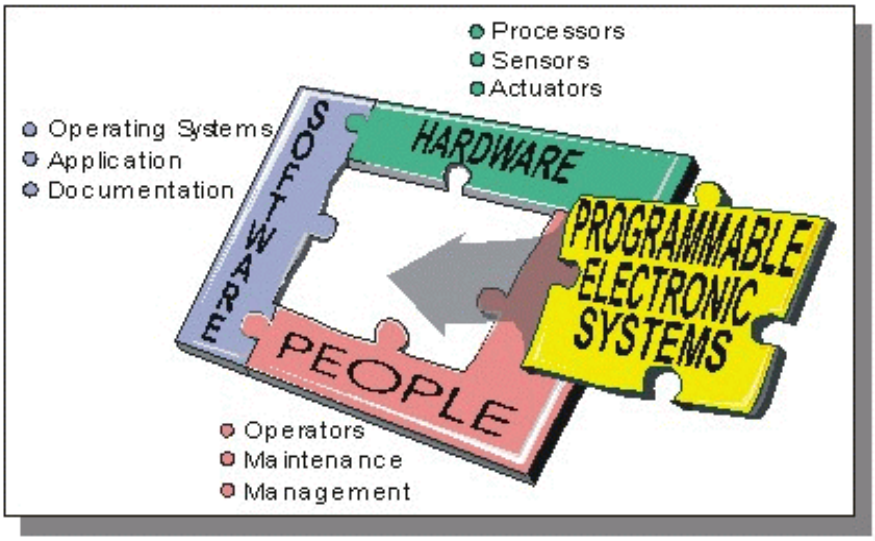
SYSTEM SAFETY EVALUATION PROGRAM

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



Part 5: 4.0 Independent Functional Safety Assessment

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, 2003

CONTENTS

Page

ILLUSTRATIONS

TABLES

ABBREVIATIONS USED IN THIS REPORT

ANSI	American National Standards Institute
CM	configuration management
E/E/PE	electrical/electronic/programmable electronic
E/E/PES	electrical/electronic/programmable electronic system
HAZOP	hazard and operability studies
IEC	International Electrotechnical Commission
MOC	management of change
MOCP	management of change plan
MSHA	Mine Safety and Health Administration
NIOSH	National Institute for Occupational Safety and Health
PE	programmable electronics
PES	programmable electronic system
PFSA	Preliminary Functional Safety Assessment
SIL	safety integrity level
SSPP	System Safety Program Plan
SWSP	Software Safety Plan
UL	Underwriters Laboratories, Inc.

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

Part 5: 4.0 Independent Functional Safety Assessment

By John J. Sammarco[1] and Edward F. Fries[2]

ABSTRACT

This report (Independent Functional Safety Assessment 4.0) is the fifth 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 meets the appropriate level of safety for the 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.

[1]Electrical engineer.

[2]Supervisory general engineer.

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

• 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.

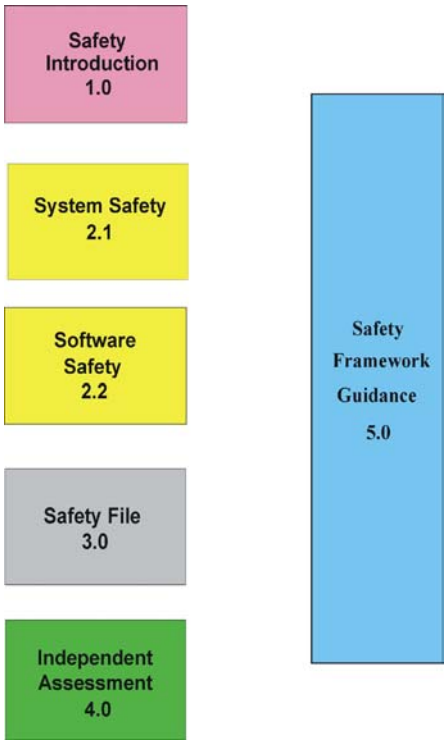


Figure 4.—The safety framework and associated guidance.

ACKNOWLEDGMENTS

The authors thank the System Safety Mining Industry Workgroup for reviewing and providing practical, constructive feedback for this and all previous recommendation documents. Members of the workgroup are listed below.

