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

(In Nine Parts)

Part 1: Introduction to Functional Safety

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 **1**depicts all nine titles in the series.

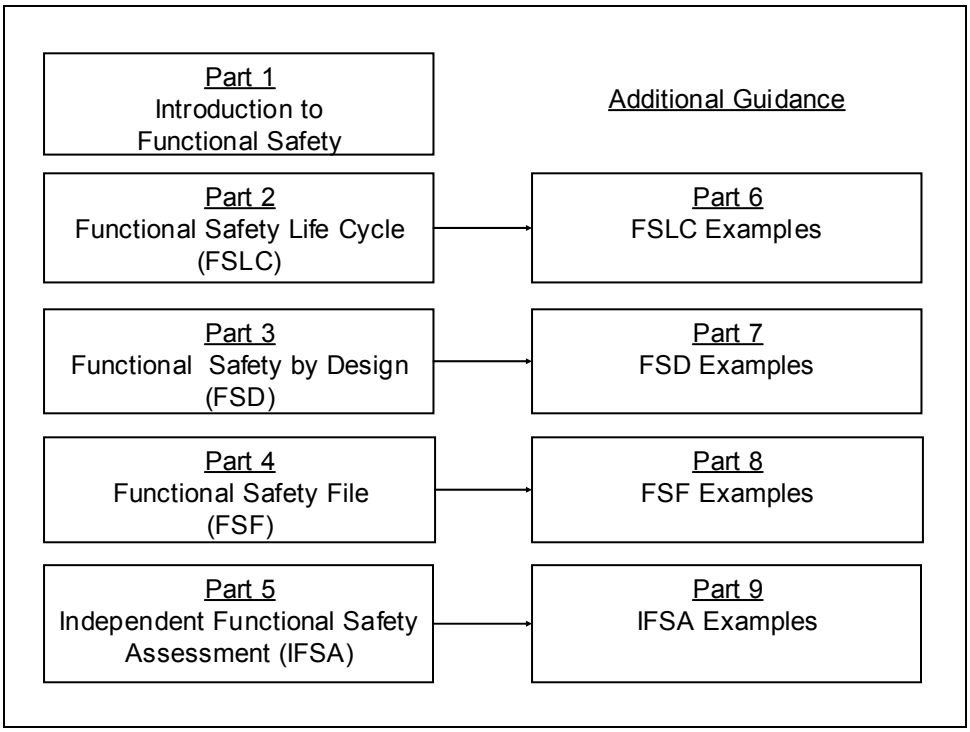

Figure 1 - The functional safety report series.

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.

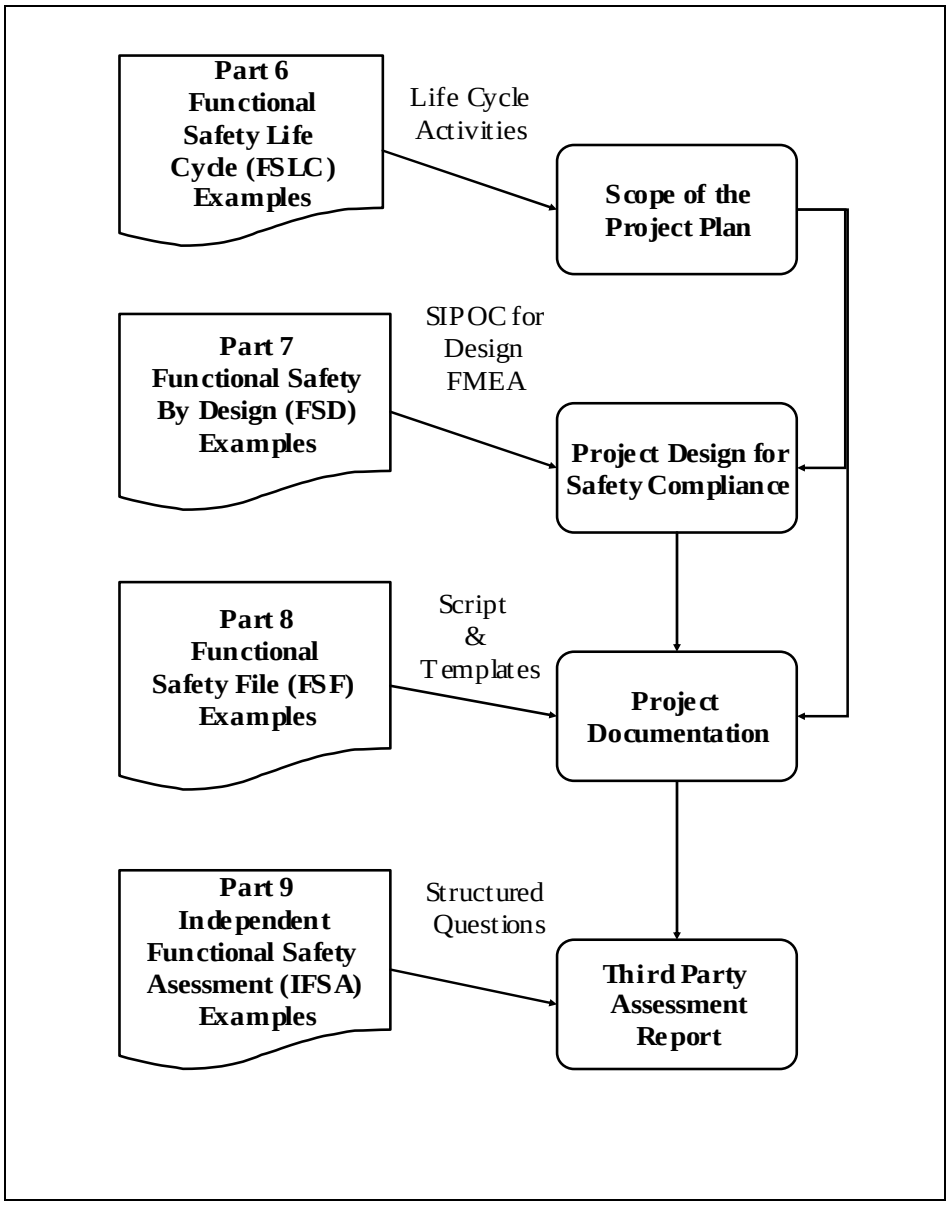

Figure 2 - Relationships among Parts 6, 7, 8, and 9

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

Table 1 - Mining Industry Guidelines

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

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

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

Table 2 - Overview of ANSI UL 1988 and IEC 61508

ACKNOWLEDGEMENT

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

ABSTRACT

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

Advanced Personal 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, An Introduction to Functional Safety is the first in a nine-part series of recommendations addressing the functional safety of advanced PPE for emergency responders. 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 usage and integration guidance to minimize their exposure to hazards.

Part 1 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.

1.0. INTRODUCTION

1.1. Emergency Responders - Dedicated to Saving Lives

At 4:19 p.m., the Brookside Public Safety Answering Point (PSAP) receives a 9-1-1 call from the relative of a man who has returned home from playing tennis and is reporting chest pains.

At 3:17 a.m., the Brookside PSAP receives a 9-1-1 call from a cab driver that the apartment building at 725 Pine is smoking and appears to be on fire. Several families have already evacuated the unit.

A large explosion occurs at a chemical plant in Barberville, a suburb of Brookside. There is the potential for hazardous chemical leaks as well as toxic smoke from the chemicals burning[4]*.*

Hazardous situations like those identified above require rapid intervention by emergency responders − firefighting, law enforcement, and emergency medical services personnel. There are over two million paid and volunteer emergency responders in the United States5 who answer calls for assistance and service. These individuals play a critical role in responding to medical emergencies, in protecting property and people from fires and natural disaster, and in guarding public safety. They rely on PPE to reduce their risk of harm and to increase the survivability of victims.

