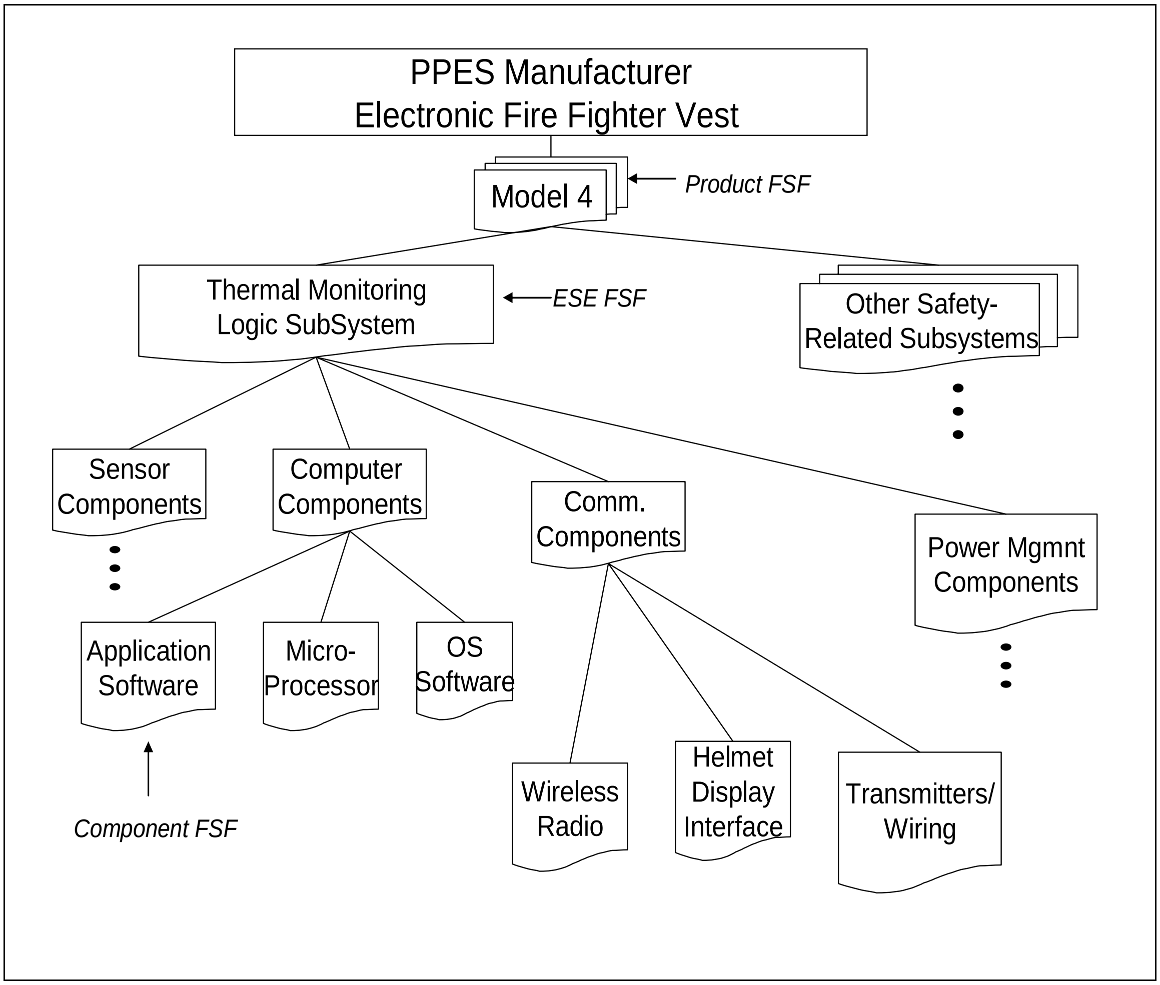

Figure 5 - Organization of FSFs for electronic fire fighter vest.

NOTE: An advantage to the organization shown is that the subsystem and component safety files may be reused. For example, if the PPE manufacturer decides to build a Model 5, which uses the thermal monitoring logic subsystem, then the PPE manufacturer could reuse the logic subsystem FSF. This may require some updating if the logic subsystem has changed from one model to the next..

3.0. RECOMMENDED CONTENTS OF THE FSF

3.1. Objectives

3.1.1. Specify the written safety documentation and supporting engineering data recommended for inclusion in the FSF.

3.1.2. Provide records of activities and results that accurately reflect compliance with the safety plans and demonstrate that the safety requirements are met.

