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

(In Nine Parts)

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

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.

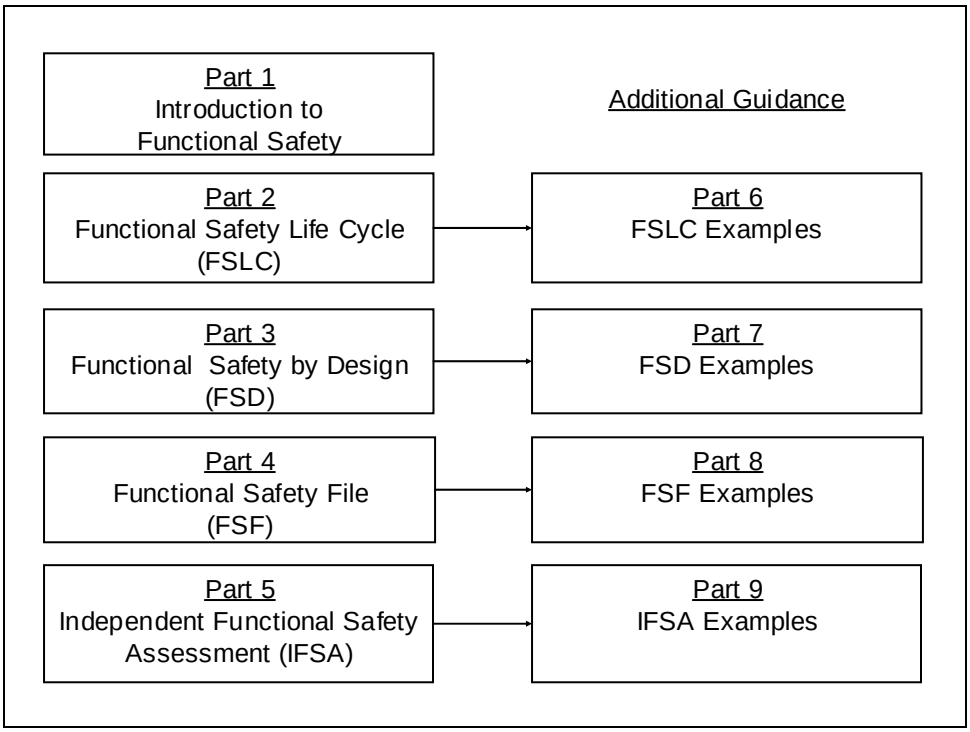


Figure 1 - The functional safety report series.

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 the intended application.

Part 5: Independent Functional Safety Assessment (IFSA)

---

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

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

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

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

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

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

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

- Part 6 – Additional Guidance: Functional Safety Life Cycle Examples are used to develop the Scope of the Project Plan. The scope guides Project Functional Safety by Design (FSD) Compliance and Project Documentation.
- Part 7 – Additional Guidance: Functional Safety by Design Examples drives Project Design for Safety Compliance, which then becomes part of the Project Documentation.
- Part 8 – Additional Guidance: Functional Safety File Examples help to complete the Project Documentation, to enable a third party assessment.
- Part 9 – Additional Guidance: Independent Functional Safety Audit Examples are employed in the development of the Third Party Assessment Report. Figure 2 overviews the relationships among Parts 6, 7, 8, and 9.

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

Many manufacturers are ISO 9001 compliant as a result of requirements in NFPA codes and standards, follow Six Sigma approaches, and are using the Department of Defense (DoD) Software Engineering Institute (SEI) Capability Maturity Model (CMM) to improve

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

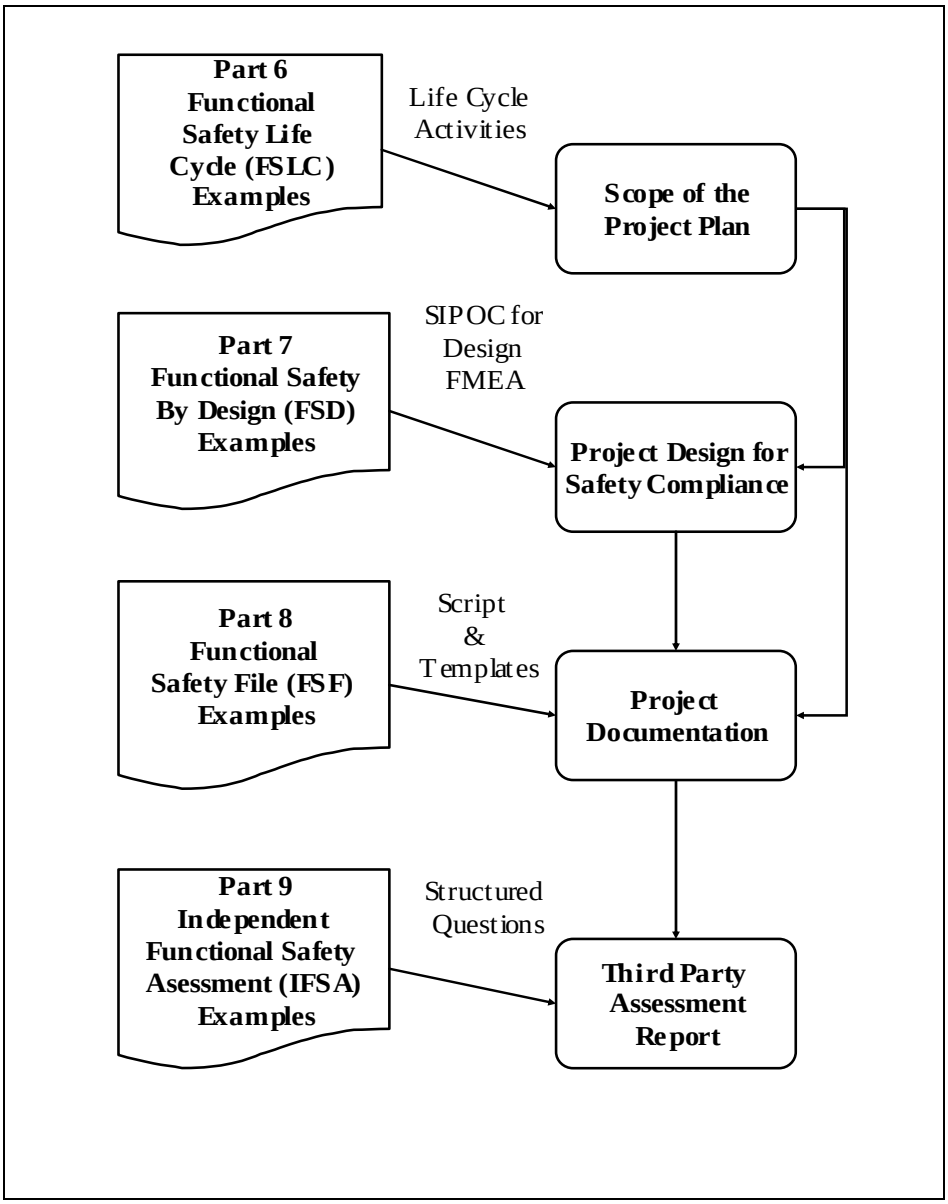


Figure 2 - Relationships among Parts 6, 7, 8, and 9

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

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

Analysis (FSA) for person locator functions embedded in the DKYS components. The illustration addresses the conduct of a Job Hazard Analysis (JHA), a Hazard Analysis (HA), a Design Failure Modes and Effects Analysis (Design FMEA), and a Risk Analysis (RA). The report also references tools for conducting a Design FMEA.

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

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

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

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

Intended Scope of Application

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

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

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

Intended Users

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

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

Relevance of the Guidelines

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

Reference Guidelines and Standards

Mining industry guidelines prepared by NIOSH, MSHA and the mining industry manufacturers and entitled *Programmable Electronic Mining Systems: Best Practices Recommendations (in Nine Parts)* serves as a basis for these guidelines. Table 2 lists the published documents that form part of the mining industry guidelines. These documents can be found at http://www.cdc.gov/niosh/mining/topics/topicpage23.htm.

The mining guidelines are based on the requirements in existing standards—two of which are particularly applicable to PPE. These standards are the *ANSI UL 1998, Standard for Safety: Software in Programmable Components and IEC 61508, Functional Safety: E/EE/PE Safety-Related Systems*. Table 3 provides an overview of

both standards.

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

Table 1 - Mining Industry Guidelines

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

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

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

Table 2 - Overview of ANSI UL 1988 and IEC 61508

ACKNOWLEDGEMENT

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

ABSTRACT

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

Advanced Personal Protective Equipment (PPE) incorporates product-ready technology in electrical, electronic, and programmable electronics. Use of newer materials, software, and wireless communications reduce safety risks. Experience has shown though, that these personal protective technologies may fail in ways not previously anticipated. Therefore, guidance for their use and integration is necessary.

The report, 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.

The report, Additional Guidance: Functional Safety Life Cycle (FSLC) Examples is Part 6 in the nine-part series of recommendations addressing the functional safety of advanced personal protective equipment (PPE) for emergency responders. As the companion document to Part 2, Part 6 describes activities which make up a FSLC.

1.0. INTRODUCTION

1.1. Report Scope

The report, Additional Guidance: Functional Safety Life Cycle (FSLC) Examples is Part 6 in the nine-part series of recommendations addressing the functional safety of advanced personal protective equipment (PPE) for emergency responders.

As the companion document to Part 2, Part 6 describes activities which make up a Functional Safety Life Cycle (FSLC). It provides a reusable FSLC Project Management Template (FSLC- PMT) that may be followed by both new and seasoned manufacturers of PPE. By following the template, manufacturers address the practicality and relevance of each activity specified for the project being considered.

Part 6 also introduces a hypothetical yet realistic case study of a next generation Electronic Safety Equipment product, code-named DKYS for Device that Keeps You Safe. The names and events depicted in the case study are purely fictional. They do not identify any particular product, company or situation.

The proposed National Fire Protection Association (NFPA) Standard 1800 for Electronic Safety Equipment (ESE) for Emergency Services [4] states that PPE manufacturers must be ISO 9001:2000 compliant. Part 6 identifies the relationship between FSLC recommended practices and ISO 9001:2000 requirements.

Additionally, some PPE manufacturers have adopted Six Sigma approaches to better meet the needs of their customers, reduce equipment defects, and minimize costs. These manufacturers are leading the way in using the Six Sigma tools for continued product safety achievement. Part 6 identifies Six Sigma tools that may be applied throughout the FSLC.

To reduce the potential for design inadequacies in electronics and software, some

[4] Proposed National Fire Protection Association (NFPA) Standard 1800 for Electronic Safety Equipment for Emergency Services (Pre-ROP Draft – 17 November 2006), Section 4.5. For further detail, see http://www.nfpa.org . Date accessed:September 20, 2007.

manufacturers follow the United States Department of Defense (DoD) Software Engineering Institute (SEI) Capability Maturity Model (CMM) approaches. These approaches parallel those of Six Sigma. Part 6 introduces the application of these approaches to safety.

2.0. 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

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

3.0. GLOSSARY

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

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

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

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

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

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

Electronic Safety Equipment: Products that contain electronics embedded

in or associated with the product for use by emergency services personnel that provides

enhanced safety functions for emergency services personnel and victims during emergency incident operations (from NFPA 1800).

