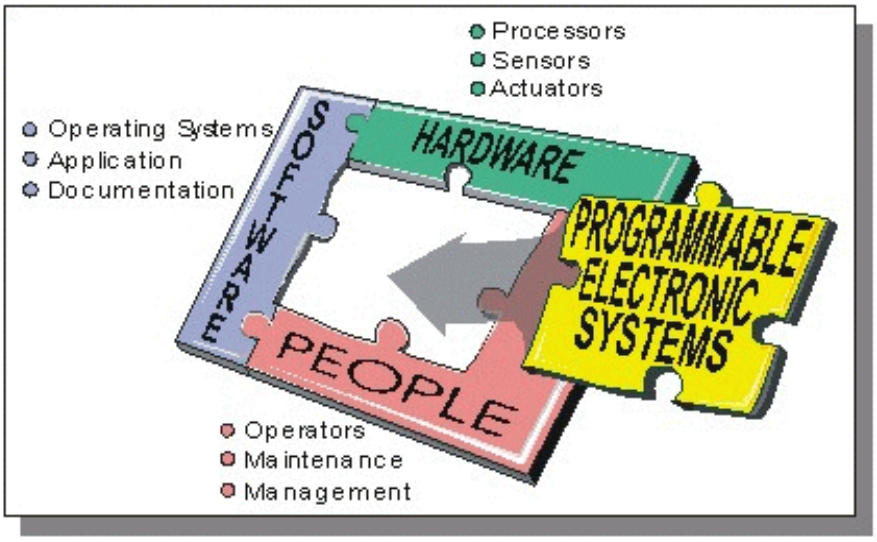
SYSTEM SAFETY EVALUATION PROGRAM

Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts)



Part 4: 3.0

Safety File

Mine Safety and Health Administration
Approval and Certification Center
Electrical Safety Division
Triadelphia, West Virginia

Department of Health and Human Services
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health
Pittsburgh Research Laboratory
Pittsburgh, Pennsylvania

May, 2002

CONTENTS

Page

Abstract 1
Acknowledgments 3
Background 3
Acronyms 4
1.0 Introduction 4
1.1 Document conventions 4
1.2 Scope 4
1.3 General 4
2.0 Key documents 5
3.0 Definitions 5
4.0 Safety file 8
4.1 Safety file: definition 8
4.2 Safety file: general concepts 9
4.2.1 Importance 9
4.2.2 Benefits 10
4.2.3 Format 11
4.2.4 Structure 12
4.2.5 Implementation 13
4.2.6 Design for assessment 13
5.0 Information model for the safety file 14
5.1 Safety summary 15
5.2 Safety statement 15
5.3 Risk management summary 16
5.4 Reference file 17
5.5 Safety plans 17
5.6 System safety program plan 18
5.7 Software safety plan 18
5.8 Management of change plan(s) 18
5.9 Operation and maintenance plan 19
5.10 Safety validation plan 19
5.11 Installation and commissioning plan 19
5.12 Safety data and methods 20
5.13 Product description 20
5.14 Implementation documentation 21
5.15 User document 21
5.16 History file 22
5.17 Hazard log 22
5.18 Concluding statement 22
6.0 Safety file summary 22
References 23
Appendix A.—Safety file checklist 26
Appendix B.—Relationship model for the safety file (with diagrams) 27
Appendix C.—Sample process for constructing the safety file 38
Appendix D.—Sample templates for safety file documents 41

ILLUSTRATIONS

1. The safety framework and associated guidance 2
2. High-level model of information categories for the safety file 14
3. The risk management results for each hazard 16

B-1. Model symbol key 30
B-1*A*. Structural relationship model for the safety file - part A 31
B-1*B*. Structural relationship model for the safety file - part B 32
B-1*C*. Structural relationship model for the safety file - part C 33
B-1*D*. Structural relationship model for the safety file - part D 34
B-1*E*. Structural relationship model for the safety file - part E 35
B-1*F*. Structural relationship model for the safety file - part F 36
B-1*G*. Structural relationship model for the safety file - part G 37
C-1. The safety file development process 39

TABLES

1. Key documents used for these recommendations 5

ABBREVIATIONS USED IN THIS REPORT

ANSI	American National Standards Institute
CMF	common mode failure
COTS	commercial off-the-shelf
FMEA	failure mode and effects analysis
HAZOP	hazard and operability studies
IEC	International Electrotechnical Commission
MCMS	mining control and/or monitoring system
MOCP	management of change plan
MSHA	Mine Safety and Health Administration
NIOSH	National Institute for Occupational Safety and Health
OEM	original equipment manufacturer
PE	programmable electronics
SIL	safety integrity level
SIS	safety instrumented system
SSPP	System Safety Program Plan
SWSP	Software Safety Plan
UL	Underwriters Laboratories, Inc.
V&V	verification and validation

PROGRAMMABLE ELECTRONIC MINING SYSTEMS: BEST PRACTICE RECOMMENDATIONS (In Nine Parts)

Part 4: 3.0 Safety File

By Gary L. Mowrey,[1] Thomas J. Fisher,[2] John J. Sammarco,[1] and Edward F. Fries[3]

ABSTRACT

This report (Safety File 3.0) is the fourth in a nine-part series of recommendations addressing the functional safety of processor-controlled mining equipment. It is part of a risk-based system safety process encompassing hardware, software, humans, and the operating environment for the equipment's life cycle. Figure 1 shows a safety framework containing these recommendations. The reports in this series address the various life cycle stages of inception, design, approval and certification, commissioning, operation, maintenance, and decommissioning. These recommendations were developed as a joint project between the National Institute for Occupational Safety and Health and the Mine Safety and Health Administration. They are intended for use by mining companies, original equipment manufacturers, and aftermarket suppliers to these mining companies. Users of these reports are expected to consider the set in total during the design cycle.

• 1.0 *Safety Introduction*.—This is an introductory report for the general mining industry. It provides basic system/software safety concepts, discusses the need for mining to address the functional safety of programmable electronics (PE), and includes the benefits of implementing a system/software safety program.

• 2.1 *System Safety* and 2.2 *Software Safety*.—These reports draw heavily from International Electrotechnical Commission (IEC) standard IEC 61508 [IEC 1998a,b,c,d,e,f,g] and other standards. The scope is "surface and underground safety-related mining systems employing embedded, networked, and nonnetworked programmable electronics." System safety seeks to design safety into all phases of the entire system. Software is a subsystem; thus, software safety is a part of the system's safety.

• 3.0 *Safety File*.—This report contains the documentation that demonstrates the level of safety built into the system and identifies limitations for the system's use and operation. In essence, it is a "proof of safety" that the system and its operation meet the appropriate level of safety for the

[1]Electrical engineer.

[2]Senior research physical scientist.

[3]Supervisory general engineer.

Pittsburgh Research Laboratory, National Institute for Occupational Safety and Health, Pittsburgh, PA.

intended application. It starts from the beginning of the design, is maintained during the full life cycle of the system, and provides administrative support for the safety program of the full system.

• 4.0 *Safety Assessment*.—The independent assessment of the safety file is addressed. It establishes consistent methods to determine the completeness and suitability of safety evidence and justifications. This assessment could be conducted by an independent third party.

• 5.0 *Safety Framework Guidance*.—It is intended to supplement the safety framework reports with guidance providing users with additional information. The purpose is to assist users in applying the concepts presented. In other words, the safety framework is *what needs to be done* and the guidance is the *how it can be done*. The guidance information reinforces the concepts, describes various methodologies that can be used, and gives examples and references. It also gives information on the benefits and drawbacks of various methodologies. The guidance reports are not intended to promote a single methodology or to be an exhaustive treatment of the subject material. They provide information and references so that the user can more intelligently choose and implement the appropriate methodologies given the user's application and capabilities.

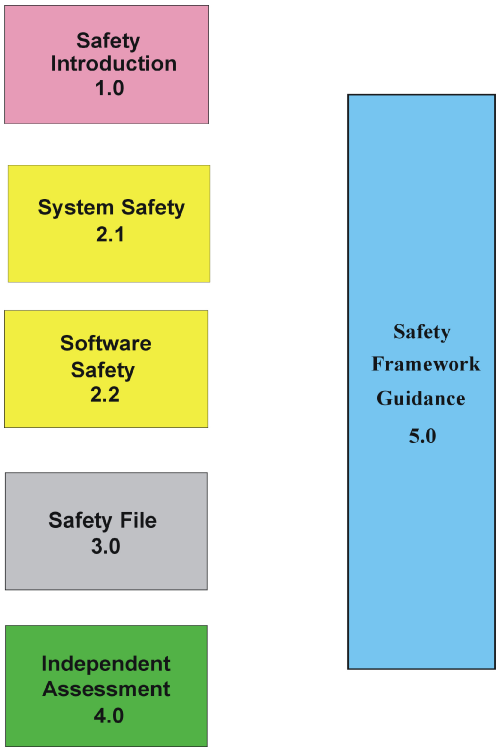


Figure 1.—The safety framework and associated guidance.

ACKNOWLEDGMENTS

The authors thank David C. Chirdon, Gerald D. Dransite, and Chad Huntley with the Mine Safety and Health Administration's (MSHA) Approval and Certification Center, Triadelphia, WV, for their assistance in developing this series of reports.

BACKGROUND

The mining industry is using programmable electronic (PE) technology to improve safety, increase productivity, and improve mining's competitive position. It is an emerging technology for mining that is growing in diverse areas, including longwall mining systems, automated haulage, mine monitoring systems, and mine processing equipment. Although PE provides many benefits, it adds a level of complexity that, if not properly considered, may adversely affect worker safety [Sammarco et al. 1997]. This emerging technology can create new hazards or worsen existing ones. PE technology has unique failure modes that are different from mechanical systems or hard-wired electronic systems traditionally used in mining. PE includes microprocessors, embedded controllers, programmable logic controllers (PLCs), and the associated software.

The use of a safety life cycle helps to ensure that safety is applied in a systematic manner for all phases of the system, thus reducing the potential for systematic errors. It enables safety to be "designed in" *early* rather than being addressed after the system's design is completed. Early identification of hazards makes it easier and less costly to address them. The life cycle concept is applied during the entire life of the system since hazards can become evident at later stages or new hazards can be introduced by system modifications. The safety life cycle for mining is an adaptation of the safety life cycle in part 1 of IEC 61508 [IEC 1998a].

System safety activities include identifying hazards, analyzing the risks, designing to eliminate or reduce hazards, and using this approach over the entire system life cycle. These system safety activities start at the system level and flow down to the subsystems and components. More detailed information on the fundamentals of system safety is presented by Sammarco et al. [1999].

This report incorporates some of the "best practices" for safety in the world and some of the latest international thinking on safety for PE. It uses a key group of standards selected from about 200 safety standards pertaining to PE. These key standards are listed in table 1.

Existing safety standards are built on collections of expertise and experiences (lessons learned) involving fatalities, injuries, and near misses of systems using PE. In general, standards also provide uniform, systematic approaches. History has shown standards to be an effective tool for safety [Leveson 1992]. Thus, by adapting existing standards, mining can build upon the valuable information captured in these standards documents.

1.0 Introduction

1.1 Document Conventions

This report follows a general format where major sections consist of an objective and associated recommendations. The formats are as shown.

Objective(s):
Recommendation(s):
NOTE:

The **NOTES** give brief clarification, reasoning, or guidance. More in-depth information is found in supplemental guidance documents.