Name	Company
Anson, Jerry	P&H Mining Co.
Antoon, John[1]	Pennsylvania Bureau of Deep Mine Safety
Ceschini, Bob[1]	Pennsylvania Bureau of Deep Mine Safety
Cooper, David	Forced Potato
Cumbo, Terry	Line Power
Dechant, Fabian	Matric Ltd.
De Kock, Andre	ADK Systems
Erdman, Paul	Joy Mining Machinery
Ferguson, Dan[1]	DBT America, Inc.
Fidel, Mike	Eastern Associated Coal
Fisher, Tom[1]	NIOSH
Flemmer, Mike	NIOSH
Flynn, Chris[1]	Joy Mining Machinery
Flynt, Janet[1]	SSTS, Inc.
Fries, Edward F.[1]	NIOSH
Honaker, Jim[1]	Eastern Associated Coal
Kelly, Gene	MSHA, Coal Mine Safety and Health, District 2
Kenner, Jim	Wisdom Software
Ketler, Al	Rel-Tek Corp.
Koenig, Johannes	Marco
Kohart, Nick[1]	MSHA, Coal Mine Safety and Health, District 2
Lee, Larry	NIOSH
Lewetag, David C.[1]	MSHA, Coal Mine Safety and Health, District 2
Lowdermilk, Scott	Cattron, Inc.
Martin, Jim[1]	Rad Engineering
Murray, Larry	Marco North America, Inc.
Nave, Mike[1]	Consol, Inc.
Oliver, David	Cutler-Hammer Automation
Paddock, Bob[1]	Independent Consultant
Paques, Joseph-Jean[1]	Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) (Montreal, Quebec, Canada)
Podobinski, Dave	DBT America
Rhoades, Randy	CSE Corp.
Rudinec, Steve	Oldenburg Group, Inc.
Sammarco, John J.[1]	NIOSH
Schmidt, John[1] (retired)	DBT America
Sturtz, Doug[1]	Matric Ltd.
Van der Broek, Bert	Forced Potato
Watzman, Bruce	National Mining Association
Willis, John	Mitsubishi

[1]Workgroup meeting attendee.

The authors also 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." 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], Software Safety document 2.2 [Fries et al. 2001], and Safety File document 3.0 [Mowrey et al. 2002].

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 mainly to the safety-related parts of the system. However, many of the recommendations can also be applied to the basic system.

1.4 Purpose

The purpose of this document is to provide recommendations for an independent person or persons conducting a Functional Safety Assessment of a programmable electronic mining system. These recommendations address an assessment process covering the preliminary, initial, and periodic followup phases. It also addresses the specific safety documentation for a safety file, management of change, and a proven in use service history.

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].

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 IEEE Standard 610.12-1990 IEEE Standard Glossary of Software Engineering Technology, IEC 61508, and the *System Safety Analysis Handbook* [Stephans and Talso 1997]. A few definitions are adaptations or newly formed definitions specific to mining.

Action Item - A noted issue or task that the system/equipment provider should resolve before completing the Functional Safety Assessment or Followup Safety Assessment.

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.

Followup Safety Assessment - A systematic, independent, and periodic assessment to determine if the safety integrity of the product/machine/control system previously evaluated by the Functional Safety Assessment is being maintained. This assessment may include design modifications, fixes, etc., applied to the assessed product. This assessment should determine whether the actual procedures and rules specific to the functional safety requirements comply and adhere to the planned procedures and rules and that the planned procedures and rules are implemented effectively and suitably to achieve the specified safety objectives.

Functional Safety Assessment - A systematic analysis and study, based on evidence, to judge the functional safety achieved by one or more electrical/electronic/programmable electronic (E/E/PE) safety-related systems, other technology safety-related systems, or external risk reduction facilities. This assessment further includes a systematic and independent examination to determine whether

the actual procedures and rules specific to the functional safety requirements comply and adhere to the planned procedures and rules and that the planned procedures and rules are implemented effectively and suitably to achieve the specified safety objectives. Thus, the Functional Safety Assessment is a complete and independent assessment 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.

NOTE 1: The degree of independence depends on the SIL (see table 2).

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

Independent Person - A person who is separate and distinct from the activities and direct responsibilities taking place during a specific phase of the overall electrical/electronic/programmable electronic system (E/E/PES) or software safety life cycle that is subject to Functional Safety Assessment or validation.

Independent Department - A department that is separate and distinct from the departments responsible for the activities, subject to Functional Safety Assessment or validation, taking place during the specific phase of the overall E/E/PES or software safety life cycle.

Internal Assessment - Conducted by the service/equipment provider 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.

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.

Preliminary Functional Safety Assessment (PFSA) - An assessment before and/or during the product development process to determine if the appropriate design/development process controls have been or are being implemented and the recommended work products (safety file documentation) are planned for, are being, or will be produced. This assessment is not intended to determine if the product/machine/control system being designed and produced complies with applicable recommendations/standards/regulations, but that the procedural controls and processes applied during the design and development of such equipment and work products are in accordance with those recommendations/standards/regulations. The PFSA is conducted by those meeting the recommended level of independence of table 2.

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 (PES) - 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.

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

Safety - Freedom from unacceptable risk.

Safety Instrumented System - 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 2: SILs apply to safety functions of systems, protection layers, and devices using PE. "SIL" is a term used to specify the probability that a safety function satisfactorily performs given a set of conditions and constraints.

SIL 1 - Safety Integrity Level 1 indicates that a failure may be expected to result in an injury to persons requiring nonemergency medical treatment or damage to property requiring nonextensive repairs.

SIL 2 - Safety Integrity Level 2 indicates that a failure may be expected to result in serious injury to persons requiring emergency medical treatment or damage to property requiring moderate repairs and/or temporary shutdown of operations.

