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

(In Nine Parts)

Part 8 - Additional Guidance: Functional Safety File (FSF) 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.

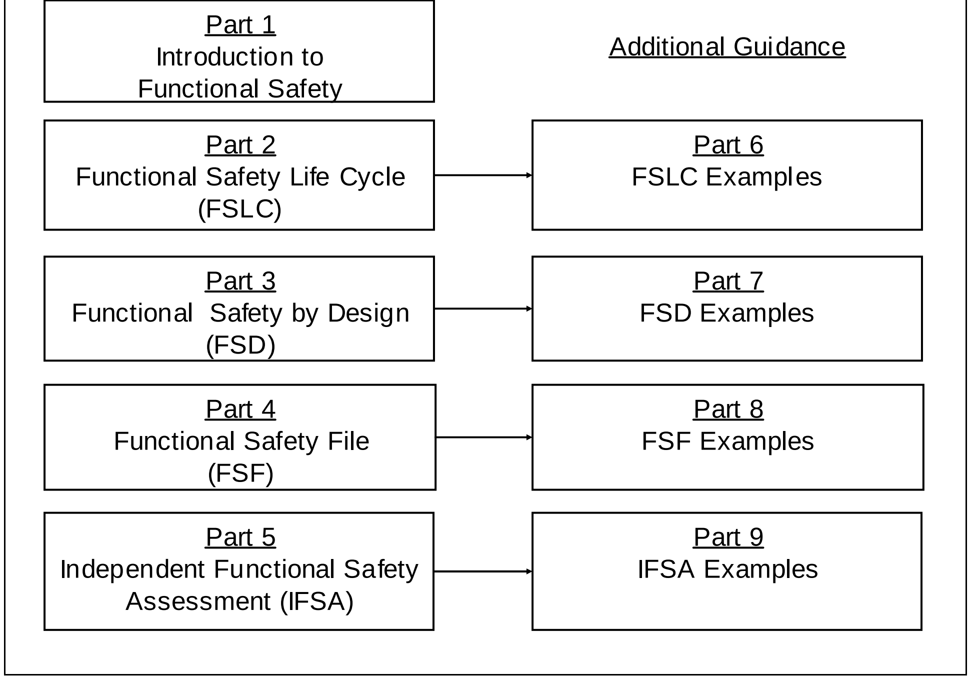

Part 1
Introduction to Functional Safety
Additional Guidance
Part 2
Functional Safety Life Cycle (FSLC)
Part 6
FSLC Examples
Part 3
Functional Safety by Design (FSD)
Part 7
FSD Examples
Part 4
Functional Safety File (FSF)
Part 8
FSF Examples
Part 5
Independent Functional Safety Assessment (IFSA)
Part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

Figure 1 - The functional safety report series.

Report Scopes

Part 1: Introduction to Functional Safety

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

Part 2: The Functional Safety Life Cycle (FSLC)

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

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

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:

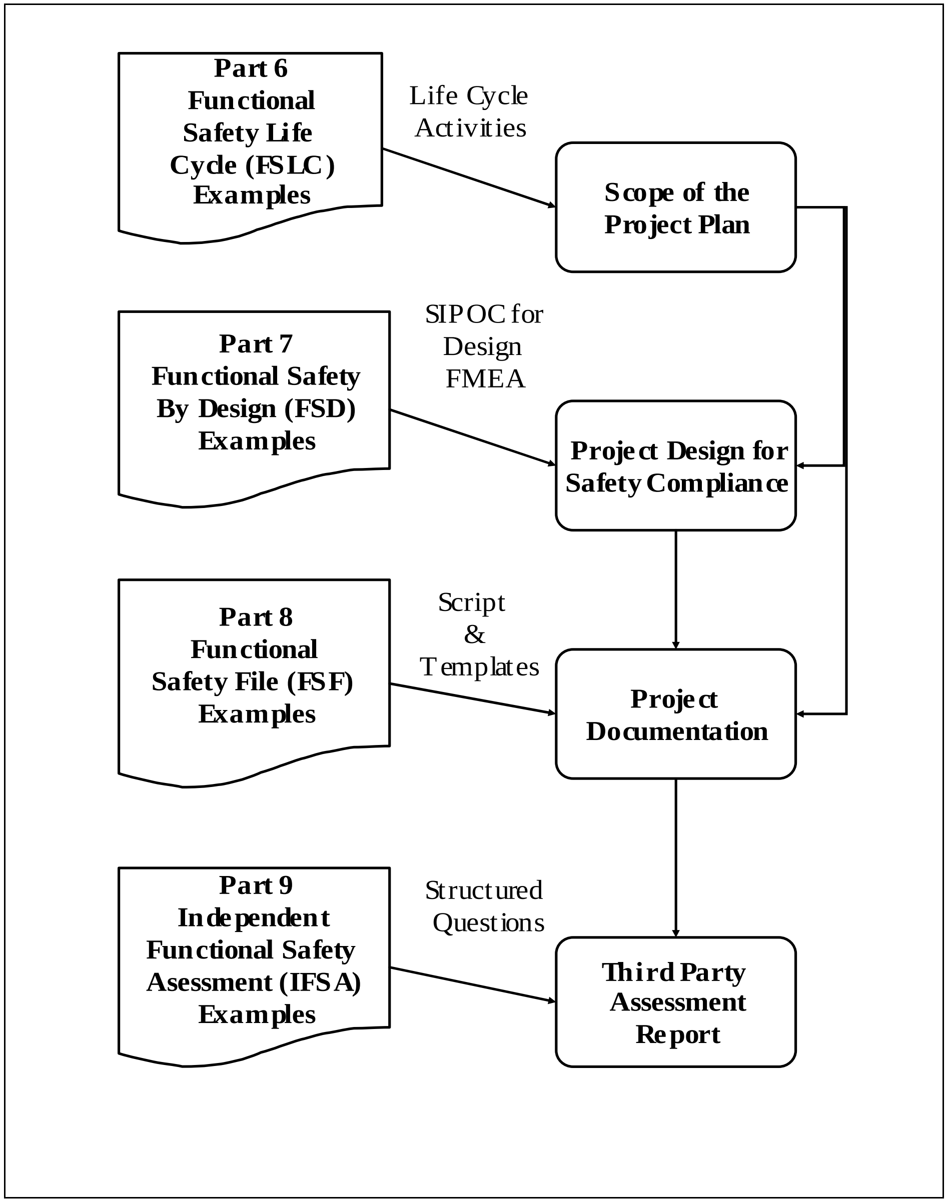
- Part 6 – Additional Guidance: Functional Safety Life Cycle Examples are used to develop the Scope of the Project Plan. The scope guides Project Functional Safety by Design (FSD) Compliance and Project Documentation.
- Part 7 – Additional Guidance: Functional Safety by Design Examples drives Project 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

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.



