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

Part 2 - The Functional Safety Life Cycle

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.

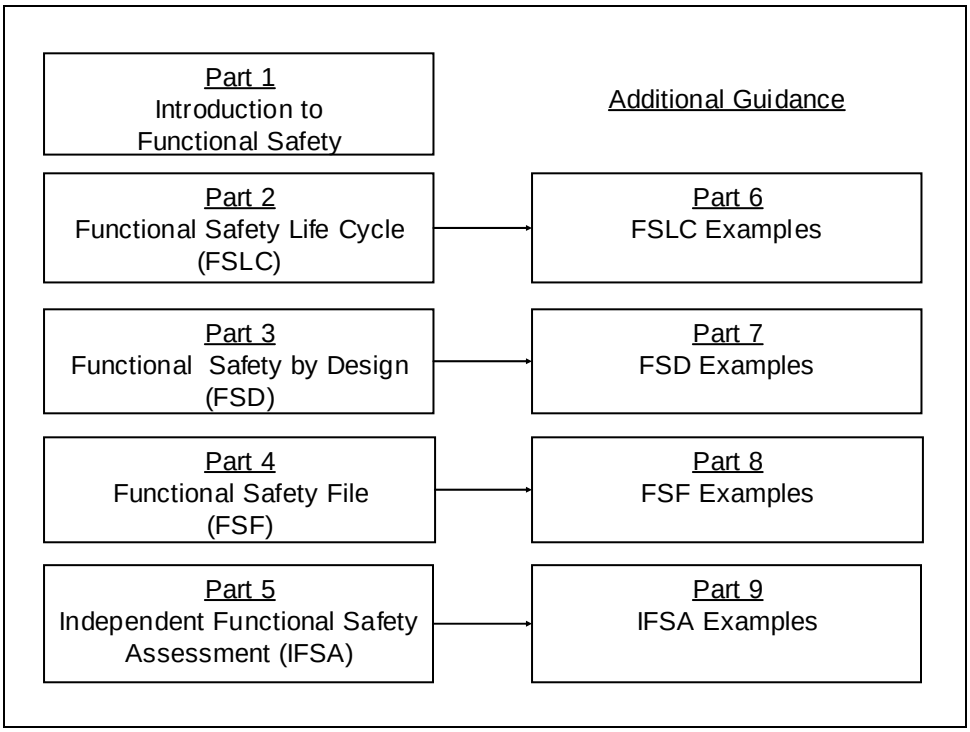

Figure 1 - The functional safety report series.

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 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

---

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.

the intended application.

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.

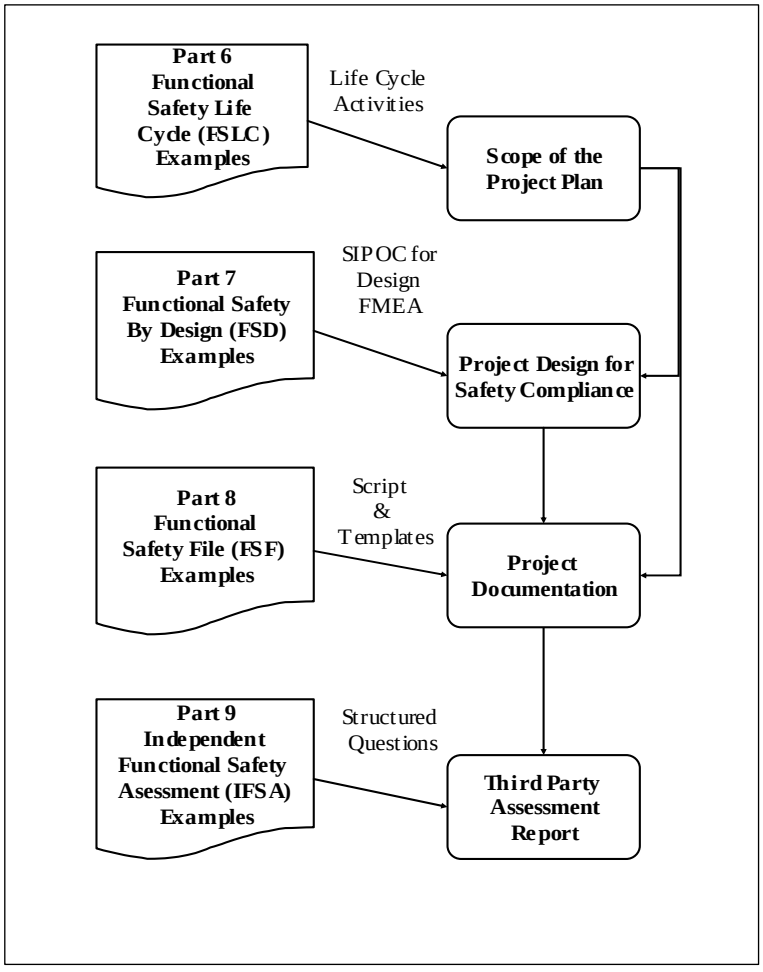

Figure 2 - Relationships among Parts 6, 7, 8, and 9

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 PPES. 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, Part 2 - Functional Safety Life Cycle is the second in a nine-part series of recommendations addressing the functional safety of advanced personal protective equipment (PPE) for emergency responders. 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.

1.0. INTRODUCTION

1.1. Background

The PPE industry is using electronics and software technology to improve the 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 standardization of life cycle phases and activities to follow when designing and building safety into the entire system from initial conceptualization to retirement. Functional safety life cycle (FSLC) refers to this standardization.

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.

1.2. Attributes of a Functional Safety Life Cycle (FSLC)

The FSLC applies during the entire life of the system since hazards may become evident at later stages or system modifications may introduce new hazards. The FSLC

expands the product development life cycle. The expansion is necessary because safety issues influence product development issues and vice versa. Secondly, an expanded approach minimizes the likelihood of addressing safety as an afterthought of the system design.

The use of a FSLC assures the consideration of safety during all phases of developing a PPE from conceptualization to retirement, thus reducing the potential for errors. Safety activities include identifying hazards, analyzing the risks, designing to eliminate or reduce hazards, and using this approach over the entire life cycle. These activities start at the system level and flow down to the subsystems and components.