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

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

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

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

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

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

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

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

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

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

Hazard and risk analysis team: The group of emergency responders, electrical, electronics, computer hardware/software, manufacturing, and safety specialists responsible for the safety and integrity evaluation of PPE from its inception through its implementation and transfer to operations to meet corporate safety guidelines.

Hazard List: A list used to identify for tracking hazards throughout the FSLC. The list describes each hazard in terms of the event (s) that would lead to an accident scenario. When the hazard is identified during an accident analysis, the description of the hazard will also reference the accident scenario and consequences and measures that may be taken to avoid or prevent recurrence. The hazard list is used as input to the FMEA.

Human-computer interaction: The application of ergonomic principles to the design of human-computer interfaces.

Human-machine interface: The physical controls, input devices, information displays, or other media through which a human interacts with a machine in order to operate the machine.

Independent department: A department whose members are capable of conducting an IFSA. The department must be separate and distinct from the departments responsible for the activities and subject to Functional Safety Assessment or validation, taking place during the specific phase of the FSLC.

Independent functional safety assessment (IFSA): A systematic and independent examination of the work processes, design, development, testing, and safety file documentation for a product/machine/control system to determine compliance with applicable safety recommendations/standards/regulations.

Independent organization: An organization that is legally independent of the development organization whose members have the capability to conduct IFSAs. The organization member conducting the audit must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent person: A person who is capable of conducting an IFSA. The person must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent protection layer (IPL): Engineered safety features or protective systems or layers that typically involve design for safety in the equipment, administrative procedures, alarms, devices, and/or planned responses to protect against an imminent hazard. These responses may be either automated or initiated by human actions. Protection should be independent of other protection layers and should be user and hazard analysis team approved.

Internal assessment: Conducted by the manufacturer to determine that the design and development process continues to comply with the safety plans and the safety file procedures. A report is issued and reviewed by appropriate management personnel.

Interoperability: The ability of PPE equipment and systems to provide services to and accept services from other PPE equipment and systems and to use the services so exchanged to enable them to operate effectively together.

Layer of protection analysis (LOPA): An analysis that identifies risk reduction targets by evaluating selected risk scenarios.

Lean Manufacturing: Implementing steps to reduce waste during the manufacturing process. There are eight types of waste – defects, overproduction, waiting, unused talent, transportation, inventory, motion, and extra processing.

Maintainability: The ability to maintain a PPE with minimum maintenance and repair so that the PPE can remain in service with full operation.

Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Periodic follow-up safety assessment: A systematic, independent, and periodic assessment which determines if the functional safety of the PPE is maintained.

Personal alert safety system (PASS): Devices that sense movement or lack of movement and that automatically activate an audible alarm signal to alert others in locating an emergency responder.

Personal protection equipment (PPE): Equipment and systems that provide the following life-safety protection functions:

- Protection against thermal, abrasion, puncture wounds, respiratory, vision, hearing and limited chemical and biological pathogen exposure hazards
- Monitoring of physiological, chemical, biological, and environmental parameters
- Communication among emergency responders and between emergency responders and victims

PPE functional requirements: Functions provided by the application including those functions required to meet NFPA equipment safety requirements.

PPE performance requirements: Timing and resource constraints imposed by the application including constraints needed for safety performance, such as delivering data

to the user within the time frame required.

Preliminary hazard analysis (PHA): This technique uses the results of PHL, lessons learned, system and component design data, safety design data, and malfunction data to identify potential hazard areas. In addition, its output includes ranking of hazards by severity and probability, operational constraints, recommended actions to eliminate or control the hazards, and perhaps additional safety requirements.

Preliminary hazard list (PHL): This is the first analysis performed in the system safety process and strives to identify critical system functions and broad system hazards. It uses historical safety data from similar systems and mishap/incident information hazard logs to guide the safety effort until more system-specific is developed.

Probability of failure on demand (PFD): A value that indicates the probability of a system failing to respond on demand. The average probability of a system failing to respond to a demand in a specified time interval is referred to as "PFD avg."

Project plan: A document that addresses the entire life cycle including development and use activities, management of change activities, and the documentation of safety. The project plan is updated throughout the life cycle.

Proven In Use: The component is considered reliable because it has been used in several products in the application over a period of time and reliability data is available for the component.

Random hardware failure: A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Rapid fire progression: A rapid rise in temperature that leads to an almost instantaneous combustion of materials over a larger area.

Record: Stating results achieved or providing evidence of activities performed.

Requirements Specification: A list of PPE requirements where each requirement is uniquely identified, traceable, and has safety performance criteria specified.

Retrospective Validation: Validation after the ESE has been fielded which is based on review of development documentation and testing and on field problem reports.

Risk analysis: Determination of the risk reduction requirement for the equipment or system based on qualitative or quantitative approaches.

Risk management summary: Details the risk management activities and summarizes the important risks identified and the means used to remove or mitigate them.

Risk reduction factor (RRF): Measure of the amount of risk reduced through implementation of safety equipment, training, and procedures. RRF is usually expressed as a reduction in the risk of loss of life.

Risk Priority Number (RPN): A number which establishes the priority for addressing the risk. RPN is computed based on severity, probability, and detectability. The higher the number obtained the higher the priority for addressing the potential failure.

Safety: Freedom from unacceptable risks.

Safety claims: A safety claim is a statement about a safety property of the PPE, its subsystems and components.

Safety integrity: The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period.

Safety Policy: A statement which describes in general the organizational commitment to safety and how safety issues will be addressed.

Safety statement: A succinct summary statement affirming the completeness

and accuracy of the FSF and the level of safety demonstrated for the PPE.

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

Scalability: The ability to scale up PPE to respond to threats, which cross jurisdictional boundaries.

Suppler Input Process Output Customer (SIPOC) Diagrams: Diagrams which show suppliers, the required input, the steps in a process, the output produced, and the customer of that output.

Systematic failure: A failure related to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors. Examples of systematic failures include design errors in interfaces and algorithms, logic/coding errors, looping and syntax errors, and data handling errors.

Traceability: Ability to trace the history, application or location of that which is under consideration.

Usability: Ease of use of the PPE. Usability is specified by stating performance requirements that define what users expect to accomplish.

Validation: Analysis, review, and test activities that establish that the PPE is built in accordance with the emergency responder needs. Did we build the right PPE?

Verification: Analysis, review and test activities that establish that the PPE is built in accordance with the PPE specifications. Did we build the PPE right?

Voice of the Customer (VOC): Six Sigma methods for collecting data on the desires and expectations of the customer. These methods include focus groups, surveys, websites, customer site visits, and interviews with distributors and/or retailers, current and lost customers.

Appendix A – Project Management Tools identifies resources/tools that support the management of the FSLC.

3.1. Functional Safety Life Cycle Project Management Template (FSLC-PMT)

The Functional Safety Life Cycle Project Management Template (FSLC-PMT) provides a comprehensive list of recommended practices. Project managers may use the FSLC-PMT as guidance for planning and managing activities associated with the development and deployment of electronics technology in a PPE product. The PPE product functionality and the project's scope would dictate the subset of the practices shown in the FSLC-PMT to be followed.

Companies may choose to standardize on the FSLC-PMT as an initial baseline for corporate best practices. Use of the FSLC-PMT minimizes the potential for overlooking practices which are critical to functional safety achievement. Overlooking these practices may lead to delays in getting the product to market. It may take several project experiences before the FSLC-PMT is optimized for a specific company and product line. Project management tools such as those identified in Appendix A may be used to support the practical implementation of a standardized and optimized FSLC-PMT.

3.2. An Integrated Approach

The FSLC-PMT integrates best practices from functional safety standards such as, ANSI/UL1998 Standard for Safety: Software in Programmable Components[5] and IEC 61508: Functional safety of E/EE/PE safety related systems[6] , and quality systems

[5] ANSI UL 1998 Standard for Safety: Software in Programmable Components. For further detail, see http://www.ul.com/software/ansi.html. Date accessed September 20, 2007.

[6] IEC 61508 Functional safety of E/EE/PE safety related systems. For further detail, see http://www.iec.ch/61508. Date accessed September 20, 2007.

approaches such as ANSI/PMI Project Management Standard 99-001-2004[7], ISO 9001:2000 Quality Systems Management requirements[8], and Six Sigma[9] practices. The FSLC-PMT can also serve as an initial baseline for process improvement because it identifies practices consistent with those defined at the highest level of maturity according to the United States Department of Defense (DoD) and the Federal Aviation Administration (FAA) integrated Capability Maturity Model (iCMM). The iCMM extends the DoD Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for safety and security.

3.2.1. ANSI/PMI Project Management Standard 99-001-2004

The organization of the FSLC-PMT follows the five key process groups identified in the American National Standards Institute (ANSI)/ Project Management Institute (PMI) Standard 99-001-2004.[10] These five process groups are:

- Initiating – Activities which define and authorize the project or a project phase
- Planning – Activities which define and refine objectives and plan the course of action required
- Executing – Activities which bring together resources related to executing the project
- Closing – Activities which involve formal review and acceptance of the project or project phase to bring it to an orderly completion
- Monitoring and Controlling - Project management activities for monitoring and measuring variances from the project scope and plan (Critical milestones or

[7] ANSI/PMI Project Management Standard 99-001-2004. For further detail, see http://www.pmi.org. Date accessed September 20, 2007.

[8] ISO 9001:2000 Quality Management Systems. For further detail, see http://www.iso.org . Date accessed September 20, 2007.

[9] For further detail, see http://www.asq.org/sixsigma. Date accessed September 20, 2007.

[10] ANSI/PMI Project Management Standard 99-001-2004, For further detail, see http://www.pmi.org. Date accessed September 20, 2007.

review gates are considered for monitoring and controlling activities.)

Tables 2, 3, 4, 5 and 6 define FSLC-PMT practices for each of the five key process groups. The descriptions provide references to ISO 9001:2000 requirements, identify both six sigma and functional safety methods that may be applied, and bring in electronics and software considerations.

3.2.2. ISO 9001:2000 Quality Management System Practices and ISO 9003:2004.

Proposed NFPA1800[11] requirements state that manufacturers shall have a quality management program and that the system that is used to implement the program shall be registered to ISO 9001 by a registrar accredited in personal protection equipment. The scope of the registration shall include at least the design and manufacturing systems management for the type of PPE being certified.

The ISO 9001:2000 Quality Management System standard requires the adoption of a process approach that increases the likelihood that customer requirements are met. A process approach provides the advantage of on-going control among the individual activities and the communications between and among activities. Within the ISO 9001: 2000 framework, the addition of an activity is carefully considered for value added and if added, objectively measured in terms of process performance and effectiveness.[12]

The work of the ISO/IEC Joint Technical Committee 1 (JTC1)/ Subcommittee 7 (SC7) develops standards for software and system engineering[13] provides additional standards and guidance for engineering software based systems. Specifically,

---

[11] Proposed National Fire Protection Association (NFPA) Standard 1800 for Electronic Safety Equipment for Emergency Services (draft 9). For further detail, see http://www.nfpa.org . Date accessed: October 31, 2006.