PPE 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

To implement these functions in PPE, manufacturers are using advanced materials, electronics, and software.

4 The SAFECOM Program—Department of Homeland Security Version 1.0. Date accessed: June 2, 2004.

5 Houser A, Jackson BA, Bartis JT, Peterson DJ [2004]. Emergency responder injuries and fatalities. TR-100-NIOSH, RAND Corporate, Science and Technology Policy Institute [http://www.rand.org/publications/TR/TR100/]. Date accessed: June 2, 2004.

1.2. Emergency Responders Put Their Lives at Risk

Emergency responders are willing to risk their lives to save the lives of others. They encounter significant risk of injury, illness, and death as they answer calls for help. Although responders accept their jobs as hazardous, this acceptance does not diminish the importance of protecting them from hazards.

A recent study[6] conducted by the RAND Corporate, Science and Technology Policy Institute under NIOSH sponsorship, identified that an average of 97 firefighters and 155 police officers died each year between 1990 and 2001. Additionally, an average of 11 non-firefighter EMS personnel died in the line of duty each year between 1998 and 2001. These losses are in addition to the tragic events of September 11, when 450 emergency responders lost their lives.

According to the study,

- "The injuries most frequently experienced by firefighters are traumatic injuries, cuts and bruises, burns, asphyxiation and other respiratory injuries, and thermal stress. Physical stress and overexertion, falls, being struck by or making contact with objects, and exposure to fire products are the primary causes of injury at the fire scene. Physical stress, becoming lost or trapped in a fire situation, and vehicle accidents are the primary causes of death. Physical stress is responsible for nearly half of all on-duty deaths."

- "Most injuries to police are traumatic injuries and cuts and bruises resulting from vehicle accidents, falls, assaults, or physical stress. Nine out of ten line-of-duty deaths are due to vehicle accidents or assaults. Police are most often injured in falls, assaults, vehicle-related accidents, and through stress or overexertion. The most common injuries from all causes are traumatic injuries, such as sprains and strains and cuts and bruises. Police are also at risk of burns and symptoms of illness as a result of exposure to fire and hazardous substances. These exposure-related injuries represent less than 1 percent of all law enforcement injuries."

6 Ibid, page xv.

- "EMS personnel are most at risk of sprains and strains. Back injuries represent a higher proportion of injuries for EMS personnel than they do for other responders. EMS personnel also have a high risk of infectious disease exposure, mostly through percutaneous injuries such as needle sticks. Nearly all on-duty deaths for which data are available are due to aircraft and vehicle accidents."

In addition to this study, the RAND Corporation organized and reported on a NIOSH-sponsored conference in December 2001. The conference brought together individuals with experience in responding to acts of terrorism. It provided a forum for voicing emergency responders' concerns regarding the performance, availability, and appropriateness of their PPE as they responded to the 9/11, Oklahoma City, and anthrax incidents. Table 1 highlights the lessons learned from these incidents as documented by RAND Corporation[7]. These lessons learned pose new challenges in PPE design and development.

1.3. Manufacturers of PPE - Responding to New Challenges

Manufacturers of PPE are responding both by incorporating advanced technology in equipment and by participating in the development of safety design and performance standards associated with the use of these technologies. Electronics and software implemented in PPE provide functions critical to life safety including:

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

7 Jackson BA, Peterson DJ, Bartis JT, LaTourrette T, Brahmakulam IT, Houser A, Sollinger J M [2002]. Protecting emergency responders: Lessons learned from the terrorist attacks. CF-176-OSTP. Santa Monica, CA: RAND Corporate, Science and Technology Policy Institute. [http://www.rand.org/publications/CF/CF176/http://www.rand.org/publications/TR/TR100/]. Date accessed: June 2, 2004.

- 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

While providing life safety benefits, the use of electronics and software also adds a level of complexity that, if not properly considered, may adversely affect the safety of emergency responders. This situation has led to the consideration of adding functional safety requirements for electronics and software to PPE design and performance standards.

Broader definition of emergency responder: Emergency responders now include construction workers and medical personnel in addition to fire fighters and the police.

Staggering range of hazards: wet conditions, flames, intense heat, combustion by-products, smoke, unstable rubble and debris, dust and smoke, biological and infectious disease hazards, hazardous materials (anhydrous ammonia, Freon, battery acids, large amounts of unburned jet fuel, chemical and radioactive contaminants), secondary explosive devices or a follow-on attack, stores of ammunition, live power lines, mold and mildew growth, exposed and broken rebar, constant lower-frequency noise from heavy-duty equipment

PPE usability problems: equipment designed for one hazard not a range of hazards, equipment not comfortable or durable enough to allow for extended wear during demanding physical labor, lack of interoperability between different types of equipment, multiple problems with equipment performance

Communications: Mobile and landline communications unavailable, wireless communications unavailable due to high call volume and then loss of tower, surplus of information, different information sources telling different things

Table 3 - Lessons learned from the terrorist incidents

1.4. Functional Safety: What Is It And Why Is It Needed?

Functional safety is part of the overall system that depends on a system or equipment operating correctly in response to its inputs. Emergency responders want their PPE to function as intended. This has always been the case with all PPE regardless of the technology implementation. The use of electrical components (e.g., a thermal fuse in an appliance) and mechanical components (e.g., a combination lock on an electrical box) provides functional safety. Safety engineers have rightfully questioned whether this is really a new situation.

Why introduce the concept “functional safety” to characterize this situation? The incorporation of the electronics and software provides increased scope and complexity of functionality. The expanded functionality provided warrants an expanded approach to achieve PPE performance in life safety applications. Equipment designs based on electronics and software are usually more complex than electrical or mechanical designs because they provide additional functionality. The complexity results from the use of electronics and software logic to supply features that may codify or provide the basis for life safety decisions. Because increased complexity inevitably leads to an increased potential for design inadequacies and systematic errors, there exists a risk of incomplete or incorrect implementation of functionality.

The International Electro-technical Commission (IEC) and American National Standards Institute (ANSI) standards communities began distinguishing functional safety considerations from purely electrical and mechanical or basic safety considerations through the issuance of standards such as IEC 60601, IEC 61508, IEC 61511[8], ANSI/ISA S84[9], and ANSI/UL 1998[10]. These standards follow an expanded approach that includes the following elements:

- Consider existing design and performance standards as an integral part of

8 For further detail about IEC Standards, see [http://www.iec.ch]. Date accessed: June 2, 2004.

9 For further detail about ANSI/ISA S84, see [http://www.isa.org]. Date accessed: June 2, 2004.

10 For further detail about ANSI/UL 1998, see [http://www.ul.com/software/ansi.html]. Date accessed: June 2, 2004.

functional safety achievement

- The safety and performance testing of materials, electrical, mechanical, and electromechanical components remains important. Failure of these components may lead to equipment failure and to compromises of life safety goals.
- Characterize the functional safety of electronics and software components and subsystems in addition to the entire equipment or system
- Use of qualified components and subsystems may be the best building blocks for achieving functional safety. Without characterization of these building blocks, it becomes difficult if not impossible to characterize the life safety performance of the equipment or system.
- Address the entire system in addition to the components and subsystems
- A diverse group of suppliers would likely design and manufacture equipment used to provide protection for emergency responders; therefore, proper compatibility and interaction of the components to achieve an integrated, hybrid package is essential to the safety of emergency responders. Ultimately, the PPE support worn by emergency responders will be an integrated package from a diverse group of manufacturers. Proper integration is the key for instance to ensure the compatibility and sufficiency of power supplies, computer controllers, component isolation and the lack of inter-component interference and failure mode contingencies.
- Reduce the potential for equipment and system failure by following functional safety practices
- It is important from the very beginning of the PPE design to take into account functional safety considerations for the entire life cycle, including training, installation, operation, maintenance, and upgrades. Functional safety considerations must not be an afterthought once the design is completed.