SIL 3 - Safety Integrity Level 3 indicates that a failure may be expected to result in life-threatening injury to persons or damage to property requiring extensive repairs and/or prolonged shutdown of operations.

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 Program Plan - The Software Safety Plan (SWSP) specifies the safety requirements for the software in a programmable electronic system and describes how the requirements will be met and how it will be demonstrated that the requirements have been met. The SWSP also describes the functionality, safety features, and operating modes of the software.

Software Verification - To the extent required by the safety integrity level, a test and evaluation of 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.

System Safety Program Plan - The System Safety Program Plan (SSPP) specifies the safety management and requirements for a programmable electronic system and describes how the requirements will be met and how it will be demonstrated that the requirements have been met. The SSPP also describes the functionality, safety features, and operating modes of the system.

Third Party - An organizational division, subsidiary, or other organization that is separate and distinct, by management and other resources, from the organization or department responsible for the activities, subject to Functional Safety Assessment or validation, taking place during the specific phase of the overall E/E/PES or software safety life cycle.

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 Independent Functional Safety Assessment Plan

Objectives:

4.1 To assess if appropriate methods, techniques, and processes have been used to—

- Identify and analyze all reasonably foreseeable hazards and risks
- Mitigate the identified hazards and risks to achieve an appropriate level of safety
- Assign SILs
- Verify that the SIL is met
- Document the system with a safety file document

4.2 To assess if adequate evidence exists to support and document 4.1.

4.3 To create a plan enabling a systematic, consistent, and comprehensive Functional Safety Assessment.

Recommendations:

4.4 The Functional Safety Assessment Plan should be created by the manufacturer, integrator, or system end-user. Ideally, the plan should be a collaborative effort by the manufacturer, system integrator, and system end-user.

4.5 The Functional Safety Assessment Plan should accommodate incremental implementation carried out in parallel with the system's development.

4.6 The Functional Safety Assessment Plan should be divided into three parts:

- Part 1 - Preliminary Independent Functional Safety Assessment
- Part 2 - Initial Independent Functional Safety Assessment
- Part 3 - Followup Functional Safety Assessment

NOTE 3: The Functional Safety Assessment Plan is applied to the process of developing and maintaining a programmable system for a particular piece of equipment at a particular mining site. The required document attributes to be reviewed by an assessor increase in scope with the SIL. See table 5 for a listing of these attributes.

4.7 Items that a Preliminary Independent Functional Safety Assessment should address include—

- A review of the preliminary safety file
- Evidence of the intent to provide a means to increase the likelihood of successfully completing the Initial Functional Safety Assessment

4.8 Items that an Initial Functional Safety Assessment should address include—

- Evidence that it was preceded by a Preliminary Functional Safety Assessment
- An assessment of the safety file for the system under review
- Intentions to confirm and document the SIL for the system or equipment and SILs for all subsystems
- An assessment to determine the capability to maintain these SILs

Appendix A contains a typical agenda for the Independent Functional Safety Assessment.

4.9 Items that the Followup Safety Assessment should address include—

- An analysis of the modification control documents and revised risk analysis
- A successful completion of the Initial Independent Functional Safety Assessment
- A scheduled assessment in accordance with the established SIL of the system or equipment (see table 4)
- A level of assurance that the system/equipment provider continues to be capable of maintaining the established SIL

Appendix B contains a typical agenda for the Periodic Followup Safety Assessments.

4.10 The independent Functional Safety Assessment Plan should accommodate various levels of independence that vary in relation to the SIL, as shown in table 2.

Table 2.—Recommended degree of independence

Degree of independence	SIL 1	SIL 2	SIL 3
Independent person	HR	HR	nr
Independent department . . .	—	HR	HR
Third party	—	—	HR

HR = highly recommended. nr = not recommended.
A dash (—) indicates no recommendation.

Source: Adapted from IEC [1998a].

Other application-specific factors may also be used to help determine the appropriate level of independence [IEC 1998a]:

1. Greater complexity
2. Greater novelty of design
3. Greater novelty of technology
4. Lack of standardized design
5. Higher SIL requirement
6. Lack of experience with a similar design
7. Lack of service history

5.0 Independent Functional Safety Assessment Processes

5.1 Preliminary Independent Functional Safety Assessment

Objectives:

5.1.1 To provide an early independent Functional Safety Assessment of the system, plans, and preliminary safety file so as to reduce the potential for costly rework at the final stages of assessment.

5.1.2 To provide an early independent Functional Safety Assessment of the SIL(s) so as to reduce the potential for costly rework at the final stages of assessment because of an inappropriate assignment of SIL(s).

Recommendations:

5.1.3 The Independent Functional Safety Assessment Plan should be part of the preparation for the Initial Independent Functional Safety Assessment.