Part 6 Functional Safety Life Cycle (FSLC) Examples
Life Cycle Activities
Scope of the Project Plan
Part 7 Functional Safety By Design (FSD) Examples
SIPOC for Design FMEA
Project Design for Safety Compliance
Part 8 Functional Safety File (FSF) Examples
Script & Templates
Project Documentation
Part 9 Independent Functional Safety Asessment (IFSA) Examples
Structured Questions
Third Party Assessment Report

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

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

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

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

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

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

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

Intended Scope of Application

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

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

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

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 Protection Equipment (PPE) incorporate 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, Additional Guidance: Functional Safety File (FSF) Examples is Part 8 in a nine-part series of recommendations addressing the functional safety of advanced PPE for emergency responders. As the companion document to Part 4 - it describes a prototype FSF Document Management System (FSF-DMS) that illustrates an approach to developing a document management and support tool.

1.0. INTRODUCTION

1.1. Report Scope

The report, Additional Guidance: Functional Safety File (FSF) Examples is Part 8 in the nine-part series of recommendations addressing the functional safety of PPE for first responders. As the companion document to Part 4, Part 8 describes a prototype Functional Safety File Document Management System (FSF-DMS). Screen shots from the FSF-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 Document Management System (DMS) development.

1.2. Case Study: DKYS – Device that Keeps You Safe

DKYS developed by Responder Safety, Inc. consists of an electronic dickey; that is easily donned, lies flat against the wearer's body, and is held down by the weight of turnout gear. The electronic dickey communicates safety information in real time to the first responder's PDA (personal digital assistant) which in turn communicates it to the command center's control system. Part 6.1 Additional Guidance: Functional Safety Life Cycle Examples and Part 6.2 Additional Guidance: Functional Safety by Design provides more detail about the hypothetical product.

Responder Safety, Inc. identifies the documents that make up the FSF for DKYS. The documents will be accessed through a controlled interface used by their employees and their subcontractors High Tech, Inc and Independent Functional Safety Assessors, Inc. The FSF contains the documents shown in Table 3.

2.0. FUNCTIONAL SAFETY FILE DOCUMENT MANAGEMENT SYSTEM (FSF-DMS)

2.1. Purpose of the FSF-DMS Prototype

The prototyping of the Functional Safety File Document Management System (FSF-DMS) provides an example approach for organizing, controlling, and accessing FSF documents. Project managers may use the FSF-DMS approach for developing and managing documents associated with the development and deployment of electronics technology in a PPE product. The PPE product functionality and the project’s scope identify the applicable FSF documents required by standards and third party assessment. Not all projects will produce all of the documents shown.

The FSF-DMS provides guidance during the safety program implementation and a way to organize functional safety documentation. The FSF-DMS reduces the burden of FSF document development and management by allowing quick access to needed documents. The illustrations included in this section show the prototyped system with example FSF documents organized in a way to facilitate the assessing process.

The prototype FSF-DMS may be used as a basis for generating a FSF Expert System that would prompt users for all needed information to meet documentation requirements and compile these requirements directly into the FSF system.

2.2. Prototype FSF-DMS Architecture

The prototype FSF-DMS architecture consists of a database that defines the document navigation and a software program that generates the FSF in Adobe Acrobat (PDF format) with navigation and indexing included for all documents. Documents that are included in the FSF are converted into PDF file format and stored in the same network as the document navigation database resides. The documents are initially stored with no navigation or standard headers included.

Document navigation is achieved through the use of a data table that defines key parameters for each document and the path to where the input document is located. Other data tables define the relationships between documents and where they appear in the navigation tree. The approach uses SAROS's proprietary system called PDF Director for the software program. PDF Director converts the basic FSF documents without navigation into the final FSF version using the relationships defined in the database.

The basic steps for implementing a PDF Director based FSF documentation system would be:

1. Fill in document templates with specific manufacturer content
2. Establish keyword structure that best suits manufacturer terminology
3. Gain internal approvals.
4. Convert completed documents into PDF format and update document definitions as required.
5. Import document and keyword input into the PDF Director database.
6. Establish standard form templates that will be merged with all documents. The prototype system merges in a standard form header.
7. Run PDF Director to produce navigable FSF files.

Figure 3 provides an overview of the PDF Director FSF generation process.

DKYS-1	Functional Safety Summary	Affirms and provides references to the salient safety information about the equipment functionality, intended use, and the manufacturer's responsibilities.	Version 1.5 25 Oct 2006	Responder Safety,
DKYS-2	Functional Safety Policy and Plans	Defines what activities will be conducted to meet product safety objectives.	Version 1.3 25 Oct 2006	Responder Safety.
DKYS-3	Product Manager Manual and Records	Defines steps in the functional safety life cycle to be considered by the product manager. Includes SIPOCs and references data records.	Version 1.6 25 October 2006	Responder Safety.
DKYS-4	Training Manual and Records	Identifies training requirements for the product team. Includes SIPOCs and references training records.	Version 1.9 25 Oct2006	Responder Safety.
DKYS-5	Product Requirements Specification	Specifies what the product will and will not do. The specification includes functional, safety, and performance requirements.	Version 1.12 25 Oct 2006	High Tech.
DKYS-6	Development Manual and Records	Includes SIPOCs for the development team and references records of development activities.	Version 1.4 25 Oct 2006	High Tech.
DKYS-7	Technical Review, Testing, Verification Manual and Records	Includes SIPOCs for the verification team to and references records of verification activities.	Version 1.7 25 Oct 2006	High Tech.
DKYS-8	Production Manual and Records	Includes SIPOCs for the production team and references records of development activities.	Version 1.3 25 Oct 2006	Responder Safety.
DKYS-9	Installation, Commissioning, and Validation Manual and Records	Includes SIPOCs for the validation team to and references records of validation activities.	Version 1.2 25 Oct 2006	Responder Safety.
DKYS-10	User Manual and Records	Includes instructions for the product user and references records of use activities.	Version 1.6 25 Oct 2006	High Tech.
DKYS-11	Distribution Manual and Records	Includes SIPOCs for distributing the product and references records of distribution activities.	Version 1.1 25 Oct 2006	Responder Safety.
DKYS-12	Maintenance and Repair Manual and Records	Includes SIPOCs for maintenance and repair of the product and references records of maintenance and repair activities.	Version 1.3 25 Oct 2006	High Tech.
DKYS-13	Management of Change Manual and Records	Includes SIPOCS for how change will be handled and references records of change activities.	Version 1.10 25 Oct 2006	Responder Safety.
DKYS-14	Decommissioning Manual and Records	Includes SIPOCS for product decommissioning and references records of decommissioning activities.	Version 1.2 25 Oct 2006	Responder Safety.
DKYS-15	Product Description	Describes the product function and intended use. Identifies any restrictions on use.	Version 1.7 25 Oct 2006	Responder Safety.
DKYS-16	Independent Functional Safety Assessment Report	Describes the approach to conducting the IFSA, the individuals involved, and records the findings.	Version 1.1 25 October 2006	Independent Functional Safety Assessors.