- As manufacturers use electronics and software to provide better life safety equipment for emergency responders, it is important to consider expanding current safety evaluations to include functional safety evaluations of equipment and systems. The National Fire Protection Association (NFPA) Technical Committee on Electronic Safety Equipment, NFPA 1982, is developing an umbrella standard for electronic safety that will cover all electrical/electronic products used by fire fighters, EMS and other emergency responders.

2.0 REDUCING LIFE SAFETY RISK

"The need for safety and reliability in computer-controlled machines is certainly no less than in the electromechanical systems they often displace. For non-technical reasons (e.g., environmental, legal) ... safety demands on computer-controlled systems may in fact, be higher[11]."

2.1. Risk Reduction Objective: The ALARP Principle

The as low as reasonably practical (ALARP) principle drives the selection of tools for reducing risk and hence achieving functional safety in PPE.

Innovative designs of PPE using electronics and software technology have more embedded safety functions and an increased number of interfaces. These innovations provide more life safety features for the emergency responder as well as an enhanced ability to respond to complicated threat scenarios. A primary objective then is to achieve an acceptable level of risk that is as low as reasonably practical.

Figure 3 illustrates the ALARP principle. In some situations, the risk is refused altogether because it is so great; or the risk is considered insignificant; or the risk is somewhere in between refusal and insignificant and has been reduced to the lowest practicable level. The triangle conveys the concept of diminishing importance. The higher the risk, the more important it is to reduce it. Correspondingly, lower risks are proportionately less important to reduce.

2.2. Using PPE to Reduce Risk in a Residential Apartment Fire Scenario

Figure 4 shows an example of using PPE to reduce risk in a residential apartment fire scenario. The example builds on the residential fire scenario mentioned in the SafeCom Statement of Requirements (SoR) (Section 3.3 Fire-Residential Fire Scenario)[12]. The SoR for public safety communications and interoperability provides information on base level requirements for a system of interoperable public safety communications across all local, tribal, state, and federal "emergency responder" communications systems.

11 McCarthy E [1988]. Present and future challenges of safety control. Proceedings of the 1988 IEEE Conference on Computer Assurance (Compass '88). P.1. National Institute for Standards and Technology.

12 The SAFECOM Program—Department of Homeland Security Version 1.0. Date accessed: June 2, 2004.

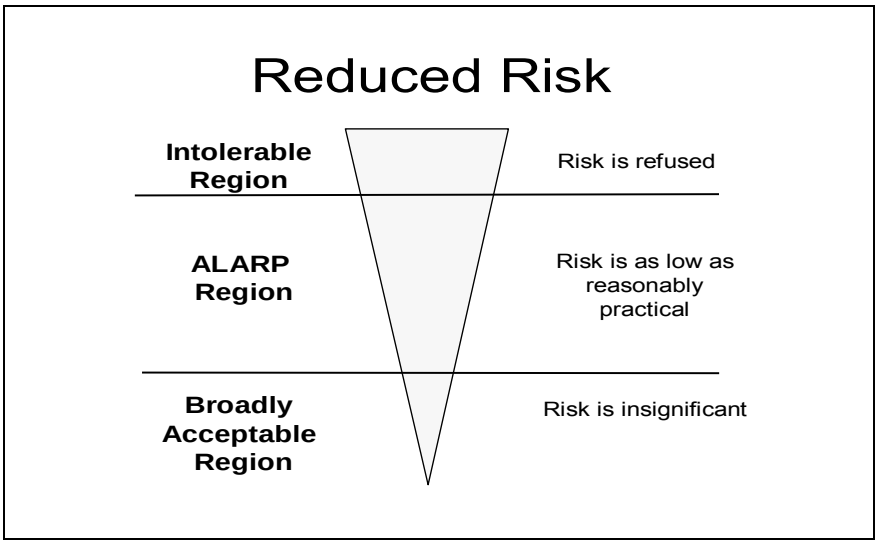

Figure 3 - The as low as reasonably practical (ALARP) principle

Suppose the city council has requested that the local fire chief look into the purchase of PPE to reduce loss of life in residential apartment fires. The local fire chief looks into purchasing specially equipped fire fighter vests and wireless monitoring/communication systems. To justify these acquisitions, he considers use in the context of the total system by identifying layers of protection and analyzing risk reduction. By conducting the analysis, the fire chief will be able to prepare a statement of requirements for the functional safety of the equipment to be purchased. The fire chief will also be able to report an expected risk reduction back to the city council.

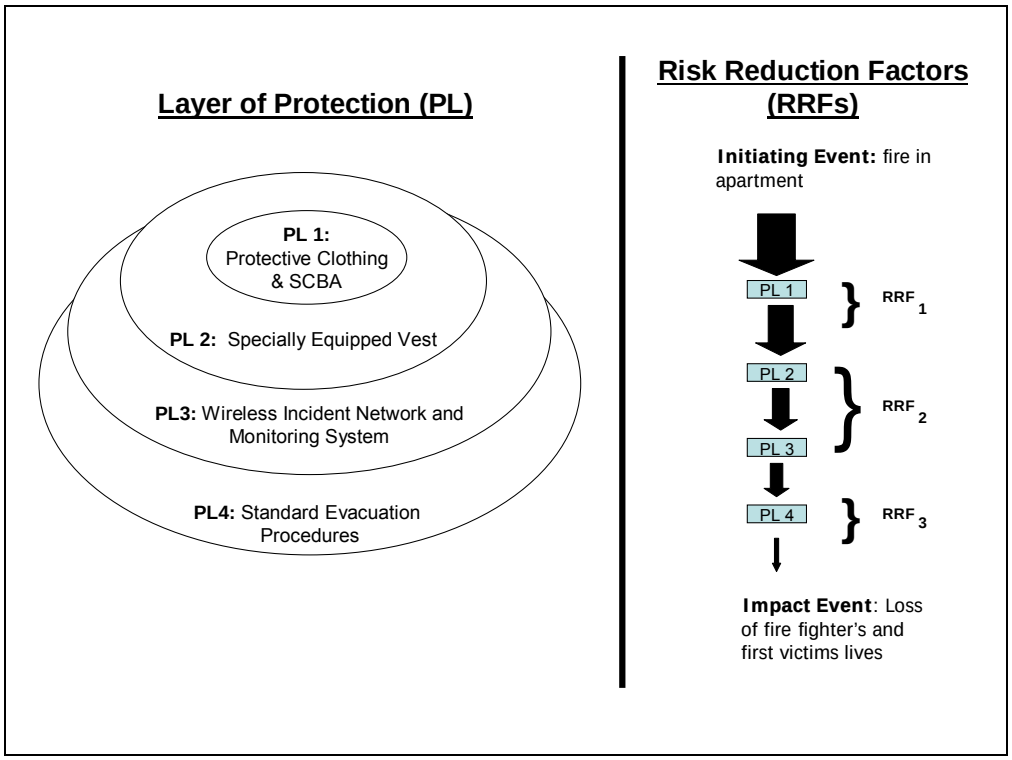

Figure 4 - Example identification of protection layers for reducing risk

Figure 4 shows the multiple protection layers (PLs) in place to protect the fire fighter as follows:

- **PL 1 –** Advanced nonflammable protective clothing and self-contained breathing apparatus (SCBA) to reduce the risk of death of the fire fighter due to high temperatures and loss of oxygen.

- **PL 2 –** Specially equipped vest that measures a firefighter's vital signs and senses the available air supply in the self-contained breathing apparatus (SCBA). The vest also provides ambient temperature data and geo-location information for each firefighter.

- **PL 3 –** Because apartment buildings are not always large enough to require a built-in wireless incident area network for emergency services, the protection layer includes self-organizing wireless network pods. Fire crews place these pods on each of the floors as they progress through the building. This enables

the fire crews to talk continuously with each other. It also transmits the vital data and location information for emergency responders and victims to multiple computer displays at the incident command post. Therefore, the computer display, the display management software, and the wireless communications provide a third PL for the emergency responder.