1.2 Scope

The scope is "surface and underground safety mining systems employing embedded, networked, and nonnetworked programmable electronics." The safety file documents safety claims and supporting information that the programmable electronic safety system is adequately safe over its lifetime for a given application. Information on background, introduction, key documents, and additional definitions not covered in this document can be found in the System Safety document 2.1 [Sammarco and Fisher 2001] and Software Safety document 2.2 [Fries et al. 2001].

1.3 General

1.3.1 These recommendations do not supersede Federal or State laws and regulations.

1.3.2 These recommendations are not equipment- or application-specific.

1.3.3 These recommendations do not serve as a compliance document.

1.3.4 These recommendations apply to the entire life cycle for the mining system.

1.3.5 These recommendations apply primarily to the safety-related parts of the system. However, many of the recommendations can also be applied to the basic system.

2.0 Key Documents

2.1 This recommendation document is based on information and concepts from the documents listed in table 1. References for these standards can be found in System Safety document 2.1 [Sammarco and Fisher 2001] and Software Safety document 2.2 [Fries et al. 2001].

Table 1.—Key documents used for these recommendations

Standard identification	Title
IEC 61508 Parts 1-7	Functional safety of electrical/electronic/programmable electronic safety-related systems.
ANSI/ISA S84.01	Application of safety instrumented systems for the process industries.
ISA Draft Technical Report and TR84.0.02 - Parts 1-5	Safety Instrumented Systems (SIS); Safety Integrity Level (SIL) Evaluation Techniques.
MIL-STD-882C	Standard practice for systems safety program requirements.
UK Def Stan 00-58	HAZOP studies on systems containing programmable electronics.
ANSI/UL 1998, 2nd edition	Software in programmable components.

3.0 Definitions

The definitions are directly from IEC 61508, part 4 (4) and ISA S84.01(8). A few definitions are adaptations or newly formed definitions specific to mining.

Critical Software - Computer software components and units whose errors can result in a potential hazard or loss of predictability or control of a system.

Error - A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

Fail-Safe - Pertaining to a system or component that automatically places itself in a safe operating mode in the event of a failure, e.g., a traffic light that reverts to blinking red in all directions when normal operation fails.

Failure - The termination of the ability of a functional unit to perform a required function.

Fault - An abnormal condition or state that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

NOTE 1: A “failure” is an event; a “fault” is a state.

NOTE 2: Faults are random or systematic.

Field Devices - Peripheral devices hard-wired to the input/output terminals of a logic system. Field devices include sensors, transmitters, operator interface devices (i.e., displays, control panels, pendant controllers), actuators, wiring, and connectors.

Hazard - Environmental or physical condition that has the potential for causing injury to people, property, or the environment.

Human-Machine Interface - The physical controls, input devices, information displays, or other media through which a human operator interacts with a machine for the purpose of operating the machine.

Management of Change - Discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle.

Mean Time to Failure (MTTF) - The expected time that a system will operate before the first failure occurs.

Mining Control and/or Monitoring System (MCMS) - A system, using programmable electronics (PE), that responds to input signals from the equipment under control and/or from an operator and generates output signals, causing the equipment under control to operate in the desired manner.

Mishap - An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. In the real world, complete freedom from adverse events is not possible. Therefore, the goal is to attain an acceptable level of safety.

Noncritical Software - Software whose failure would not have an impact on safety or would not cause large financial or social loss.

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."

Programmable Electronics (PE) - Refers to electronically programmable or configurable devices (e.g., embedded controller, programmable logic controller, single-loop digital controller, distributed control system controller) that are effectively the "brain" of a PE system.

Programmable Electronic System - Any system used to control, monitor, or protect machinery, equipment, or a facility that has one or more programmable electronics (PE), including all elements of the system such as power supplies, sensors and other input devices, data highways and other communications paths, and actuators and other output devices.

Random Hardware Failure - A failure, occurring at a random time, which results from one or more possible degradation mechanisms in the hardware.

NOTE 3: There are many degradation mechanisms occurring at different rates in different components. Since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates, but at unpredictable (i.e., random) times.

NOTE 4: A major distinguishing feature between random hardware failures and systematic failures is that system failure rates (or other appropriate measures) arising from random hardware failures can be predicted with reasonable accuracy, but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy, but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot be easily predicted.

Risk - The combination of the probability of occurrence of harm and severity of that harm.

Risk Reduction Factor (RRF) - A measure of lowering the probability of an event from happening. RRF = inherent risk/acceptable risk, or RRF = 1/PFD .

Safety - Freedom from unacceptable risk.

Safety Availability - Fraction of time that a safety system is able to perform its designated safety service when the process is operating (PFD = 1 – safety availability).

Safety Function - A function implemented by singular or multiple MCMSs, protection layers, and devices using PE intended to achieve or maintain a safe state for a specific hazardous event.

Safety Instrumented System (SIS) - System composed of sensors, logic solvers, and final control elements for the purpose of taking the mining system to a safe state when predetermined conditions are violated. Other terms commonly used include "emergency shutdown system," "safety shutdown system," and "safety interlock system."

Safety Integrity Level (SIL) - One of three possible discrete integrity levels (SIL 1, SIL 2, SIL 3) of safety instrumented functions. SILs are defined in terms of quantitative or qualitative methods. SIL 3 has the highest level of safety integrity.

NOTE 5: SILs apply to safety functions of systems, protection layers, and devices using PE.

Safety Life Cycle - The necessary activities involved in the implementation of safety-critical systems. The activities begin at the concept stage and cease after the systems' decommissioning.

Software - Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.

Software Safety Integrity - Measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time.

Software Safety Integrity Level - One of three discrete levels for specifying the safety integrity of software in a safety system.

Software Safety Validation - To ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Software Verification - To the extent required by the safety integrity level, to test and evaluate the outputs from a given software safety life cycle phase to ensure correctness and consistency with respect to the outputs and standards provided as inputs to that phase.

Supervisory Software - A computer program, usually part of an operating system, that controls the execution of other computer programs and regulates the flow of work in a computer system.

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.

NOTE 6: Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 7: A systematic failure can be induced by simulating the failure cause.

NOTE 8: Example causes of systematic failures include human error in the—
- Safety requirements specification
- Design, manufacture, installation, and operation of the hardware
- Specification, design, implementation, and modification of the software

Tolerable Risk Level - Risk that is accepted in a given context based on the current values of society.

Validation - The activity of demonstrating that the safety system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety system.

Verification - The activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

4.0 Safety File

4.1 Safety File: Definition

The safety file is an organized, traceable set of documentation that demonstrates the degree of safety, gives the supporting evidence, and identifies limitations for the system and its operation. In essence, it is a "proof of safety" that the system and its operation meet the appropriate level of safety for the intended application. It starts from the beginning of the safety life cycle or when system modification commences, is maintained during the full life cycle of the system, and provides administrative support for the safety program of the full system.

NOTE 9: In creating the safety file, it is important to cover all system components and the interrelationships, as well as to provide a system level view. While a safety file is directed to the particular purpose of proving system safety to an external reviewer, it is developed using existing product engineering information.

NOTE 10: While it is important to specify the types of documents that are necessary for a safety file, it is also important to specify how those documents relate to the other components of system development and to specify the process by which the safety file is developed.

NOTE 11: Traceability is an important feature of the safety file. If the life cycle model is followed and the safety file is appropriately populated with deliverables from each phase, one will be able to select a hazard and trace from the hazard/risk analyses, through specifications and safety function allocation, to design, verification, and implementation, and finally, see at validation that the selected hazard was addressed, designed for, and resolved in an acceptable manner. When the concept of traceability is applied throughout a project, the cohesiveness of the safety file is greatly improved.

4.2 Safety File: General Concepts

A good definition of a safety file is given by Bishop and Bloomfield [1998]:

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

The safety file is a "living document"; it evolves over the entire safety life cycle. It may also be known as a "safety case," "safety argument," "safety assessment report," or "safety justification."

The safety file provides the documented evidence of compliance with System Safety 2.1 and Software Safety 2.2 documents. It specifies safety claims, summarizes both quantitative and qualitative supporting evidence, and communicates any limitations on installation and operation. It indicates that the system has been systematically engineered in accordance with standards and is fit for use within its intended environment operating under its defined operational limits.

The safety file should include written documentation and supporting engineering data that demonstrate—

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

Such documentation comprises the major portion of the safety file.

NOTE 12: Without adequate documentation, it is extremely difficult and, in some cases, impossible to validate and verify that a programmable electronic-based system is adequately safe for its intended application. Secondly, without such documentation, it is also very difficult and, in some cases, impossible to adequately investigate an incident to determine if root causes and contributing factors were attributable to the programmable electronics.

4.2.1 Importance

It is important that an adequate safety file be produced for a safety-critical system in order to—

(1) Ensure an adequate level of safety during operation and maintenance of the system
(2) Ensure that safety is maintained throughout the lifetime of the system
(3) Minimize MSHA approval risk (being able to demonstrate safety to MSHA, if required)
(4) Minimize commercial risk (improving implementation and maintenance costs are acceptable)
(5) Minimize liability/litigation risk

At the very least, sound safety and software engineering practices must be used (including structured planning and design; in-depth analysis at all levels of system development; appropriate documentation, reviews, and testing). Additional safety assurances can be derived by adopting specific coding practices and establishing an acceptable safety test program.

Research and practical experience from various international organizations have highlighted the following crucial requirements [Eastaughffe et al. 1997]:

(1) It is essential to have a *system* approach to safety file development that incorporates techniques that are valid for software and software-like processes (such as custom hardware development).

(2) The issues raised during safety analysis must be allowed to impact the system design, if necessary.

(3) The use of safety integrity levels allows the application of effort and rigor that is appropriate to the criticality of a component. A practical, sound approach is needed for assessing integrity levels for system components, whether these are implemented by means of software, hardware, operator, etc.

(4) Requirements that need to be highly trusted must be shown to be implemented to a high degree of integrity.

(5) A well-defined set of appropriately rigorous steps must be applied to deliver *assurance* of safety once an integrity level is determined.

4.2.2 Benefits

There are several important benefits in having a safety file.

(1) It reduces the overall system life cycle cost by considering safety problems at the beginning of the design. (This shifts the effort from maintenance and support to development and reduces the overall maintenance burden, which leads to an overall life cycle cost reduction).

(2) It documents evidence of safety and associated reasoning for safety approaches and decisions. This is important for subsequent changes so that changes do not undo or degrade the original degree of safety.

(3) It helps to support the vendor in any accident investigations, liability, and/or litigation issues by demonstrating that the vendor has in fact done everything reasonably possible to make the system safe.

(4) It provides evidence of ongoing compliance with other regulatory and/or guidance documents (i.e., SSPP, SWSP, etc.).

(5) It aids in future designs of related systems. Consequently, most of the work will have already been accomplished for any additional modifications and/or enhancements to the system.

(6) It establishes the engineering process capability needed for staying in business in the future as the demand for more complex, more highly integrated automated systems increases.

4.2.3 Format

In creating the safety file, it is important to cover all system components and the interrelationships, as well as to provide an overall system-level view. While a safety file is directed to the particular purpose of proving system safety to an external reviewer, it is developed using existing product engineering information. Thus, while it is important to specify the types of documents that are necessary for a safety file, it is also important to specify how those documents relate to the other components of system development and to specify the process by which the safety file is developed.

The safety file is the summary of the rationale as to why the system is safe to deploy. The content of the safety file is always accumulated incrementally through the safety life cycle. There is no required specific format, but it should contain the following sections:

Executive Summary: Key issues and final recommendations.

Introduction: Aim, purpose, and structure of the safety file.

System Overview: Overview of the main functions, main design points, and operational characteristics of the system.

Safety Requirements: A summary of the system safety requirements (from the SSPP).