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

[13] ISO/IEC JTC 1 SC 7 Software and System Engineering see http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=40&scopelist=PROGRAMME

JTC1/SC7 prepared the contents of the ISO/IEC 90003-2004 Guidelines for the application of 9001:2000 to computer software Standard. [14] The standard provides requirements for managing and controlling software and systems engineering processes.

3.2.3. Six Sigma Recommended Practices

Six Sigma recommended practices address the reduction of product defects to "near perfect". A defect is anything that does not meet a customer's requirement. The recommended practices include recently developed management tools and proven tools that have been used since the 1940s. These practices reduce variation in the development process and hence reduce defects in the delivered product. Near perfect is defined by the measure of interest being less than or equal to six standard units from average. For example, a measure of interest may be number of defective products fielded. In this case, six sigma means the number of defective parts would be less than 3.4 parts per million.

The Six Sigma recommended practices can be divided into three basic parts, with each part focusing on basic processes used by an organization. These processes are:

- Process design/redesign
- Process management
- Process improvement

They are sometimes referred to as the three engines of Six Sigma[15].

The value of the six sigma recommended practices for developing PPE is that their application during the various project management phases supports the reduction and

---

[14] ISO/IEC 90003-2004 Guidelines for the application of 9001:2000 to computer software. For further detail, see http://www.iso.org/iso/en/ISOOnline.frontpage. Date accessed October 31, 2006.

[15] Peter S. Pande, Robert P. Neuman, and Rolande R. Cavanagh. The Six Sigma Way Team Fieldbook: An Implementation Guide for Process Improvement Teams. New York: McGrawHill. 2002. ISBN:0-07-137314-4.

elimination of product defects which if fielded could lead to a hazard. The “near perfect” goal corresponds to reducing risk of equipment failing in an unsafe manner to “as low as is reasonably practical”. The FSLC-PMT lists the applicable six sigma methods for each of five process groups: initiating, planning, executing, closing, and monitoring and controlling.

3.3. Improving Best Practice Capability

3.3.1. U.S. DoD and the FAA Integrated-Capability Maturity Model (iCMM)

In the 1980’s, a United States Department of Defense initiative set an objective of improving the quality of the delivered software-based systems purchased from contractors. The objective was to develop criteria that could be used by software development teams to:

1) appraise ability to perform their software process successfully
2) provide guidance to improve their process capability

Initially, the criteria were questioned for their value-added, but today there is much supporting evidence that applying the criteria reduces cost, schedule, and technical risks. In addition, applying the criteria supports reduction of mistakes, inclusion of best practices, and standardizations of tasks. The criteria, now identified as the Capability Maturity Model Integrated® (CMMI®)[16],[17], provide guidance for improving organizational performance. Organizational performance can be measured and improved by comparing actual practice to essential practices contained in the CMMI. The DoD/SEI has also developed a guide for assessment named SCAMPI℠ for Standard CMMI® Appraisal Method for Process Improvement[18].

---

[16] CMMI Product Team, CMMI for Development, CMMI-DEV, (Version 1.2), CMU/SEI-2006-TR-008. CMMI is a registered trademarks of the Department of Defense Software Engineering Institute. For further detail, see http://www.sei.cmu.edu/cmmi/models. Date accessed October 31, 2006.

[17] CMMI Product Team, CMMI for Acquisition, CMMI-AM, Version 1.1, CMU/SEI-2005-TR-011. For further detail, see http://www.sei.cmu.edu/cmmi/models Date accessed October 31, 2006.

[18] SCAMPI Upgrade Team, Standard CMMI® Appraisal Method for Process

Following the CMMI guidance typically yields clearly defined design and development processes; however these processes may not have included the best practices for functional safety achievement identified in safety standards.

Recently, the U.S. Department of Defense and the United States Federal Aviation Administration have extended the CMM criteria to include criteria for system engineering practices for applications with safety and security requirements. The approach is identified as the FAA – integrated CMM (FAA-iCMM)[19] with safety and security extensions[20]. The FAA-iCMM has six defined levels that can be used to gauge how capable a manufacturer is in implementing specific practices. Each level has practices that must be in place to advance to that level. These levels are defined in Columns 1 and 2 of Table 3.

3.3.2. Application to PPE

Defining a complete iCMM as a reference model for functional safety of PPE is beyond the scope of the report series. Column 3 of Table 3 does provide examples of each level for an FSLC.

An ISO 9001:2000 compliant process would most likely satisfy many of the practice requirements associated with Capability Level 2: Managed, Planned and Tracked and Capability Level 3 Defined by the FAA-iCMM. However, it is important to note that a high level of process capability neither guarantees ISO 9001: 2000 compliance nor PPE product safety compliance (e.g. compliance to NFPA standards).

Improvement (SCAMPI) A, Version 1.2: Method Definition Document, CMU/SEI-TR-06hb002. For further detail, see http://www.sei.cmu.edu/cmmi/models Date accessed October 31, 2006.

[19] Federal aviation Administration Integrated Capability Maturity Model (FAA-iCMM) Version 2.0, Federal Aviation Administration, September 2001. For further detail, see http://www.faa.gov/about/office_org/headquarters_offices/aio/business_value/iCMM/index.cfm. Date accessed October 31, 2006.

[20] Safety and Security Extensions for Integrated Capability Maturity Models, Federal Aviation Administration, 2004. For further detail, see http://www.faa.gov/about/office_org/headquarters_offices/aio/business_value/iCMM/index.cfm. Date accessed October 31, 2006.

The FSLC-PMT includes best practice recommendations consistent with ISO 9001:2000 compliance and the Capability Level 5 of the FAA-iCMM. Optimization of processes for PPE that reduce safety risks to as low as is reasonably practical, seems warranted. The recommended practice tables provided in the following sections include Capability Level 5 practices.

Table 3 - Defined levels of capability for the FAA-iCMM with FSLC examples

Capability Level	Definition	FSLC Examples
0 Incomplete	An incomplete process is either not performed or partially performed. One or more of the goals of the process area are not achieved.	The FMEA is conducted but does not consider failures due to systematic faults.
1 Performed	A performed process is a process that achieves the goals of the process area. Base practices of the process area are generally performed.	The FMEA is performed by following ad hoc approaches. A Supplier Input Process Output Customer (SIPOC) chart is not defined.
2 Managed, Planned, and Tracked	A managed process is a performed process that is also planned and tracked. The process is managed to ensure its institutionalization, and to ensure the achievement of specific objectives for the process, such as customer satisfaction, cost, schedule, and quality objectives.	The Project Manager (PM) identifies the FMEA as a process step in the FSLC for the project. He or she plans for and tracks the adherence to the documented SIPOC and the progress made, instituting corrective actions when necessary. The PM checks that the design FMEA considers all customer functional safety requirements by reviewing the Job Safety Analysis (JSA) and the requirements specification including use cases..
3 Defined	A defined process is a managed, planned and tracked	Experiences in following the FMEA SIPOC

Capability Level	Definition	FSLC Examples
	process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to the organization's process assets.	are communicated from one project to the next through lessons learned repositories, PM forums, and training.
4 Quantitatively Managed	A quantitatively managed process is a defined process that is controlled using statistical and other quantitative techniques.	The effectiveness of the FMEA SIPOC is measured using the quantity and severity of reported design inadequacies prior to and after product release to the customer.
5 Optimizing	An optimizing process is a quantitatively managed process that is changed and adapted to meet relevant current and projected business objectives.	Feedback from measuring the effectiveness of the FMEA is used to improve the SIPOC checklists that underpin the FMEA.

.

4.0. FSLC-PMT

4.1. Project Initiating Activities Template

Table 4 - Project Initiation Practices provides an example template showing recommended practices for initiating a PPE project. Project Initiation Practices define and authorize the project or a project phase. The table also identifies cross-references to ISO 9001:2000 requirements.

Table 4 - Project Initiation Practices

Task Id	Task	ISO 9001:2000 Clause
1	**PROJECT INITIATION PRACTICES**	
1.1	*Research Market*	*7.2.1 Product Realization - Determination of Requirements Related to the Product*
1.1.1	Identify project stakeholders	7.2.3 Product-Realization -Customer Communication
1.1.2	Define needs for PPE using Outcome-Driven Data Acquisition Methods	7.2.1 Product Realization- Determination of Requirements Related to the Product
1.1.3	Review and analyze field data for predecessor and related products	7.2.1 Product Realization - Determination of Requirements Related to the Product

Task Id	Task	ISO 9001:2000 Clause
1.2	*Scope Project*	7.2.1 Product Realization - Determination of requirements related to the Product 7.3.2 Product realization Design and development – Design and development inputs
1.2.1	Define project charter	7.2.1 Determination of requirements related to the Product
1.2.2	Identify and justify governing Safety Policy and Procedures.	4.1QMS General Requirements 5.1 Management Responsibility: Management Commitment 5.2 Management Responsibility: Customer Focus 5.3 Management Responsibility: Quality Policy

4.2. Project Planning Activities Template

Table 5 - Project Planning Practices provides an example template showing best practice recommendations for planning an ESE project. Project Planning practices define and refine project objectives and plan the course of action required. The table also identifies cross-references to ISO 9001:2000 requirements.

Table 5 - Project Planning Practices

Task Id	Task	ISO 9001:2000 Clause
2	**PLANNING**	
2.1	*Define FSLC*	*4.1 Quality Management Systems -General Requirements*
2.1.1	Identify project life cycle	4.1 Quality Management Systems - General Requirements 5.4 Management responsibility - Planning
2.1.2	Prepare a Critical to Quality Tree for the project life cycle	4.1 Quality Management Systems - General Requirements 5.4 Management responsibility – Planning
2.1.3	Create chart showing work breakdown structure and project schedule	4.1 Quality Management Systems - General Requirements
2.1.4	Determine Infrastructure Requirements	6.3 Resource management - infrastructure

Task Id	Task	ISO 9001:2000 Clause
2.1.4.1	Determine work environment requirements	6.4 Resource management – work environment
2.1.4.2	Determine tooling/platforms requirements	6.3 Resource management - infrastructure
2.1.4.3	Determine design and production standards to be followed	7.3.2 Product realization Design and development – Design and development inputs
2.1.4.4	Determine purchasing processes	7.4 Product Realization -Purchasing
2.2	*Specify documentation requirements*	*4.2 QMS- Documentation requirements* 5.4 Management responsibility - Planning
2.2.1	Scope of quality/safety management system	4.2.2 QMS-Documentation requirements -Quality Manual 5.4 Management responsibility - Planning
2.2.2	Records and documentation required by applicable standards	4.2.1 QMS- Documentation requirements – General 5.4 Management responsibility - Planning
2.2.3	Engineering documentation	4.2.1 QMS- Documentation requirements - General
2.2.4	Planning, operation, and control	4.2.1 QMS- Documentation requirements –

Task Id	Task	ISO 9001:2000 Clause
	documentation	General
2.2.5	How documents will be controlled	4.2.3 QMS- Documentation Requirements – Control of documents
2.2.6	How records will be controlled	4.2.4 QMS- Documentation Requirements – Control of records
2.3	*Select Project Staff*	*6.2.Resource Management – Human Resources*
2.3.1	Identify skills needed	6.2.2 Resource Management – Human Resources- Competence awareness and training
2.3.2	Prepare summary of staff qualification requirements	6.2.2 Resource Management – Human Resources- Competence awareness and training
2.3.3	Identify project-specific training requirements	6.2.2 Resource Management – Human Resources- Competence awareness and training
2.3.4	Establish project organizational structure	6.1 Resource Management – Provision of Resources
2.3.6	Recruit and hire staff using staff qualification requirements	6.2.1 Resource Management – Provision of Resources -General
2.3.7	Stipulate internal communication processes	5.5.3 Responsibility Authority and Communication – Internal Communication
2.3.8	Define and communicate responsibility and authority	5.5.1 Responsibility Authority and Communication – Internal Communication – Responsibility and authority

Task Id	Task	ISO 9001:2000 Clause
2.3.8.1	Identify management representative	5.5.2 Responsibility Authority and Communication – Internal Communication – Management Representative
2.4	*Prepare Project Plans and Procedures*	*7.1 Product Realization: Planning of Product Realization*
2.4.1	Prepare QMS Plan	5.4 Management responsibility - Planning
2.4.2	Prepare Project Management Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*
2.4.3	Prepare Specification/Design Development Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*
2.4.4	Prepare Review, Verification and Validation Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*

Task Id	Task	ISO 9001:2000 Clause
2.4.5	Prepare Production Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*
2.4.6	Prepare Maintenance and Decommissioning Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*
2.4.7	Prepare Management of Change Plan	7.1 *Product Realization: Planning of Product Realization* 7.3.1 *Product Realization – Design and development – Design and development planning*

4.3. Project Execution Practices Template

Table 6 - Project Execution Practices provides an example template showing best practice recommendations for executing a PPE project. Project Execution Practices bring together resources related to executing the project. The table also identifies cross-references to ISO 9001:2000 requirements.