5.1.4 The following reports and plans should be considered as inputs:

- The system/equipment description
- The System Safety Plan
- The Software Safety Plan
- Documents and procedures for the safety file
- Quality assurance policies, procedures, and processes

5.1.5 The following steps should be considered as the process:

(1) A review of the declared SIL with respect to the type of mining product or system to be produced
(2) A review of the System Safety Plan
(3) A review of the Software Safety Plan
(4) Review of documented procedures for the safety file
(5) Review of the risk management procedures and initial risk assessment activities

5.1.6 The output should result in a report indicating the level of conformance of the plans and procedures with that expected for the declared SIL.

5.1.7 The results of the Preliminary Independent Functional Safety Assessment should be documented in a preliminary report containing the following information [U.K. Ministry of Defence 1996]:

- A description of the assessment's scope
- A very brief description of the system and the application domain of the system
- A listing of all documentation examined
- A listing of all reference material used for the assessment
- A listing of all SILs that are adequately designated and justified
- A listing of SILs lacking sufficient support and justification, if any exist
- A listing of concerns or deficiencies
- A summary of results
- Identification of the assessor(s) and their associated affiliations

5.1.8 The Preliminary Independent Functional Safety Assessment should be conducted on a per-system basis for a given application.

5.1.9 Although the Preliminary Independent Functional Safety Assessment is desirable, it is an option exercised at the discretion of the manufacturer. The Preliminary Independent Functional Safety Assessment becomes more desirable as the SIL increases, as shown in table 3.

Table 3.—Recommended preliminary safety assessment schedule

	SIL 1	SIL 2	SIL 3
Preliminary safety assessment . . .	—	R	HR

R = Recommended. HR = highly recommended.
A dash (—) indicates no recommendation.

5.2 Initial Independent Functional Safety Assessment

Objectives:

5.2.1 To obtain an Independent Functional Safety Assessment that the system/equipment provider has established and has the capability to maintain the appropriate safety integrity level for the programmable electronics and software in the system/equipment provided.

Recommendations:

5.2.2 The following should be considered as inputs:

- Product or system description
- Qualified and authorized system/equipment provider personnel
- Registered quality system or equivalent
- Safety file for the system/equipment
- Independent qualified assessor to conduct the assessment
- Proven in use evidence conforming to the recommendations of section 8.0

5.2.3 The following steps should be considered as the process:

(1) A review of the documents submitted by the manufacturer as evidence of compliance
(2) Review of documented procedures
(3) Review of the configuration management system applied to the system/equipment during development and at production time
(4) Review of the risk/hazard analysis and prioritization of identified risks at the system/equipment level
(5) A detailed analysis of the risk management design and implementation
(6) A traceability analysis of system risk mitigation throughout the defined development life cycle processes, including verification means at each defined breakpoint
(7) Verification and validation tests to be selected and witnessed by the independent assessor

NOTE 4: The review acquires information from the staff members involved about the design and safety management practices as implemented in the product development life cycle.

NOTE 5: The system/equipment provider is responsible for the resolution of all action items.

5.2.4 The following should be provided by the independent assessor as output:

(1) Assessment report
(2) Periodic Followup Safety Assessment Plan

5.2.5 The results of the Independent Functional Safety Assessment should be documented in a report containing the following information [U.K. Ministry of Defence 1996]:

- The assessment result (see **NOTE 6**)
- A description of the assessment's scope
- A description of the system and the application domain of the system
- A listing of all documentation and document version numbers examined
- A listing of all reference material used for the assessment
- A listing of all SILs that are adequately designated and justified
- A listing of SILs lacking sufficient support and justification, if any exist

- Identification of prior service history information used in the assessment, if any such information exists
- A listing of safety claims lacking sufficient support and justification
- A listing of action items to change the assessment category to acceptance
- A summary of results
- Identification of the assessor(s) and their associated affiliations

NOTE 6: The assessment result can be one of three categories: acceptance, qualified acceptance, or rejection.

5.2.6 The Initial Independent Functional Safety Assessment should be conducted on a per-system basis for a given application. For example, the assessment would specifically address a given make and model of continuous mining machine for use at a specific mining site.

NOTE 7: Models can be based on common components with specific features being added/deleted or enabled/disabled based on user requirements. Results of previous Functional Safety Assessments may be reused as long as these assessment data are augmented with data from additional assessments of the impact of changes made.

5.3 Periodic Followup Safety Assessments

Objectives:

5.3.1 To obtain an Independent Functional Safety Assessment of the system/equipment provider's continued capability to maintain the appropriate safety integrity level for the programmable electronics and software in the system/equipment provided.

Recommendations:

5.3.2 The following should be considered as inputs:

- Initial Functional Safety Assessment Report
- System/equipment provider's internal assessment reports
- Records of changes/modifications to the software and programmable electronics
- Records of the reevaluated and updated safety file
- Qualified and authorized system/equipment provider personnel
- Registered quality system or equivalent
- Independent qualified assessor
- Records of changes in the user/application environment, as appropriate

NOTE 8: If the use of the equipment has changed, then there may be a need for redesign, testing, and validation. This may or may not be known to the equipment vendor; thus, the term "as appropriate" is added. However, whenever there is ongoing dialogue during equipment servicing about changes in use of the equipment, it is important to consider the impact of these changes on the achievement of functional safety. Examples of changes to be considered include adding or removing other protective functions or changing operating procedures.