Safety Management: A summary of the approach used for system management. A brief resume of the appropriate safety plan highlights with justification (from the SSPP).

Safety Audit and Assessment: A summary of the safety audits and assessments carried out.

Safety Analysis: Overview of how the safety analysis has been carried out (from the SSPP and SWSP).

Safety Engineering: A summary of the approach to and justification of the safety engineering methods used (from the SSPP and SWSP).

Compliance With Safety Requirements or Recommendations: Evidence of compliance with MSHA and all other Federal, State, and local regulations.

Other Issues: Any other safety issues not covered by explicit requirements.

Conclusions: Presumably that the system is safe for deployment under certain limitations and constraints.

Safety files tend to be hierarchical in nature, e.g., there may be individual safety files for subsystems (particularly where these may be produced by a subcontractor) with an overall safety file providing the summary for the complete system.

4.2.4 Structure

The safety file is composed of three basic elements:

(1) A set of claims regarding the safety of the system
(2) Evidence for supporting each claim
(3) An argument for supporting each claim

A claim is a statement about a safety property of the system (or subsystem or component). Types of safety-related claims include:

- Functional correctness
- Fail-safeness
- Reliability and availability of the system
- Robustness
- Maintainability
- Usability
- Modifiability

The evidence forms the basis for the argument in support of the claim by way of actual facts, assumptions used, and other subclaims. Sources of evidence will come from either system and Software Safety Plan outcomes (such as design, development, simulated experiences (e.g., reliability testing), and/or the safety life cycle process) and/or prior field experience with a similar system.

The argument links each piece of evidence to the claim by deterministic, probabilistic, or qualitative means. For example, the deterministic argument uses predetermined rules to derive a true/false claim based on some initial assumptions such as a formal proof or demonstration. A probabilistic argument uses quantitative statistical reasoning to establish numerical levels such as mean time to failure (MTTF) and reliability. The qualitative argument uses indirect links to the desired attributes, such as staff skills and prior experience with similar systems. The choice of argument used to support a particular claim will depend on the availability of evidence, e.g., claims for reliability could be based on field experience for an established design or development processes and reliability testing for a new design.

An explicit set of various claims about the safety-related aspects of the system is determined. Then all of the evidence to support each of these claims is gathered. Next, arguments are prepared that link each claim to its associated evidence.

As modern electronic systems are generally somewhat complex, it is recommended that a multilevel safety file be constructed, e.g., begin with a very simple high-level safety file model and then begin to go into additional detail, as much as is deemed appropriate for the various subsystems and components associated with the system. The top-level requirement is progressively translated into derived requirements for subsystems.

4.2.5 Implementation

The safety file should be considered throughout the entire life cycle. Start at project inception by constructing a preliminary safety file. Then, as the design becomes developed, incrementally modify the safety file to evolve simultaneously with the design before the system is used in the mine.

NOTE 13: The safety file is built incrementally as the System Safety Program Plan (SSPP) is implemented, as shown by Sammarco and Fisher [2001]. The safety file is built primarily with information produced by the SSPP implementation. Also included is supporting information from other sources, such as prior field experience of the system or subsystems. Moreover, portions from a prior safety file might be reusable.

To keep the safety file structure simple, layer the safety file into a top-level safety file, with subsidiary safety files for each subsystem and component. In this way, the safety issues associated with each subsystem or component can be individually addressed and, in turn, can be used to support arguments associated with higher level claims. Another important aspect when developing a safety file is to provide traceability between the overall system and its associated subsystems or components.

4.2.6 Design for Assessment

Assessments provide evidence for the safety file and should be viewed as assistance to the project, providing necessary confidence as to the integrity of the system or equipment. The assessment of safety should be carried out incrementally.

NOTE 14: Conducting preliminary assessments during the development and design of the system enables deficiencies and inadequacies to be detected earlier rather than waiting until the entire system is designed. Thus, early detection can allow corrections to be made more efficiently. Secondly, the potential for a better safety assessment exists since the assessor(s) can witness the development process and build the level of understanding at each checkpoint.

NOTE 15: When developing the design of the system with the safety file, keep in mind the following questions:

- Does the design implement the safety functions and attributes?
- Are the design criteria satisfied in terms of both functionality and safety?
- Is the design feasible?
- Are the safety arguments credible?
- Is the approach cost-effective?

NOTE 16: To minimize the design costs and risks, it is highly recommended to consider the following:

- Use a simple design, if possible. This eases system safety analysis considerably.
- Avoid novelty by using established designs. However, if the novelty provides additional benefits such as increased safety, etc., then such novelty would be acceptable.
- Ensure that supporting evidence is readily available.

5.0 Information Model for the Safety File

The information model for the safety file (figure 2) is a high-level model used to illustrate the three categories of information that comprise a safety file, namely:

- Safety summary documentation
- Safety plans documentation
- Safety data and methods documentation

NOTE 17: Since this is a high-level model of information categories, it does not include low-level details about the information, such as the requirements and detailed contents for the safety file components. Likewise, relationships and links between information components and development activities, plans, and constraints are not included in the information model. However, these details about the safety file are important in order to give a complete picture of how a safety file is constructed. Appendix A presents a brief checklist for generating the safety file. Appendix B presents a view of the information in the safety file, which provides lower-level details and links to development activities, plans, and constraints. Appendix C presents the activities involved in creating a safety file. Appendix D gives some sample templates for safety file documents.

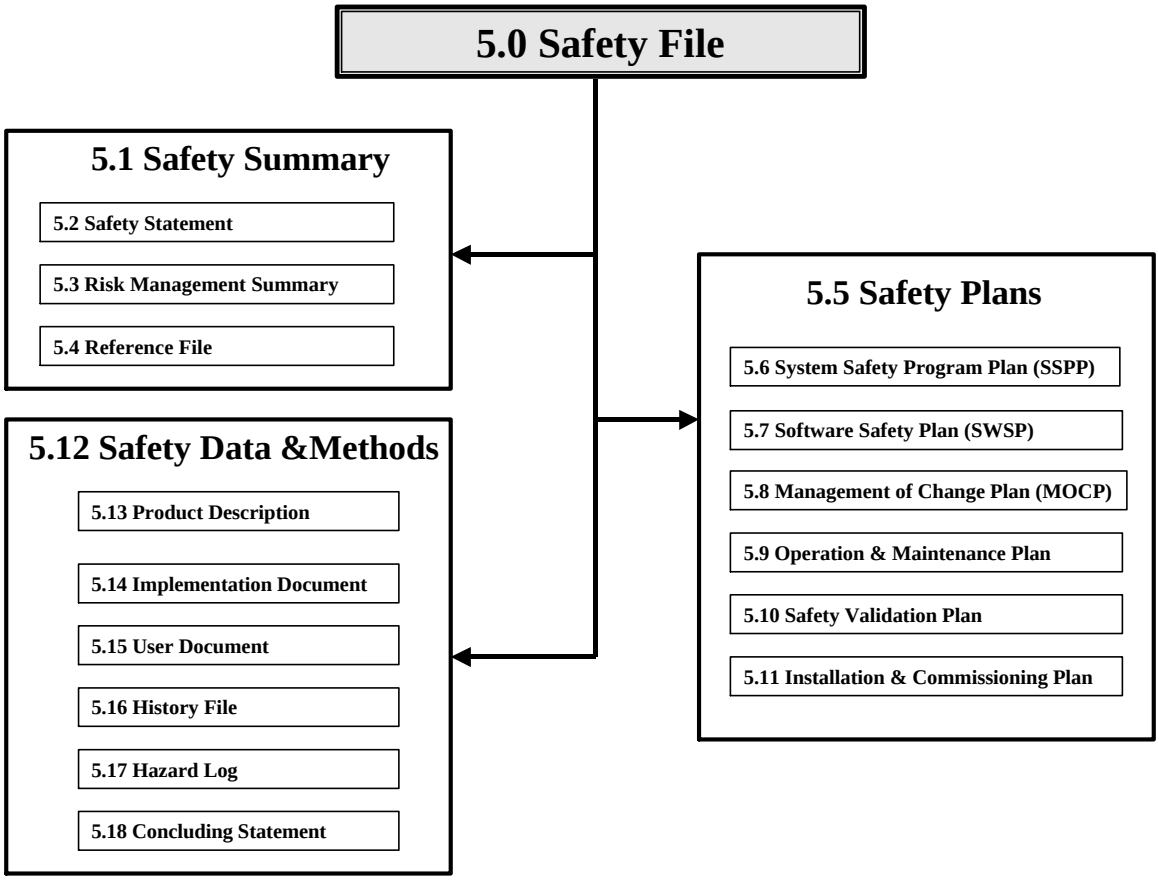


Figure 2.—High-level model of information categories for the safety file.

5.1 Safety Summary

Objective:

To provide a succinct safety statement of the safety file, a risk management summary summarizing the risks associated with the product and their management, and a reference file providing appropriate links to all documents that form a part of the safety file.

5.2 Safety Statement

Objective:

A succinct summary statement affirming the completeness and accuracy of the safety file and the level of safety demonstrated for the system.

Recommendations:

5.2.1 Identification and scope of system or components covered are to be included.

5.2.2 Intended use of system or components covered is to be identified.

5.2.3 Conditions of acceptability, including operating ranges and any restrictions/limitations on use, are to be listed.

5.2.4 The appropriate safety integrity level and/or standard being attested to is to be identified.

5.2.5 A signed statement shall be included that affirms that the safety file—

(1) Accurately reflects the engineering of the system;
(2) Documents all identified conditions of acceptability; and
(3) Identifies compliance with standards, if any.

NOTE 18: A safety summary section may be developed by referencing other program documentation, such as technical manuals, the System Safety Plan, Software Safety Plan, etc., and should include—

(1) The purpose and intended use of the system.
(2) A brief historical summary of the development of the system.
(3) A brief description of the system and its components. Include name, type, model number, and general physical characteristics of the overall system and its major subsystems and components. Software should also be included in this description.
(4) As applicable, a description of any other system(s) that will be tested or operated in combination with this system.
(5) As applicable, either photos, charts, flow/functional diagrams, sketches, or schematics to support the system description, test, or operation.

5.3 Risk Management Summary

Objective:

The risk management summary details the risk management activities and summarizes the important risks identified and the means used to remove or mitigate them. It is one of the central components of the safety file.

Recommendations:

5.3.1 The risk management approach (i.e., paradigms followed, such as fail-safe design, selection of design and programming languages, controlled and encouraged practices, use of traceability matrix) is to be identified.

5.3.2 The risk management activities (i.e., references to System and Software Safety Plans and any other risk control documents) are to be listed.

5.3.3 The risk management summary document should include (see figure 3)—

- Identified hazards and their causes
- Estimated risk for each hazard
- Risk control(s) for each hazard
- Verification method(s) and results for risk control

5.3.4 The limitations on use are to be listed.

5.3.5 A summary of SIL values assigned to safety functions is to be listed.

5.3.6 The traceability between hazard analysis, risk analysis, risk control, and verification results are to be identified.

NOTE 19: The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived, including the definition of acceptable risk, should be referenced.

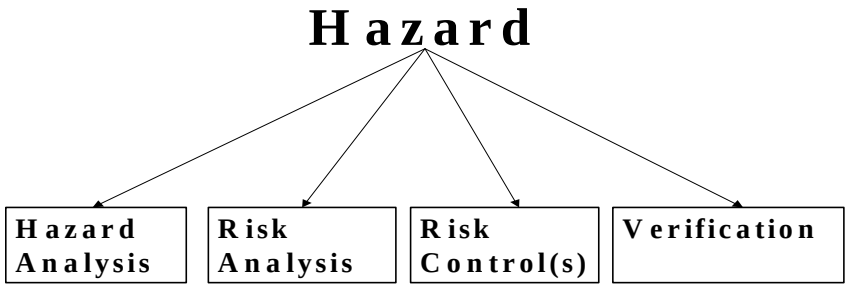


Figure 3.—The risk management results for each hazard.