- **PL 4 –** The fire chief and EMS professionals monitor the computer displays and issue evacuation orders in accordance with the standard operating evacuation procedures. The human-in-the-loop monitoring provides the fourth and final protective layer.

Each of these protective layers provides different degrees of risk reduction often referred to as Risk Reduction Factors or RRFs as described below:

- **PL1** has a risk reduction factor of RRF_1.

- **PL 2** and **PL 3** have a combined risk reduction factor of RRF_2, because even though they are separate products developed by different manufacturers, they are functionally dependent. That is, if PL 2 fails to transmit real-time data, then **PL 3** will not provide the necessary warnings and location information. Conversely, if **PL 2** transmits real-time data in accordance with the specification and **PL 3** does not handle it correctly then **PL 3** will not provide the necessary warnings and location information.

- **PL 4** may or may not fail if **PL 2** or **PL 3** fails. Since **PL 4** is functionally independent, it has a separate risk reduction of RRF_3.

For some types of equipment, such as, industrial process control equipment, the engineer specifies values of these factors numerically based on field experience data. However, for PPE, it is difficult if not impossible to obtain valid usage data thus the determination of RRF values uses a qualitative approach. Figure 5 provides a risk graph approach to qualitatively determining RRFs proposed by the NFPA Electronic Systems Committee for PPE. PPE environmental exposure and life-criticality are the two primary factors used in the risk graph for identifying the RRF

Category.

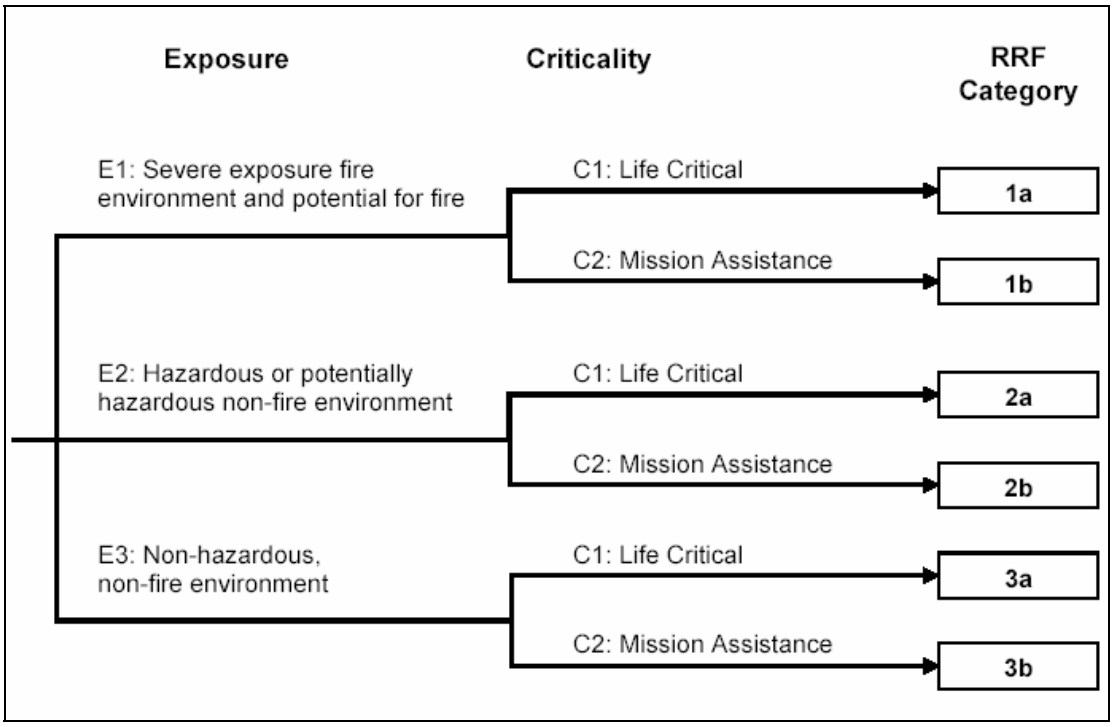

Figure 5 - NFPA proposed risk reduction categories

For the above example, the following risk reduction categories would apply:

- PL 1 would need to meet the requirements of RRF Category 1a to achieve an acceptable risk reduction. Thus, RRF_1 equals the risk reduction provided by Category 1a requirements.
- PL 2 would also need to meet the requirements of RRF Category 1a.
- At first glance, PL 3 would need to meet the requirements of RRF Category 2b. However, since PL 2 and PL 3 are functionally dependent, PL 3 would need to meet the RRF Category 2a. Thus, RRF_2 equals the risk reduction provided by Category 1a requirements plus Category 2a requirements.
- Any equipment used to implement PL 4 procedures would need to meet the appropriate category depending on its exposure and criticality, and whether other

safety functions were functionally dependent on it. Thus, RRF_3 equals the risk reduction provided by the combined category requirements.

When a single piece of equipment provides multiple safety functions, the RRF category is based on the safety function with the severest exposure and criticality.

The residential fire example illustrates that the electronics, embedded software, application software, and computer hardware must perform acceptably to prevent loss of firefighter's and victim's lives. Failure of any of these components or these interfaces may lead to harm, especially if emergency responders are relying on these systems. The following section highlights the more significant challenges to reducing life safety risk using electronics and software.

3.0. ENGINEERING FOR FUNCTIONAL SAFETY

"How does one address the safety of this system? By making the system more reliable, employing redundancy, or conducting extensive testing? All of these are necessary, but are not sufficient to ensure safety. Making a system more reliable is not sufficient if the system has unsafe functions. What could result is a system that reliably functions to cause unsafe conditions! Employing redundancy is not sufficient if both redundant parts are not safe. Testing alone is not sufficient for safety. Studies show that testing does not find all of the "bugs," and some systems are too complex to test every condition. The key to safety is to "design in" safety early in the design by looking at the entire system, identifying hazards, designing to eliminate or reduce hazards, and doing this over the system life cycle[13]."

3.1. The Functional Safety Life Cycle

The functional safety life cycle concept can be traced back to 1947. In following a functional safety life cycle, the manufacturer takes a systems approach by designing and building safety into the entire system from initial conceptualization to retirement.

13 NIOSH [2001]. Programmable electronic mining systems: best practices recommendations (in nine parts). Part 1: Introduction. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Information Circular 9456. p.2.

The concept now addresses the safety of complex electronics and software based systems. Leveson [1995] states: "The primary concern of the safety life cycle is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures." The functional safety life cycle emphasizes:

- Integrating safety into the design,
- Systematic hazard identification and analysis
- Addressing the entire system in addition to the subsystems and components
- Using protection layers for risk reduction
- Qualitative and quantitative approaches

To achieve functional safety, manufacturers construct and implement a safety life cycle suitable for each application.

Figure 6 shows a functional safety life cycle. The safety life cycle activities require active participation from and interaction with product engineers, electronic engineers, system analyses, software developers, quality assurance/testing professionals, and users. The development team must be familiar with the intended use of the product, taking into account the environment in which it will operate. Early and continuing participation from the user provides information about how the user plans to use the system and under what conditions.

3.1.1. Project Plan

This activity involves the development of a project plan that addresses the entire life cycle including development and use activities, management of change activities, and the documentation of safety. Updating the project plan occurs throughout the life cycle.