Table 6 - Project Execution Practices

Task Id	Task	ISO 9001:2000 Clause
3	**Project Execution Practices**	
3.1	**Research and Develop PPE**	**7.3 Product realization: Design and development**
3.1.1	*Specify PPE Requirements*	*7.2 Product realization – Customer-related processes* *7.3.2 Product realization Design and development – Design and development inputs* *7.3.3 Product realization Design and development – Design and development outputs*
3.1.1.1	Identify Equipment Functions from JSA and use case descriptions	7.2.1 Product realization – Customer-related processes – Determination of requirements

Task Id	Task	ISO 9001:2000 Clause
		related to product 7.2.3 Product realization – Customer-related processes – Customer communication
3.1.1.2	Determine PPE Safety and Performance Requirements and establish traceability to PPE Functions	7.3.5 Product realization Design and development – Design and development verification
3.1.1.3	Document PPE Requirements in a requirements specification which includes a requirements traceability matrix or database	7.3.3 Product realization Design and development – Design and development outputs
3.1.2	*Design PPE using best practices*	7.3.2 Product realization Design and development – Design and development inputs
3.1.2.1	Design PPE by allocating the requirements to subsystems	7.3.2 Product realization Design and development – Design and development outputs
3.1.2.2	Identify subsystem architectures showing materials, electrical, electronics/hardware, software/firmware, and mechanical components and their interfaces	7.3.2 Product realization Design and development – Design and development outputs
3.1.2.3	Identify Component Function, Safety, and	7.4 Purchasing

Task Id	Task	ISO 9001:2000 Clause
	Performance Criteria	
3.1.2.3.1	Decide on Buy vs. Build	7.4.1 Purchasing – Purchasing Process
3.1.2.3.2	Establish Components List	7.4.2 Purchasing – Purchasing Information 7.4.3 Purchasing – Verification of purchased product
3.1.2.4	Document PPE Design in a design specification	7.3.2 Product realization Design and development – Design and development outputs
3.1.3	*Build/Assemble Prototype*	*7.3.2 Product realization Design and development – Design and development outputs*
3.1.3.1	Build/Assemble Components	7.3.2 Product realization Design and development – Design and development outputs 7.4 Purchasing
3.1.3.2	Build/Assemble Subsystems	7.3.2 Product realization Design and development – Design and development outputs 7.4 Purchasing

Task Id	Task	ISO 9001:2000 Clause
3.1.3.3	Build/Assemble Equipment	7.3.2 Product realization Design and development – Design and development outputs 7.4 Purchasing
3.1.3.4	Implement Equipment/Subsystem/Component Identification and Traceability Scheme	7.3.5 Design and Development – Design and development verification 7.3.2 Product realization Design and development – Design and development outputs 7.5.3 Production and service provision – Identification and traceability
3.1.3.5	Identify, verify, protect, and safeguard customer property	7.5.4 Production and service provision – customer property
3.1.4	*Verify and Validate PPE*	7.3.5 Design and Development – Design and development verification 7.3.6Design and Development – Design and development validation 7.6 Control of monitoring and measuring devices
3.1.4.1	Design, Build, and Validate Design and Test	7.3.5 Design and Development –

Task Id	Task	ISO 9001:2000 Clause
	Platforms	Design and development verification 7.3.6Design and Development – Design and development validation 7.6 Control of monitoring and measuring devices
3.1.4.2	Verify Equipment, Subsystem, and Component Requirements	7.3.5 Design and development – Design and development verification
3.1.4.4	Verify Equipment, Subsystem, and Component Designs	7.3.5 Design and development – Design and development verification
3.1.4.4	Verify Software Components, Assemblies and Subsystems	7.3.5 Design and development – Design and development verification
3.1.4.5	Analyze and Test Component, Subsystem, and Prototype	7.3.5 Design and Development – Design and development verification 7.3.6Design and development – Design and development validation
3.1.4.6	Conduct Failure Modes and Effects Analysis for each hazard identified by the Hazard Analysis	7.3.5 Product realization Design and development – Design and development verification
3.2	**Manage Change**	**7.3.7 Design and development – Control of design and development changes**

Task Id	Task	ISO 9001:2000 Clause
3.2.1	*Establish traceability from hazards to functions to test*	*7.5.3 Production and Service Provision – Identification and traceability*
3.2.2	*Track problem report closure*	*7.5.3 Production and Service Provision – Identification and traceability*
3.2.3	*Take Preventive and Corrective Action*	*8.5.2 Measurement, analysis and improvement- Improvement – Corrective action* *8.5.3 Measurement, analysis and improvement- Improvement – Preventive action*
3.3	**Produce Equipment using Lean Manufacturing Practices**	**7.5 Production and service Provision**
3.3.1	*Establish Equipment Production Processes*	7.5 Production and Service Provision
3.3.1.1	Specify manufacturing processes	7.5.1 Production and service provision – Control of production and service provision
3.3.1.2	Configure production line tools and equipment	7.4 Purchasing
3.3.1.3	Select and train manufacturing staff	6.1 Resource management – Provision of resources

Task Id	Task	ISO 9001:2000 Clause
		6.2.Resource management – Human resources
3.3.1.4	Establish Traceability of equipment assembly	7.5.3 Production and service provision – Identification and traceability
3.3.2	*Run Production Line*	*7.5 Production and service provision 7.6 Control of monitoring and measuring devices*
3.3.2.1	Implement Equipment Identification and Traceability Scheme	7.5.3 Production and service provision – Identification and traceability
3.3.2.2	Build/Assemble equipment to order or in batch	7.5 Production and service provision
3.3.2.3	Identify, verify, protect, and safeguard customer property	7.5.4 Production and service provision – customer property
3.3.3	*Validate Equipment by showing coverage of safety and performance requirements*	*7.3.3 Design and development - Design and development outputs 7.3.6 Design and development – Design and development validation 7.5.2 Production and service provision – Validation of processes for production and service provision*

Task Id	Task	ISO 9001:2000 Clause
3.3.3.1	Component Test	*7.3.3 Design and development - Design and development outputs 7.3.6 Design and development – Design and development validation 7.5.2 Production and service provision – Validation of processes for production and service provision*
3.3.3.2	Subsystem Test	*7.3.3 Design and development - Design and development outputs 7.3.6 Design and development – Design and development validation 7.5.2 Production and service provision – Validation of processes for production and service provision*
3.3.3.3	Equipment Factory Test/Burn In Testing	*7.3.3 Design and development - Design and development outputs 7.3.6 Design and development – Design and development validation 7.5.2 Production and service provision – Validation of processes for production and service provision*

Task Id	Task	ISO 9001:2000 Clause
3.3.3.4	Document Equipment Verification and Validation Processes	*7.3.1 Design and development - Design and development planning* *7.3.5 Design and development - Design and development verification* *7.3.6 Design and development – Design and development validation* *7.5.2 Production and service provision – Validation of processes for production and service provision*
3.3.4	*Manage Change in Production Processes*	*7.3.7 Design and development – Control of design and development changes*
3.3.4.1	Establish traceability	*7.5.3 Production and Service Provision – Identification and traceability*
3.3.4.2	Track problem report closure	*7.5.3 Production and Service Provision – Identification and traceability*
3.3.4.3	Update FMEA for each hazard identified by the hazard analysis	7.3.5 Product realization Design and development – Design and development verification

Task Id	Task	ISO 9001:2000 Clause
3.3.4.4	Take Preventive and Corrective Action	*8.5.2 Measurement, analysis and improvement- Improvement – Corrective action* *8.5.3 Measurement, analysis and improvement- Improvement – Preventive action*
3.4	Ship the equipment using packaging that preserves the equipment	**7.5.5 Production and service provision – Preservation of product**
3.5	**Install Equipment**	**7.5 Production and service provision**
3.5.1	*Equipment Field Test*	7.3.6 Design and Development – Design and development validation
3.5.2	Update FMEA for each hazard in the hazard list	7.3.5 Product realization Design and development – Design and development verification
3.6	**Operate Equipment**	**7.5 Production and service provision**
3.6.1	*Use Equipment*	*7.5 Production and service provision*
3.6.2	*Conduct routine field maintenance*	*7.3.7Design and development - Control of design and development*

Task Id	Task	ISO 9001:2000 Clause
		changes
3.6.3	*Elicit and handle customer complaints*	*7.2.3c Product Realization – Customer communication customer feedback , including customer complaints* *8.2.1 Measurement, analysis, and improvement – Monitoring and Measuring – Customer Satisfaction* *8.3 Measurement, analysis, and improvement – Control of nonconforming product*
3.6.4	*Submit problem reports*	*4.2.4 QMS – Control of records*
3.6.5	*Establish problem report closure*	*7.5.3 Production and Service Provision – Identification and traceability*
3.6.6	*Update Hazard Analysis and FMEA*	*7.3.5 Product realization Design and development – Design and development verification*
3.6.7	*Decommission*	*8.2.4Measurement, Analysis and Improvement – Monitoring and measurement of product*

4.4. Project Closing Practices Template

Table 7 - Project Closing Practices provides an example template showing best practice recommendations for closing an ESE project. The table also identifies cross-references to ISO 9001:2000 requirements.

Table 7 - Project Closing Practices

Task Id	Task	ISO 9001:2000 Clause
4	**Project Closing Practices**	**4 QMS**
4.1	*Archive Functional Safety File*	*4.2 QMS – Documentation Requirements*
4.2	*Prepare and Act on Lessons Learned*	*4.1 QMS – General Requirements* *8.5 Measurement Analysis and Improvement - Improvement*

4.5. Project Monitoring and Controlling Practices Template

Table 8 - Project Monitoring and Controlling provides an example template showing best practice recommendations for monitoring and controlling a PPE project. Project Monitoring and Controlling Practices monitor and measure variances from the project scope and plan. The table also identifies cross-references to ISO 9001:2000 requirements and Functional Safety File Documents.