Table 3 - Responder Safety's FSF Document List for DKYS

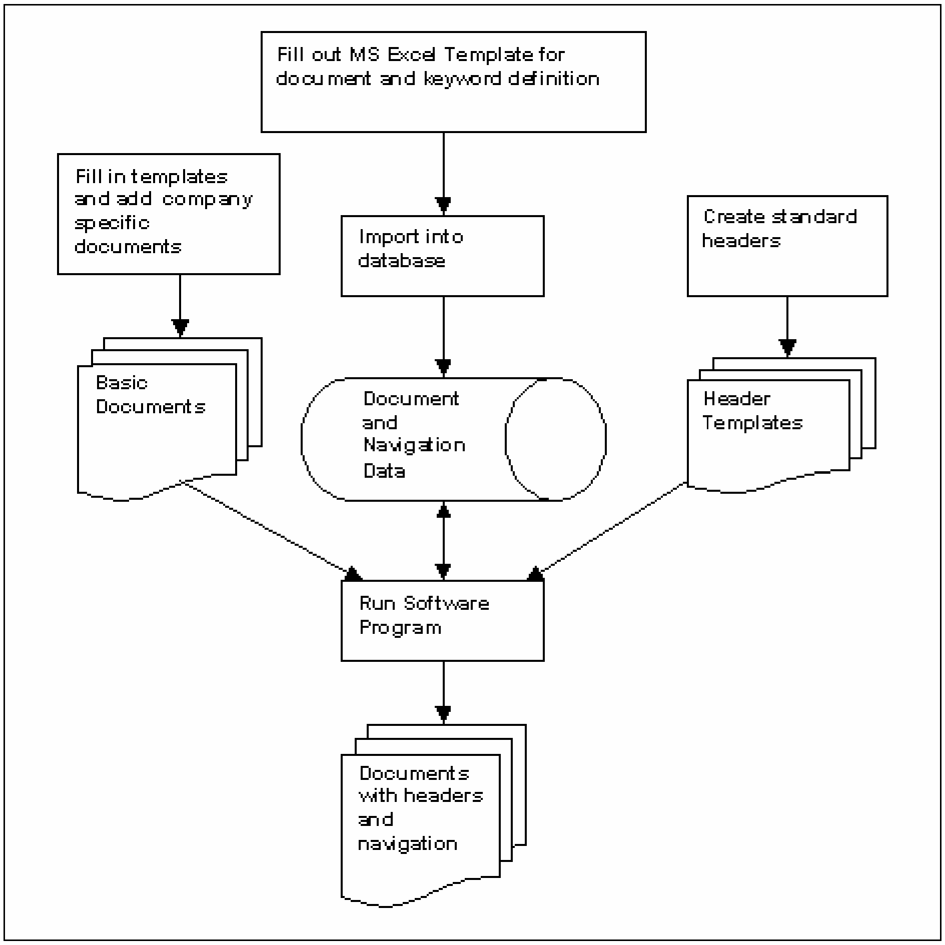

Fill out MS Excel Template for document and keyword definition
Fill in templates and add company specific documents
Import into database
Create standard headers
Basic Documents
Document and Navigation Data
Header Templates
Run Software Program
Documents with headers and navigation

Figure 3 Overview of PDF Director FSF Generation Process

2.3. FSF – DMS Navigation

2.3.1. Approach

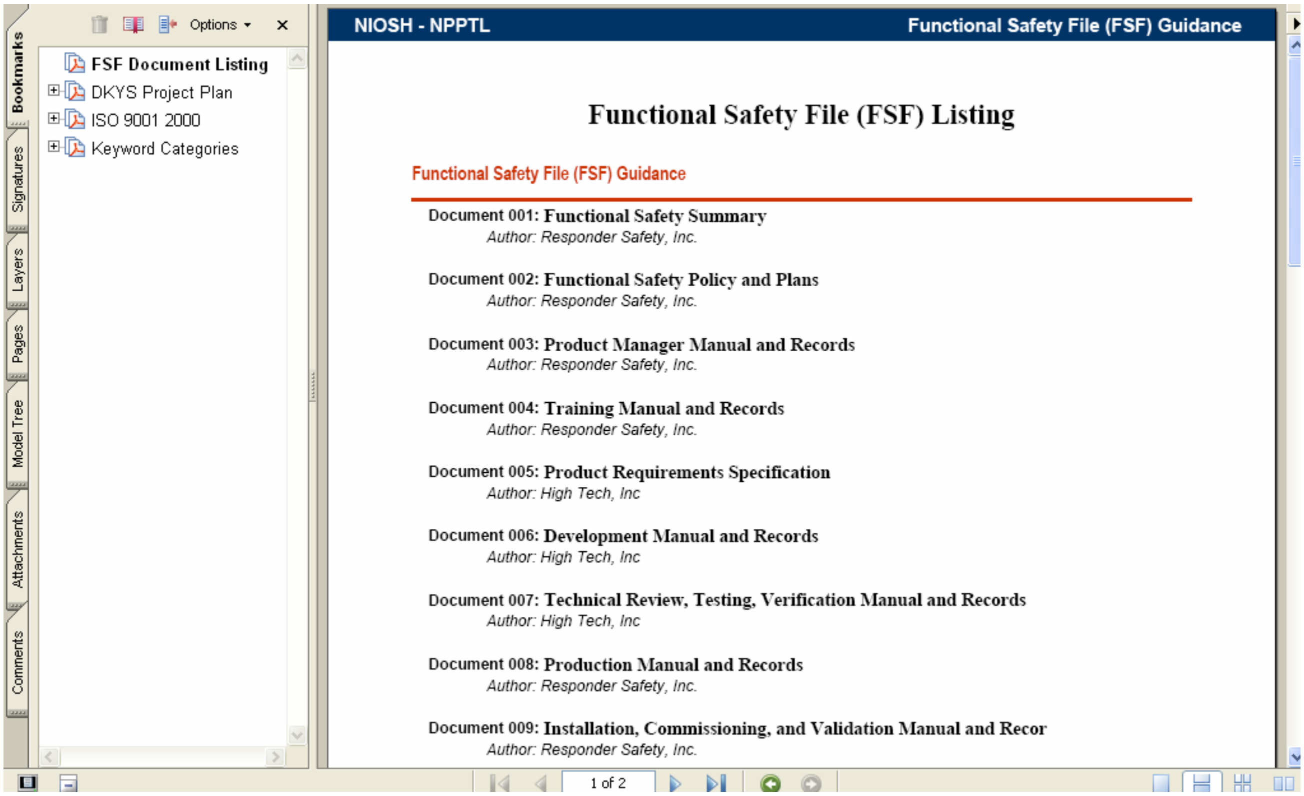
The following sections display the FSF-DMS navigation approach for the hypothetical DKYS FSF system. The approach consists of four navigation paths as follows:

1. FSF Document Listing
2. Project Plan
3. ISO 9001:2000
4. Keywords

The left windows in Figure 4, 5, 6, 7, 8, and 9 provide the navigation interface which allows selecting the desired document by opening up bookmarks. Bookmarks associated with a document display that document in the right window. If the document is also referenced in other sections of the navigation, those sections are displayed opened up to the displayed document. Bookmarks of the currently displayed document are highlighted in each of the referenced sections. Navigation relationships are easily updated as standards evolve.

2.3.2. FSF Document Listing Path

For quick access to the documents included in the FSF system, a listing is provided that is displayed with the first top-level bookmark. The user can click on the document number to quickly view the referenced document. The FSF document listing is generated programmatically and can be updated quickly as documents are added or modified. Figure 4 shows a user view of the FSF Listing.



Functional Safety File (FSF) Listing

Functional Safety File (FSF) Guidance

Document 001: Functional Safety Summary
Author: Responder Safety, Inc.

Document 002: Functional Safety Policy and Plans
Author: Responder Safety, Inc.

Document 003: Product Manager Manual and Records
Author: Responder Safety, Inc.

Document 004: Training Manual and Records
Author: Responder Safety, Inc.

Document 005: Product Requirements Specification
Author: High Tech, Inc

Document 006: Development Manual and Records
Author: High Tech, Inc

Document 007: Technical Review, Testing, Verification Manual and Records
Author: High Tech, Inc

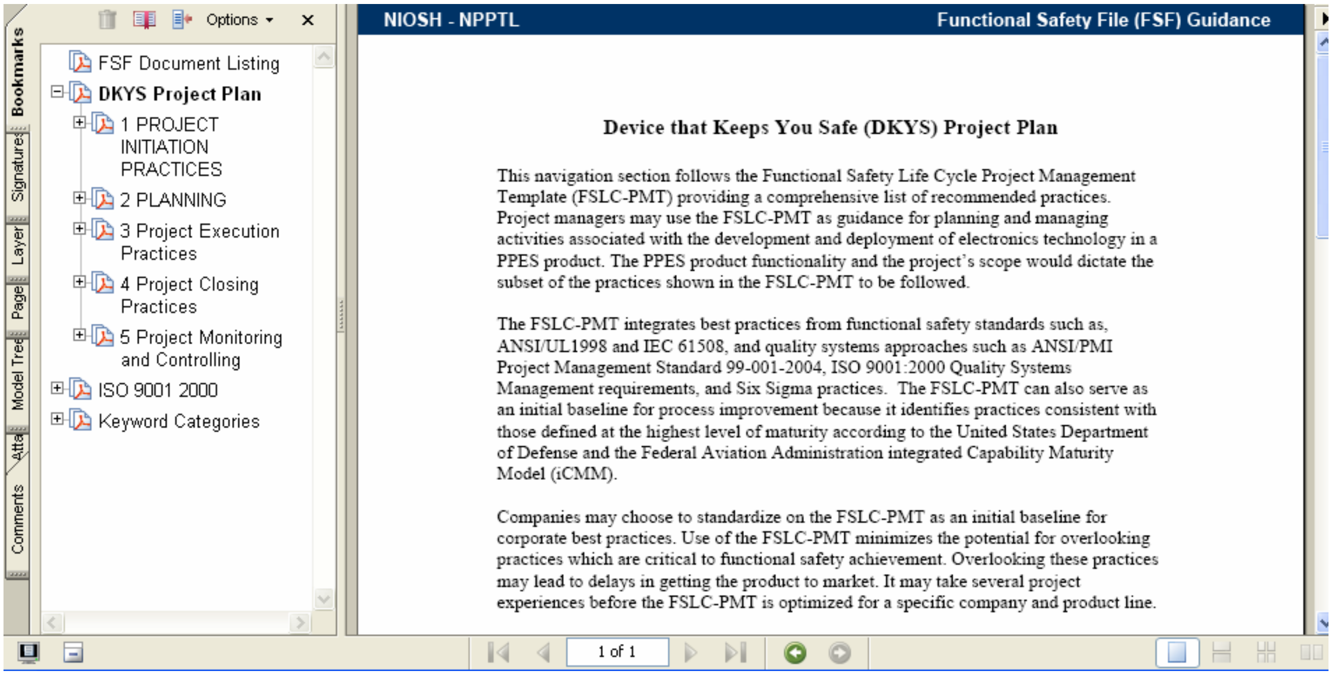
Document 008: Production Manual and Records
Author: Responder Safety, Inc.

Document 009: Installation, Commissioning, and Validation Manual and Recor
Author: Responder Safety, Inc.