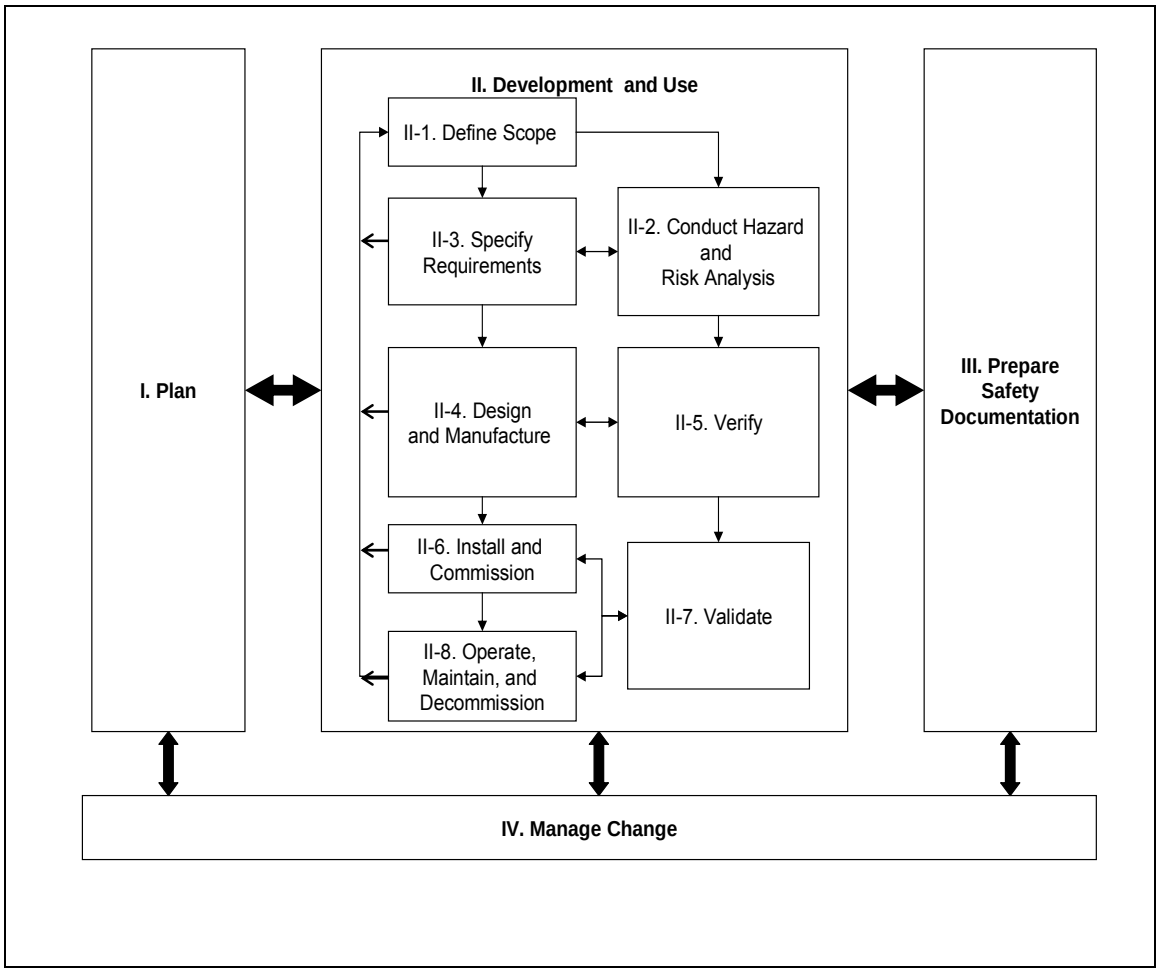

Figure 6 - A functional safety life cycle

.

3.1.2. Development and Use of Project Plan

Development and use activities include standard product engineering activities plus additional activities that address safety as follows:

- Define Scope - Scope definition provides an understanding of the application, the conceptual equipment design, equipment interfaces and the overall functionality of the system. Determination of the boundaries between the equipment under control, the control system, and the people using the equipment establish the scope.

- Conduct Hazard and Risk Analysis - The second activity involves identifying

hazards, analyzing event sequences leading to hazardous events and determining risks associated with these events. Risk analysis determines the risk reduction requirement for the equipment or system based on qualitative or quantitative approaches.

- Specify Requirements - Achieving functional safety involves identifying safety functions and specifying design and performance requirements associated with these safety functions. This activity considers the equipment scope, the protection layers provided by other equipment and systems, and apportions the overall risk reduction requirements to the safety functions.

- Design and Manufacture - Designing and manufacturing the equipment to meet the required specifications is the fourth activity. The efficient, safe operation of a system requires that the design of all components consider the equipment scope and its context of use.

- Verify - The activity includes design for safety reviews, such as, checking consistency among requirements and reviewing software design for compliance with safe computing practices. It also includes test and verification of all components and sub-systems, such as, electronic devices, power supplies, sensors, data communication paths, actuators, and software. 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 addresses interaction problems among components.

- Install and Commission - The act of installing and commissioning equipment or a system may incur safety risks. Therefore, requirements for installation and commissioning include safety practices.

- Validate - The seventh activity occurs in parallel to the sixth and eighth activities. It validates that the installation meets the equipment or systems requirements during commissioning and throughout operation and maintenance.

- Operate, Maintain, and Decommission - Operate and maintain the equipment or system for continuing functional safety. As with installation and commission, the act of decommissioning may involve safety risks.

3.1.3. Prepare Safety Documentation

Preparation of safety documentation occurs throughout the equipment or system life cycle. It provides a documented body of evidence that communicates a convincing and valid argument that a system is adequately safe for a given application in a given environment. The safety documentation is a living document and may be known as the "Technical File," the "Safety Case," the "Safety Argument," the "Safety Assessment Report," or the "Safety Justification."

3.1.4. Manage Change

Management of change activities address, among other things, the handling of requirement changes, feature modification, platform modification, and scope creep. For all changes, the repeating of the appropriate steps in the safety life cycle occurs to address the safety impact of the change.

3.2. Design and Performance of Electronics and Software

Products and systems that use electronics and software technologies to deliver functions are often more complex than their predecessors. For example, a monitor that once measured the presence of a single gas is now multi-functional and measures the presence of multiple gases. A LED display in a fire fighter's facemask displays remaining oxygen levels in an SCBA tank. A personal alert safety system device, in addition to emitting audible alarms, now communicates location information back to a command center. Increased complexity may also result from additional features that codify safety decisions thus introducing the potential for design inadequacies. For example, the oxygen monitoring equipment could indicate "get out" based on the amount of oxygen remaining. Consequently, the PPE design engineer now focuses on this complexity by addressing how non-performance of the electronics and software components affects the proper functioning of the operational product.

Given the failure properties of electrical and mechanical components, data is available

to support accurate reliability estimates. There is also a large body of engineering expertise on how to prevent failures, when they may occur if not preventable, and what the failure effects are. Engineering consensus based on carefully collecting failure data underpins the test specifications in NFPA and other basic safety standards. The situation also applies to wear-out failures in electronics components.

On the other hand, failures of electronics and software due to design and logic inadequacies and environmental effects may be subtle with failure modes not yet well characterized. This results in a seemingly sporadic manifestation of failure effects. For PPE, the product design engineer now considers both the potential for failures due to random phenomena and failures due to design or systematic phenomena. The *IEC 61508* standard uses the following definitions:

Random hardware failure - "A failure occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware[14]."

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[15]."

Operating environments contribute to random failure of electronic components by affecting electronic function. Interference from outside sources, such as electromagnetic emissions; temperature extremes; humidity, moisture, and water exposure; heat and flame exposure; chemicals, dust, and debris, and extreme impacts can corrupt electronically maintained data and software instruction processing.

Systematic failures result from inadequacies in the design and logic. These include design errors such as incorrect software algorithms and interfaces; coding errors, including syntax, incorrect signs, endless loops and the like; timing errors that can cause program execution to occur prematurely or late, latent errors not detectable until a given set of conditions occur; and failure of the system to perform any function at all. Systematic failures affect functional safety in two ways: 1) output values and/or timing

14 IEC 61508-4, Functional safety of electrical/electronic/programmable electronic safety-related systems. 2002 Nov. Available from URL: [http://www.iec.ch/zone/fsafety/fsafety_entry.htm]. Date accessed: June 2, 2004.