Table 8 - Project Monitoring and Controlling Practices

Task Id	Task	ISO 9001:2000 Clause

Task Id	Task	ISO 9001:2000 Clause
5	**Project Monitoring and Controlling**	
5.2	**Management Reviews**	**8.1 Measurement, Analysis and Improvement - General**
5.2.1	*Hold Kick-off Meeting*	*7.3.4 Design and development – design and development review*
5.2.2	*Conduct Project Management Reviews using a Balanced Scorecard Approach*	*5.1 Management responsibility – management commitment* *5.6 Management responsibility – Management review* *8.4 Measurement, analysis and improvement – Analysis of data* *8.5.1 Improvement – Continual Improvement*
5.2.2.1	Compliance with Safety Policy	5.1 Management responsibility – management commitment
5.2.2.2	Data Collection, Measurement, and Effectiveness Management	4.1 Quality management system- General requirements 8 Measurement, analysis and improvement
5.2.2.3	Resource and Information Availability	4.1 Quality management system- General requirements 5.1 Management responsibility – management commitment

Task Id	Task	ISO 9001:2000 Clause
		6 Resource Management
5.2.2.4	Institute and Follow-up on Corrective Actions	4.1 Quality management system- General requirements
5.2.2.5	Assess control of outsourced processes	4.1 Quality management system- General requirements
5.2.2.6	Evaluate adequacy of Human Resources, Infrastructure and Work Environment	6.2 Resource management – human resources 6.3 Resource management – Infrastructure 6.4 Resource management – Work environment
5.2.2.7	Take Preventive and Corrective Action	8.5.2 Measurement, analysis and improvement – Improvement – Corrective action 8.5.3 Measurement, analysis and improvement – Improvement – Preventive action
5.2.3	*Production Management Reviews*	*5.1 Management responsibility – management commitment* *5.6 Management responsibility – management review* *7.5.1Production and service provision – Control of production and service provision*
5.2.3.1	Compliance with Quality/Safety Policy and Quality/Safety Objectives	5.1 Management responsibility – management commitment

Task Id	Task	ISO 9001:2000 Clause
5.2.3.2	Data Collection, Measurement, and Effectiveness Management	4.1 Quality management system- General requirements 8 Measurement, analysis and improvement
5.2.3.3	Resource and Information Availability	4.1 Quality management system- General requirements 5,1 Management responsibility – management commitment 6 Resource Management
5.2.3.4	Institute and Follow-up on Corrective Actions	4.1 Quality management system- General requirements
5.2.3.5	Assess control of outsourced processes	4.1 Quality management system- General requirements
5.2.3.6	Evaluate adequacy of Human resources, Infrastructure and Work Environment	6.2 Resource management – human resources 6.3 Resource management – Infrastructure 6.4 Resource management – Work environment
5.2.3.7	Take Preventive and Corrective Action	8.5.2 Measurement, analysis and improvement – Improvement – Corrective action 8.5.3 Measurement, analysis and improvement – Improvement – Preventive action
5.2.4	*Field Management Reviews*	*5.1 Management responsibility – management commitment*

Task Id	Task	ISO 9001:2000 Clause
		5.6 Management responsibility – management review
5.2.4.1	Compliance with Quality/Safety Policy and Quality/Safety Objectives	5.1 Management responsibility – management commitment
5.2.4.2	Data Collection, Measurement, and Effectiveness Management	4.1 Quality management system- General requirements 8 Measurement, analysis and improvement
5.2.4.3	Resource and Information Availability	4.1 Quality management system- General requirements 5,1 Management responsibility – management commitment 6 Resource Management
5.2.4.4	Institute and Follow-up on Corrective Actions	4.1 Quality management system- General requirements
5.2.4.5	Assess control of outsourced processes	4.1 Quality management system- General requirements
5.2.4.6	Evaluate adequacy of Human resources, Infrastructure and Work Environment	6.2 Resource management – human resources 6.3 Resource management – Infrastructure 6.4 Resource management – Work environment
5.2.4.7	Control of Non-Conforming Product	8.3 Measurement analysis and improvement –

Task Id	Task	ISO 9001:2000 Clause
		Control of non-conforming product
5.2.4.8	Take Preventive and Corrective Action	8.5.2 Measurement analysis and improvement – Improvement – Corrective action 8.5.2 Measurement analysis and improvement – Improvement – Preventive action
5.2.5	*Review Quality Management System*	*8.2.2 Measurement, analysis, and improvement - Monitoring and measurement – Internal Audit* *8.2.3 Measurement, analysis and improvement - Monitoring and measurement – Monitoring and measuring of processes*
5.3	**Control of infrastructure tools including monitoring and measuring devices**	**7.6 Product realization – Control of monitoring and measuring devices**
5.4	**Meetings with Stakeholders**	**5.1 Management responsibility – management commitment**
5.4.1	*Engineering team meetings*	*5.5.3 Management and responsibility – Responsibility, authority, and communication – Internal Communication*
5.4.2	*Voice of the customer meetings*	*5.1 Management responsibility – management commitment* *7.2.3 Product realization – Customer-related*

Task Id	Task	ISO 9001:2000 Clause
		processes – Customer communication
5.4.3	*Top management meetings*	*5.1 Management responsibility – management commitment*
5.4.4	*Certification organization meetings*	*5.1 Management responsibility – management commitment*
5.5	**Management Review Milestones (Gates)**	**8.2 Monitoring and measurement**
5.5.1	*Gate 1: Project Go/No Go*	*7.2.2 Product realization – Customer related processes – Review of requirements related to the product* *8.2 Monitoring and measurement*
5.5.2	*Gate 2: Initial Requirements Stability/Design Readiness Review*	*7.3 Design and development – Design and development review* *8.2 Monitoring and measurement*
5.5.3	*Gate 3: Second Requirements Stability/Design Readiness Review*	*7.3 Design and Development – Design and development review* *8.2 Monitoring and measurement*
5.5.4	*Gate 4: Design Stability/Prototype Readiness Review*	*7.3 Design and Development – Design and development review* *8.2 Monitoring and measurement*
5.5.5	*Gate 5: Prototype Completion/*	*7.3 Design and Development – Design and*

Task Id	Task	ISO 9001:2000 Clause
	Production Readiness Review	*development review* *8.2 Monitoring and measurement*
5.5.6	*Gate 6: Product Test Completion/Ship Readiness Review*	*7.3 Design and development – Design and development review* *8.2 Monitoring and measurement*
5.5.7	*Gate 7: Installation and Commissioning/Operational Readiness Review*	*7.3 Design and development – Design and development review* *8.2 Monitoring and measurement*
5.5.8	*Gate 8: Monitor Fielded Product*	*8.2.4 Monitoring and measurement – Monitoring and measuring of product*
5.5.9	*Gate 9: Project Closure Review*	*8.2 Monitoring and measurement*
5.6	**Independent Functional Safety Assessments**	**5.1 Management responsibility – management commitment** **7.2 Customer related processes** **8.2.2 Measurement analysis and improvement – Monitoring and measuring- Internal audit**
5.6.1	*Preliminary Independent Functional Safety Assessment (Preliminary IFSA)*	*5.1 Management responsibility – management commitment* *7.2 Customer related processes* *8.2.2 Measurement analysis and improvement – Monitoring and measuring- Internal audit*

Task Id	Task	ISO 9001:2000 Clause
5.6.2	*Initial Independent Functional Safety Assessment (Initial IFSA)*	*5.1 Management responsibility – management commitment* *7.2 Customer related processes* *8.2.2 Measurement analysis and improvement – Monitoring and measuring- Internal audit*
5.6.3	*Periodic Independent Functional Safety Assessments (Periodic IFSAs)*	*5.1 Management responsibility – management commitment* *7.2 Customer related processes* *8.2.2 Measurement analysis and improvement – Monitoring and measuring- Internal audit*

5.0. CASE EXAMPLE: DEVICE THAT KEEPS YOU SAFE (DKYS)

5.1. Overview of DKYS

To support the illustration of the examples in Parts 5 through 9, a hypothetical case study code named DKYS is developed and used. Protecting emergency responders requires that vital personal and surrounding safety information be communicated in real-time to responders and the unit or team commander.

To meet these needs, Responder Safety, Inc., a hypothetical firm, envisions that a viable solution would be a garment, a dickey; that is easily donned, lies flat against the wearer's body, and is held down by the weight of turnout gear. Accordingly, it would be worn under turnout gear at the emergency scene. The project is code-named DKYS, for Device that Keeps You Safe.

Figure 3 illustrates the initial DKYS concept, equipped with the following functions and features:

- Recordable audio warning signal that alerts wearer when to evacuate, employing a closed loop control
- Physiological sensors for measuring heart rate, core body temperature, and respiration rate
- Motion sensors for measuring pitch and yaw of the wearer. These sensors in combination provide information about the fire fighters physical position --- specifically is the emergency responder falling or has he or she already fallen?
- External electronic port for data communication to other emergency responders and the unit command
- Use of function keys to identify the emergency responder
- Communications from internal microcontroller to transmitting device in coat pocket are wireless, a la Blue Tooth, and able to have data encrypted
- Transceiver transmits to a mobile cell tower which relays to a unit commander's digital assistant

- Connection to transmitter is configurable for different transceivers
- Data is sent to command center but also saved in unit as backup
- Radio Frequency Identifier (RFID) tag for locating emergency responder
- Unit commander can enable error message popup-like notification of lost communication link, otherwise messages just display in warning part of screen
- Unit has capability to transmit vitals on same frequency on route that ambulance would pick up
- Day/night setting for application specific PDA
- Materials hold heat, e.g., light-weight TESS Mesh Thermal Enhancement Material – Fishnet or Nomex
- Washable covers, inexpensive, easily replaceable, made of moisture wicking material

It cannot be over-emphasized, regarding any approach to emergency responder safety, that the comprehensiveness of the emergency responder's DKYS, the adequacy of the visor display, and the effectiveness of the unit commander's digital assistant play crucial roles in communicating safety information in real-time.

Responder Safety, Inc.'s expertise is in the manufacturing of emergency responder turnout gear and suits and accordingly would hire an embedded system design team for the design and implementation of the electronic control system for DKYS.