The FSLC is an iterative process where life cycle phases have paths back to the previous phases in the life cycle. For example, in the design phase there must be a path back to the specifications phase to modify or further define the specifications resulting from design activity. This includes regressing back to the hazard and risk analysis phase if design activities result in the identification of a previously unconsidered hazard or risk.

In summary, implementing a FSLC results in the systematic consideration of safety, thus reducing the potential for random and systematic errors. It enables safety to be designed in early rather than after the system's design is completed. Early identification of hazards makes it easier and less costly to address them.

2.0. MANAGING FOR FUNCTIONAL SAFETY

2.1. Objectives

2.1.1. Manage the PPE project development and operation activities for functional safety by:

- Addressing the elements of Figure 3
- Providing appropriately qualified staff
- Establishing and reviewing a FSLC for the project
- Identifying a FSF for the project and reviewing its contents at the end

of each project phase

- Supporting the conduct of IFSAs.

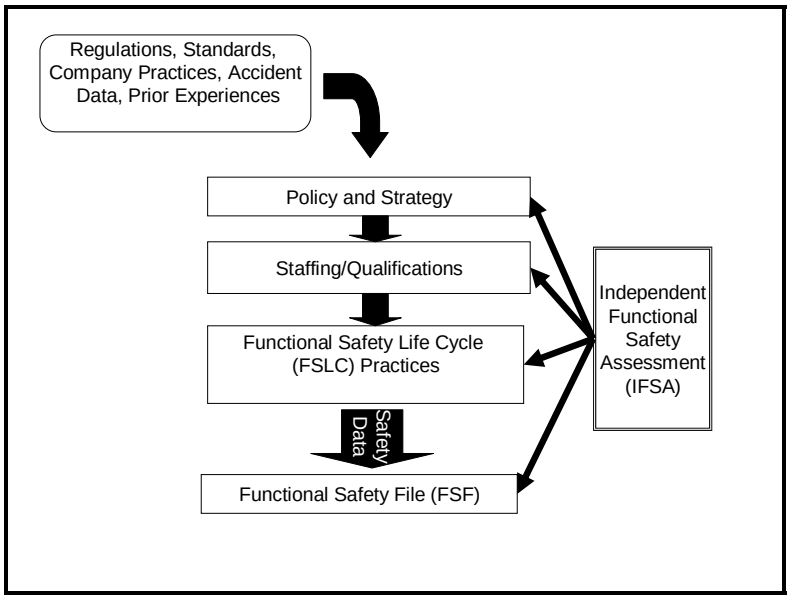

Figure 3 - Managing for Functional Safety.

2.2. Recommendations

2.2.1. Set project functional safety policy and strategy by:

- Establishing best practices in accordance with governing regulations, recognized standards, and corporate policy.
- Reviewing accident data from OSHA, NIOSH, NFPA, International Association of Fire Fighters (IAFF) and other sources to avoid repeat occurrences.
- Incorporating lessons learned from prior projects.

2.2.2. Establish FSLC activities and demonstrate follow-through commitment through planning, organizing, controlling, leading, and communicating recommended practices.

NOTE 1: In many cases, a relationship exists between a list of management responsibilities and activities and established quality procedures. For example, if the manufacturer is ISO 9000-2000 qualified or has basic corporate level quality procedures, then many of the management practices

can reference the appropriate quality procedure(s) or use the framework of a quality procedure as the basis for a project-specific procedure.

NOTE 2: The Project Management Body of Knowledge [4] Standard and the United States Department of Defense Software Engineering Institute efforts in defining best practices for software process and people capability improvement are useful references for establishing project management practices.

2.2.3. Define the minimum qualifications criteria required for staff to perform specific project roles related to functional safety.

2.2.4. Qualify the competency of and select persons, including subcontractors, involved in critical functional safety life cycle activities and management activities.

NOTE 3: When assessing the competence of persons, consider the following:

- Engineering knowledge, training, and experience appropriate to the PPE application.
- Engineering knowledge, training, and experience appropriate to the technology (e.g., electrical, electronic, programmable electronic, software engineering).
- Safety engineering knowledge, training, and experience.
- Knowledge of the PPE legal and safety regulatory framework.
- Management knowledge, training, and experience appropriate to the PPE application.
- The novelty and complexity of the technology and application.

2.2.5. Oversee the placement of the following in the project FSF:

- A summary of the safety policy and strategy.
- A description of the FSLC to be used for the project.
- The criteria for and the rationale for selecting project staff.
- All project specific plans.
- All project development, use, operation, and maintenance documents important to functional safety demonstration.

[4] A Guide to the Project Management Body of Knowledge (PMBOK Guide) --- 2000 Edition; ISBN 1880410230, by the Project Management Institute. The guide has been adopted as IEEE Standard 1490-2003.

- The results of the independent functional safety assessments conducted.

2.2.6. Review the contents of the project's FSF for sufficiency and accuracy at the end of each phase and before proceeding to the next phase.

2.2.7. Monitor functional safety outcomes through the conduct of IFSAs.

3.0. PROJECT PLANNING

3.1. Objectives

3.1.1. Establish a plan that supports the implementation of the selected FSLC by identifying project life cycle phases, activities, objectives and project safety documentation to be maintained using Figure 4 as guidance.