Figure 4 Illustration of DKYS FSF Document Listing Navigation Path

2.3.3. Project Plan Navigation Path

For the hypothetical DKYS project, a navigation path that follows the overall project plan was established. FSF document bookmarks that are relevant to a project step will appear when that bookmark is opened up. In a production system all relevant documents and procedures can be included in this structure, thus facilitating on-going, secure, revision-controlled access to project information. Figure 5 displays what the user sees when they click on the top-level “DKYS Project Plan” bookmark.



NIOSH - NPPTL   Functional Safety File (FSF) Guidance

Device that Keeps You Safe (DKYS) Project Plan

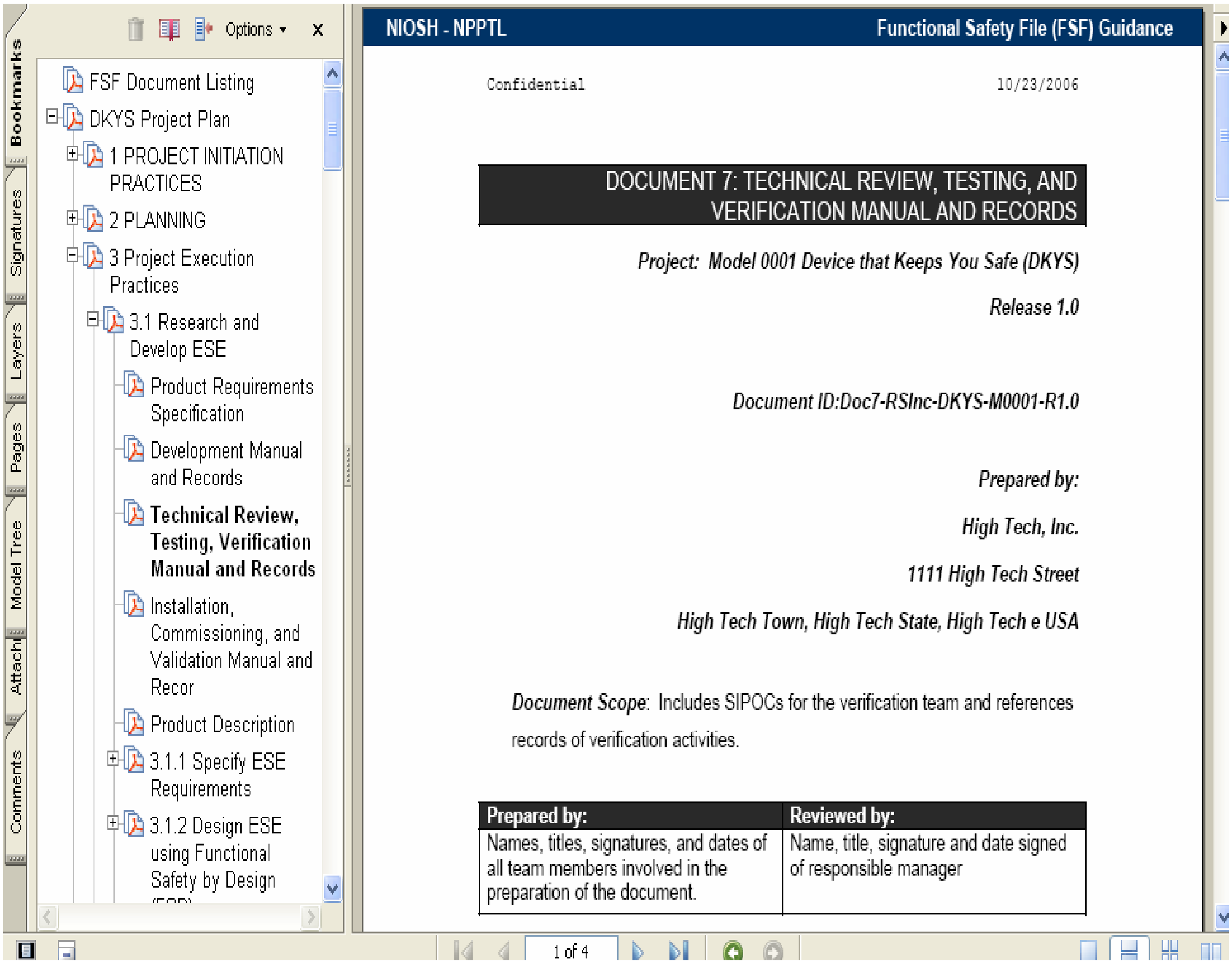
This navigation section follows the Functional Safety Life Cycle Project Management Template (FSLC-PMT) providing a comprehensive list of recommended practices. Project managers may use the FSLC-PMT as guidance for planning and managing activities associated with the development and deployment of electronics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

The FSLC-PMT integrates best practices from functional safety standards such as, ANSI/UL1998 and IEC 61508, and quality systems approaches such as ANSI/PMI Project Management Standard 99-001-2004, ISO 9001:2000 Quality Systems Management requirements, and Six Sigma 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 and the Federal Aviation Administration integrated Capability Maturity Model (iCMM).

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.

Figure 5 DKYS Project Plan User Interface

Figure 6 shows the user view if they had selected Document 7 from the FSF Document Listing or had drilled down through the project plan bookmarks to the document bookmark.


Options
Bookmarks
Signatures
Layers
Pages
Model Tree
Attachi
Comments
FSF Document Listing
DKYS Project Plan
1 PROJECT INITIATION PRACTICES
2 PLANNING
3 Project Execution Practices
3.1 Research and Develop ESE
Product Requirements Specification
Development Manual and Records
Technical Review, Testing, Verification Manual and Records
Installation, Commissioning, and Validation Manual and Recor
Product Description
3.1.1 Specify ESE Requirements
3.1.2 Design ESE using Functional Safety by Design
1 of 4

NIOSH - NPPTL Functional Safety File (FSF) Guidance

Confidential 10/23/2006

DOCUMENT 7: TECHNICAL REVIEW, TESTING, AND VERIFICATION MANUAL AND RECORDS

Project: Model 0001 Device that Keeps You Safe (DKYS)

Release 1.0

Document ID:Doc7-RSInc-DKYS-M0001-R1.0

Prepared by:

High Tech, Inc.

1111 High Tech Street

High Tech Town, High Tech State, High Tech e USA

Document Scope: Includes SIPOCs for the verification team and references records of verification activities.