15 Ibid, page 39.

that permit the system to reach a state that could lead to a mishap or 2) failure to identify or properly handle hazardous events to which it must respond[16]. A systematic failure in a software component that converts values from an analog pressure gauge to facemask readout of oxygen remaining could result in a potential mishap for the emergency responder. Suppose that the failure is due to a scaling mistake in the software logic so that the value displayed shows more oxygen remaining than actually available in the tank. Further suppose that all other electrical (e.g., battery connection), electronics (e.g., LEDs, microprocessor), and software components (e.g., logic to flash the display when the amount of oxygen remaining is becoming critical) are working properly. Achievement of functional safety does not occur in this situation as not all components are functioning properly. Thus, the functional chain is only as strong as its failing link.

3.3. Configurability, Compatibility/Interoperability, and Scalability

In addition to addressing the design and performance of PPE at the individual level, life safety objectives include systems-level protection goals. Examples of systems-level protection activities include communications, location monitoring, and hazard monitoring. To achieve systems-level protection, PPE must be easy to configure, and be interoperable and scalable as follows:

3.3.1. Configurability goals specify the requirements for rapidly configuring a PPE system to meet different life safety threats and to account for different user needs. An example of a configurability goal is to require “configuration control” or standard specification of PPE component dimensions and interfaces, such as integrating LED based status indicator displays into facemasks.

3.3.2. Compatibility/Interoperability goals address the need for equipment developed for different uses or by different manufacturers to work together. This involves 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. Interoperability goals range from

16 Leveson N [1995]. Safeware: System safety and computers. Addision-Wesley.

addressing battery replacement in hand-held devices to open architecture standards for voice, data, and video communication systems. Radios provide an example of interoperability goals from specifying compatibility of jacks and other components among different radio unit models to allowing multiple parties to exchange information seamlessly.

3.3.3. Scalability goals identify requirements for PPE when scaling up a system to respond to threats which cross-jurisdictional boundaries. To achieve scalability in a practical manner involves coordination among emergency responder teams as well as the ability to transport equipment from one location to another. Achieving scalability, for example, may require mutual aid agreements among neighboring localities that resolve equipment overlap and sharing.

3.4. Usability and Human Computer Interaction (HCI)

"Why do people make mistakes when operating safety-critical systems? What is it that makes someone misread a display, ignore a warning signal, or press the wrong button? To the world outside the situation, it can look like dangerous stupidity or gross negligence. Yet close inspection of cases of considered human error often reveals that the problem was linked more closely to design than operation[17] …."

The integration of electronics and software into PPE, although desirable for improving life safety, still must pass the test of usability by emergency responders. For example, for personal alert safety system (PASS) devices, fire fighters have raised the following usability considerations:

- The distress sounds of the PASS devices mixed in with the ambient sounds and thus were difficult to isolate.
- Rapid intervention teams were unable to localize the alert tone immediately and had to rely on a standard search pattern.
- False activations lowered the arousal state of firefighters.

17 Redmill F [1997]. Human factors in safety-critical systems: Introduction to human computer interaction in safety-critical systems. Oxford, England, Butterworth-Heinemen, pp 99.

- Devices failed to sound during a flashover or rapid-fire progress[18].

Usability considerations are not unique to equipment incorporating electronics and software, nor are they unique to PPE PASS devices. Small control knobs on radios and helmets interfering with SCBA gear are two non high-technology examples. Gas monitors that display too much data or data that requires too much interpretation also limits usability.

3.5. Maintainability

Addressing maintainability of electronics and software in PPE for emergency responders introduces additional factors for consideration. Environmental exposure, cleaning effects, inadequate power supply, and field changes all affect the performance of electronics and software functions. Achieving continuing functionality and hence functional safety warrants consideration of the following maintainability aspects:

3.5.1. Exposure to environmental parameters

Emergency responder use of PPE expose the equipment and systems to heat, flames, temperature extremes, corrosion, abrasion, liquids, chemicals, gases, puncture, cutting, tearing, and mechanical shocks. Additionally, these PPE may be stored in emergency responder vehicles increasing the likelihood of environmental degradation.

3.5.2. Cleaning effects

PPE require some form of cleaning. Cleaning garments may require the removal of electronic components from a garment. Cleaning raises questions, such as:

Could the increased difficulty in performing cleaning functions due to integration of devices cause users to fail to properly maintain and clean the garment?

Can removed PPE be properly and easily re-installed?

Would preventing damage to the device during cleaning require the revision of garment maintenance and cleaning instructions?

18 Adams D, [2001]. Distress alert signals from personal alert safety systems do not trigger physiological responses. National Fire Academy. Available from URL: [http://www.usfa.fema.gov/pdf/efop/tr_01da.pdf]. Date accessed: June 2, 2004.

3.5.3. Adequacy of power supply

Electronic devices require sustaining power in that the performance is susceptible to power fluctuations and degradation. Different equipment has different power requirements. For example, infrared cameras or goggles may only need to last as long as a SCBA (1 hour), while a PASS device should last for up to 3 days.

3.5.4. Management of change

Changes in versions of sensors, actuators, software, firmware, integrated circuits, circuit boards and other components may result in life safety compromises. Labels and markings on electronics and software will need to provide unique version identification.

3.5.5. Premature failure

Integration of electronics may also result in premature failure at stress or wear points. For example, incorporating electronics in a garment may reduce the physical protection provided by the garment by creating openings and by compromising the strength of materials used. As a result, the garment may no longer meet existing requirements in PPE design and performance standards.

4.0. AN APPROACH TO ACHIEVING FUNCTIONAL SAFETY

Functional safety is “part of the overall system that depends on a system or equipment operating correctly in response to its inputs[19].” Emergency responders want their PPE to function as intended. Products and systems that use electronics and software technologies to deliver functions are often more complex than their predecessors. This results in consideration of additional design and test requirements.

4.1. The Functional Safety Framework

The Functional Safety Framework shown in Figure 7 provides one approach to demonstrating functional safety achievement for advanced personal protective equipment and systems (PPE) for emergency responders. It joins the significant issues described in Section 3 of the report with current design and test requirements so that a

19 See definition at International Electro-technical Commission functional safety zone [http://www.iec.ch/zone/fsafety]. Date accessed: June 2, 2004.

roadmap to achieving coverage is readily discernable.

The approach begins with specifying functional safety goals for the PPE. The functional safety goals are broadly stated goals associated with issues identified in the previous sections of the report. Combining coverage of these goals with specific design and testing requirements provides a mechanism for both building on existing compliance requirements and identifying the need for additional safety requirements.