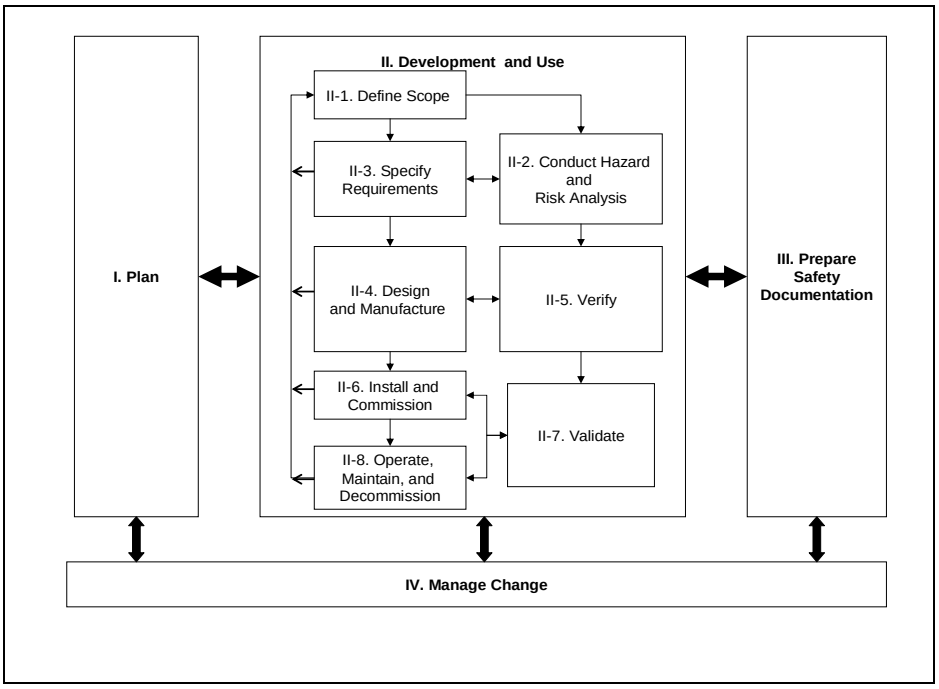

Figure 4 - Recommended activities for a FSLC

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.	• A summary of the safety policy and strategy. • A description of the FSLC to be used for the project including phase definitions, activities, objectives, and identification of safety documentation. • The criteria for and the rationale for selecting project staff. • All project plans.
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 project plans. • Product description.
	II.2 Hazard and Risk Analysis	Identify hazards, analyze event sequences leading to hazardous events and determine risks associated with these events.	• Updated project plans. • Results of hazard and risk analyses.
	II.3 Specify Requirements	Identify safety functions and specify design and performance requirements associated with these safety functions.	• Updated project plans. • Specification of safety functions including traceability to identified hazards. • Risk management summary.
II.Development and Use – Realization	II.4 Design and Manufacture	Design and manufacture the equipment to meet the required specifications.	• Updated project plans.
	II.5 Review, Test, and Verify	Conduct design for safety reviews, test and verification activities for electronics and software components, subsystems, and systems.	• Updated project plans. • Safety reviews, tests, and verification procedures 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 including problem reports. • Records of training schedules, topics covered, and results.
	II.7 Validate	Validate that the installation meets the equipment or	• Updated project plans. • Validation procedures and results.

		operation and maintenance.	
II.Development and Use – Operation and Maintenance	II.8 Operate, Maintain, and Decommissio n	Properly operate and maintain the equipment or system for continuing functional safety.	• Updated project plans. • Operation and maintenance manuals and records. Decommissioning procedures and records.
III. Prepare Safety Documentation (See Part 4 of this Series)		Prepare safety documentation throughout the functional safety life cycle.	• A safety statement. • All project planning, development, use, operation, and maintenance documents important to functional safety demonstration. • Results of IFSA.
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. • Configuration Identification Information. • Change history file.

Table 3 - Objectives by FSLC phase and activity

NOTE 4: The specific FSLC activities for a project and the degree of detail to meet the objectives of a phase vary for each component and system and the specific project circumstances. The user of these recommendations identifies phases and objectives based on specific factors, including project size, previous experience with a similar design, degree of complexity, risk reduction requirements, and context of use..

3.1.2. Develop project safety plans as specified in the project's FSLC.

3.1.3. Update the safety documentation and the FSF.

3.2. Recommendations

3.2.1. General Project Planning

3.2.1.1. Apply the FSLC to all components and systems used in PPE, specifically the electrical, mechanical, electronics and software components and systems.

3.2.1.2. Consider the use of concurrent life cycles when developing the FSLC for the electronics, software/firmware, and communication components development and integration as shown in Figure 5.

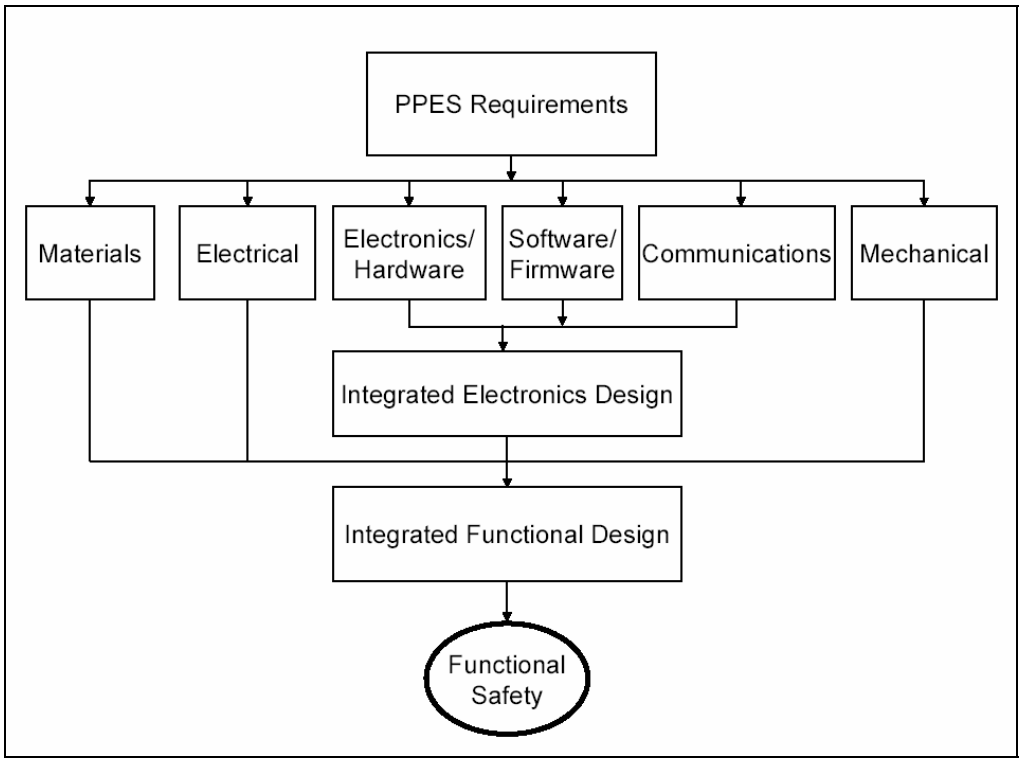

Figure 5 - Example of a concurrent engineering approach

NOTE 5: For example, a concurrent development and integration life cycle for software would reference the functional safety requirements for the software components and describes the software component

development and integration activities. (For more detail, for example see Hardware/Software Codesign[5]).