5.3.3 The following steps should be considered as the process:

(1) A review of the system/equipment provider's documented internal assessment plan and reports

(2) A review of the risk management summary
(3) A review of the defined process for initiating a change request, modifying the hardware and/or software, and updating the associated documentation, including—

(a) The risk analysis and the determination that the proposed changes do (or do not) impact the programmable electronics and/or software.
(b) An explanation summarizing the software changes and a brief rationale for making these changes (e.g., additional functionality requested from the customer; a bug fix; the removal, improvement, and/or addition of a software feature; etc.). Depending on the complexity of the proposed changes, the auditor may request additional documentation to get a more detailed description of the changes.
(c) The verification and validation activities relating to the software changes, regression testing, and results of the implementation of the verification and validation activities and testing.

NOTE 9: Again, the system/equipment provider is responsible for the resolution of all action items.

The Periodic Followup Safety Assessment is determined during, but scheduled after, the Initial Functional Safety Assessment. Table 4 details the recommended audit schedule based on the SIL.

Table 4.—Recommended safety assessment schedule

	SIL 1	SIL 2	SIL 3
Annual safety assessment	—	HR	HR
Semiannual safety assessment . . .	—	R	HR

HR = highly recommended. R = Recommended.
A dash (—) indicates no recommendation.

NOTE 10: This table follows the degree of independence specified in table 2. Thus, if a third-party assessment is recommended by table 2, then the followup assessment should also be performed by a third party.

5.3.4 The following should be provided as output:
- Report provided by the independent auditor
- Update Independent Functional Safety Assessment documents, as needed

5.3.5 The report should include—
- Identification of the system/equipment provider
- A listing of all documentation and document version numbers examined
- A listing of all reference material used for the audit
- A listing of management and safety processes used for the development and maintenance of systems that are deficient
- A listing of management and safety processes for the development and maintenance of systems that lack evidence that the processes are being used consistently and properly

- A listing of action items to change the audit category from “rejection” or “qualified acceptance”
- A summary of results
- Identification of the assessor(s) and their associated affiliations

Table 5.—Safety file document assessment attributes

Safety file document sets	Attributes	SIL 1	SIL 2	SIL 3
Risk management	Risk management summary	X	X	X
	Hazard identification	X	X	X
	Hazard/risk analysis	X	X	X
	SIL	X	X	X
	Risk prioritization		X	X
	Risk control measures	X	X	X
Requirements	Traceability to risk management documents	X	X	X
	Consistency			X
	Completeness	X	X	X
	Measurable/verifiable	X	X	X
	Memory management		X	X
	Timing constraints		X	X
	Units of measurement			X
	Hardware platform	X	X	X
Architecture	Block diagrams	X	X	X
	Hardware/software interfaces	X	X	X
	Hierarchical diagrams			X
	Memory mapping		X	X
Design	Traceable to the requirements specifications	X	X	X
	Defined risk-addressed state(s)	X	X	X
	Site transitions with events and actions		X	X
	Error handling routines		X	X
	Data dictionaries			X
	Control flow			X
	Data flow			X
Implementation	Traceable to the design specifications	X	X	X
	Coding standards			X
	Tools used		X	X
	Maintainability, documented, modular	X	X	X
	No extraneous code or added unspecified features			X
Verification	Test cases are traceable to the risk analysis and requirements specification.	X	X	X
	Completion criteria defined	X	X	X
	Design reviews			X
	Static analysis	X	X	X
	Dynamic analysis		X	X
	Branch coverage testing		X	X
	Unit tests			X
	Integration tests		X	X
	Test tools			X
Validation	Traceability analysis throughout document sets	X	X	X
	Product testing		X	X
	Independent validator			X
Document control procedures	Identification code	X	X	X
	Name	X	X	X
	Date	X	X	X
	Revision history	X	X	X
	Provider authorization		X	X
Configuration management procedures	Version(s) identifier(s)	X	X	X
	Revision history of modifications	X	X	X
	Risk analysis reviewed before modification	X	X	X

Assigned personnel only for modifications			X	X
Authorization procedures as specified in the MOCP . . .	X	X	X	

5.3.6 The safety assessment may address multiple systems because the safety assessment focuses on the system provider's safety processes and plans.

6.0 Assessing the Safety File

Objectives:

6.1 To evaluate the adequacy of the safety file based on attributes of the system and the development process as described in the documents that comprise the safety file.

NOTE 11: These attributes are listed in table 5, and the SIL at which each attribute is assessed is indicated. The required attributes increase in scope with the SIL. The higher the SIL, the larger the set of attributes that must be satisfied.