5.4 Reference File

Objective:

The reference file provides a succinct index, as well as a cross-referencing index, to all documents that form a part of the safety file, which are retained by the component manufacturer, the system integrator, and the operating company. It eases the auditing and traceability burden by providing a readily available index to all safety file documents.

Recommendations:

5.4.1 The scope of the safety file is to be listed.

5.4.2 References to architecture and configuration information are to be listed.

5.4.3 References to all safety file documents and data are to be listed.

5.4.4 References to all safety-related test data and reports are to be listed.

5.4.5 References to all operating, maintenance, and training manuals are to be listed.

5.4.6 A summary listing of project safety personnel (including subcontractors) involved in critical safety life cycle activities and management activities, titles, responsibilities, and contact information are to be included.

NOTE 20: *Personnel Qualifications File*.—The qualifications, responsibilities, roles, and experience of key safety personnel on the project should be documented, along with other staff that manage and perform other safety-related critical tasks. Documented evidence of a team member's qualifications and experience is recommended. Records of training should also be kept and, if possible, training should include some form of assessment.

NOTE 21: It may often be necessary (and desirable) to introduce persons with no previous experience of safety-critical development. However, their supervision and contribution must be carefully controlled.

5.5 Safety Plans

The "Safety Plans" category is composed of all of the plans required for the development of safety-related systems, including the System Safety Program Plan (SSPP), Software Safety Plan (SWSP), Management of Change Plan (MOCP), Operation and Maintenance Plan, Safety Validation Plan, and Installation and Commissioning Plan. These plans are identified in the overall planning phase of the safety life cycle [Sammarco and Fisher 2001].

5.6 System Safety Program Plan

Objective:

The System Safety Program Plan details the safety, engineering and manufacturing processes, techniques, and methods used when developing the system that are important to safety achievement.

Recommendations:

The System Safety Plan recommendations are fully developed and explained in the System Safety document 2.1 [Sammarco and Fisher 2001].

5.7 Software Safety Plan

Objective:

The Software Safety Plan is a component of the System Safety Program Plan. It details the safety, engineering and manufacturing processes, techniques, and methods used when developing the software that are important to safety achievement.

Recommendations:

The Software Safety Plan recommendations are fully developed and explained in the Software Safety document 2.2 [Fries et al. 2001].

5.8 Management of Change Plan(s)

Objective:

The Management of Change Plan(s) describes how changes to the software, microelectronic hardware, and interfaces (human, electrical, and mechanical) are managed to ensure that safety is not adversely impacted.

Recommendations:

5.8.1 A description of the change process is to be given. This includes the configuration identification scheme, responsibilities, and activities used to maintain and control baselines.

5.8.2 A description of the methods and activities used to formally control receipt, storage, handling, and release of configurable items is to be given.

5.8.3 A description of the initiation, transmittal, review, disposition, implementation, and tracking of discrepancy reports (such as defects found) and change requests is to be given.

5.8.4 Management of change for software, microelectronic hardware, and interfaces (human, electrical, and mechanical) can be documented in a single plan or as a collection of multiple plans, each addressing a specific area, such as the system, software, and hardware.

NOTE 22: Management of change must apply to any safety-related software changes.

NOTE 23: The software is part of the system; thus, software modifications can adversely impact safety. Software modifications, as well as hardware modifications, must be analyzed for hazards. Those software modifications impacting safety should be well documented and managed. Management of software modifications are addressed in all of the key standard documents listed in table 1.

5.9 Operation and Maintenance Plan

Objective:

To plan how to operate, maintain, and repair the PE-based system to ensure functional safety.

Recommendations:

Operation and maintenance should follow the plan detailed by the SSPP [Sammarco and Fisher 2001].

5.10 Safety Validation Plan

Objective:

To plan how to confirm by examination and provision of objective evidence that the PE-based safety system meets the safety requirements.

Recommendations:

Safety validation should follow the plans detailed by the SSPP [Sammarco and Fisher 2001] and SWSP [Fries et al. 2001].

5.11 Installation and Commissioning Plan

Objective:

To plan how to install and commission the PE-based safety system in a safe manner and ensure that functional safety is achieved.

Recommendations:

5.11.1 Installation and commissioning should follow the plan detailed by the SSPP [Sammarco and Fisher 2001].

5.11.2 The adjustment and selection of adjustable parameter values should be within the allowable ranges defined in the system requirements.

NOTE 24: The adjustment and selection of adjustable parameter values, within the allowable ranges defined in the system requirements, is not considered a modification subject to an MOCP. However, the final values of adjustable parameters must be documented.

5.11.3 The selection of any parameter value that is not within the allowable values or ranges as defined in the system requirements is considered a change and is subject to the MOCP.

5.12 Safety Data and Methods

The "Safety Data and Methods" includes all of the documents that are produced during development and that provide evidence of compliance with the safety plans and demonstrate that the safety requirements are met. These documents include a product description, implementation document, user document, history file, hazard log, and concluding statement.

5.13 Product Description

Objective:

The product description is a multilevel summary description of the system or component architecture that describes the programmable system, microelectronic hardware, and software, including interfaces to electrical and mechanical hardware and humans.

Recommendations:

5.13.1 References to a description of the mining environment and the relationship of the computerized system to the mining environment are to be given.

5.13.2 References to specifications of the performance characteristics and limitations of the programmable system (e.g., operating limits, required backups, machine settings) are to be listed.

5.13.3 References to diagrams showing configuration information are to be included.

5.13.4 References to specifications of mechanical, electrical, and human interfaces, including identification of all limitations, are to be made.

5.13.5 References to specific code configuration and code in code libraries (includes *make files* and the like) are to be included.

NOTE 25: Items such as the performance specifications and description of the relationship between the system and its operating environment, all configuration diagrams, interface specifications and limitations, and references to specific code configurations should be included in this summary.

5.14 Implementation Documentation

Objective:

To record the results from applying the SSPP, SWSP, and the MOCP.

Recommendations:

5.14.1 References to the engineering procedures (i.e., risk management, hazard analysis, design reviews, code reviews, unit/component/system/hardware and software integration tests, etc.) are to be identified.

5.14.2 References to the results of applying engineering procedures (i.e., FMEA table, design and code review meeting minutes, test cases and results, etc.) are to be included.

5.14.3 References to the documentation on COTS and contracted software are to be included.

5.14.4 References to the specifications of the system safety requirements are to be included.

NOTE 26: All results of the safety program efforts should be included, e.g., the results of analyses and tests performed to identify system hazards, including—

(1) Those hazards with residual risk and the actions that have been taken to reduce the associated risk to a level contractually specified as acceptable.
(2) Results of tests conducted to validate safety criteria, requirements, and analyses.

Include a list of all hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment.

Categorize the list of hazards as to whether or not they may be expected under normal or abnormal operating conditions.

5.15 User Document

Objective:

To document the safe procedures for the operation and maintenance of the equipment.

Recommendations:

5.15.1 A description of the equipment is to be given.

5.15.2 A description of the safety functions and devices is to be given.

5.15.3 References to procedures on how to operate the equipment are to be given.

5.15.4 References to procedures on how to maintain the equipment are to be given.

5.15.5 References to the purpose or the intended use of the equipment are to be described.

5.16 History File

Objective:

The history file provides documentation on any software or hardware changes that could impact the safety of the system.

Recommendations:

5.16.1 All design and field changes are to be included in the history file.

5.16.2 All incident reports are to be included in the history file.

5.17 Hazard Log

Objective:

The hazard log is the key safety record and maintains the current status of all hazards.

Recommendations:

5.17.1 It should include the results of hazard analysis, hazard identification, and hazard elimination or control activities.

5.17.2 It should maintain a list of safety records and a chronological journal of entries.

5.18 Concluding Statement

Objective:

The safety file should be concluded with a signed statement that all identified hazards have been eliminated or their associated risks controlled to levels specified as acceptable and that the system is ready to test or operate.

6.0 Safety File Summary

Objectives:

6.1 To justify to others the confidence that designers and intending purchasers have in the safety of the system.

6.2 To provide evidence that, although an event may occur that was not foreseen or considered when the system was designed, all reasonably determinable safety-related concerns were considered and dealt with properly. This may provide an important legal defense.

Recommendations:

6.3 The safety file makes claims on safety-critical system behavior using suitable supporting arguments.

6.4 Ideally, a preliminary safety file should be developed simultaneously with the design process, thereby keeping the design within a reasonable safety envelope. By integrating the safety file development into the design process, any unsuitable designs and associated costs are thereby avoided or at least minimized.

6.5 Depending on the complexity of the system, the developer may decide to layer the safety file into several subsystem safety files, which in turn can be used in support of the top-level (main) safety file of the system being certified.

6.6 The safety file evolves to summarize, before deployment of the system, the evidence for the conclusion that the system is safe to deploy. Early versions of the safety file record planned activities, as well as those completed, and justify increasing confidence in the safety of the system.

NOTE 27: In summary, the safety file is an organized collection of safety-related documents that provide a demonstrable, convincing, and valid suite of arguments that the system is adequately safe for a given mining application in a given mining environment over the lifetime of the system (concept, design, fabrication, testing, installation, operation, and decommissioning).

NOTE 28: The safety file can be held on paper or electronic media.

REFERENCES

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

Eastaughffe KA, Cant A, Ozols MA [1997]. Computer-based safety critical systems in defense: evolution of the safety case. In: Proceedings of the 15th International System Safety Conference (Washington, DC). Unionville, VA: System Safety Society, pp. 599-608.

Fries EF, Fisher TJ, Jobes CC [2001]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 3: 2.2 Software safety. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2001-164, IC 9460.

IEC [1998a]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-1, Part 1: General requirements, version 4, May 12, 1998.

IEC [1998b]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-2, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, version 4, May 12, 1998.

IEC [1998c]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-3, Part 3: Software requirements, version 4, May 12, 1998.

IEC [1998d]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-4, Part 4: Definitions and abbreviations, version 4, May 12, 1998.

IEC [1998e]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-5, Part 5: Examples of methods for determination of safety integrity levels, version 4, May 12, 1998.

IEC [1998f]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-6, Part 6: Guidelines on the application of parts 2 and 3, version 4, May 12, 1998.

IEC [1998g]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC61508-7 Part 7: Overview of techniques and measures, version 4, May 12, 1998.

IEEE [1990]. IEEE Standard 828-1990: IEEE standard for software configuration management plans. Institute of Electrical and Electronics Engineers, Inc.

Leon A [2000]. A guide to software configuration management. Norwood, MA: Artech House Publishers.

Leveson NG [1992]. High-pressure steam engines and computer software. In: Proceedings of the International Conference on Software Engineering (Melbourne, Australia).

Leveson NG [1995]. Safeware: system safety and computers. Addison Wesley Publishing Co.

RTCA [1992]. DO-178B, software considerations in airborne systems and equipment certification. Washington, DC: RTCA, Inc.

Sammarco JJ, Fisher TJ [2001]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 2: 2.1 System safety. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2001-137, IC 9458.

Sammarco JJ, Kohler JL, Novak T, Morley LA [1997]. Safety issues and the use of software-controlled equipment in the mining industry. In: Proceedings of the IEEE-Industrial Applications Society 32nd Annual Meeting (October 5-9, 1997).