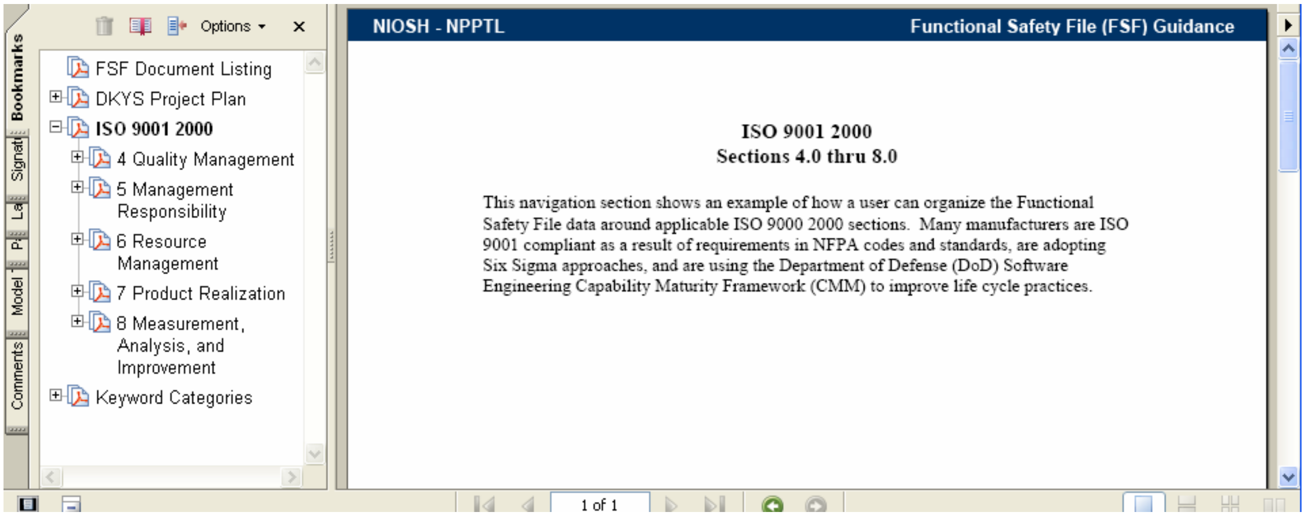
Prepared by:	Reviewed by:
Names, titles, signatures, and dates of all team members involved in the preparation of the document.	Name, title, signature and date signed of responsible manager

Figure 6 - Doc. 7 Technical Review, Testing, and Verification Manual and Records

2.3.4. ISO 9001: 2000 Requirements Navigation Path

For the DKYS prototype FSF-DMS, a navigation path that follows the relevant sections of the ISO 9001:2000 standard was established. Documents that are relevant to both DKYS Project Plan and ISO 9001:2000 will be highlighted within all applicable sections. See Figure 7.

In a FSF Expert System, the navigation structure shown in Figure 7 would organize applicable ISO 9001:2000 documents and procedures to facilitate audits to this standard as well as provide an alternate method of ongoing access to information.

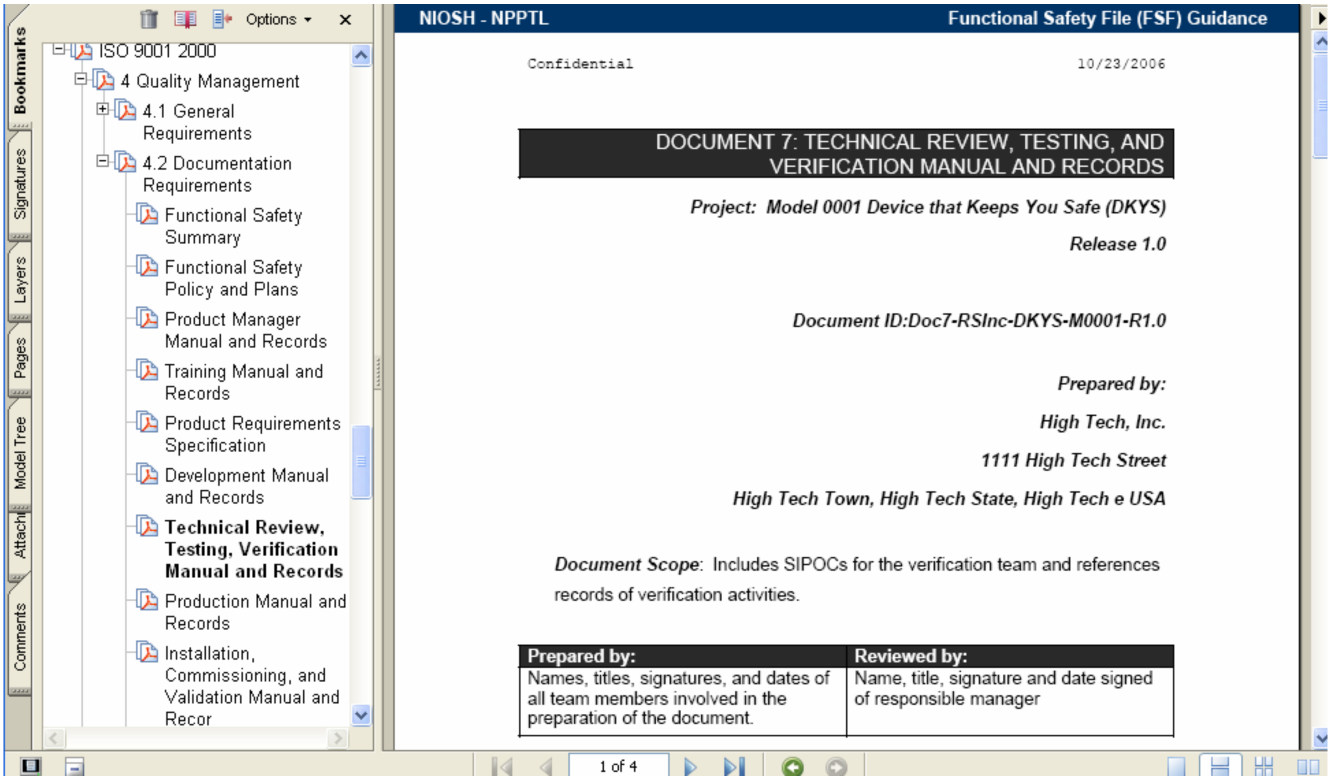


ISO 9001 2000
Sections 4.0 thru 8.0

This navigation section shows an example of how a user can organize the Functional Safety File data around applicable ISO 9000 2000 sections. Many manufacturers are ISO 9001 compliant as a result of requirements in NFPA codes and standards, are adopting Six Sigma approaches, and are using the Department of Defense (DoD) Software Engineering Capability Maturity Framework (CMM) to improve life cycle practices.