Recommendations:

6.2 Assessment shortcomings should be identified and documented by the Independent Functional Safety Assessment party. Shortcomings should be identified by the following classifications:

- Missing evidence or justification
- Insufficient evidence or justification
- Inappropriate evidence or justification

7.0 Management of Change (MOC)

Objectives:

7.1 To obtain an Independent Functional Safety Assessment that the system/equipment provider has conducted a safety analysis of proposed change(s) and has established the appropriate safety integrity level(s) for the programmable electronics and software in the system/equipment provided.

7.2 To obtain an Independent Functional Safety Assessment that the system/equipment provider has implemented MOC for the programmable electronics and software in the system/ equipment provided in accordance with the Management of Change Plan (MOCP).

Recommendations:

7.3 Modifications of programmable electronics and software in the system/equipment should be assessed for safety as recommended by table 6.

Table 6.—Recommended Management of Change

Degree of independence	SIL 1	SIL 2	SIL 3
Independent person	HR	HR	nr
Independent department . . .	—	HR	HR
Third party	—	—	HR

HR = highly recommended. nr = not recommended.
A dash (—) indicates no recommendation.

7.4 The Independent Safety Assessments in table 6 should be completed and assessed as passed before implementing the change(s).

7.5 The Independent Functional Safety Assessment should assess the safety analysis of proposed change(s) and the proposed safety integrity level(s).

7.6 The Independent Functional Safety Assessment of proposed change(s) should include an audit of the MOCP.

8.0 Proven in Use (Service History)

Objectives:

8.1 To use systems, subsystems, and components having a proven and documented safe history of service, but lacking formal and rigorous verification.

8.2 To facilitate the Functional Safety Assessment of systems, subsystems, and components by using prior functional safety assessments.

8.3 To facilitate the Functional Safety Assessment of systems by using prior functional safety assessments of the same system for a different application and installation.

8.4 To facilitate the Functional Safety Assessment of systems with a service history.

Recommendations:

8.5 The independent functional safety assessor may accept existing systems under the proven in use concept.

8.6 The proven in use concept should support, justify, and validate functional safety by producing documented evidence of a safe service history.

8.7 Safe service history documentation should include incident rates and severity, as well as problem reports of in-service problems that may have not resulted in an incident.

8.8 Safe service history documentation should include—

- Exposure data
- Environmental conditions

- Operational profiles
- Maintenance frequencies and rigor
- MOC data
- Random hardware failure data

NOTE 12: Exposure data could include the length of service history and the number of systems. One system operating for 1 year has a much lower exposure than 50 systems operating for 1 year.

8.9 The safe service history duration, in terms of failure-free operating hours, should increase with respect to the SIL, as shown in table 7.

Table 7.—Recommended safe service duration for various SILs

SIL	Hazard-free operating hours
1	3×10^2
2	3×10^3
3	3×10^4

NOTE 13: A failure resulting in a fail-safe condition or state is considered hazard-free.

8.10 The Initial Independent Functional Safety Assessment must assess functional safety in the context of the entire system.

NOTE 14: Safety is an emergent property of the entire system. All of the individual parts of a new system could have a safe service history. However, the safe service history of the parts alone does not provide assurance that these parts will combine and function safely in a new system.

REFERENCES

CASS Scheme Ltd. [2002]. Conformity assessment of safety-related systems. [http:// www.cass.uk.net]. Date accessed: March 11, 2002.

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 IEC65108-1, 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 IEC65108-2, 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 IEC65108-3, 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 IEC65108-4, 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 IEC65108-5, 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 IEC65108-6, 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 IEC65108-7 Part 7: Overview of techniques and measures, version 4, May 12, 1998.

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

Mowrey GL, Fisher TJ, Sammarco JJ, Fries EF [2002]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 4: 3.0 Safety file. 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. 2002-134, IC 9461.

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.

Stephans RA, Talso WW [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: The System Safety Society, Section 3.

U.K. Ministry of Defence [1996]. Safety Management Requirements for Defence Systems. Parts 1 and 2. INT DEF STAN 00-56. Glasgow, U.K.: Ministry of Defence.

APPENDIX A.—TYPICAL AGENDA FOR INDEPENDENT FUNCTIONAL SAFETY ASSESSMENT

The Independent Functional Safety Assessment consists of eight primary activities:

(1) An introduction
(2) A review of documentation
(3) An analysis of the configuration management system and its application
(4) An analysis of the risk management process
(5) A review of safety-related design issues
(6) A traceability analysis of hazard mitigation throughout the development process
(7) Test witnessing
(8) A closing meeting

The following section lists the specific items reviewed during each of these parts.

NOTE 15: Those items identified by the Preliminary Functional Safety Assessment may be part of the PFSA process. The items so identified may be selected as needed based on the timing of the PFSA during the design/development life cycle.