Sammarco JJ, Fisher TJ, Welsh JH, Pazuchanics MJ [1999]. Programmable electronics in mining: an introduction to safety. Pittsburgh, PA: NIOSH Special Workshop Report. Unpublished.

U.S. Department of Defense [1980]. Procedures for performing a failure mode effects and criticality analysis. Military Standard MIL-STD1629A.

Wilson SP, Kelly TP, McDermid JA [1997]. Safety case development: current practice, future prospects. In: Shaw R, ed. Proceedings of the 12th Annual CSR Workshop on Safety and Reliability of Software-Based Systems (Bruges, Belgium, September 12-15, 1995). New York, NY: Springer-Verlag, pp. 135-156.

APPENDIX A.—SAFETY FILE CHECKLIST

Following is a checklist of all of the documents to be included in the final safety file.

A.1 Safety Summary Documentation

_____Safety statement
_____Risk management summary (provided in SSPP and SWSP)
_____Reference file (Index and cross-references of all documents, contacts)
_____Personnel qualifications file

A.2 Safety Plans

_____System Safety Program Plan (if provided separately, then it only needs to be referenced)
_____Software Safety Plan (if provided separately, then it only needs to be referenced)
_____Management of Change Plan (if provided separately, then it only needs to be referenced)
_____Operation and Maintenance Plan(s) (if provided separately, then it only needs to be referenced)
_____Safety Validation Plan (if provided separately, then it only needs to be referenced)
_____Installation and Commissioning Plan (if provided separately, then it only needs to be referenced)

A.3 Safety Data and Methods Documentation

_____Product description (vendor's sales literature, general specifications, features)
_____Implementation document
_____User documents (operator's manual, maintenance manual, training manual)
_____History file
_____Hazard log
_____Hazard and risk analysis methods

A.4 Safety File Conclusion

_____Summary/conclusions
_____Signed statement affirming that the system is safe to operate

NOTE 29: It is highly recommended to first develop a preliminary high-level safety file during the initial design phase of the system, always keeping in mind that all safety-related claims need to have a justifiable basis, i.e., sufficient evidence and reasonable argument. Formal documentation at this stage is not necessary, but might eventually be required for a third-party assessment.

APPENDIX B.—RELATIONSHIP MODEL FOR THE SAFETY FILE (WITH DIAGRAMS)

The documents that comprise the safety file are developed during the development of the product and are results of the development activities. The goal is that the documents provide an auditable record that system safety has been addressed to the level required. However, the audit trail is dependent upon the external relationships of the documents to the system requirements and the development process, as well as to the internal contents of the documents.

To illustrate these relationships between the safety file documents and the activities, plans, and constraints of the development process, a relationship model is presented in figures B-1*A* through *G*. This model is based on a goal-structuring notation proposed by Wilson et al. [1997]. The model links together requirements, plans, and development results and documents by associating them with the goals of the development and the strategies used to attain those goals. It also links requirements from standards and regulations to the components of the safety file. Figure B-1 explains the symbols used in the model.

The proposed model contains eight goals:

(1) Mining system safety as applied to equipment used onsite
(2) Equipment requirements
(3) Equipment hardware requirements
(4) Equipment software (firmware) requirements
(5) Equipment microelectronic hardware requirements
(6) Documented plans and procedures
(7) Equipment implementation documentation
(8) Validation

These goals are briefly described below.

(1) Goal 1 (G1) - Mining System Safety As Applied to Equipment Used Onsite

Model (M1) - Equipment Definition: Product concept and expectations

Constraints 1, 2, and 3 (C1, C2, and C3): The limitations for functionality, reliability, and safety may involve tradeoffs in equipment design.

C1 - *Functionality:* What the equipment is intended to do and the intended use of the equipment.

C2 - *Reliability:* Estimation of the required availability-on-demand for the equipment.

C3 - *Safety:* Safety integrity level of the equipment used in the mining system.

Strategy 1 (S1) - *Risk Management Plan:* By developing a risk management plan, tradeoffs between functionality, reliability, and safety constraints can be made to maintain the required safety integrity level.

Solutions (SL)

Hazard identification: Reasonably foreseeable system-level and equipment-level hazards are identified and logged.

Risk analysis: The risk of each identified hazard is estimated and prioritized in accordance with the severity (level of consequence) and likelihood of occurrence (estimated for the equipment in the mining system). Determines probable source of risk at the system and equipment levels.

Risk mitigation: Design decisions that assign responsibility to subsystems of the system or of the equipment for reducing the severity and/or the likelihood of the hazard causing the risk to an acceptable level.

(2) Goal 2 (G2) - Equipment Requirements

Product is specified at an increasing level of detail.

(3-5) Goals 3, 4, and 5 (G3, G4, and G5) - These goals are subgoals of goal 2.

G3 - Equipment Hardware requirements

Strategy 2 (S2) - Intrinsic safety as required by MSHA; Title 30, Code of Federal Regulation, Part 18.68, and ACRI2001, Criteria for Evaluation and Test of Intrinsically Safe Apparatus and Associated Apparatus, specify MSHA's design requirements for intrinsically safe equipment for use in gassy underground operations; other acceptable standards.

G4 - Equipment software (firmware) requirements

G5 - Equipment microelectronic hardware requirements

Strategy 3 (S3): System Safety Program Plan

Standards, such as Standard for Safety for Software in Programmable Components, ANSI/UL 1998, may be used.

Validation of specified requirements for intended use, functionality, reliability, and safety integrity levels; traceability of safety-related aspects of the programmable subsystem throughout the safety file product-level documents.

Solution 1 (SL 1) - An auditable safety file for programmable subsystems in the equipment.

(6) Goal 6 (G6) - Documented Plans and Procedures - These documents are developed as guidelines for content and presentation of equipment documents, including forms and checklists. These are system-level documents.

Solution 2 (SL 2) - Models 2-7 (M2-M7): Types of system-level documents that need to be developed.

Strategies 4-9 (S4-S9): Lists criteria for each document for the safety file.

(7) Goal 7 (G7) - Equipment Implementation Documentation - These documents are developed as the safety file for the equipment under development. These are product-level documents and are produced uniquely for each product.

Solutions 3-10 (SL3-SL10): Types of product-level documents that make up the safety file.

Strategies 10-18 (S10-S18): Lists criteria for each document in the safety file.

Solution 11 (SL11): *Risk management summary:* A roadmap that points to the safety-related aspects of the product-level documents.

Strategy 19 (S19): Lists criteria for content of the summary for the safety file.

Justifications 1-11 (J1-J11): Relevant standards and regulatory requirements.

(8) Goal 8 (G8) - Validation - Validation to specified requirements for intended use, functionality, reliability, and safety integrity levels; traceability of safety-related aspects of the programmable subsystem throughout the safety file product-level documents.

Strategy 20 (S20): Traceability from document to document; traceability to established justifications; product-level tests to determine compliance with goals and requirements; safety statement.

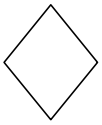
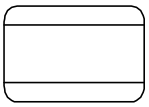
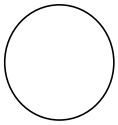
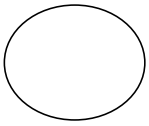
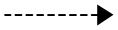
Items:	Definitions:	Abbreviations:	Symbols:
Goal	What is to be achieved	G	
Model	Framework for achievement	M	
Constraint	Limitations for achievement	C	
Justification	Nationally or internationally recognized Standards, Regulations, guidance documents, previously approved examples	J	
Strategy	How it is to be achieved	S	
Solution	Item produced as evidence of goal achievement.	SL	
Relationship	A primary relationship exists between the two items	PR	
	A secondary relationship exists between the two items	SR	

Figure B-1.—Model symbol key.

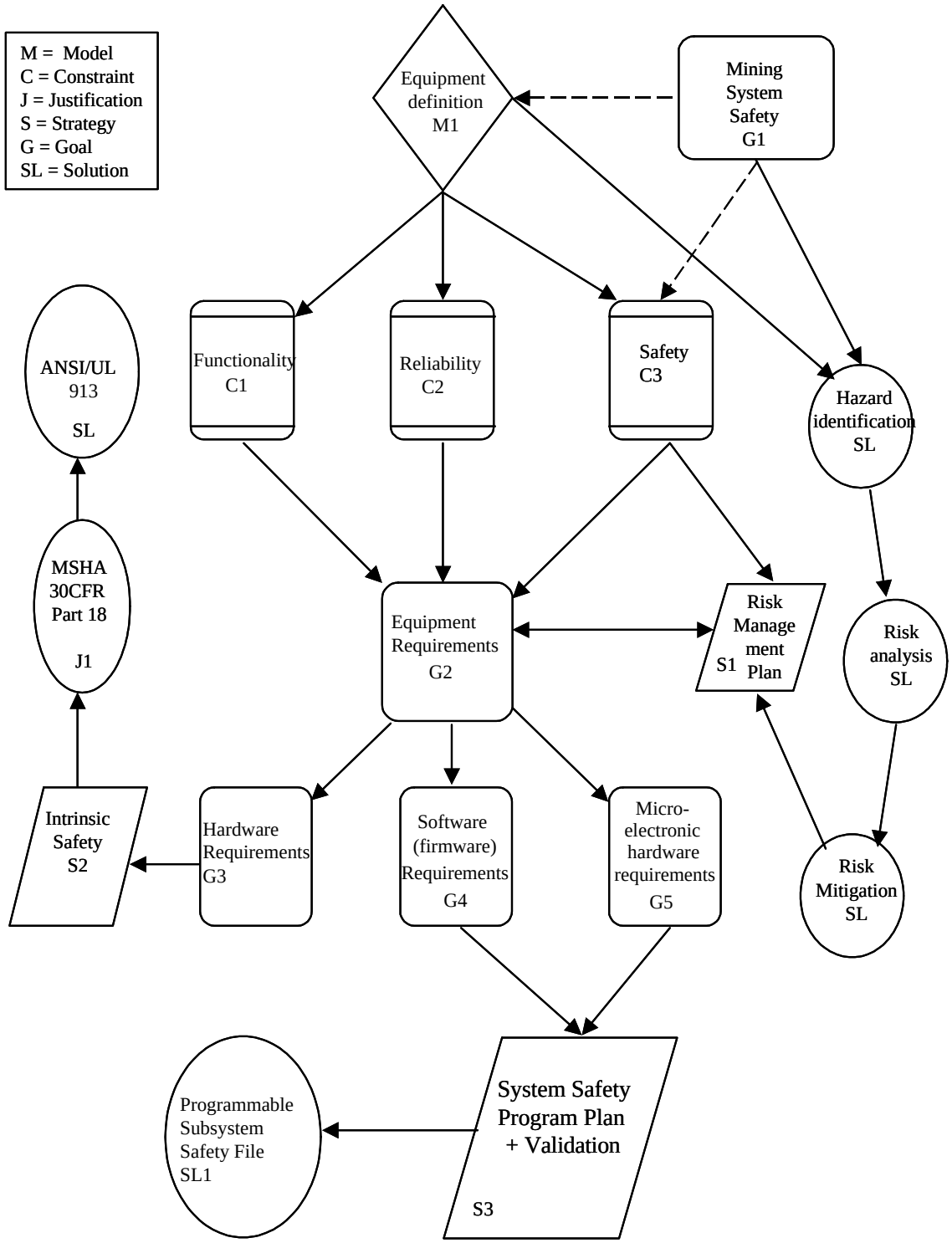


Figure B-1A.—Structural relationship model for the safety file - part A.