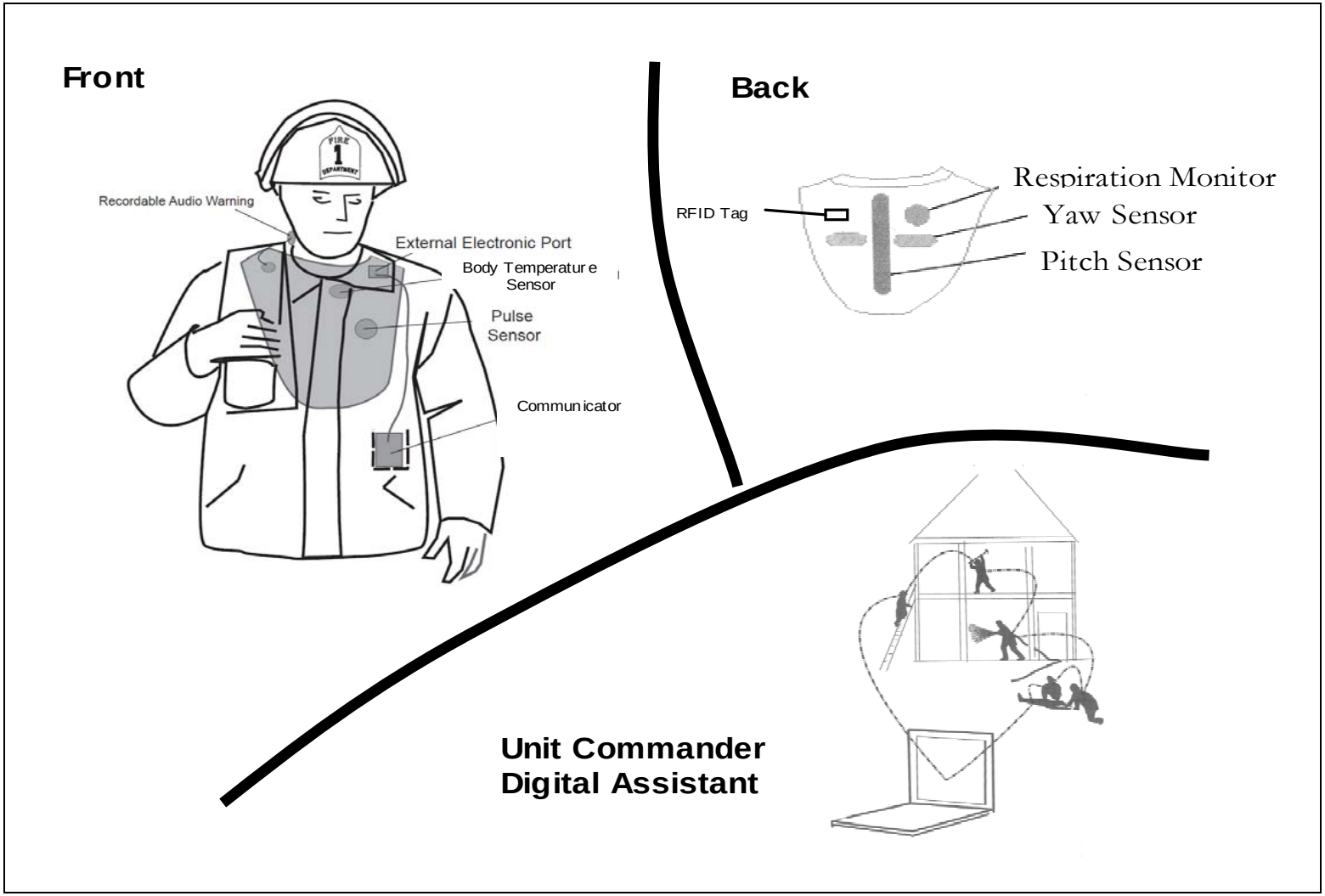


Figure 3 - Illustrations of DKYS

5.2. High Tech, Inc.'s Electronics and Software Development Practices

HighTech, Inc. is interested in responding to Responder Safety, Inc.'s Request for a Proposal for electronics and software based control system for DKYS. As part of their response, Hi Tech, Inc. has provided documentation on their electronics and software development practices. (See Figure 4 for an overview).

HighTech, Inc. proposes an Embedded System Engineering process with seven steps for engineering the embedded control system for DKYS. All processes are further supported by SIPOC procedures.

Note: High Tech, Inc. may condense the seven steps into a smaller number of steps depending on the project size and the number of development team members. For example, some projects may involve only three team members –a systems engineer/project leader, a hardware designer, and a software designer. All activities are conducted. However, due to the small project size, some of the activities may be further consolidated into a single step. Additionally, the team members review each others work during development for independent verification.

Step 1: Specify Embedded System Functional Requirements

Execution of Step 1 begins with one or more customer meetings to identify project scope and to prepare estimates. High Tech, Inc. emphasizes understanding user needs, so the engineering process begins with requesting a JSA and a hazard list from their emergency responder customers. A meeting with the customer and users is recommended to clarify any questions regarding user needs and safety concerns. These meetings typical occur as part of the proposal preparation though they may also occur after contract signing. Signing of the contract constitutes *Project Go/No Go (Gate 1)*.

Once Gate 1 criteria are met, HighTech, Inc. prepares requirements specification that includes functional safety performance criteria. The requirements specification includes a requirements-to-test traceability matrix or a relational database which cross-references hazards to functional requirements. When the requirements specification is complete, a *Requirements Stability/Design Readiness Review (Gate 2)* occurs. The

review addresses coverage of all requirements relative to safety concerns by assessing the completeness of the traceability documentation.

Step 2: Allocate Functions to Control Boards and Analyze/Simulate

Using the requirements specification, High Tech, Inc's system engineer allocates functions to control boards. The activity refines the requirements specification and permits additional analyses, such as processor work-load balancing and simulated timing to occur. A second *Requirements Stability/Design Readiness Review (Gate 3)* occurs again. The review focuses on potential side-effects of updated requirements and re-assesses the completeness of the traceability documentation.

Step 3: Design Embedded Control

Step 3 involves designing the embedded control. High Tech, Inc. uses a hardware/software co-design approach. The system engineer splits the design activities into two parallel activities by assigning these activities to a hardware and a software design teams. Some team members are co-located in the design laboratory, while others are remotely located. Members of the team communicate via a web-based discussion board so that issues and solutions are recorded and available to all team members. Hardware team members review the software issues and solutions and vice versa. All team members can identify and help resolve issues.

Figure 5 Shows Step 3A the Electronic Hardware Design Process.

Figure 6 shows Step 3B the Embedded Software/Firmware Development Process.

In addition to the discussion board, representatives from both hardware and software teams participate in the review gates 3A1, 3A2, 3A3, 3A4 and 3B1, 3B2, 3B3, and 3B4.

During Step 3 High Tech, Inc. identifies electronic parts that will be purchased as Commercial Off The Shelf or COTS components. These include sensor nodes and motes, printed circuit boards, digital signal processing chips, field programmable gate arrays, and microcontrollers. They also acquire a commercial off-the-shelf embedded operating system. Off-the-shelf components are qualified using a proven-in-use[21]

[21] The proven-in-use approach is an accepted practice when design details

approach. The qualification involves a review of manufacturer reliability data, field data, and functional testing.

Step 4: Prototype DKYS

Step 4 begins with a go decision from Gate 4 Design/Prototype Readiness Review. Step 4 breaks into four sequential steps as follows:

- Step 4a: Load embedded software/firmware onto control hardware.

This step surfaces software/firmware electronic hardware interface discrepancies.

- Step 4b: Run Emulated/Simulated Usage Tests

This step surfaces user interface, boundary value, and stressed usage discrepancies.

- Step 4c: Integrate Embedded Control into Equipment

This step surfaces embedded control – equipment interface discrepancies.

- Step 4d: Run Usage Tests

This step surfaces user interface, boundary value, and stressed usage discrepancies.

Figure 7 - Prototype Development Process provides more details about the sequencing of these steps including the review gates.

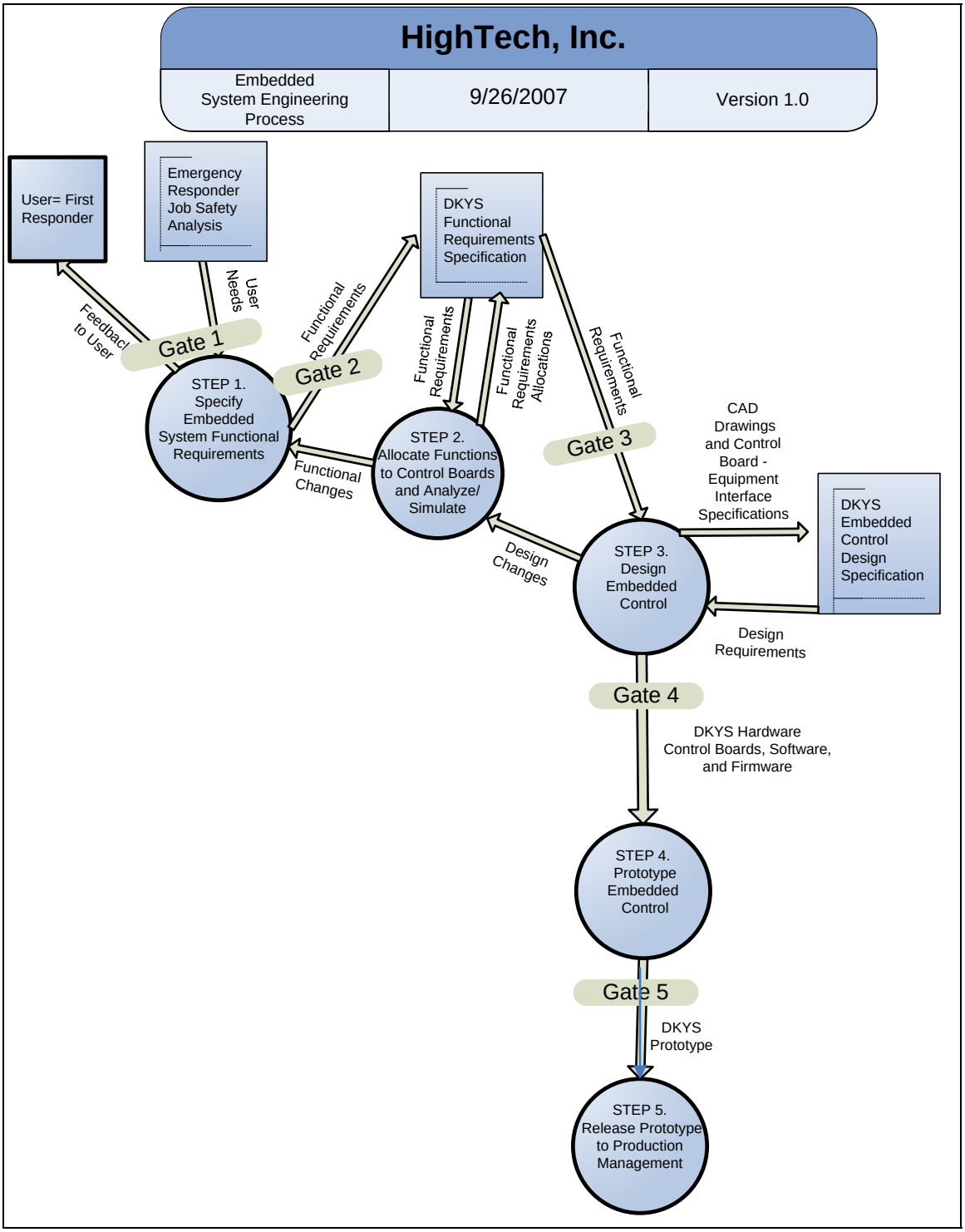
Step 5: Release Prototype to Production Management

Step 5 begins with a go decision from Gate 5: Prototype Completion/ Production Readiness Review. As part of the release, the necessary documentation is finalized and delivered to Responder Safety, Inc. for cataloging in the FSF for the DKYS.