3.2.1.3. Consider the need for separate plans for design and integration of electronic, software/firmware, and communications components.

NOTE 6: 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 hazards3. Berge J, Levia, O, Rouillard J eds. [1996]. Current issues in electronic modeling: Hardware-software codesign and co-verification. Vol.8. Boston, MA: Kluwer Academic Publishers.
- Consequences in the event of failure.
- Degree of complexity.
- Degree of design novelty.
- Risk reduction requirements.

NOTE 7: 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.

3.2.1.4. Consider the need for separate plans for operation and maintenance, safety validation, installation and commissioning, and management of change

NOTE 8: These plans may be incorporated in other documents (i.e., company procedures, quality plans), exist as separate plans, or exist all in one plan. These documents may be referenced from the project management plan.

3.2.1.5. When developing plans identify the following:

[5] Berge J, Levia, O, Rouillard J eds. [1996]. Current issues in electronic modeling: Hardware-software codesign and co-verification. Vol.8. Boston, MA: Kluwer Academic Publishers.

- Distinct entry points, exit points, and criteria for transitioning among activities,
- Work products (e.g. meeting minutes, analysis and test results, formal documentation, etc.), procedures for communicating issues that could impact the safety functioning of the PPE, and staff responsibilities and sign-off authority.

3.2.1.6. Update the project plan and the specific safety plans as life cycle phases and design knowledge progresses.

3.2.2. Design and Manufacturing Planning

3.2.2.1. Identify design criteria when specifying design procedures for the electronics, software/firmware and communications components.

3.2.2.2. Identify methods to be used for avoiding, detecting, and recovering from random hardware failures and systematic failures.

3.2.2.3. Specify manufacturing plans for the electronics, software/firmware, and communications components.

3.2.3. Verification and Validation Planning

3.2.3.1. Specify verification and validation plans for confirming by examination and provision of objective evidence, i.e. by verifying and validating, that the PPE meets the safety requirements.

NOTE 9: The verification plan defines the activities that confirm the meeting of the requirements of each PPE functional safety life cycle phase. Verification activities also confirm that each phase of activity correctly uses the information of the previous phase to avoid introducing errors from one phase in the life cycle to the next. Verification activities include review, traceability, testing, and audit.

NOTE 10: The validation plan defines the activities that confirm that the safety systems and the external risk reduction measures achieve the overall safety requirements and, in

particular, the required risk reductions. Validation activities demonstrate that the safety requirements for the PPE will achieve the benefits claimed for them in the environment. Thus, validation activities could include safety requirements analysis, system simulation, system testing, and monitoring during operation.

NOTE 11: Verification and validation are iterative activities. Verification checks the outputs from various design phases and validation checks the completed system.

3.2.3.2. Develop the verification and validation plans using person(s) independent of the component and systems designer(s).

NOTE 12: This does not preclude the system designer(s) from participating in the plan development.

3.2.3.3. Develop verification and validation plans early in the functional safety life cycle.

3.2.3.4. Include, at a minimum, in the verification and validation plans the following:

- When analysis, testing, or assessment activities take place,
- Who conducts the analysis testing or assessment activities,
- Activities and tests that confirm the safety requirements,
- Activities and tests that confirm the system modes, and
- Confirmation of operating modes and transitions such as, startup, shutdown, reset, manual, remote, semiautomatic, automatic, monitor, standby, emergency, and stuck/jammed (abnormal).

NOTE 13: This is not a comprehensive listing. A given system might have a subset of the listed modes and/or additional modes such as pass and fail criteria and procedures for addressing activities that fail the criteria established for achieving functional safety.

3.2.4. Installation, Commissioning, and Training Planning

3.2.4.1. Specify a plan for installing and commissioning the PPE in a safe manner that achieves functional safety and training for its users

and maintainers.

3.2.4.2. In the installation and commissioning plans, include at a minimum, the following:

- Possible hazards during installation and commissioning,
- Safety precautions during installation and commissioning,
- Installation, commissioning, and training procedures,
- Integration sequences, and
- Criteria for declaring installation, commissioning, and training complete.

3.2.5. Use, Maintenance, and Decommissioning Planning

3.2.5.1. Specify a plan for using, maintaining, and repairing the PPE to maintain functional safety.

3.2.5.2. When developing an operation, maintenance and repair plan, consider at a minimum, the identification of:

- 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, and
- Circumstances and procedures for restoring and verifying safety functions or interlocks after they have been bypassed or overridden.

3.2.6. Management of Change (MOC) Planning

3.2.6.1. Specify a management of change (MOC) plan for systematically making and tracking changes so that changes do not adversely affect functional safety.

NOTE 14: Changes include repairs, upgrades, and parts replacements for the PPE, its subsystems and components. Changes also include changes made to documentation.

3.2.6.2. Include configuration management and document control activities in the MOC plan.

3.2.6.3. All safety-critical procedures, systems, subsystems, software, firmware, and hardware should be subject to an MOC plan.

3.2.6.4. MOC plans do not pertain to:

- Replacements in kind,
- Repairs that are not of a corrective nature, nor
- Rrecalibrations within specification ranges.

3.2.6.5. The MOC plan establishes the change process and documents the results.

3.2.6.6. The MOC plan should contain the following items to identify, analyze, control, and track safety modifications:

- Documentation describing the proposed change, the reasons for the change, and the impact on safety and health,
- A hazard and risk analysis,
- A method to identify and track the change,
- A review and authorization process conducted before implementing the change, and
- A method to verify modifications.

3.2.6.7. Make changes using manufacturer authorized representatives who are competent and knowledgeable about the entire PPE.

3.2.6.8. Provide a unique version identifier for the software, firmware, and electronic hardware.

3.2.6.9. Update all relevant documentation affected by the change as necessary.

NOTE 15: This is especially important if the change affects operation and maintenance procedures.