Figure 7 ISO 9001 2000 Requirements Path Navigation

In Figure 8 document navigation scrolled down to view one of the sections in ISO 9001:2000 that reference this document.


Options
Bookmarks
Signatures
Layers
Pages
Model Tree
Attach
Comments
ISO 9001 2000
4 Quality Management
4.1 General Requirements
4.2 Documentation Requirements
Functional Safety Summary
Functional Safety Policy and Plans
Product Manager Manual and Records
Training Manual and Records
Product Requirements Specification
Development Manual and Records
Technical Review, Testing, Verification Manual and Records
Production Manual and Records
Installation, Commissioning, and Validation Manual and Recor
NIOSH - NPPTL
Functional Safety File (FSF) Guidance
1 of 4

Confidential 10/23/2006

DOCUMENT 7: TECHNICAL REVIEW, TESTING, AND VERIFICATION MANUAL AND RECORDS

Project: Model 0001 Device that Keeps You Safe (DKYS)

Release 1.0

Document ID:Doc7-RSInc-DKYS-M0001-R1.0

Prepared by:

High Tech, Inc.

1111 High Tech Street

High Tech Town, High Tech State, High Tech e USA

Document Scope: Includes SIPOCs for the verification team and references records of verification activities.

Prepared by:	Reviewed by:
Names, titles, signatures, and dates of all team members involved in the preparation of the document.	Name, title, signature and date signed of responsible manager

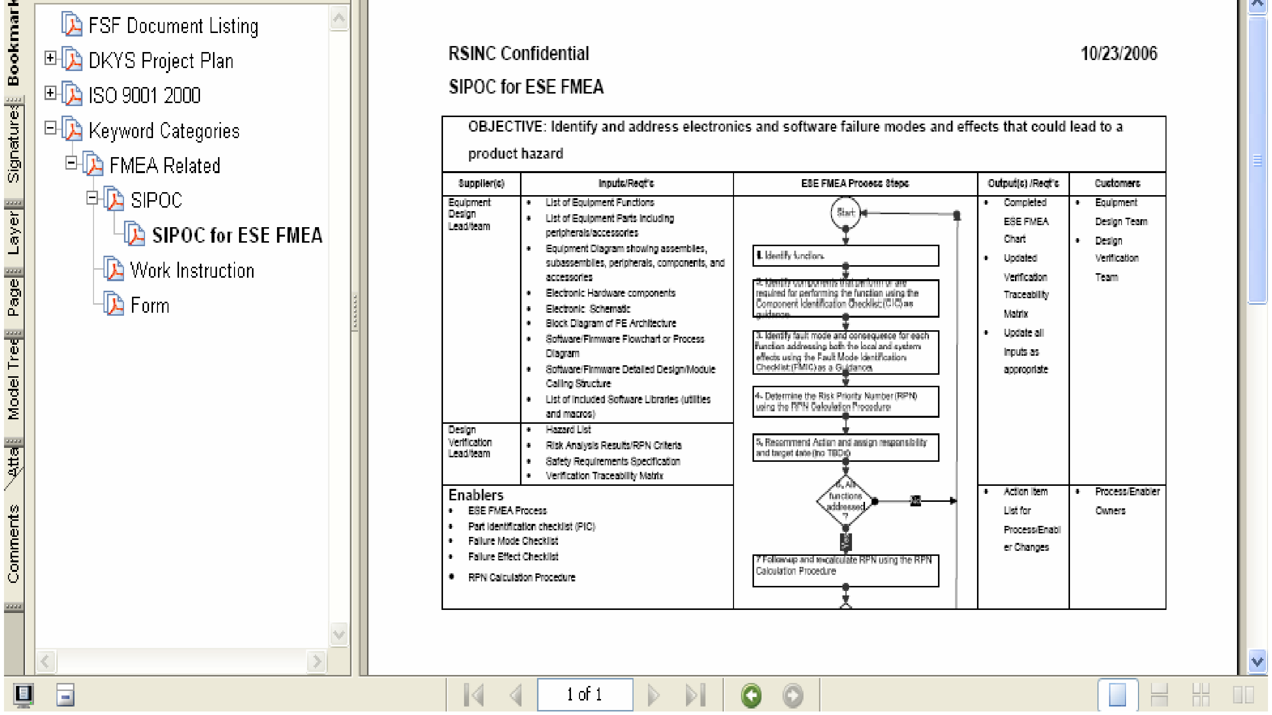
Figure 8 ISO 9001 Navigation to FSF Document 7

2.3.5. Keyword Navigation Path

The Keyword Navigation Path is designed to be user specific by including user terminology to simplify and expedite access to needed documents. The example shown illustrates a keyword category called “FMEA Related” which organizes documents in keywords under that category. Additional keyword categories and associated keywords can be imported into the PDF Director database and the PDF Director rerun to update FSF documents. The example below Figure 9 is for a Supplier Input Process Output Customer (SIPOC) document that is linked to the keyword SIPOC which is further linked to the “FMEA Related” category.

2.4. Extending FSF-DMS for IFSAs

FSF-DMS may be extended by adding a step by step “wizard” to guide users (i.e. NIOSH/NPPTL or third party assessors) through the process of conducting an IFSA. The wizard prompts users for all information required for certification to a NIOSH or NFPA standard. Based on answers to questions, the “wizard” walks the assessor through the appropriate line of questioning to gather all needed information. An example of a tool for configuring a FSF-DMS for IFSA’s is a proprietary framework called Knowledge Director (KD) that is a companion product of the PDF Director product used for the FSF prototype system. Once all information has been gathered the extended FSF-DMS would automatically fill out the IFSA report template and update the FSF-DMS database.