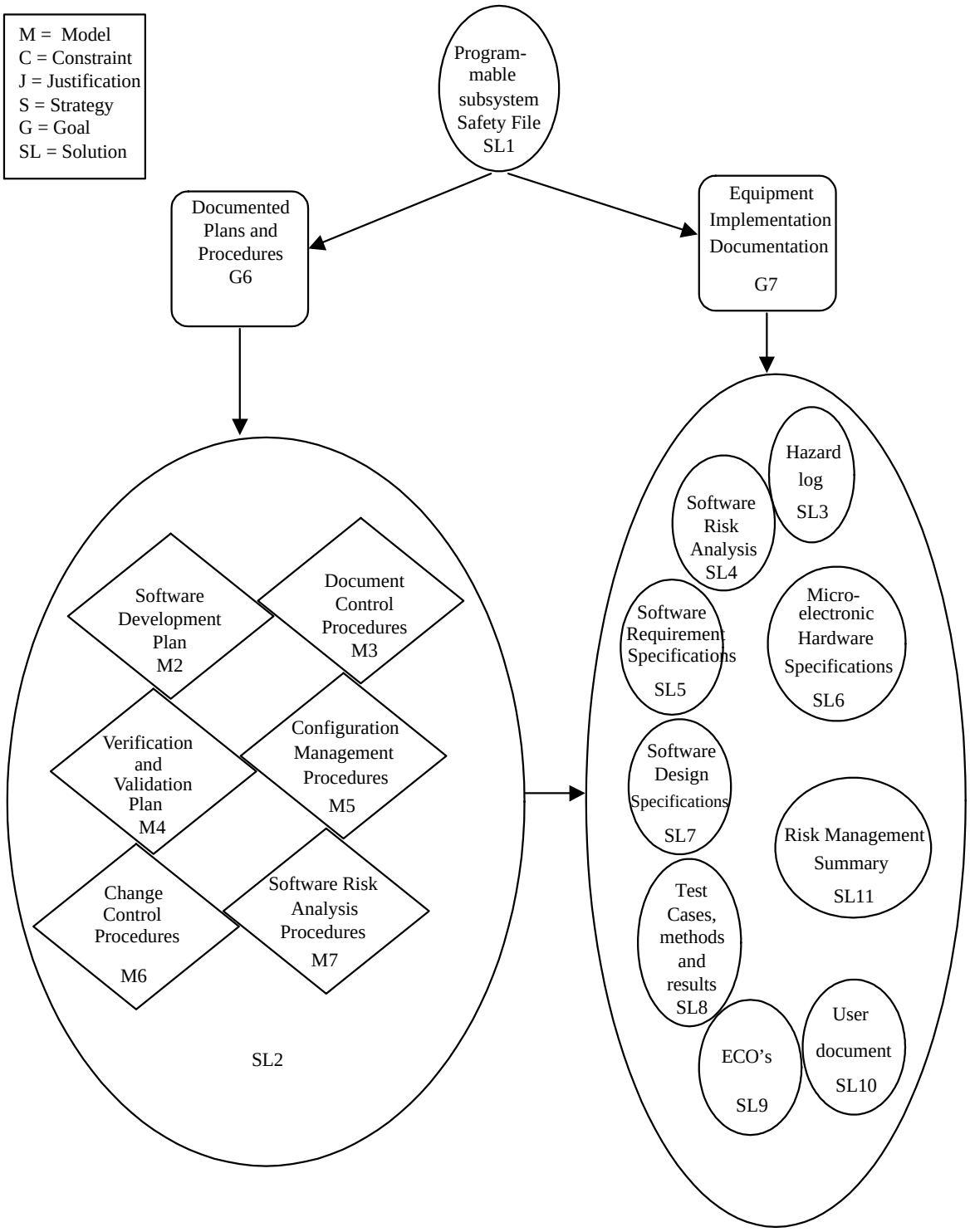


Figure B-1B.—Structural relationship model for the safety file - part B.

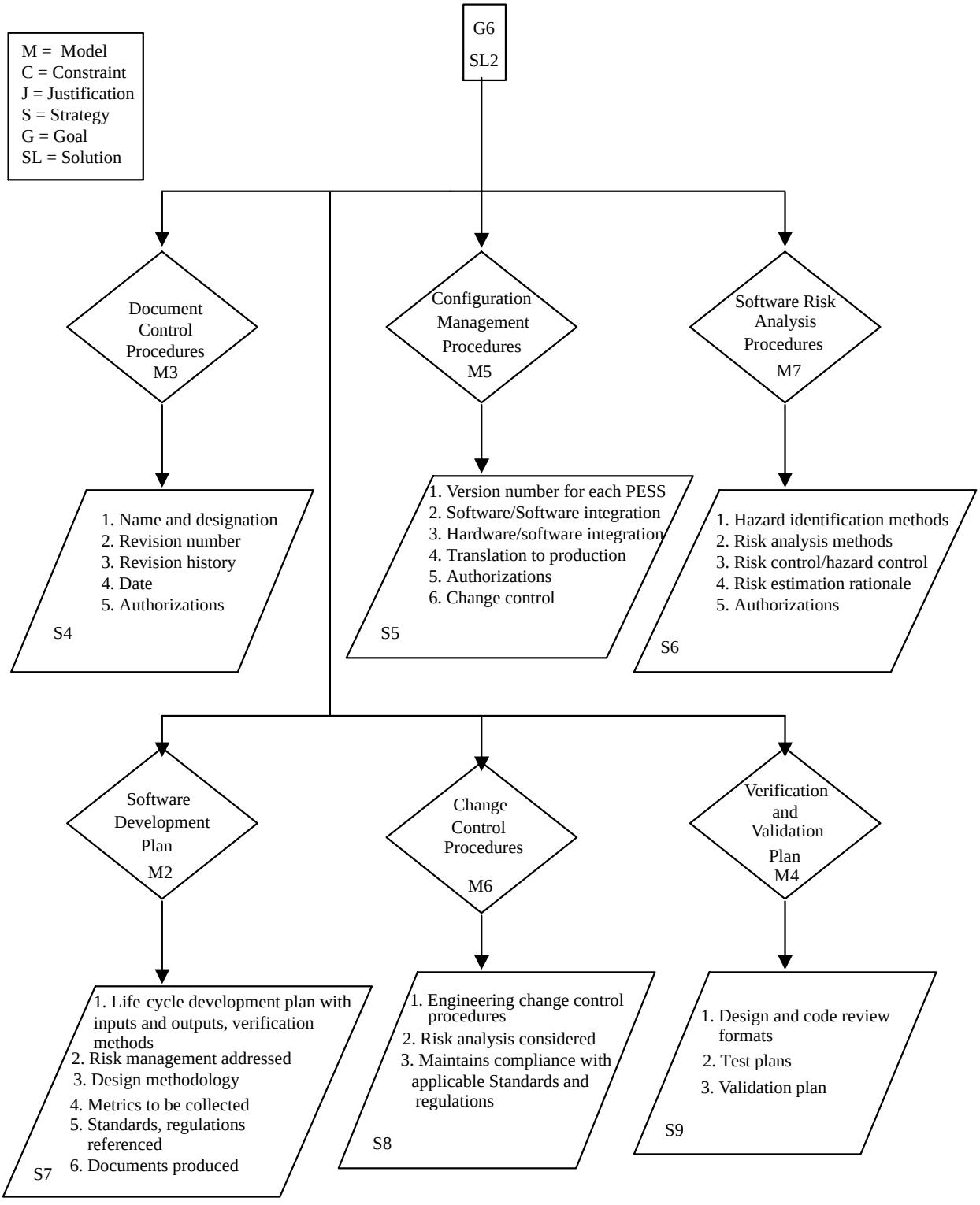


Figure B-1C.—Structural relationship model for the safety file - part C.

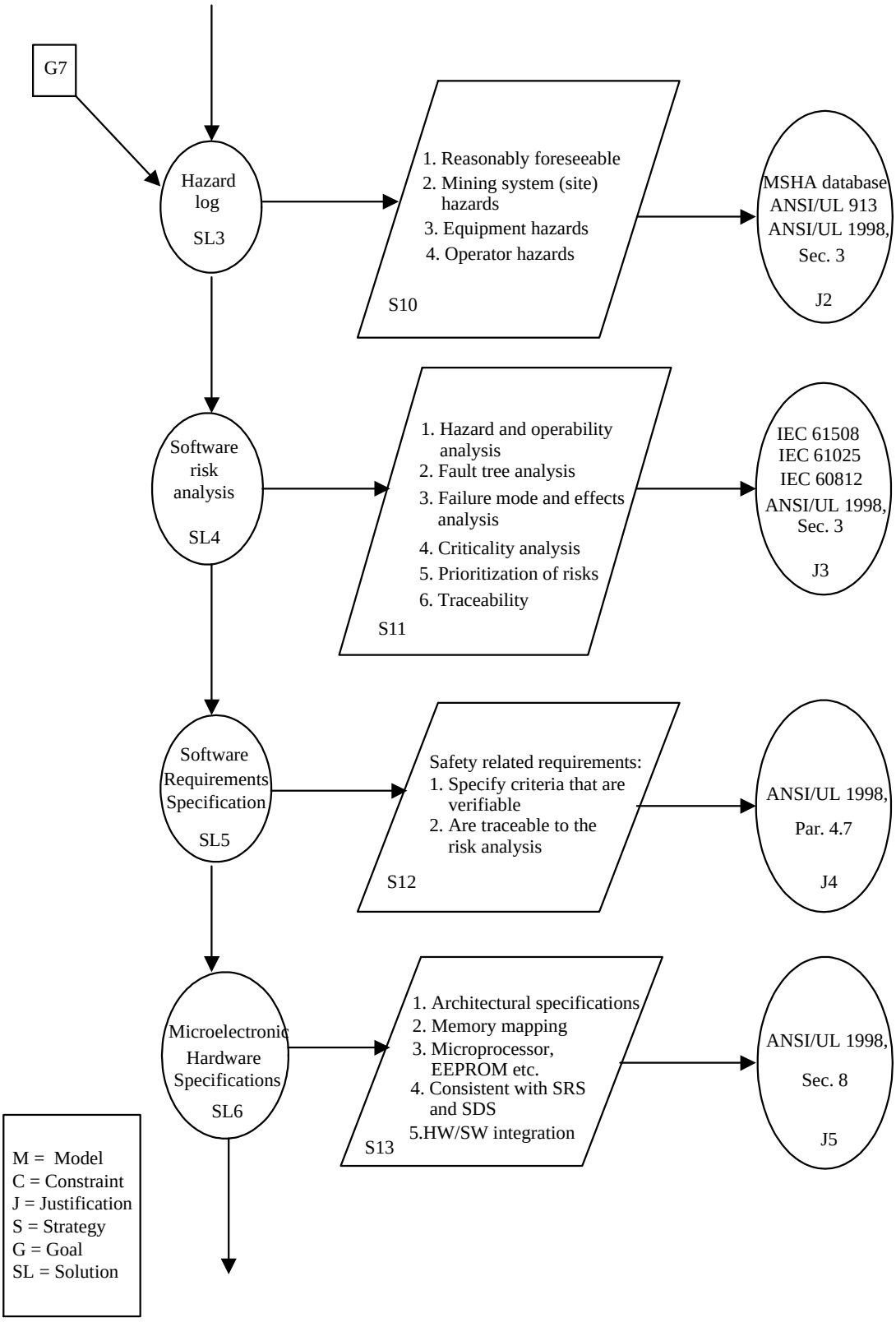


Figure B-1D.—Structural relationship model for the safety file - part D.