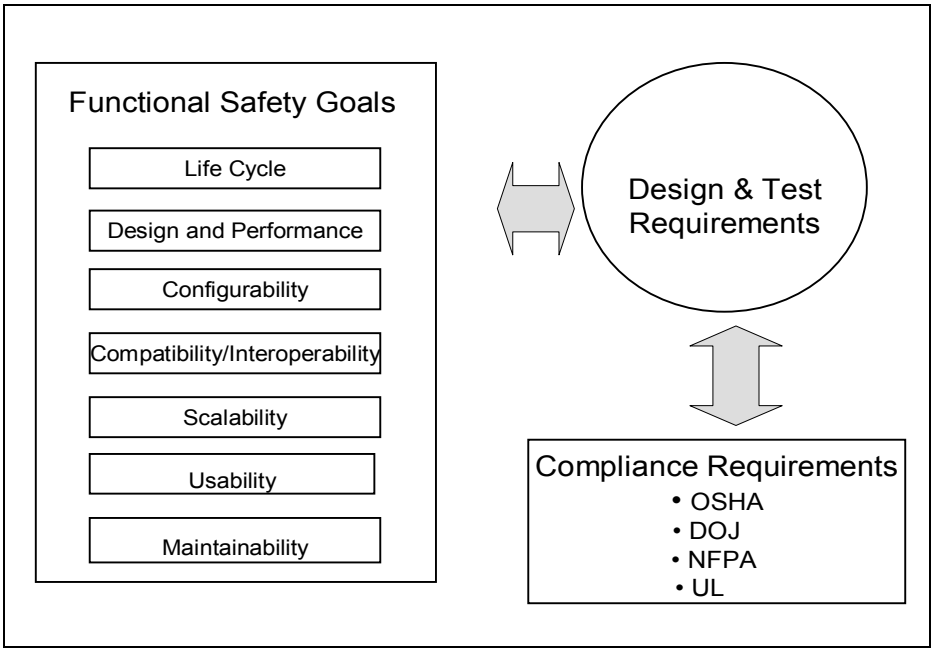

Figure 7 - A functional safety framework

For example, the electronic pedometer located on the vest of a emergency responder identified as PL 2 in Section 2 provides the following safety function:

- Locate the emergency responder to within a ten-foot tolerance and display this information on the incident commander's monitor within ten seconds.

Achieving the RRF category specified for this safety function requires that specific design and test requirements be met. Figure 8 illustrates the path through the Functional Safety Framework for the requirements of water resistance and software integrity. The path culminates in identifying the safety requirements as shown in Figure 9.

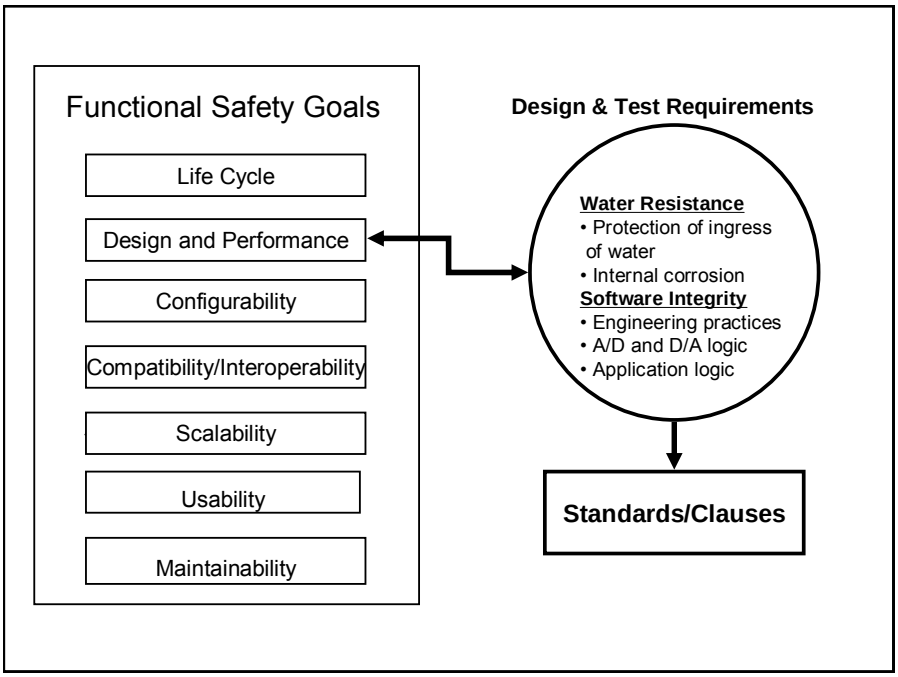

Figure 8 - Example path through Functional Safety framework

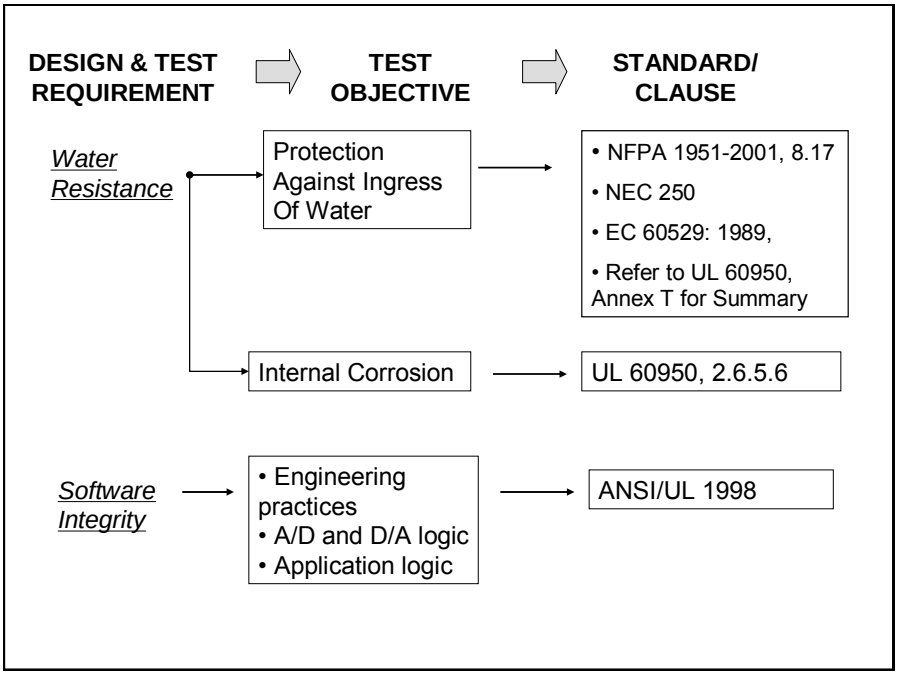

Figure 9 - Design and test requirements for example path

5.0 BENEFITS OF EXPERIENCES AND RISK REDUCTION

Other industries have confronted the issue of building safe products that use electronics and software to implement safety-related functionality but unforeseen mishaps have still occurred. In an effort to avoid making the same mistakes, it is worthwhile for PPE manufacturers to consider the root causes of mishaps experienced by other industries. Additionally, reduced total life cycle costs are achievable when manufacturers implement risk reduction practices that contribute to functional safety achievement starting early in the life cycle.

5.1. Experiences of Related Industries

5.1.1. United States Chemical Safety and Hazard Investigation Board

The Chemical Safety and Hazard Investigation Board[20] investigates chemical mishaps and determines their root causes. The root causes typically result from deficiencies in safety management systems and often involve equipment failures, human errors, and unforeseen chemical reactions. The Alabama Interlock Failure mishap of September 2002 is an example of a control system mishap[21]. The mishap resulted from a failure in an emergency shutdown system (ESD) to control logic based on hard wiring and software that safeguarded the operational integrity of the entire plant. The ESD provided interlocks to the manufacturing process with the supply feed trains and other indicators, such as concentration of materials, temperature and pressure. A design error in the ESD system software blocked the interlocks from functioning properly in special cases.

5.1.2. National Institute for Occupational Safety and Health (NIOSH) Pittsburgh Research Laboratory and U.S. Mine Safety and Health Administration (MSHA) Automated Mining Equipment Partnership

NIOSH has conducted investigations of accidents with long wall mining and remotely controlled continuous mining machines. One study conducted by NIOSH analyzed incident reports from Japan, U.S. and Sweden. The study found that of 104 incidents,

20 For additional information, see [http://www.chemsafety.gov/]. Date accessed: June 2, 2004.

21 See Chemical safety and hazard investigation board, incident number 2002-5953 for further detail.

8% resulted in deaths, 38% resulted in injury and 54% resulted in near injury. Through this analysis and additional discussion, it was determined that the potential for injury was higher in the following situations:

- A person switching the machine to automatic operation.
- Another control circuit inputting a switching signal.
- A bug or error in the control software.
- A hardware failure.
- Automatic restart after a power interruption.
- Electromagnetic interference.