3.1.3. Demonstrate the following:

- Satisfaction of the safety claims of the PPE
- Justification of engineering and management approaches to safety issues
- Conformance to recognized standards

3.2. Recommendations

3.2.1. Functional Safety Summary (Figure 4, #1)

3.2.1.1. Provide a Functional Safety Summary that affirms the completeness and accuracy of the FSF file and the level of safety demonstrated for the system including:

- Aim, purpose and structure of the FSF
- Identification and scope of PPE and components
- Purpose and intended use of PPE
- Safety claims for the PPE
- A brief description of the system and its components including name, type, model number, and electronics/software versions
- A description of the FSLC and the techniques and tools used
- A description of any other system(s) that will be tested or operated in combination with the PPE

- Conditions of acceptability, including operating ranges and any restrictions/limitations on use
- Standards being attested to
- Summary of independent Functional Safety Activities conducted and results
- A signed statement that affirms that:
  - The FSF accurately reflects the engineering of the system,
  - All identified hazards have been eliminated or their associated risks controlled to levels specified as acceptable,
  - The system is ready to test or operate,
  - Documents all identified conditions of acceptability,
  - Identifies compliance with standards, if any.

3.2.2. Policy and Plans (Figure 4, #2)

3.2.2.1. Provide a summary of the safety policy and strategy which documents:

- Adherence to governing regulations, recognized standards, and corporate policy
- References to accident data from OSHA, NIOSH, NFPA, International Association of Fire Fighters (IAFF) and other sources to avoid repeat occurrences
- References to lessons learned from prior projects
- FSLC Best Practices including practices for defining the minimum qualifications criteria required for staff, including subcontractors, to perform specific project roles related to functional safety

NOTE : Whether there is one or multiple safety plans will depend on the given application, organization, and other factors, including the:

- Organization’s management structure,
- Organization’s technical processes, skills, and resources,
- Size of system,
- Previous experience for the system and application,

- Nature of the hazards
- Consequences in the event of failure
- Degree of complexity
- Degree of design novelty
- Risk Reduction requirements

3.2.2.2 Provide a Project Management Plan which includes:

- Project scope, schedule, and resources
- The risk management approach and activities (i.e., paradigms followed, such as fail-safe design, selection of design and programming languages, controlled and encouraged practices, use of hazard log) is to be identified
- A statement of how relationships and lines of communication are set up between organizational functions that may impact or have responsibility for tasks with system implications
- A qualifications summary of personnel involved in the development of software, including a statement of the minimum qualifications criteria required of members of the electronics and software development teams
- A statement of the level of authority developers have to implement the tasks necessary to complete the project should be developed
- A description of the relationship between safety and other functional elements of the system should be developed
- A description of the mechanisms by which concerns are or can be brought to light by project personnel should be developed

3.2.2.3. Provide an Electronics and Software Development Plan which provides a clear statement of the documents produced and the activities undertaken as part of the development life cycle and details:

- A statement of the approach and activities used for electronics and software development including metrics to be collected and applicable standards
- Requirements specification activities and tools including hazard and risk analysis and safety requirements allocation

- A description of how the functional safety requirements will be met including the design for safety principles to be followed and the design methods and tools to be used
- A description of how the functional safety requirements will be verified and validated including:
  - When analysis, testing, or assessment activities take place
  - Who conducts the analysis testing or assessment activities
  - Activities and tests that confirm the safety requirements including confirmation of operating modes and transitions such as, startup, shutdown, reset, manual, remote, semiautomatic, automatic, monitor, standby, emergency, and stuck/jammed (abnormal)

NOTE: This is not a comprehensive listing. A given system might have a subset of the listed modes and/or additional modes.

- Pass and fail criteria
- Policies and procedures for addressing functions that fail the criteria established for the safety requirements

NOTE: Given the increasing dependence on software to achieve functional safety, it is important to consider having a software development and maintenance plan. The software development and maintenance plan typically includes a statement of requirements, the approach to the software development, including design rationale, metrics collected, applicable standards, how changes will be handled, and the engineering methods and techniques employed.[7]

3.2.2.4. Provide an Installation, Commissioning, and Training Plan that addresses how to install and commission the PPE and how to train the operator and maintainer which includes the following:

- Possible hazards during installation and commissioning
- Safety precautions during installation and commissioning
- Installation, commissioning, and training procedures,
- Integration sequences

[7] Watts S. Humphrey. Managing the Software Process. ISBN 0-201-18095-2. New York: Addison Wesley Publishing Company, 1990. The SEI Series in Software Engineering.