3.2.7. Safety Documentation

3.2.7.1. Place the following in the project FSF:

- A summary of the safety policy and strategy.
- A description of the FSLC to be used for the project including phase definitions, activities, objectives, and identification of safety documentation.
- The criteria for and the rationale for selecting project staff.
- All project specific plans.

4.0. DEVELOPMENT AND USE: DEFINING THE SAFETY REQUIREMENTS

4.1. Objectives

4.1.1. Define the safety requirements by defining the scope of the PPE, conducting hazard and risk analysis and specifying the safety requirements. It is common to cycle among these life cycle activities as shown in Figure 6.

4.1.2. Update the safety documentation and the FSF.

4.2. Recommendations

4.2.1. Define Scope (See II-1 of Figure 6.)

4.2.1.1. Define the conceptual equipment design, component and equipment interfaces, and the overall functionality of the PPE.

4.2.1.2. Determine the interfaces between the equipment, its components, and the people using the equipment.

4.2.1.3. Consider the architectural elements shown in Figure 7 when defining the scope of a PPE.

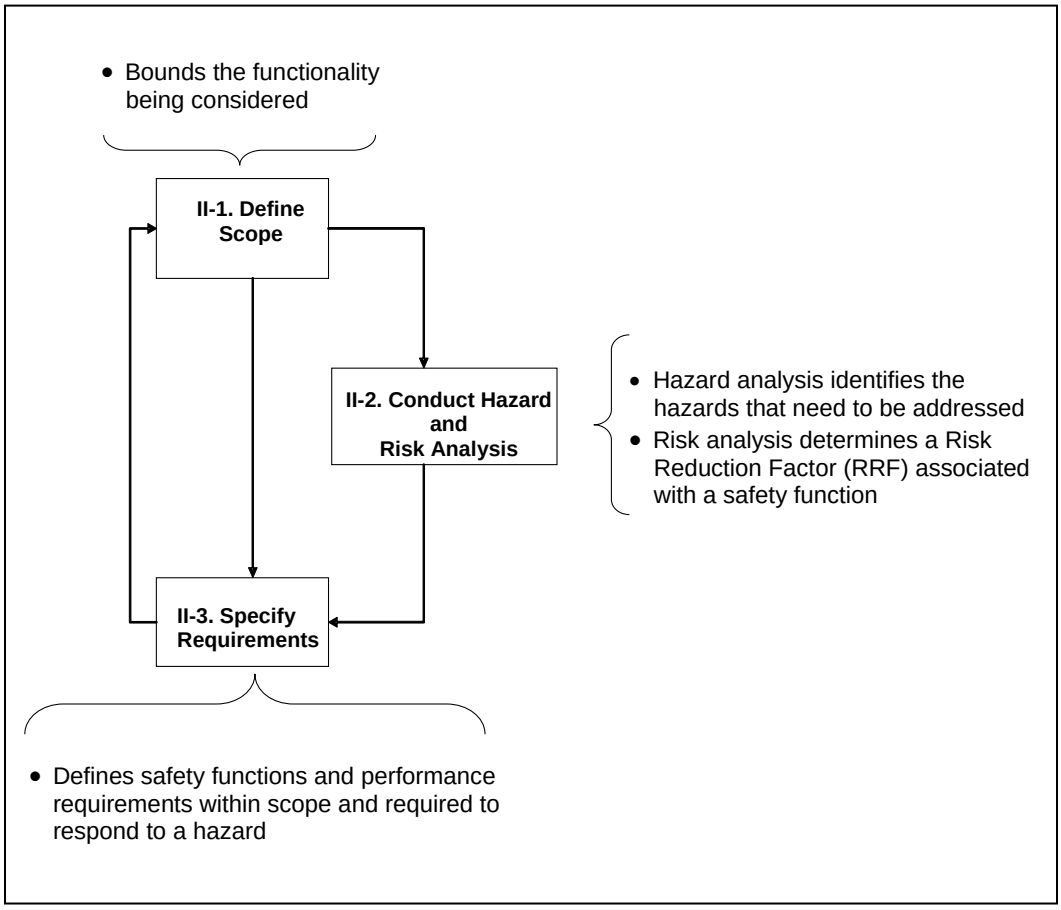

Figure 6 - Defining the safety requirements.

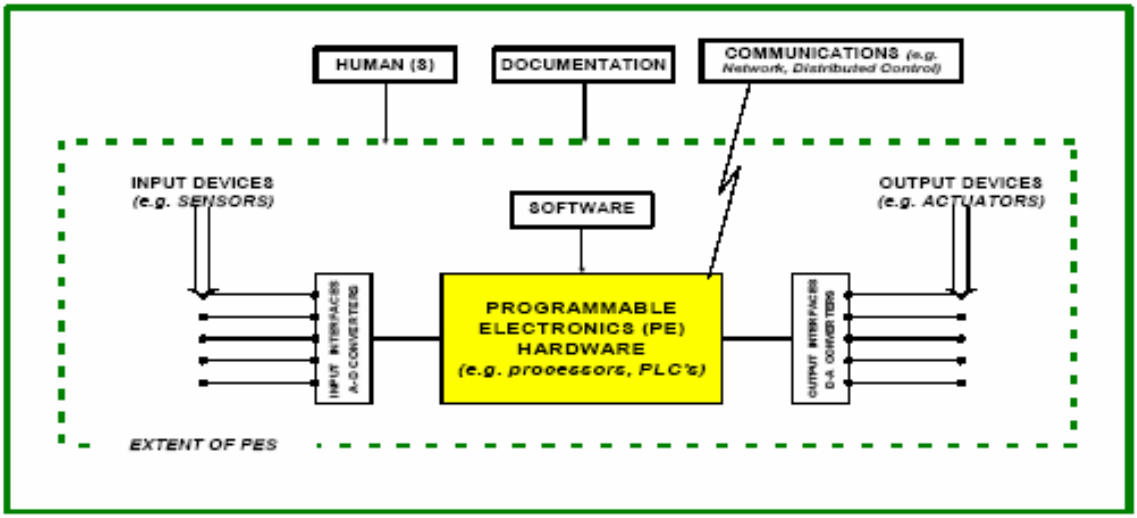

Figure 7 - Boundaries of a PPE using electronics and software.