An initial study in 1990 by MSHA addressing System Safety Applications in mining, found that 20 out of 57 automated long-wall mining installations visited had experienced unplanned movement. These and subsequent mishaps surfaced concern about electronics and software used in mining applications. For example, one mishap involved software not removing a manually entered program function command after initiation of an automatic override function command. Because of this study, MSHA issued recommendations for the following areas:

- Operator training
- Timely maintenance
- Maintaining integrity of enclosure sealing
- Maintaining alertness for abnormal operational sequences which might be indicative of a software programming problem

Subsequent to this initial study, additional safety concerns associated with long-wall shields resumed in 1994. Failure to conduct timely maintenance and inadequate

operator training contributed to the identified mishaps[22].

5.1.3. EPA Study of Leading Causes of Chemical Accidents

EPA and OSHA investigations of chemical plant accidents identified five common causes of accidents[23]:

1. Inadequate hazard review or process hazard analysis –these methods either did not identify all process hazards or did not occur at all.
2. Inadequate hazard analysis and inadequate management of change procedures when upgrading processes to improve health and safety by installing pollution control equipment.
3. Use of inappropriate or poorly designed equipment - in several mishaps the equipment was inappropriate or not in accordance with current standards.
4. Inadequate indications of process condition - process instrumentation did not provide operators with indications needed to identify unsafe process conditions.
5. Warnings went unheeded - as history repeatedly shows, a series of smaller mishaps often precede major disasters.

5.1.4. NASA Study

A study by Lutz 1992 [24]on National Aeronautics and Space Administration software

---

22 Dransite GE [2000]. System safety applications in mining. Presented at the 18th International System Safety Conference. Fort Worth, TX. For the complete paper, see [http://www.msha.gov/s&hinfo/techrpt/electrical/syssafeapp.pdf]. Date accessed: June 2, 2004.

23 For a brief summary, see [http://www.isa.org/Content/ContentGroups/InTech2/Departments/Safety1/200123/Safety_study_IDs_leading_causes_of_accidents.htm]. Date accessed: June 2, 2004.
The entire report is viewable at [http://www.denix.osd.mil/denix/Public/Intl/MAPP/Dec99/Belke/belke.html].

24 Lutz RR [1992]. Analyzing software requirements errors and safety critical, embedded systems. In: Proceedings of the Software Requirements Conference, pp. 99 106.

found that most problems with safety-related software came from misunderstandings and discrepancies in the requirement specification, i.e., inaccuracies, inadequacies, or confusion in defining the behavior that the computer-controlled equipment is desired to have.

5.1.5. UK Health and Safety Executive Study

A study by the Health and Safety Executive (HSE)[25] in the United Kingdom (UK) of 34 mishaps involving processor control in industrial applications, found that 44.1% of the causes were attributed to the safety requirement specification (see Figure 10). At 20.6%, changes after commissioning were the second leading cause of mishaps. For example, a software modification after installing and operating equipment unknowingly introduced hazards.

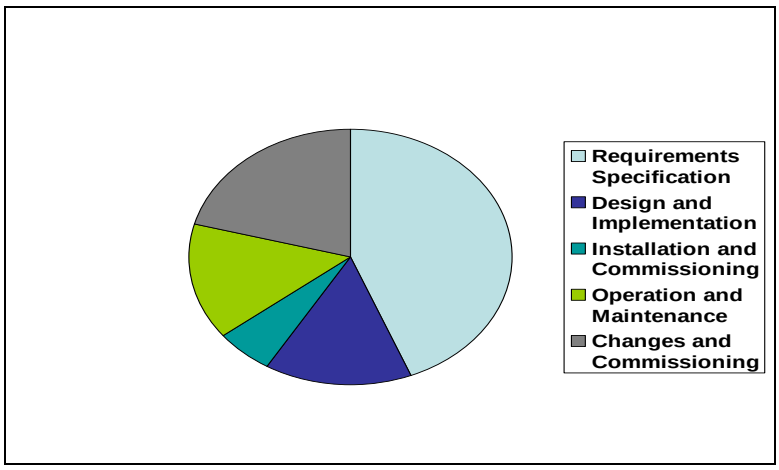

Figure 10 - Analyses of 34 mishaps in UK HSE study.

5.2. Early Risk Identification Contributes to Reduced Life Cycle Costs

For computer-controlled equipment, early identification of risk helps to isolate potential safety concerns, thereby eliminating the costs associated with making design changes later in development. Early risk identification also builds the foundation for streamlined on-going functional safety compliance as upgrades occur. Figure 11[26] shows that

25 Health and Safety Executive [1995]. Out of control: why control systems go wrong and how to prevent failure. Sheffield, U.K.: Health and Safety Executive.

26 From "Impact of Change During Development and Operational Phases, Figure 6". Sammarco, John 2001. Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts) Part 1: 1.0 Introduction, p. 9.

changes made early in the life cycle are easier and less costly to make.

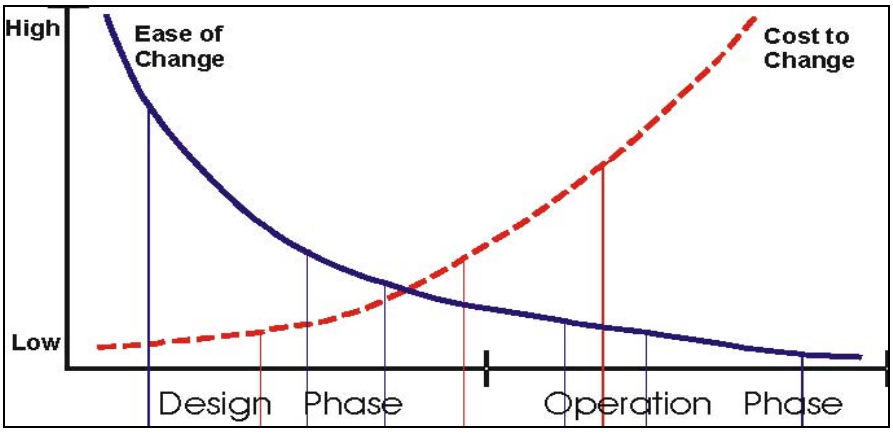

Figure 11 - Ease and cost of making changes by life cycle phase.

5.3. Benefits for Emergency Responders and PPE Manufacturers

Responding to the lessons learned from other industries and tailoring guidelines accordingly, may be of benefit to the PPE industry. The following lists highlight some of the possible benefits.

5.3.1. Emergency Responders

- Improves worker safety
- Provides a uniform and systematic approach to safety management
- Improves design and reliability to increase operational safety and effectiveness
- Facilitates communication

5.3.2. Emergency Responder Unit Managers

- Better control of emergency responder exposure to hazardous situations
- Improves feedback channels to address safety issues and training

requirements

- Reduces field modifications (improved safety specification, resulting in a better design)
- Higher uptime
- Enhances support from manufacturer

5.3.3. Equipment manufacturer

- Reduces likelihood of hazardous initial and future designs
- Problems identified quickly (provides better diagnosis)
- Reduces product liability costs (safer design)
- R&D provided with qualitative and quantitative focus for new product development (reduced false starts and reduced development of unnecessary devices)
- New business opportunities presented due to safer designs
- Lowers design change and support costs

6.0. 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.

Achieving functional safety for PPE requires a system “Design for safety” approach that addresses electronics, software, mechanical, chemical and other functionality, human behavior, and the operating environment over the equipment’s life cycle. This report stresses the need for integrated safety engineering, from conception through decommissioning. It introduces important considerations for identifying best practices. Implementation of best practices may also lead to a reduction in total life cycle costs.

Part 1 provides an overview of functional safety concepts for advanced personal protective equipment and discusses the need to address them.

7.0 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

8.0 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 emergency 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.