- Criteria for declaring installation, commissioning, and training complete

3.2.2.5. Provide an Operation, Maintenance, and Decommissioning Plan that address how to operate, maintain, and decommission the PPE system to maintain functional safety by identifying:

- Normal and abnormal operation activities
- Preventative maintenance activities and schedules
- Repair activities
- Diagnostic activities
- Procedures to prevent an unsafe state during operation and maintenance
- Circumstances and procedures for bypassing or overriding safety functions or interlocks
- Circumstances and procedures for restoring and verifying safety functions or interlocks after they have been bypassed or overridden

3.2.2.6. Provide a Management of Change Plan (MOCP) that describes how changes to the electronics and software and interfaces (i.e. human, electrical, mechanical, and other software and electronics) are identified, analyzed, controlled and tracked to ensure that safety is not adversely impacted including:

- Documentation guidelines for describing the proposed change, the reasons for the change, and the impact on safety
- Methods to identify, analyze, verify, validate, and track the change
- Required review and authorization process before installing the change

NOTE: The adjustment and selection of adjustable parameter values, within the allowable ranges defined in the system requirements, is not considered a modification subject to an MOCP. However, the final values of adjustable parameters must be documented. The selection of any parameter value that is not within the allowable values or ranges as defined in the system requirements is considered a change and is subject to the MOCP.

3.2.3. Functional Safety Requirements Specification (Figure 4, #3)

3.2.4. Provide a Functional Safety Requirements Specification for the electronics and software, which includes the following information:

- List of hazards
- Mapping of each hazard to a safety function
- Clear description of each safety function
- Default and risks addressed states of each safety function
- Constraints associated with each safety function
- Event or combinations of events that trigger operating mode changes or safety functions
- Risk reduction factors for each safety function including references to historical or other data used to support the RRF claim
- Performance requirements and constraints (e.g., range, rate, response time) of each safety function
- The hazard and risk analysis procedures and criteria used to classify and rank hazards, plus any assumptions on which the procedure or criteria were based or derived, including the definition of acceptable risk
- A hazard log showing coverage of each hazard and traceability between hazard analysis, risk analysis, risk control, and verification results
- Interface requirements (i.e. human, electronics, software)
- Unique reference to the applicable version and configuration of the PPE
- Operating, diagnostic, testing, and maintenance requirements
- Training requirements

3.2.5. Product Description (Figure 4, #4)

3.2.5.1. Provide a Product Description of the PPE components and systems including:

- A list of safety functions provided by the electronics and software and how these functions relate to product functions
- A list of safety-critical components

- A description of the intended use including the use environment and the operating modes of the PPE (e.g. Sample operational scenarios and conditions of use)
- Specifications of the performance characteristics and limitations of the product and especially the operating limits, required backups, machine settings for the electronics and software
- Specifications of mechanical, electrical, and human interfaces, including identification of all limitations
- Design descriptions for the electronics and software including system architecture drawings, CAD diagrams, timing diagrams, data dictionaries, etc.
- Identification of the safety-related components including resident hardware component or storage location, hardware and software configuration items and, future proposed changes
- Communication protocols used
- References to design and code libraries and build files
- Unique reference to the applicable version and configuration of the PPE
- When using second or third party electronics, software and tools include the following:
  - The name and version/revision identifier of the electronics, software and tools,
  - Information about the electronics, software and tools providers,
  - A description of the purpose for which the electronics, software or tool is being used, and
  - A clear description of the function provided by the electronics, software or tool.

3.2.6. Review, Testing and Verification Records (Figure 4, #5)

3.2.6.1. Provide a summary of review, testing and verification activities and references to records addressing:

- Measures, techniques, and procedures used for confirming that safety functions conform with requirements
- A description of the facilities, equipment/tools used
- Dates
- Who carries out the verification, validation, and testing
- Objectives, procedures, pass/fail criteria each level of testing (e.g., unit, integration, black-box, regression, and system acceptance testing)
- Design and code review procedures and completed checklists
- Simulation procedures and tools
- Records of tests, pass/fail criteria and outcomes
- Accepted review meeting minutes
- Coverage of the safety requirements and of each function whose failure could involve a risk
- Data that fail-safe and fail-operational procedures bring the product to a risk addressed state
- Data that the scheduling requirements are met and safety functions meet the safety operating constraints specified
- Data verifying the integrity of the partitions between safety-related and non-safety-related functions
- Data validating that partition violations caused by occurrences such as data handling errors, control errors, timing errors, and misuse of resources do not occur
- Consistency in the data and control flows across interfaces
- Data showing that the electronics and software only perform intended functions and do not provide output that may compromise safety
- Results of failure mode and stress tests conducted to verify that software responds in accordance with the functional safety requirements
- Unique reference to the applicable version and configuration of the PPE

3.2.7. Installation, Commissioning, and Validation Records (Figure 4, #6)

3.2.7.1. Provide a summary of installation, commissioning, and validation activities and references to records addressing:

- Identification of validation tools and equipment used
- Calibration records for validation tools and equipment used
- Safety requirements version
- Safety function validated
- Mode validated
- Mode transition validated
- Unique reference to the applicable version and configuration of the PPE

3.2.8. Training Manual and Records (Figure 4, #7)

3.2.8.1 Provide a training manual that details the approach, topics and frequency of training.

3.2.8.2 Provide signed records identifying training content, dates, and participants.

NOTE: Training content and materials can be used from some safety life cycle activities. Examples include hazard and risk analysis results, risk controls, safety requirement specifications, and operation and maintenance manuals. The degree of rigor for training should increase as the RRF increases.