4.2.1.4. Identify all components, subsystems, and their intended scope of functionality.

4.2.1.5. Identify the following types of components and subsystems as safety-related

- Those that monitor the state of a emergency responder or another PPE for safety purposes.
- Those that control, regulate, or contain potentially dangerous energy sources.
- Those that control or regulate life saving devices.
- Those that control or partially control moving equipment, moving parts of equipment, or moving material.
- Those that collect, compute, store, display, or manipulate data critical to safety.

NOTE 16: To avoid omitting hazards from a safety analysis requires an unambiguous definition of the scope. The scope identifies important information, including characteristics and limitations of the system, for consideration when assessing functional safety.

4.2.2. Conduct Hazard and Risk Analysis (See II-2 of Figure 6)

4.2.2.1. Identify and analyze hazards and event sequences leading to hazards during operation, maintenance, or fault conditions.

4.2.2.2. Consider foreseeable misuse and foreseeable human mistakes.

4.2.2.3. Determine the risk associated with each hazard.

4.2.2.4. Begin hazard and risk analysis early and continue to update it during all functional safety life cycle phases.

4.2.2.5. Review PPE regulations, standards, accident data, and prior experience to identify hazards that could apply to the system.

4.2.2.6. Consider using one or more types of hazard analysis techniques to identify and analyze hazards and hazardous event sequences.

4.2.2.7. Use qualitative or quantitative risk analysis approaches to determine the risk reduction requirements for the PPE.

4.2.2.8. Develop a method or procedure to document and track hazards, associated risks, and their status.

4.2.2.9. Document the methods used for hazard and risk analysis in the safety documentation.

4.2.2.10. Include the following information[6] when documenting hazards and risks

- A description of each hazard and the associated risk,
- Source(s) of hazard identification (examples include subsystem and system analysis, management of change (MOC) analysis, and accident reports), and

[6] Adapted from MIL-STD-882C, Task 106 [U.S. Department of Defense 1993]

- Status of each hazard.

NOTE 17: Hazard status may be defined as

Open: A known or suspected hazard without corrective action.

Monitor: A known or suspected hazard for which corrective action, or study of corrective action, is identified. If the process of implementation is in question this status may be maintained while the fix is in work and not completed.

Closed: A known or suspected hazard for which corrective action is identified, initiated, completed, and accepted ,i.e.,

- The recommended controls to eliminate or reduce the hazard to an acceptable level of risk, and/or
- Written approvals accepting the risk and thus affecting a “closed” status.

NOTE 18: A hazard log may be used to track hazards, their associated tasks and activities, and their resolution. The hazard log may be implemented with computer database or paper document form. The hazard log may be useful for other projects by identifying common hazards and their resolutions.

4.2.3. Specify Requirements for PPE (See II-3 of Figure 6)

4.2.3.1. Define the functional safety requirements that address the risks identified by the hazard and risk analysis.

4.2.3.2. Determine safety functions used for risk reduction.

NOTE 19: Achieving an overall risk reduction objective may require additional safety technology and external risk reduction practices outside the scope of this guidance.

4.2.3.3. Specify performance requirements associated with the safety functions.

NOTE 20: Different approaches may be taken to specify performance requirements associated with PPE safety functions. Specifying the risk reduction factor (RRF) as described in Part 1 is one approach. A complementary approach is to specify a safety integrity level (SIL) (i.e., a range of acceptable probabilities of failure) for various categories of use (see IEC 61511).

4.2.3.4. Use the hazard and risk analysis results as the primary source of input for specifying safety requirements.

4.2.3.5. When apportioning the overall risk reduction requirements to the safety functions, consider the equipment scope and the protection layers provided by other equipment and systems.

4.2.3.6. Consider all operating and maintenance conditions of the PPE when specifying safety functions.

4.2.3.7. Consider specifying design, performance, usability, configurability, interoperability, scalability, and maintainability criteria for the PPE.

4.2.3.8. Specify both safety functions and performance requirements for each identified hazard.

NOTE 21: The safety functions specifications describe what the PPE does. The performance requirements describe the performance and constraints (i.e., in terms of capabilities, speed, accuracies, and probabilities).

NOTE 22: The following are examples of safety functions:

- Emergency stops,
- Mode transitions (e.g. startup, reset, automated to manual, shutdown),
- Monitoring a safe state,
- Controlling or regulating energy sources, and
- Displaying safety-critical information (e.g., diagnostic displays, warning lights and alarms).

4.2.3.9. When specifying safety functions, consider the following order of precedence for satisfying functional safety requirements:

- If hazard elimination is not practical, reduce the associated risk to as low as reasonably practical.

- When reducing the risk to as low as reasonably practical using fixed, automatic, or other protective safety design features or

devices, make provisions for periodic functional checks of safety components, subsystems, and systems.

- Use a separate means to detect an unsafe condition and produce an adequate warning signal to alert personnel of the hazard.

NOTE 23: Address minimizing the probability of incorrect personnel reaction to the warning signals and standardizing the warning signals within like types of systems.

- Develop procedures and training where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices.

- Refrain from using warning, caution, or other written advisory as the only risk reduction method.