RSINC Confidential 10/23/2006

SIPOC for ESE FMEA

OBJECTIVE: Identify and address electronics and software failure modes and effects that could lead to a product hazard

Supplier(s)	Inputs/Reqt's	ESE FMEA Process Steps	Output(s) /Reqt's	Customers
Equipment Design Lead/team	• List of Equipment Functions • List of Equipment Parts including peripherals/accessories • Equipment Diagram showing assemblies, subassemblies, peripherals, components, and accessories • Electronic Hardware components • Electronic Schematic • Block Diagram of PE Architecture • Software/Firmware Flowchart or Process Diagram • Software/Firmware Detailed Design/Module Calling Structure • List of included Software Libraries (utilities and macros)	Start 1. Identify functions 2- Identify components that perform or are required for performing the function using the Component Identification Checklist (CIC) as guidance 3. Identify fault mode and consequence for each function addressing both the local and system effects using the Fault Mode Identification Checklist (FMIC) as a Guidance 4- Determine the Risk Priority Number (RPN) using the RPN Calculation Procedure 5. Recommend Action and assign responsibility and target date (no TBDs) 6. All functions addressed ? No Yes 7 Followup and recalculate RPN using the RPN Calculation Procedure	• Completed ESE FMEA Chart • Updated Verification Traceability Matrix • Update all inputs as appropriate	• Equipment Design Team • Design Verification Team
Design Verification Lead/team	• Hazard List • Risk Analysis Results/RPN Criteria • Safety Requirements Specification • Verification Traceability Matrix			
Enablers • ESE FMEA Process • Part identification checklist (PIC) • Failure Mode Checklist • Failure Effect Checklist • RPN Calculation Procedure			• Action Item List for Process/Enabler Changes	• Process/Enabler Owners

Figure 9 Keyword Navigation

3.0. ABBREVIATIONS

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

MOC	Management Of Change
MSHA	Mine Safety and Health Administration
NFPA	National Fire Protection Association
NIOSH	National Institute for Occupational Safety and Health
NPPTL	National Personal Protective Technology Laboratory
OSHA	Occupational Safety and Health Administration
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

4.0. 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.

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 first 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.

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.

accept services from other PPE equipment and systems and to use the services so exchanged to enable them to operate effectively together.

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

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

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

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

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

Personal alert safety system (PASS): Devices that sense movement or lack of movement and that automatically activate an audible alarm signal to alert others in locating a first 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 first responders and between first 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

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.

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.

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 first 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. FSF DOCUMENT MANAGEMENT TOOLS

Background

Safety file documentation tools are designed to guide and assist in recording identified product/system safety issues and related test procedures employed to prevent safety issues from causing harm. Safety file documentation should include information such as a description of the product/system and its components, functional scope, safety claims, conditions for performance acceptability, a description of the functional safety life cycle (FSLC), test descriptions, and summaries of independent functional safety audits. Overall, the safety file is a “proof of safety” that the product/system and its operation will meet appropriate safety requirements for its intended use.

Below are six tools that can assist with safety file documentation. Although they are not specifically aimed at safety file documentation, due to the uniqueness of the requirements in this area, they offer capabilities that can assist with safety file creation. The documentation tools are shown in random order. Product descriptions were derived from information provided by the makers of the tools.

Achiever Plus

From: Achiever Business Solutions
355 East Campus View Blvd
Suite 285
Columbus, Ohio 43235
(614) 410-9000
www.achieverplus.com
info@achieverplus.com

Achiever Plus is a roles-based compliance management platform that can be used to address multiple standards, or compliance requirements. Based around a controls management framework, and a central document repository, the platform-independent software runs on Lotus Notes, Microsoft Exchange 2000 or ASP, or via a Web browser. Achiever Plus is provided as a series of modules and configurable databases, and is currently being used to address 38 different compliance requirements.

AUDITWorks

From: Primatech Inc.
50 Northwoods Boulevard
Columbus, Ohio 43235
(614) 841-9800

software@primatec.com

http://www.primatech.com/software/index.html

The software assists the user in the preparation and documentation of safety and environmental compliance audits. It provides guidance in conducting audits, a framework in which to record audit results including data management capabilities, and protocols for evaluating compliance. A variety of checklists are available containing questions that can be used to audit various programs, including OSHA’s Process Safety Management and EPA’s Risk Management Program regulations. Users can audit against government regulations, industry standards, or a company’s own health, safety and environmental standards.

Dakota Auditor

From:

Dakota Software Corporation

95 Allens Creek Road
Bldg. 2, Suite 302
Rochester, NY 14618
(585) 244-3300
Fax 585 244-3301
info@dakotasoft.com

http://www.dakotasoft.com/product/auditoroverview.asp

This is an expert system that helps to determine what regulations apply to your facility, so you focus on relevant areas. It is aimed at simplifying the process of regulatory compliance auditing. Audit checklists are determined based on your answers to profiling questions, so you can see what areas apply. Three dynamically linked auditing tools give you access to needed regulatory information and a step-by-step audit process.

FormArtist WorkFlow

From: Quask

81 Locust Avenue
Suite 324
New Canaan, CT 06840

(888) 853 1441

sales@quask.com

http://www.quask.com/en/product_FormFlowCompliance.asp?qcid=G_ComplianceSoftware

This is a tool that builds forms driven compliance processes. It can be configured to match particular documentation requirements. It maps compliance processes into forms using a form builder. The tool can be integrated with almost any other system or database.

Procuri

From:

Procuri Inc.
15 Piedmont Cnt NE STE 1100
Atlanta, GA 30305-1573
(877) 360-1600
info@procuri.com

http://www.procuri.com/solutions_compliance.asp

The product helps to ensure regulatory compliance. Real-time access and visibility in a centralized database provides corporate controls, transparent processes, audits, and disclosures. Complete audit trails are maintained.

Saros Director Series

From: Saros Incorporated

7327 Jacobs Fork Rd.

Charlotte, NC 28273

sales@saros.biz

www.saros.biz

Saros has developed a suite of configurable “Director” tools that facilitate the creation of expert systems for the purpose of streamlining complex processes. The specific offerings that are applicable to creating a FSF documentation system are:

Knowledge Director (KD) is a web based application framework system that is a practical way to create interactive applications. It is designed to be a tool for safety professionals to transfer their knowledge and experience directly into an interactive web application without the need for specialized programming. A potential use for this application is the creation of an interactive “wizard” that guides the user through a series of questions to collect all information needed to create an auditable safety file documentation system.

PDF Director is a tool that automates the process of creating an Adobe Acrobat based system of documents with multiple easy to use navigation bookmarks that simplify the development, use, and auditing of documents.