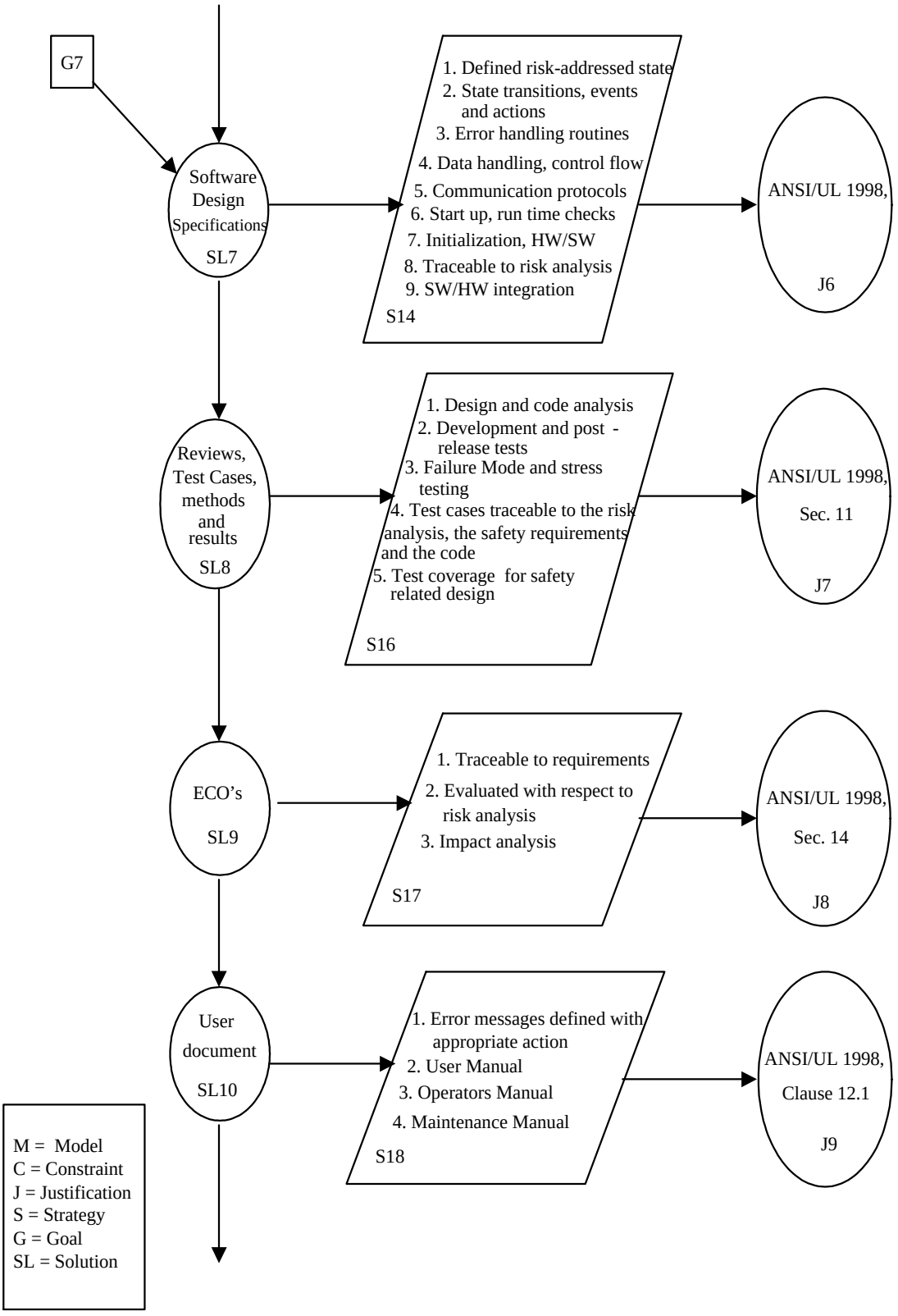


Figure B-1E.—Structural relationship model for the safety file - part E.

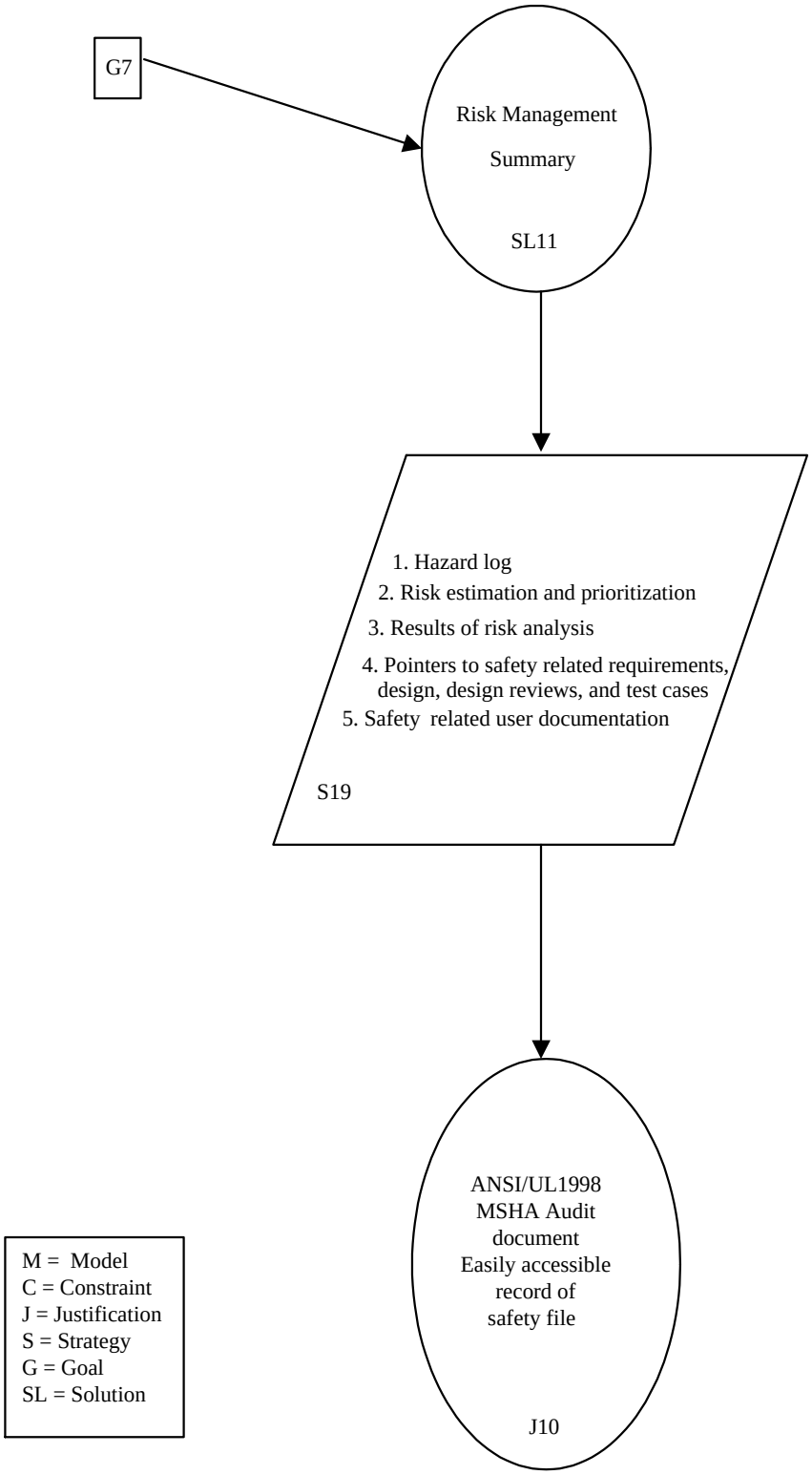


Figure B-1F.—Structural relationship model for the safety file - part F.

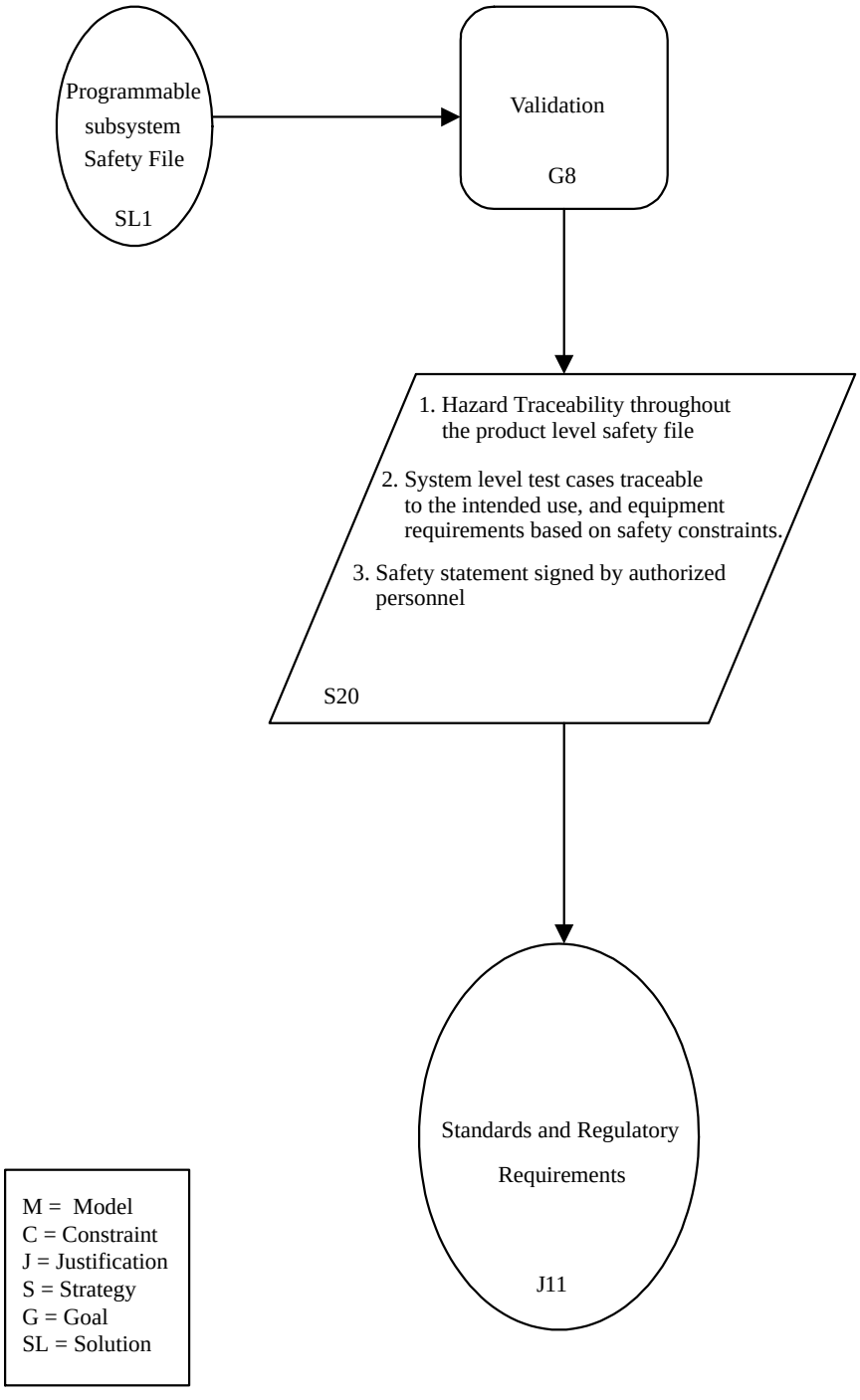


Figure B-1G.—Structural relationship model for the safety file - part G.