5.0. DEVELOPMENT AND USE: REALIZING THE PPE

5.1. Objectives

5.1.1. Design and manufacture the equipment to meet the required specifications.

5.1.2. Update the safety documentation and the FSF.

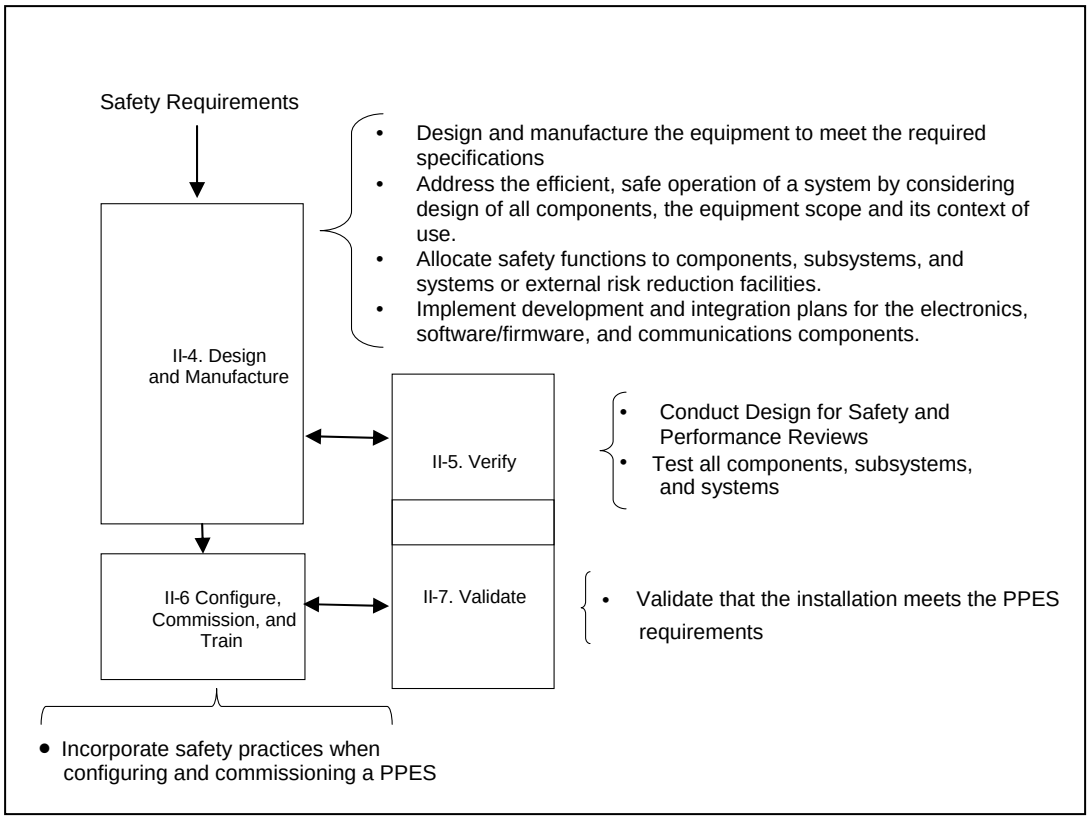

Figure 8 - Realizing the PPE.

5.2. Recommendations

5.2.1. Design and Manufacture (See II-4 of Figure 8)

5.2.1.1. Address the efficient, safe operation of a system by considering design of all components, the equipment scope, and its context of use.

5.2.1.2. Address human factors issues when designing.

5.2.1.3. Allocate safety functions to components, subsystems, and systems or external risk reduction facilities.

5.2.1.4. Consider common cause failure modes when allocating safety functions to components, subsystems, and protection layers

NOTE 24: Greater levels of independence can reduce common cause failures. Independence may be achieved by functional diversity, use of diverse technologies, physical separation, logical isolation, and no sharing of common parts or information sources.

5.2.1.5. When developing and integrating the electronics (including microelectronics), the software/firmware and the communications address the following

- Structuring the component and subsystem requirements specification with safety functions and performance requirements.
- Documenting traceability between the component and subsystem requirements to the PPE requirements.
- Describing and documenting all activities conducted and associating them with the functional safety life cycle activities.

5.2.2. Verify (See II-5 of Figure 8)

5.2.2.1. Conduct design for safety reviews, such as, checking consistency among requirements and reviewing software design for compliance with safe computing practices.

5.2.2.2. Test all components and sub-systems, such as, electronic devices, power supplies, sensors, data communication paths, actuators, and software.

NOTE 25: The test and verification applies at the component level, the subassembly level, and the integrated system level. Testing at the subassembly and the integrated system level typically addresses interaction problems among components.

5.2.2.3. The verification activities should address errors at their source.

5.2.3. Install, Commission, And Train (See II-6 of Figure 8)

5.2.3.1. Install and commission the PPE properly and safely and in

accordance with the project safety plans.

NOTE 26: The act of installing and commissioning equipment or a system may incur safety risks. Therefore, requirements for configuring and commissioning include safety practices.

5.2.3.2. Identify and resolve failures and incompatibilities.

5.2.3.3. When developing training procedures, take into account human factors considerations including

- Usability of human-computer interface,
- Donning of the PPE (when applicable), and
- Effects of cleaning the PPE (when applicable).

5.2.3.4. Establish and update training requirements and complete training before operation and maintenance.

5.2.3.5. Increase the degree of rigor for training as the risk increases.

5.2.3.6. Identify training goals early in the life cycle.

5.2.3.7. Complete training using all training materials, including operation and maintenance manuals, before commissioning.

5.2.3.8. When conducting training, consider the following

- Detailing the potential hazards during operation and maintenance and the means to control them,
- Addressing the following:
  - System description,
  - System operating principles (i.e., theory of operation),
  - Safety functions,
  - Safety systems operation, testing, and maintenance,
  - Hazards protected against,
  - Description of all modes and mode transitions,

- Safety warning and alarms,
- Operator interfaces,
- System operation,
- Emergency operation for single-failure modes,
- Emergency operation for multiple-failure modes occurring at once,
- Safe system maintenance, and
- Manual operation/intervention.

5.2.4. Validation (See II-7 of Figure 8)

5.2.4.1. Validate that the installation meets the equipment or systems requirements during commissioning and throughout operation and maintenance by carrying out of the validation plan.

5.2.4.2. Calibrate the instruments used for validation.

5.2.4.3. Document the validation activities including, at a minimum, the following items

- Safety requirements version,
- Safety function validation,
- Mode validation,
- Mode transition validation,
- Test, tools, and equipment used, and
- Validation results.