---

and source code are not available for COTS. More detailed criteria for proven-in-use can be found in IEC 61508 and ANSI/UL 1998.

Figure 4 - HighTech, Inc's Embedded System Engineering Process



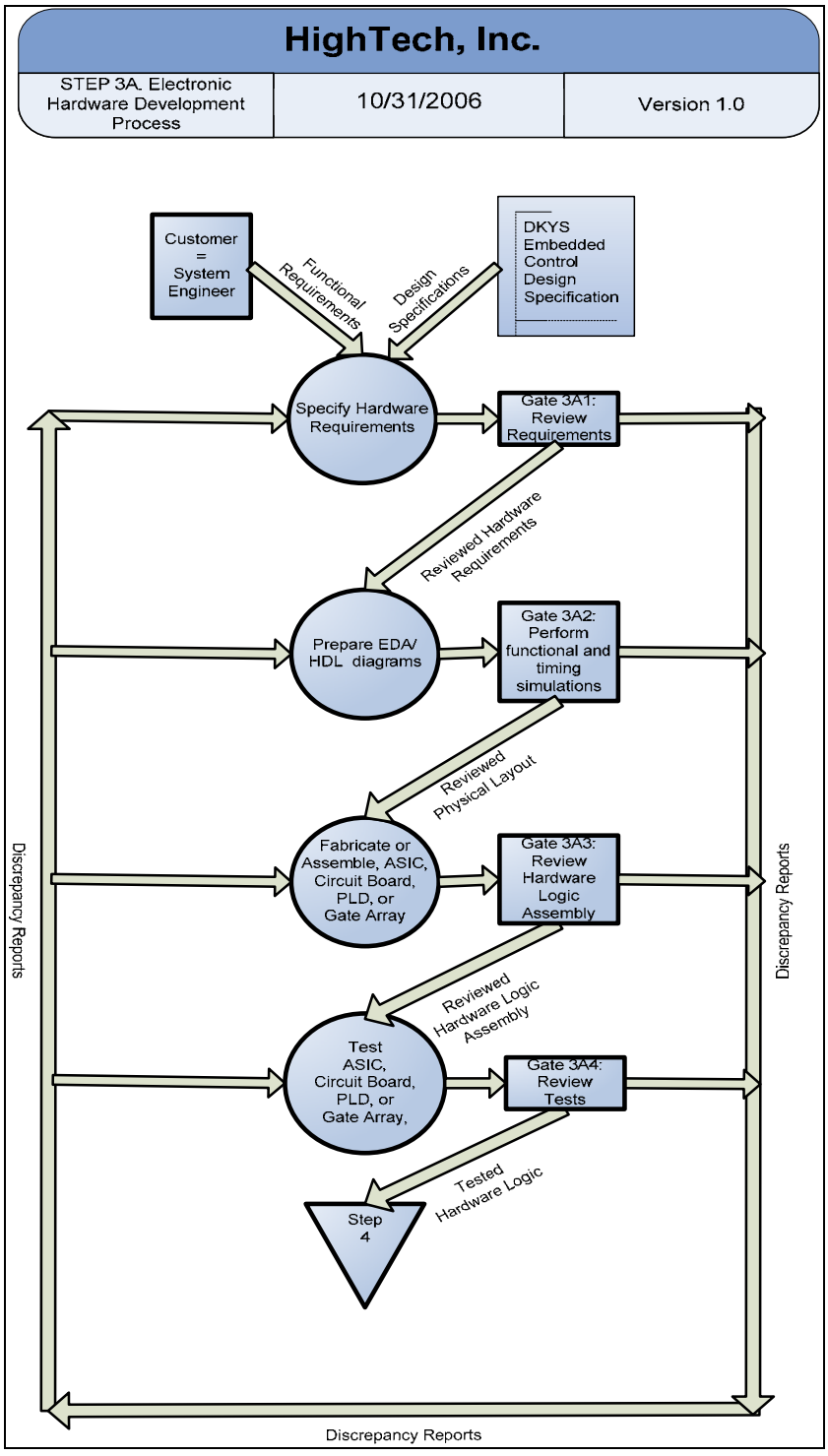


Figure 5 - Step 3A. Electronic Hardware Development Process

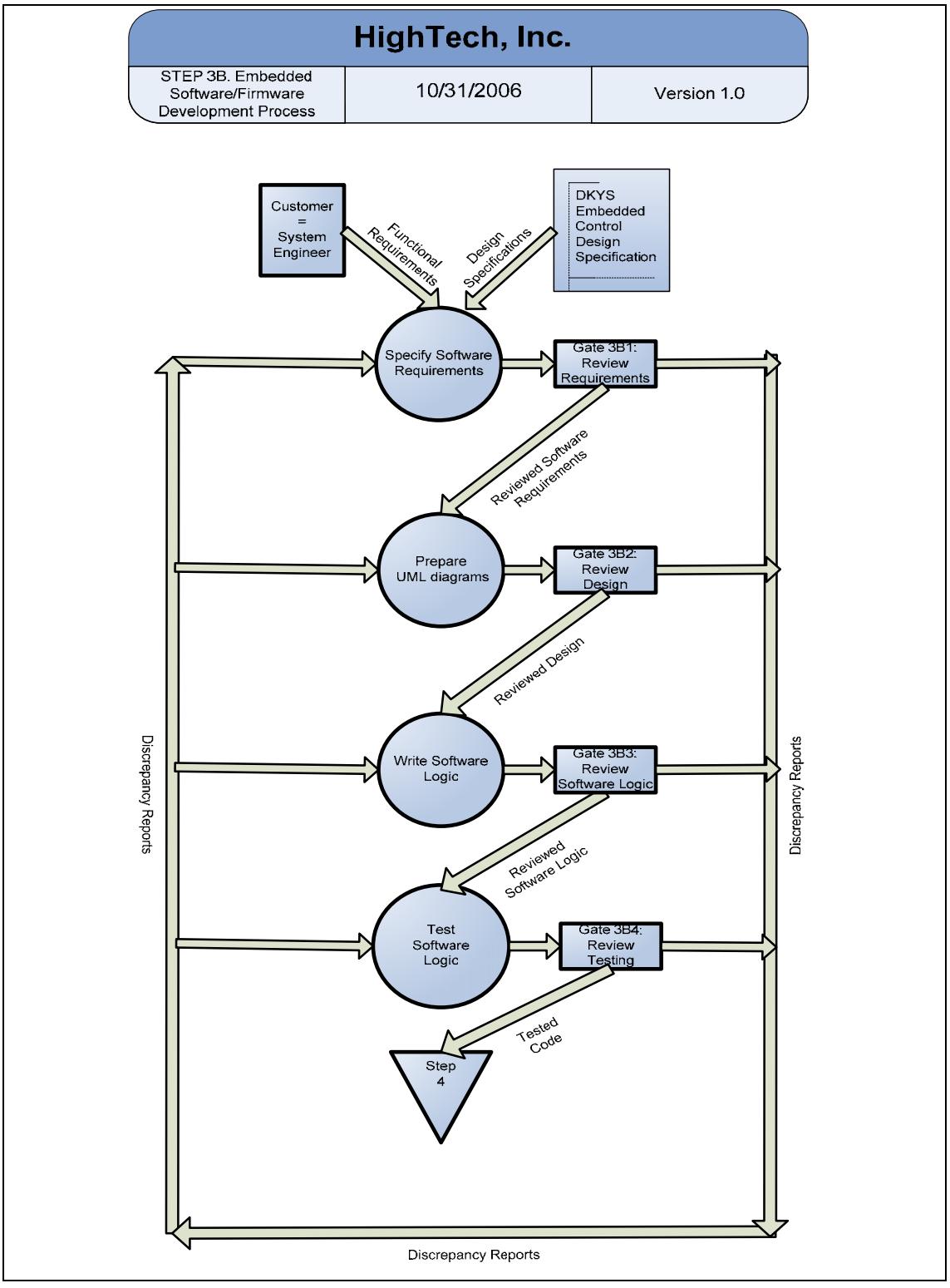


Figure 6 - Step 3B. Embedded Software/Firmware Development Process

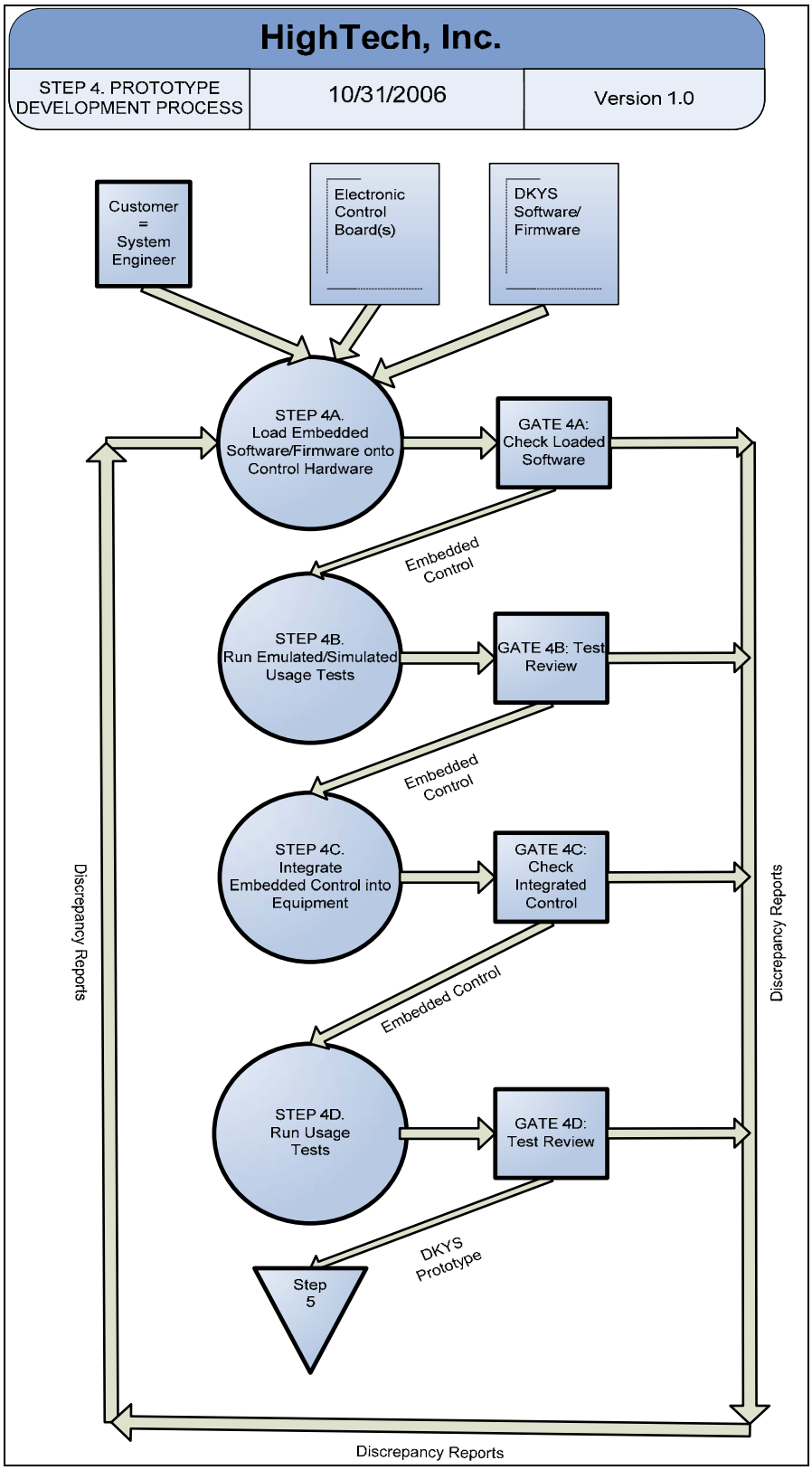


Figure 7 - Prototype Development Process

6.0. ABBREVIATIONS

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

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

7.0. GLOSSARY

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

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

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

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

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

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

Electronic Safety Equipment: Products that contain electronics embedded

in or associated with the product for use by emergency services personnel that provides

enhanced safety functions for emergency services personnel and victims during emergency incident operations (from NFPA 1800).