APPENDIX C.—SAMPLE PROCESS FOR CONSTRUCTING THE SAFETY FILE

The safety file consists of documentary evidence that safety issues have been identified and addressed. This documentary evidence is constructed as the activities associated with each development life cycle phase are performed.

Figure C-1 shows a development life cycle consisting of three phases: requirements, design, and implementation. The requirements phase consists of the activities to define and validate system requirements, including system safety requirements. The design phase consists of activities to produce system designs that meet the requirements and to conduct tradeoffs between the designs, resulting in a design that will be carried forward into the implementation phase. The implementation phase consists of the activities required to build the system and prepare it for delivery to the customer. Each of these phases has a verification and validation activity and ends with a review. Based on the results of the review, the phase is reiterated or the next phase is entered. A previous phase can also be reiterated from a latter phase if a problem is detected that requires a modification in the results of the previous phase.

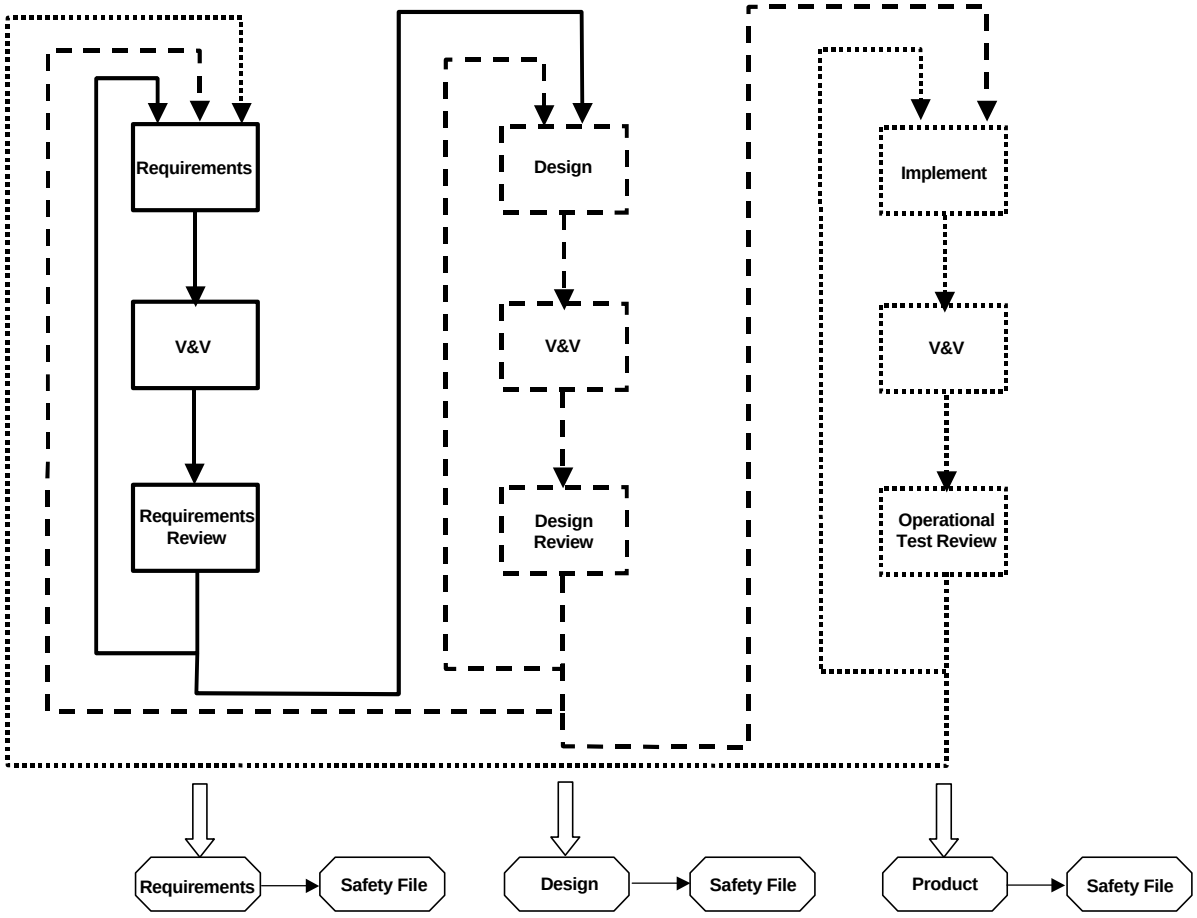


Figure C-1.—The safety file development process.

The development of the safety file in parallel with the development of the system provides an opportunity for safety issues to be addressed and verified throughout the life cycle. Early focus on safety issues and providing the evidence required to convince regulators and assessors of the safety of a product is important to a successful and timely certification process.

In general, a development life cycle consists of three phases: requirements, design, and implementation. After development, there is an operational phase and, in some cases, a decommissioning phase. The requirements phase consists of the activities to identify safety risks and to define and validate system requirements, including system safety requirements. The design phase consists of activities to produce system designs that meet the requirements and to conduct tradeoffs between the designs, resulting in a design that will be carried forward into the implementation phase. The implementation phase consists of the activities required to build the system and prepare it for delivery to the customer. The activities of each of these phases produce documents and artifacts for the safety file. For example, the results of the risk analysis produced by the requirements phase become part of the safety file.

Verification and validation (V&V) activities are included in each life cycle phase. These activities confirm that the products of each life cycle phase conform to their requirements. For example, V&V for the requirements phase includes validating that the requirements are complete. V&V activities provide important evidence for the safety file. Both the plans for and the results of V&V analyses become part of the safety file.

Each life cycle phase ends with a review to determine if the objectives of the phase have been met and if the criteria to proceed to the next life cycle phase are met. Based on the feedback from the review activity, the phase is reiterated or the next phase is initiated. A previous phase can also be reiterated if a problem is detected that requires a modification in the results of the previous phase. For example, if a problem with one of the system-level requirements is detected during the implementation phase, activities in the requirements phase will have to be performed again to correct the problem. The end-of-phase review also includes a review of the safety file to determine if the safety requirements are being met. Issues raised about the safety file at a review can be resolved before development continues.

APPENDIX D.—SAMPLE TEMPLATES FOR SAFETY FILE DOCUMENTS

The following tables illustrate a template for describing some of the documents in the safety file. The *Objective* entry describes what purpose the document serves. The *Recommended Contents* entry lists items that should be included in the document. The *Applicable Regulations or Clauses in Standards* entry is a reference back to specific regulatory requirements or requirements in standards. The *Structure ID* is a reference to the structural relationship model described in appendix B. The *Technical References* entry provides references to other documents that can be used for examples or for guidance.

PRODUCT DESCRIPTION	
Objective	Provides a multilevel summary description of the system or component architecture that describes the programmable system, the microelectronic hardware, and the software, including interfaces to electrical and mechanical hardware and humans.
Recommended Contents	1. Description of the mining environment and the relationship of the computerized system to the mining environment 2. Specification of the performance characteristics and limitations of the programmable system (e.g., operating limits, required backups, machine settings) 3. Diagrams showing configuration information 4. Specification of mechanical, electrical, and human interfaces, including identification of all limitations 5. References to specific code configuration and code in code libraries (includes *make files* and the like)
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Model 1
Technical References	None.

SYSTEM SAFETY PROGRAM PLAN	
Objective	Details the engineering and manufacturing processes, techniques, and methods used when developing the component or system that are important to safety achievement.
Recommended Contents	Refer to the System Safety document 2.1 [Sammarco and Fisher 2001].
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goals 1, 4, and 5; strategy 3
Technical References	Sammarco and Fisher [2001]

SOFTWARE SAFETY PLAN	
Objective	A component of the System Safety Program Plan. Details the engineering and manufacturing processes, techniques, and methods used when developing the software that are important to safety achievement.
Recommended Contents	Refer to the Software Safety document 2.2 [Fries et al. 2001].
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Strategy 3
References	Fries et al. [2001]

MANAGEMENT OF CHANGE PLAN	
Objective	Describes how changes to the software, microelectronic hardware, and interfaces (human, electrical, and mechanical) are managed.
Recommended Contents	1. A description of the configuration identification scheme, responsibilities, and activities used to maintain and control baselines 2. A description of the methods and activities used to formally control receipt, storage, handling, and release of configurable items 3. A description of the initiation, transmittal, review, disposition, implementation, and tracking of discrepancy reports (such as defects found) and change requests 4. A description of the hazard and risk analysis for the proposed change
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 6, solution 2, model 5, strategy 5
References	Leon A [2000] IEEE [1990]

REFERENCE FILE	
Objective	Provides a succinct index to all documents that form a part of the safety file, which are retained by the component manufacturer, the system integrator, and the operating company. Eases the auditing burden by providing a readily available index to safety file documents.
Recommended Contents	1. Scope of the safety file 2. References to architecture and configuration information 3. References to all safety file documents and data
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goals 6 and 7
Technical References	RTCA [1992]

IMPLEMENTATION DOCUMENTATION	
Objective	Records and results from applying the SSPP, SWSP, and the MOCP. May be multiple documents.
Recommended Contents	1. Engineering procedures (i.e., risk management, hazard analysis, design reviews, code reviews, unit/component/ system/hardware and software integration tests, etc.) 2. Results of applying engineering procedures (i.e., FMEA table, design and code review meeting minutes, test cases and results, etc.) 3. Documentation on COTS and contracted software See section 4, goal 7, solutions 3-10 for additional information.
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 7
Technical References	None.

USER DOCUMENT	
Objective	Provides documentation for the safe operation and maintenance of the equipment.
Recommended Contents	1. Description of equipment 2. Purpose of equipment 3. How to operate equipment 4. How to maintain equipment 5. Description of safety functions and devices See section 4, goal 7, solution 10, strategy 18 for additional information.
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 7
Technical References	None.

HISTORY FILE	
Objective	Captures document and change history for the system or the component.
Recommended Contents	1. Design and field changes 2. Incident reports See section 4, goal 7, solution 9 for additional information.
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 7, solution 9
Technical References	None.

RISK MANAGEMENT SUMMARY	
Objective	Details the risk management activities and summarizes the important risks identified and the means used to remove or mitigate them.
Recommended Contents	1. Risk management approach (i.e., paradigms followed, such as fail safe design, selection of design and programming languages, controlled and encouraged practices, use of traceability matrix) 2. Risk management activities (i.e., references to system and Software Safety Plans and any other risk control documents) 3. Risk management results 4. Limitations on use 5. Summary of SIL values assigned to safety functions 6. Traceability between hazard analysis, risk analysis, risk control, and verification results
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 7, solution 11
Technical References	U.S. Department of Defense [1980] Fries et al. [2001] Leveson [1995] Sammarco and Fisher [2001]

SAFETY STATEMENT	
Objective	Provides a succinct statement affirming the completeness and accuracy of the safety file and the level of safety demonstrated for the system.
Recommended Contents	1. Identification and scope of system or components covered 2. Intended use of system or components covered 3. Conditions of acceptability, including operating ranges and any restrictions/limitations on use 4. Identifies the safety integrity level and/or standard being attested to 5. A signed statement that affirms that the safety file— a. Accurately reflects the engineering of the system; b. Documents all identified conditions of acceptability; and c. Identifies compliance with standards, if any.
Applicable Regulations or Clauses in Standards	Complete listing of the regulations and standards that are applicable to the system. When only parts of a particular standard are applicable, the individual clauses that are applicable will be listed.
Structure ID	Goal 8, strategy 20
Technical References	None.