(1) Introduction (PFSA)
- Review agenda
- System/equipment demonstration or explanation

(2) Document Review
- Mapping of documents to required attributes (see table 5) (PFSA)
- Review of documents
  - < User documents for appropriate cautionary statements of residual risk
  - < Document control procedures (PFSA)
  - < Configuration management procedures (PFSA)
  - < PES development plan, safety life cycle project management plan (PFSA)
  - < Risk management plan; procedures for risk identification, analysis, and control (PFSA)
  - < Verification and validation procedures and assignment of personnel (PFSA, test plan only, procedures are likely under development)
  - < Modification/change control procedures (PFSA)
  - < Internal assessment plan/report (PFSA, identification plan/procedures only)

(3) Applied Configuration Management System
- Description of the PES life cycle phases, including (PFSA, only life cycle phases)—
  - < The defined inputs and expected outputs
  - < The verification methods used to verify the outputs of each life-cycle phase
  - < The validation to requirements

- < Determination of the point in the initial development that configuration management (CM) is formally applied for each software component of the system (PFSA, CM Plan only)
- < Version numbers for each software component of the system and how the version number for the system is derived from the version numbers for each subsystem (PFSA, identification plan/procedures only)

(4) Risk Management
- Risk management summary (PFSA)
- Hazard identification
- Risk identification
- Risk analysis
- Risk categorization with rationale
- SIL categorization for each risk with SIL categorization rationale
- Risk control measures with rationale

(5) Review of Safety-Related Design
- State transition diagrams
- Fail-safe state
- Error handling routines
- Partitioning
- Software architecture
- Hardware architecture
- Functional block diagrams

(6) Traceability
- Review documentation for traceability of safety requirements and hazard mitigation throughout all life cycle phases. The objective is to account for each safety requirement and hazard mitigation, thereby reducing errors of omission.
- Follow several threads (specific items) throughout the documents.

(7) Test Witnessing
- Review of test equipment, setup, and procedures
- Version/identification tests

  These tests pertain to the identification of the correct software version. These are tests run at the time of production that verify that the correct version of software has been integrated with the hardware platform.
- Memory Testing

  Testing should cover memory testing and management appropriate for the required SIL. Write-protected RAM, ROM, or other write-protected memory tests should detect injected or simulated faults and respond with the appropriate response. Memory management tests should demonstrate that program code resides in ROM or other write-protected memory and cannot be overwritten.

NOTE 16: IEC 61508 Part 7 [IEC 1998g] contains an overview of testing techniques for detecting memory failures.

- Boundary Condition Testing
  This type of testing pertains to the examination of behavior approaching and exceeding boundary conditions.
- Error handling tests for timing errors, parameter checking, and computational errors
- Selected tests from verification plan traceable to the risk analysis

(8) Closing Meeting (PFSA)
- Assessment report discussion
- Action items
- Planning for next action

APPENDIX B.—TYPICAL AGENDA FOR PERIODIC FOLLOWUP SAFETY ASSESSMENT

The Periodic Followup Safety Assessment consists of eight primary activities:
(1) An introduction
(2) A review of documentation
(3) An analysis of the configuration management system and its application
(4) An analysis of the risk management process
(5) A review of changes made to safety-related design
(6) A traceability analysis of hazard mitigation throughout the development process
(7) Verification testing
(8) A closing meeting

While the scope of the Independent Functional Safety Assessment addresses both the complete system and the full development life cycle, the scope of the Periodic Followup Safety Assessment addresses only changes and modifications to the system once the Independent Safety Assessment is completed. The following section lists the specific items reviewed during each of these parts.

(1) Introduction
- Review agenda
- System/equipment demonstration/explanation

(2) Document Review
- Internal assessment reports
- Problem reports

(3) Applied Configuration Management System
- Engineering change orders
- Configuration control

(4) Risk Management
- Risk management summary
- Risk identification
- Updated risk analysis
- Prioritizing identified risks with rationale
- Risk control measures with rationale

(5) Review of Changes to Safety-Related Design
- State transition diagrams
- Fail-safe state
- Error handling routines
- Partitioning
- Software architecture
- Hardware architecture
- Functional block diagrams

(6) Traceability Analysis

For changes or new items, review documentation for traceability of safety requirements and hazard mitigation throughout all life cycle phases. The objective is to account for each new or changed safety requirement and hazard mitigation, thereby reducing errors of omission.

(7) Verification Testing

- Regression testing
- Revalidation

(8) Closing Meeting

- Assessment report discussion
- Action items
- Planning for next action

APPENDIX C.—COMPETENCE OF PERSONS

Source: Adapted from IEC 61508-1 Annex B [IEC 1998a]

C.1.0 Objective

To outline considerations for ensuring that persons with responsibilities for any overall E/E/PES or software safety life cycle activity are competent to fulfill those responsibilities.

C.2.0 General considerations

All persons involved in any overall E/E/PES or software safety life cycle activity, including management activities, independent assessment, and independent audit activities, should have the appropriate training, technical knowledge, experience, and qualifications relevant to the specific duties they must perform.

C.2.1 The education, training, experience and qualifications of all persons involved in any overall E/E/PES or software safety life cycle activity, including any management of functional safety activities, should be assessed in relation to the particular application.