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

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

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

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

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

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

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

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

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

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

Hazard and risk analysis team: The group of emergency responders, electrical, electronics, computer hardware/software, manufacturing, and safety specialists responsible for the safety and integrity evaluation of PPE from its inception through its implementation and transfer to operations to meet corporate safety guidelines.

Hazard List: A list used to identify for tracking hazards throughout the FSLC. The list describes each hazard in terms of the event (s) that would lead to an accident scenario. When the hazard is identified during an accident analysis, the description of the hazard will also reference the accident scenario and consequences and measures that may be taken to avoid or prevent recurrence. The hazard list is used as input to the FMEA.

Human-computer interaction: The application of ergonomic principles to the design of human-computer interfaces.

Human-machine interface: The physical controls, input devices, information displays, or other media through which a human interacts with a machine in order to operate the machine.

Independent department: A department whose members are capable of conducting an IFSA. The department must be separate and distinct from the departments responsible for the activities and subject to Functional Safety Assessment or validation, taking place during the specific phase of the FSLC.

Independent functional safety assessment (IFSA): A systematic and independent examination of the work processes, design, development, testing, and safety file documentation for a product/machine/control system to determine compliance with applicable safety recommendations/standards/regulations.

Independent organization: An organization that is legally independent of the development organization whose members have the capability to conduct IFSAs. The organization member conducting the audit must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent person: A person who is capable of conducting an IFSA. The person must be separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall FSLC that is subject to Functional Safety Assessment or validation.

Independent protection layer (IPL): Engineered safety features or protective systems or layers that typically involve design for safety in the equipment, administrative procedures, alarms, devices, and/or planned responses to protect against an imminent hazard. These responses may be either automated or initiated by human actions. Protection should be independent of other protection layers and should be user and hazard analysis team approved.

Internal assessment: Conducted by the manufacturer to determine that the design and development process continues to comply with the safety plans and the safety file procedures. A report is issued and reviewed by appropriate management personnel.

Interoperability: The ability of PPE equipment and systems to provide services to and accept services from other PPE equipment and systems and to use the services so exchanged to enable them to operate effectively together.

Layer of protection analysis (LOPA): An analysis that identifies risk reduction targets by evaluating selected risk scenarios.

Lean Manufacturing: Implementing steps to reduce waste during the manufacturing process. There are eight types of waste – defects, overproduction, waiting, unused talent, transportation, inventory, motion, and extra processing.

Maintainability: The ability to maintain a PPE with minimum maintenance and repair so that the PPE can remain in service with full operation.

Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Periodic follow-up safety assessment: A systematic, independent, and periodic assessment which determines if the functional safety of the PPE is maintained.

Personal alert safety system (PASS): Devices that sense movement or lack of movement and that automatically activate an audible alarm signal to alert others in locating an emergency responder.

Personal protection equipment (PPE): Equipment and systems that provide the following life-safety protection functions:

- Protection against thermal, abrasion, puncture wounds, respiratory, vision, hearing and limited chemical and biological pathogen exposure hazards
- Monitoring of physiological, chemical, biological, and environmental parameters
- Communication among emergency responders and between emergency responders and victims

PPE functional requirements: Functions provided by the application including those functions required to meet NFPA equipment safety requirements.

PPE performance requirements: Timing and resource constraints imposed by the application including constraints needed for safety performance, such as delivering data

to the user within the time frame required.

Preliminary hazard analysis (PHA): This technique uses the results of PHL, lessons learned, system and component design data, safety design data, and malfunction data to identify potential hazard areas. In addition, its output includes ranking of hazards by severity and probability, operational constraints, recommended actions to eliminate or control the hazards, and perhaps additional safety requirements.

Preliminary hazard list (PHL): This is the first analysis performed in the system safety process and strives to identify critical system functions and broad system hazards. It uses historical safety data from similar systems and mishap/incident information hazard logs to guide the safety effort until more system-specific is developed.

Probability of failure on demand (PFD): A value that indicates the probability of a system failing to respond on demand. The average probability of a system failing to respond to a demand in a specified time interval is referred to as "PFD avg."

Project plan: A document that addresses the entire life cycle including development and use activities, management of change activities, and the documentation of safety. The project plan is updated throughout the life cycle.

Proven In Use: The component is considered reliable because it has been used in several products in the application over a period of time and reliability data is available for the component.

Random hardware failure: A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Rapid fire progression: A rapid rise in temperature that leads to an almost instantaneous combustion of materials over a larger area.

Record: Stating results achieved or providing evidence of activities performed.

Requirements Specification: A list of PPE requirements where each requirement is uniquely identified, traceable, and has safety performance criteria specified.

Retrospective Validation: Validation after the ESE has been fielded which is based on review of development documentation and testing and on field problem reports.

Risk analysis: Determination of the risk reduction requirement for the equipment or system based on qualitative or quantitative approaches.

Risk management summary: Details the risk management activities and summarizes the important risks identified and the means used to remove or mitigate them.

Risk reduction factor (RRF): Measure of the amount of risk reduced through implementation of safety equipment, training, and procedures. RRF is usually expressed as a reduction in the risk of loss of life.

Risk Priority Number (RPN): A number which establishes the priority for addressing the risk. RPN is computed based on severity, probability, and detectability. The higher the number obtained the higher the priority for addressing the potential failure.

Safety: Freedom from unacceptable risks.

Safety claims: A safety claim is a statement about a safety property of the PPE, its subsystems and components.

Safety integrity: The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period.

Safety Policy: A statement which describes in general the organizational commitment to safety and how safety issues will be addressed.

Safety statement: A succinct summary statement affirming the completeness

and accuracy of the FSF and the level of safety demonstrated for the PPE.

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

Scalability: The ability to scale up PPE to respond to threats, which cross jurisdictional boundaries.

Suppler Input Process Output Customer (SIPOC) Diagrams: Diagrams which show suppliers, the required input, the steps in a process, the output produced, and the customer of that output.

Systematic failure: A failure related to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors. Examples of systematic failures include design errors in interfaces and algorithms, logic/coding errors, looping and syntax errors, and data handling errors.

Traceability: Ability to trace the history, application or location of that which is under consideration.

Usability: Ease of use of the PPE. Usability is specified by stating performance requirements that define what users expect to accomplish.

Validation: Analysis, review, and test activities that establish that the PPE is built in accordance with the emergency responder needs. Did we build the right PPE?

Verification: Analysis, review and test activities that establish that the PPE is built in accordance with the PPE specifications. Did we build the PPE right?

Voice of the Customer (VOC): Six Sigma methods for collecting data on the desires and expectations of the customer. These methods include focus groups, surveys, websites, customer site visits, and interviews with distributors and/or retailers, current and lost customers.

APPENDIX A – PROJECT MANAGEMENT TOOLS

Project management software provides a way for management and first line employees to keep track of projects, from individual tasks to the overall status of projects. It allows project team members to work together more effectively, regardless of their location.

A review of 10 project management tools was conducted, first identifying feature categories that are common across project management tools. Next, selected project management tools were reviewed for feature richness, in relation to the identified common feature categories. Tools selected for review consisted of some better-known tools and some that are not so well known. The review process consisted of vendor online demos, examination of third party product reviews where available, and general product and feature information available from vendors. Client-based and web-based tools were reviewed. Microsoft-Project offers both choices.

As a result of this review, the project management tools shown in Table 9 are arranged from left to right according to their feature richness, that is, their satisfaction of the common feature categories.

Table 9 - Project Management Software: Features Comparison

PRODUCT	Microsoft Project	Process Director	eProject	@Task	Project Insight	Enterplicity	Vertabase Pro	eStudio	MinuteMan	AceProject
Provider	Microsoft	Saros	eProject	AtTask	Metafuse	Team Interactions	Standpipe Studios	Samepage	MinuteMan Systems	WebSystems
Product Type										
Client-Based	X	X							X	
Web-Based	X		X	X	X	X	X	X		X
Supported Systems										
XP	Client/PC	X	Web-based	Web-based	Web	NA Web	NA Web	NA Web	X	NA Web
2000	Client/PC	X	NA Web	NA Web	NA Web	NA Web	NA Web	NA Web	X	NA Web
NT		X	NA Web	NA Web	NA Web	NA Web	NA Web	NA Web	X	NA Web
FEATURES										
Project Management										
Task Control:										
Progress Tracking	X	X	X	X	X	X	X	X	X	X
Dependencies	X	X	X	X	X	X	X	X	X	X
Scheduling:										
Calendars	X	X	X	X	X	X	X	X	X	X
Time Links	X	X	X	X	X	X	X	X	X	X
Gantt Charts	X	X	X	X	X	X	X	X	X	X
Reporting:										
Statistics	X	X	X	X	X	X	X	X	X	X

PRODUCT	Microsoft Project	Process Director	eProject	@Task	Project Insight	Enterplicity	Vertabase Pro	eStudio	MinuteMan	AceProject
Size Tasks and Assess How to Best Manage Project	x	x	x	x				x	x	
Custom Reports	x	x	x	x	x	x	x		x	
Document Management	x	x	x	x	x	x	x	x	x	x
Budgeting	x		x	x	x	x	x	x	x	
Critical Path	x	x	x	x	x	x	x		x	
Resource Controls:										
Skill Profiles	x	x	x	x	x	x	x			
Time Sheets	x	x	x	x	x	x	x		x	x
Materials	x	x	x	x				x	x	
Costs	x	x	x	x	x	x	x		x	
Team Collaboration:										
Project Control Dashboard	x	x	x	x	x	x	x	x		x
Online Team Collaboration	x	x	x	x	x	x	x	x		x
Team Calendars	x	x	x	x	x		x	x		x
Issue Tracking	x	x	x	x	x	x	x	x		x
Microsoft Project Integration	Inherent	x	x	x	x	x				
User Support:										
Phone & Email	x	x	x	x	x	x	x	x	x	x
Online Forum	x	x	x	x	x	x	x	x	x	x

PRODUCT	Microsoft Project	Process Director	eProject	@Task	Project Insight	Enterplicity	Vertabase Pro	eStudio	MinuteMan	AceProject
or Training										

KEY:

X: Has Feature

Inherent – Automatically Included

Client/PC – does not support a server at this time

Web–based: internet based application