3.2.8.3. Provide a unique reference to the applicable versions and configurations of the PPE addressed by the training

3.2.9. Operation Manual and Records (Figure 4, #8)

3.2.9.1. Provide detailed instructions on how to use the equipment, including interfacing with the software and/or hardware.

3.2.9.2. Provide references to operation records.

3.2.9.3. Provide unique reference to the applicable version and configuration of the PPE.

3.2.10. Maintenance and Repair Manual and Records (Figure 4, #9)

3.2.10.1. Provide detailed instructions on how to maintain and repair the equipment, including interfacing with the software and/or hardware.

3.2.10.2. Provide references to maintenance records i.e. maintenance schedules, time, who conducted, results, problem reports.

3.2.10.3. Unique reference to the applicable version and configuration of the PPE.

3.2.11. Decommissioning Manual and Records (Figure 4, #10)

3.2.11.1. Provide a summary of decommissioning activities and references to records including:

- Identification of decommissioning tools and equipment used
- Calibration records for decommissioning tools and equipment used
- Unique reference to the applicable version and configuration of the PPE
- References to records for:
- Closing down to an inactive, safe state,
- Dismantling,
- Removal,
- Waste Processing, and
- Storage (mothballed for possible reuse).

3.2.12. Management of Change Manual and Records (Figure 4 #11)

3.2.12.1. Create a history file containing for all changes:

- Documentation describing the proposed change, the reasons for the change, and the impact on functional safety
- Records authorizing the change
- Identification and resolution of other documentation affected by the change (e.g. operations and maintenance procedures)
- Unique reference to the applicable version and configuration of the PPE
- A unique identifier to track the change

- Records of the review and authorization process conducted before implementing the change, and
- A method to verify modifications
- Details about the configuration identification scheme, responsibilities, and activities used to maintain and control baselines
- Records of receipt, storage, handling, and release of configurable items
- Description of the initiation, transmittal, review, disposition, implementation, and tracking of discrepancy reports (such as defects found) and change requests

NOTE: Software changes must be made by people as authorized by the manufacturer. They must be competent and knowledgeable about the entire system.

4.0. DEVELOP AND MAINTAIN THE SAFETY FILE

4.1. Objectives

4.1.1. Develop the safety file in parallel to the development, installation, operation, and maintenance of the PPE.

4.1.2. Provide a reference index that identifies all documentation in the safety file.

4.2. Recommendations

4.2.1. Identify procedures and tools for managing changes to the safety file as part of the management of change plan.

4.2.2. Establish a reference index that:

- Provides a succinct index, as well as a cross-referencing index, to all documents that form a part of the safety file
- Is retained by the component manufacturer, the system
- integrator, and the operating company
- Has a unique version number
- Identifies who is responsible for the contents and accuracy of the documentation

- Specifies when the referenced information was last updated and who updated it
- Identifies if FSF documentation are checked out, when and by whom

NOTE: Constructing a readily available FSF index provides for ease of identification of important FS documents.

5.0. SUMMARY

The PPE industry is using electronics and software technology to reduce life safety risks for emergency responders and victims. Electronics and software have failure modes that differ from mechanical systems or hard-wired electronic systems. The failure modes result from random phenomena (i.e., electromagnetic emissions; temperature extremes; humidity, moisture, and water exposure; heat and flame exposure; chemicals, dust, and debris, and extreme impacts). The failure modes may result as well from systematic (or logic) errors (i.e., inconsistent software algorithms and interfaces, coding errors, timing errors, latent errors, and failure of the PPE to perform any function at all. To achieve safety requires a system design approach addressing hardware, software, human behavior, and the operating environments over the equipment's life cycle.

The Functional Safety File guidance details best practice recommendations for use by manufacturers of PPE. Recommendations illustrate the contents of safety documentation and the practice of retaining safety documentation in a centralized, secure location or a Functional Safety File (FSF). The safety documentation details the degree of safety, gives the supporting evidence, and identifies limitations for the system and its operation. It is a record that the system and its operation meet the appropriate safety requirements for the intended application.

6.0. ABBREVIATIONS

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

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

7.0. GLOSSARY

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

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

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

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

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

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

Electronic Safety Equipment: Products that contain electronics embedded in or associated with the product for use by emergency services personnel that provides enhanced safety functions for emergency services personnel and victims during emergency incident operations (from NFPA 1800).

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

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

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

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

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

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

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

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

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

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

Hazard and risk analysis team: The group of 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 an 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.