5.2.4.4. Carry out the validation by qualified staff that is independent of the design and implementation.

6.0. DEVELOPMENT AND USE: OPERATE, MAINTAIN, AND DECOMMISSION

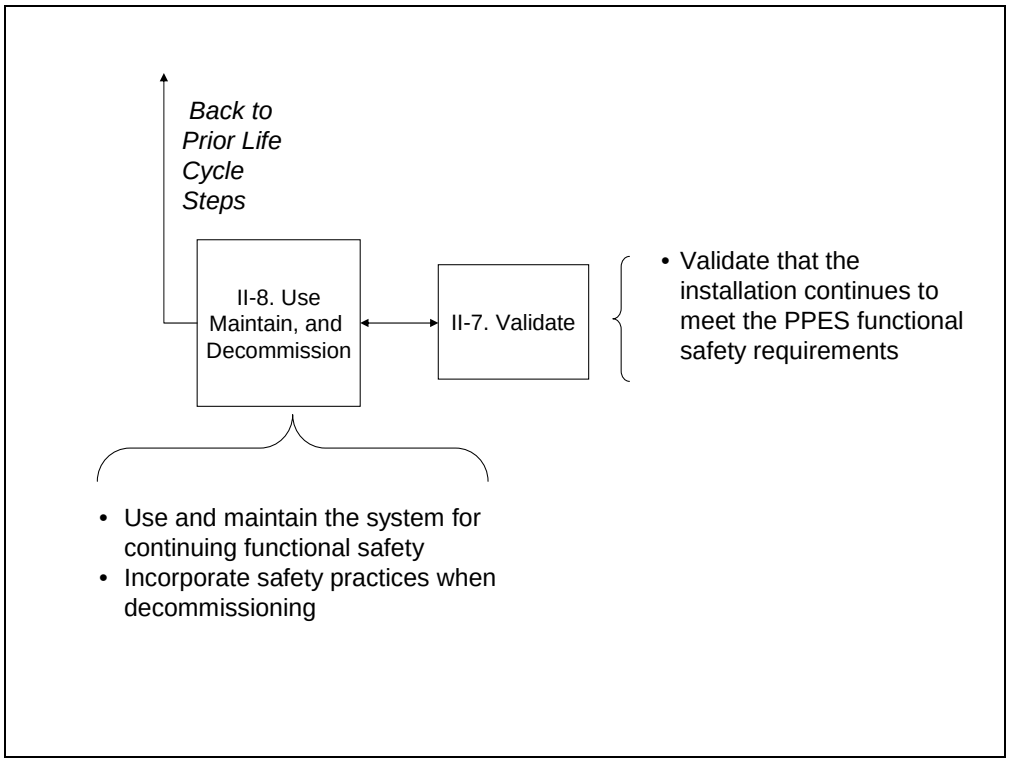

Figure 9 - Operation, maintenance, and decommissioning.

6.1. Objectives

6.1.1. Operate, maintain, and decommission the PPE in a manner that continues to meet functional safety requirements.

NOTE 27: Maintenance activities include repairing, upgrading, and using replacement parts.

6.1.2. Update the safety documentation and the FSF.

6.2. Recommendations

6.2.1. Operate, maintain, and decommission the PPE properly and safely and in accordance with applicable plans, procedures, and schedules. (See Figure 9)

NOTE 28: The act of using, maintaining, and decommissioning a PPE may incur safety risks. Therefore, requirements for operating, maintaining, and decommissioning include safety

practices.

6.2.2. Identify and resolve failures and incompatibilities.

6.2.3. Validate that the installation continues to meet the PPE functional safety requirements.

6.2.4. When maintaining equipment, account for the effects of cleaning the PPE on the functionality of the electronics, software/firmware, and communications components.

6.2.5. Complete and deliver to the end user operations and maintenance plans prior to operation and maintenance.

6.2.6. Conduct operations and MOC activities using appropriately trained persons with the appropriate skill levels.

6.2.7. Update operation and maintenance documentation in conjunction with MOC plans, procedures, and schedules.

6.2.8. Document modifications to operations, maintenance, or decommissioning activities in accordance with the MOC plans, procedures, and schedules.

6.2.9. Before decommissioning, prepare procedures for

- Closing down to an inactive, safe state,
- Dismantling,
- Removal, and
- Storage (mothballed for possible reuse).

7.0. SAFETY DOCUMENTATION

7.1. Objectives

7.1.1. Document safety claims and supporting information so that the PPE is adequately safe over its lifetime for a given application.

7.2. Recommendations

7.2.1. The recommendations for this clause are contained in Part 4 of the Report Series.

8.0. MANAGE CHANGE

8.1. Objectives

8.1.1. Make and document all modifications in accordance to the MOC plan.

8.1.2. Assure that appropriate safety is established and maintained during and after changes are made.

8.1.3. Update the safety documentation and the FSF.

8.2. Recommendations

8.2.1. Provide for review and approval, in accordance with the MOC plan, prior to making any modification that could affect safety.

8.2.2. Before normal system operation resumes, use testing or other means to verify the proper implementation of the change and the PPE performs as desired.

8.2.3. If the change affects operation or maintenance, then training must occur before normal PPE operation resumes.

9.0. SUMMARY

Emergency responders are dedicated to saving lives, but they must rely on PPE to reduce the potential for harm to themselves and others when responding to emergencies. To protect emergency responders, manufacturers are innovating PPE by adding electronics and software to provide enhanced protective features. The added functionality reduces exposure to hazards by emergency responders and enhances their ability to save lives.

Innovative designs increase the scope of protection many times by incorporating more complex embedded safety functions. To maintain safety objectives, standards (i.e. *IEC 61508* and *ANSI UL 1998*) have emerged. These standards identify functional safety practices or practices that reduce the risk of failure of safety functions implemented using electronics and software. Functional safety standards emerged to avoid problems that surfaced in other industries. Therefore, it is worthwhile for the PPE industry, similar to other industries that have benefited from these standards, to consider tailoring these standards to address their particular application.

Part 2 identifies life cycle activities for achieving functional safety consistent with best practices.

10.0. ABBREVIATIONS

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

ABBREVIATION	DEFINITION
MOC	Management Of Change
MSHA	Mine Safety and Health Administration
NFPA	National Fire Protection Association
NIOSH	National Institute for Occupational Safety and Health
NPPTL	National Personal Protective Technology Laboratory
OSHA	Occupational Safety and Health Administration
PASS	Personal Alert Safety System
PDA	Personal Digital Assistant
PFD	Probability Of Failure On Demand
PHL	Preliminary Hazard List
PM	Project Manager
PPE	Personal Protection Equipment
QFD	Quality Function Deployment
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

11.0. 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

Quality Function Deployment (QFD): A Six Sigma tool for translating what the customer wants into product requirements that meet those wants. QFD is effective in helping teams exceed customer requirements. Examples of random hardware failures include transient glitches, stuck at value, and loss of function.

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.