C.2.2 The following factors should be considered when assessing the competence of persons:

(1) Engineering knowledge appropriate to the mining application area.
(2) Engineering knowledge appropriate to the technology (e.g., electrical, electronic, programmable electronic, software engineering).
(3) Safety engineering knowledge appropriate to the technology and the mining application area.
(4) Knowledge of the legal and safety regulatory framework for mining.
(5) The consequences in the event of failure of the E/E/PE safety-related systems: the greater the consequences, the more rigorous should be the specification and assessment of competence.
(6) The SILs of the E/E/PE safety-related systems: the higher the SIL, the more rigorous should be the specification and assessment of competence.
(7) Novel, newer, or more untried designs, design procedures, or applications should have more rigorous specification and assessment of competence.
(8) Previous experience and its relevance to the specific duties to be performed and the technology being employed: the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken.
(9) The training, experience, and qualifications of all persons involved in any overall E/E/PES or software safety life cycle activity should be documented.
(10) Relevance of registrations and certifications (e.g., Registered Professional Engineer, Software Quality Engineer Certification, Certified Safety Professional (CSP), Registered Assessor for the Conformity Assessment of Safety-Related Systems (CASS) [CASS Scheme Ltd. 2002], Associate Safety Professional (ASP)).

APPENDIX D.—INDEPENDENT FUNCTIONAL SAFETY ASSESSMENT CHECKLIST AND WORKSHEET

Objectives:

D.1.0 To facilitate a structured and systematic assessment.

D.2.0 To facilitate the identification and recording of key items of the assessment.

Recommendations:

D.3.0 Safety File Products

D.3.1 The Functional Safety Assessment should focus mainly on the various products or components of a safety file. An example checklist is given below to help assess the completeness of the safety file [Mowrey et al. 2001].

NOTE 17: The checklist in this appendix is for example purposes.

SAFETY SUMMARY DOCUMENTATION

Accept	*Reject*	
_____	_____	Safety statement
_____	_____	Risk management summary (provided in SSPP and SWSP)
_____	_____	Reference file (index and cross-references of all documents, contacts)
_____	_____	Personnel qualifications file

Comments:

SAFETY PLANS

Accept	*Reject*	
_____	_____	System Safety Program Plan (just reference if provided separately)
_____	_____	Software Safety Plan (just reference if provided separately)
_____	_____	Management of Change Plan (just reference if provided separately)
_____	_____	Operation and Maintenance Plan(s) (just reference if provided separately)
_____	_____	Safety Validation Plan (just reference if provided separately)
_____	_____	Installation and Commissioning Plan (just reference if provided separately)

Comments:

SAFETY DATA AND METHODS DOCUMENTATION

Accept	*Reject*	
_____	_____	Product description (vendor's sales literature, general specifications, features)
_____	_____	Implementation document
_____	_____	User documents (operator's manual, maintenance manual, training manual)
_____	_____	History files
_____	_____	Hazard log
_____	_____	Hazard and risk analysis methods
_____	_____	Risk categorization methods
_____	_____	SIL categorization methods
_____	_____	System safety requirements
_____	_____	Software safety requirements
_____	_____	Proven in use documentation, if applicable

Comments:

SAFETY FILE CONCLUSION

Accept	*Reject*	
_____	_____	Summary/conclusions
_____	_____	Signed statement affirming that the system is safe to operate

Comments:

NOTE 18: 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.

D.4.0 Safety Processes

D.4.1 The programs, procedures, and processes, separate from or referenced by the Safety Plans, that form the basis of project management and special implementing procedures unique to the product/machine/control system being designed and developed.

HIGH-LEVEL POLICIES AND PROCEDURES

Accept	*Reject*	
_____	_____	Quality Assurance Policy and Implementing Procedures
_____	_____	Configuration Management Program and Implementing Procedures
_____	_____	Document Control Program and Implementing Procedures
_____	_____	Drawing Control Program and Implementing Procedures
_____	_____	Electronic Information System Policy and Implementing Procedures
_____	_____	Internal Assessment/Audit Program and Implementing Procedures
_____	_____	Procurement Policy and Implementing Procedures
_____	_____	Recordkeeping Policy and Implementing Procedures
_____	_____	Measuring and Test Equipment Control and Calibration Program

Comments:

PROJECT LEVEL PROCEDURES AND PROCESSES

Accept	*Reject*	
_____	_____	Project-Specific Document Control Procedure(s)
_____	_____	Project-Specific Software Configuration Management Procedure(s)
_____	_____	Project-Specific Inter-Intra-Departmental Interface Procedure(s)
_____	_____	Project-Specific Review Procedure(s)
_____	_____	Project-Specific Software Coding Conventions
_____	_____	Project-Specific Procurement Procedure(s)
_____	_____	Project-Specific Recordkeeping Procedure(s)
_____	_____	Project-Specific Measuring and Test Equipment Procedure(s)

Comments: