Functional Safety Lifecycle of the LCLS PLC PPS Systems

E. Michael Saleski*

May 31, 2006

1.0 Introduction

Safety functions are increasingly being carried out by electrical, electronic, or programmable electronic systems. These systems are usually complex, making it impossible in practice to fully determine every failure mode or to test all possible behaviors. The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from:

- Incorrect specifications of the system, hardware or software;
- Omissions in the safety requirements specification;
- Random hardware failure mechanisms;
- Systematic hardware failure mechanisms;
- Software errors;
- Common cause failures;
- Human error.

This document describes all functional safety lifecycle activities from initial concept, development of the system requirements, design and implementation, operation and maintenance, modification and configuration control.

Various aspects of configuration control, system development and review, and testing strategies depend upon specific hardware and system architecture. These issues are also discussed to the extent that they affect functional safety of the system.

1.1 Existing SLAC Documentation

SLAC already has a comprehensive program for maintaining the configuration of, and formal design and review requirements for, radiation safety systems. The SLAC Guidelines for Operations (GFO) is the highest level document defining many of such requirements:

- Guideline 24 “Safety Review of Major Modifications” defines the procedure where the Safety Overview Committee is consulted by a Project Manager to define the overall citizen committee review process for a major project. The role of the Safety Overview Committee, and all other SLAC Citizen’s Committees, are defined in ES&H Manual Chapter 31.
- Guideline 14 “Configuration Control of Radiation Safety Systems” defines the scope and applicability of the configuration control program, and the procedure for obtaining authorization for work on such systems.

* Portions of this document are paraphrased or quoted from publications of the International Electrotechnical Commission.

- Guideline 27 “Testing of Personnel Protection Systems” defines the PPS testing program.
- Guideline 23 “Safety System Deficiency Reviews and Continued Operations” defines a process for authorizing continued operations while there is non-optimal performance of a radiation safety system.

Another document playing a significant role in defining the SLAC radiation safety systems lifecycle is the *Radiation Safety Systems Technical Basis Document*. This document provides technical requirements for radiation safety systems including the Personnel Protection System (PPS), the Beam Containment System (BCS) and shielding. It also defines the review process and approval requirements for proposals of new systems and modifications of existing systems. The roles of the Radiation Safety Officer (RSO), the Radiation Physics Department (RP), the Radiation Safety Committee (RSC), Beamline Physicists, Project Managers, operational safety officers (such as ADSO), and safety systems engineers, among others, are all defined in the Technical Basis Document with respect to radiation safety systems.

1.2 The Simplified Lifecycle

The lifecycle of a radiation safety system at SLAC comprises two main elements: the Development and Review Cycle, and the Implementation, Operations, and Maintenance Cycle. Lifecycles of this nature are sometimes referred to as ‘change control programs’ (thereby not accounting for the development of new systems) or ‘configuration control programs’ (emphasizing the prevention of change, not managing change). The Implementation, Operations, and Maintenance Cycle is essentially a configuration control program combined with a testing program and a corrective action program (for broken hardware, compromised performance, and procedural errors). A Lifecycle includes all of these elements and should describe all management aspects of a radiation safety system from conception to decommission. The simplified two-part lifecycle is shown below in Figure 1.

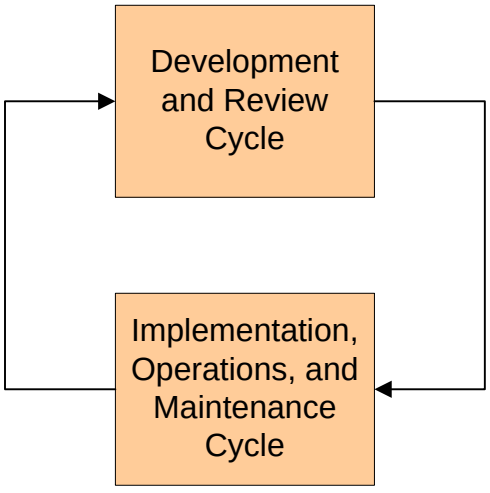

Figure 1: Simplified Configuration Management Lifecycle

1.3 Current SLAC Practices

The Development and Review Cycle describes how a new system, or changes to an existing system, is specified, designed, and reviewed. Planning for testing and development of testing procedures is also performed in this cycle. By current SLAC practice, all modifications to any radiation safety system require the approval of the RSO. This is defined in both the Technical Basis Document, and in Guideline 14 (in that any work, including change of system functionality, requires RP approval of a Radiation Safety Work Control Form). For new systems or major modifications, the RSO will typically take the matter to the RSC for approval; the decision to seek the approval or advice of the RSC is at the discretion of the RSO. Typically, the RSO or RSC review the 'conceptual design,' also known as the functional safety requirements for the system. To compliment this, a detailed technical design review is conducted with a handful of independent reviewers; a report is provided to the RSO/RSC where the system or change is formally accepted, or improvements to the system may be requested. Current SLAC practices are depicted in Figure 2 below. Described later in Section 2.0 of this document are augmentations to this existing cycle to provide an appropriate level of safety assurance for managing design and change of PLC-based PPS systems.

The Implementation, Operation, and Maintenance Cycle describes elements of configuration control, work authorization, routine testing, and assessment of failures surrounding the operation of the system. This portion of the lifecycle is effectively unchanged from current SLAC practice. Some best-practice improvements for preventing unauthorized access to critical equipment and other similar issues that do not show up on the cycle flow chart are proposed for the management of PLC-based PPS systems. These work practice augmentations are described later in this document. The Implementation, Operation, and Maintenance Cycle is depicted later in this document in Figure 4.

1.4 Management Responsibilities

Responsibilities for the various key personnel in the execution of this safety lifecycle are listed below. Ultimate responsibility for the successful design, implementation, commissioning, and initial operation of the PPS belongs to the LCLS organization.

- LCLS Controls Manager: Responsible for the allocation of appropriate financial and personnel resources for the PPS design, review, installation, certification (initial acceptance test), and commissioning effort.
- CPE Controls Manager: Responsible for the appropriate financial and personnel resources for the continuing operation, maintenance, and certification (safety assurance tests) of the PPS.
- LCLS PPS Systems Manager: Responsible for overall safety assurance of the PPS design. Provides oversight of the PPS design and review process to assure completeness and conformance with SLAC policy and LCLS review policy; facilitates reviews and development of the conceptual design.
- PPS Group Leader: Responsible for development and implementation of the PPS technical design, commissioning of the system, maintenance, and periodic testing.

- CPE Safety Systems Review Officer (SSRO): Provides oversight of the review process for modifications following system commissioning and manages the development of the testing procedures.
- Accelerator Systems Division Safety Officer (ADSO): Provides operational safety oversight of the PPS by supervising the Operations Group utilization of the PPS, providing oversight for PPS modifications and system testing, and is responsible for the initial investigation of PPS failures for commissioned systems. The ADSO nominally represents the customer of the PPS, the Accelerator Systems Division and the Accelerator Operations Group.
- CVS Manager: Person external to the PPS Group who manages the CVS file version-management software and file repository.

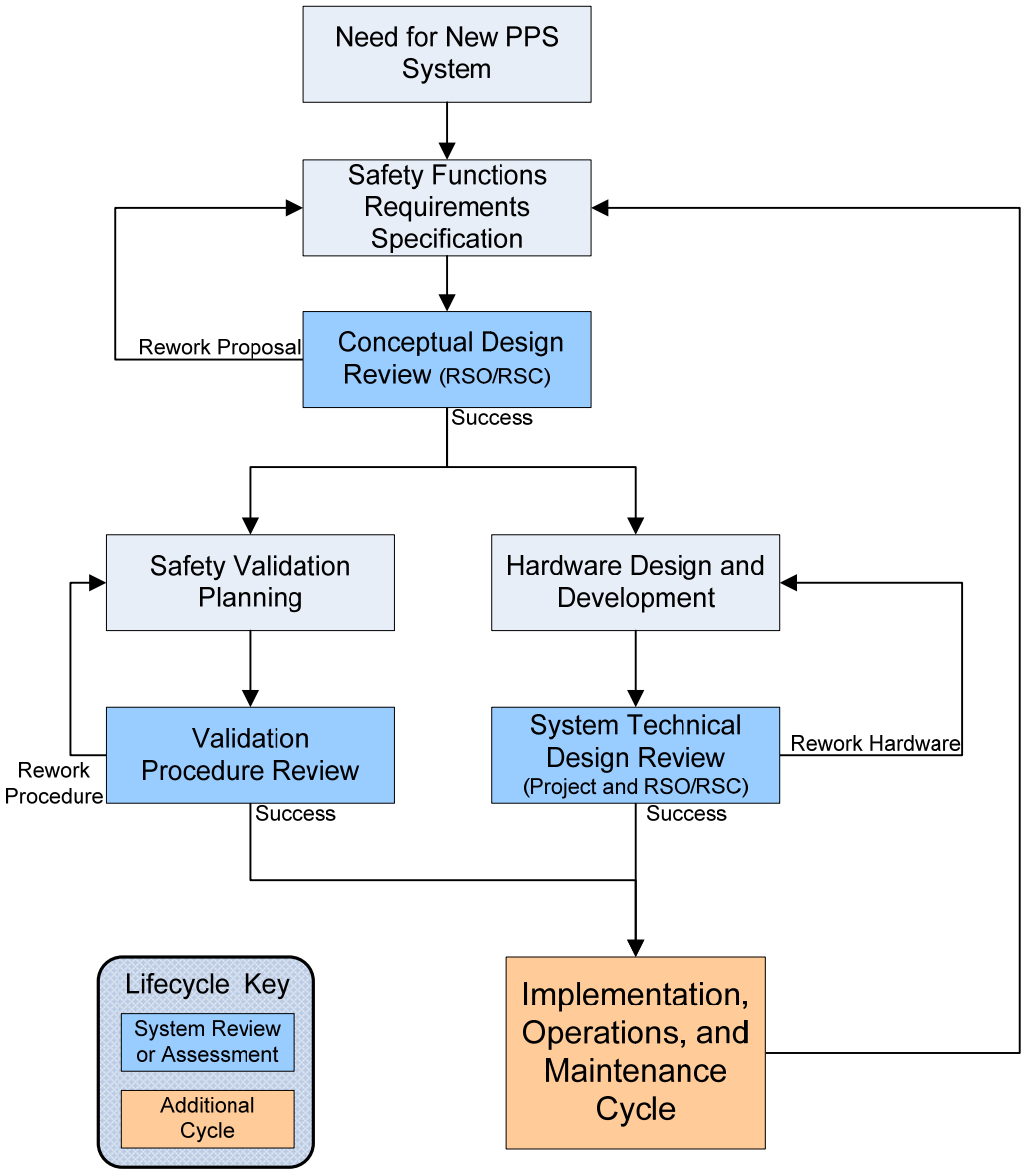

Figure 2: Current SLAC Practice, Development and Review Cycle

2.0 Improved Development and Review Cycle

The proposed review cycle is based on current SLAC practice for development and review of safety significant systems, formalizes some processes already informally utilized, and augments these processes to accommodate the unique needs of systems with software components. Numerous recommended practices concerning programmable electronic systems have been borrowed from IEC 61508.

A new PPS, or modification of an existing PPS, shall be initiated with the issue of a modification request memorandum or equivalent that details the proposed change and the reasons for the change. For the LCLS project, this is done with the PPS Engineering Specification Document.

2.1 Preliminary Design Review

From the design or modification specification, the PPS Group will develop a rough implementation plan that includes a determination of which functions will be implemented with hardware and which will be implemented with software. An analysis shall be carried out on the impact of proposed modifications on the functional safety of the system to determine which safety lifecycle phases will need to be repeated. The safety planning for the modification of safety-related software shall include a detailed specification of the modification and verification planning. All of these elements, along with confirmation of achievement of the requested performance, shall be the subject of a Preliminary Design Review.

The Preliminary Design Review is planned and facilitated by the LCLS PPS Systems Manager for proposals and revisions prior to commissioning. This responsibility is handed off to the CPE SSRO following successful commissioning of the system. Membership of the review panel is determined by the review facilitator and at a minimum shall include: either the LCLS PPS Systems Manager or the CPE SSRO; the PPS Group Leader or designee; and a representative from the Accelerator Systems Division, nominally the ADSO.

The RSO will be notified of and invited to all Preliminary Design Reviews. Depending upon the scope of the proposed change, the RSO may require an RSC Conceptual Design Review. The Preliminary Design Review Report will be provided to the RSO.

2.2 Safety Validation Planning

The approach and methodology for testing or ‘validating’ the PPS design shall be reviewed during the Preliminary Design Review. This is to ensure that proper status is provided in the design so that subsequent testing can efficiently and effectively demonstrate proper operation of the system. The overall testing strategy is described in Section 3.2.

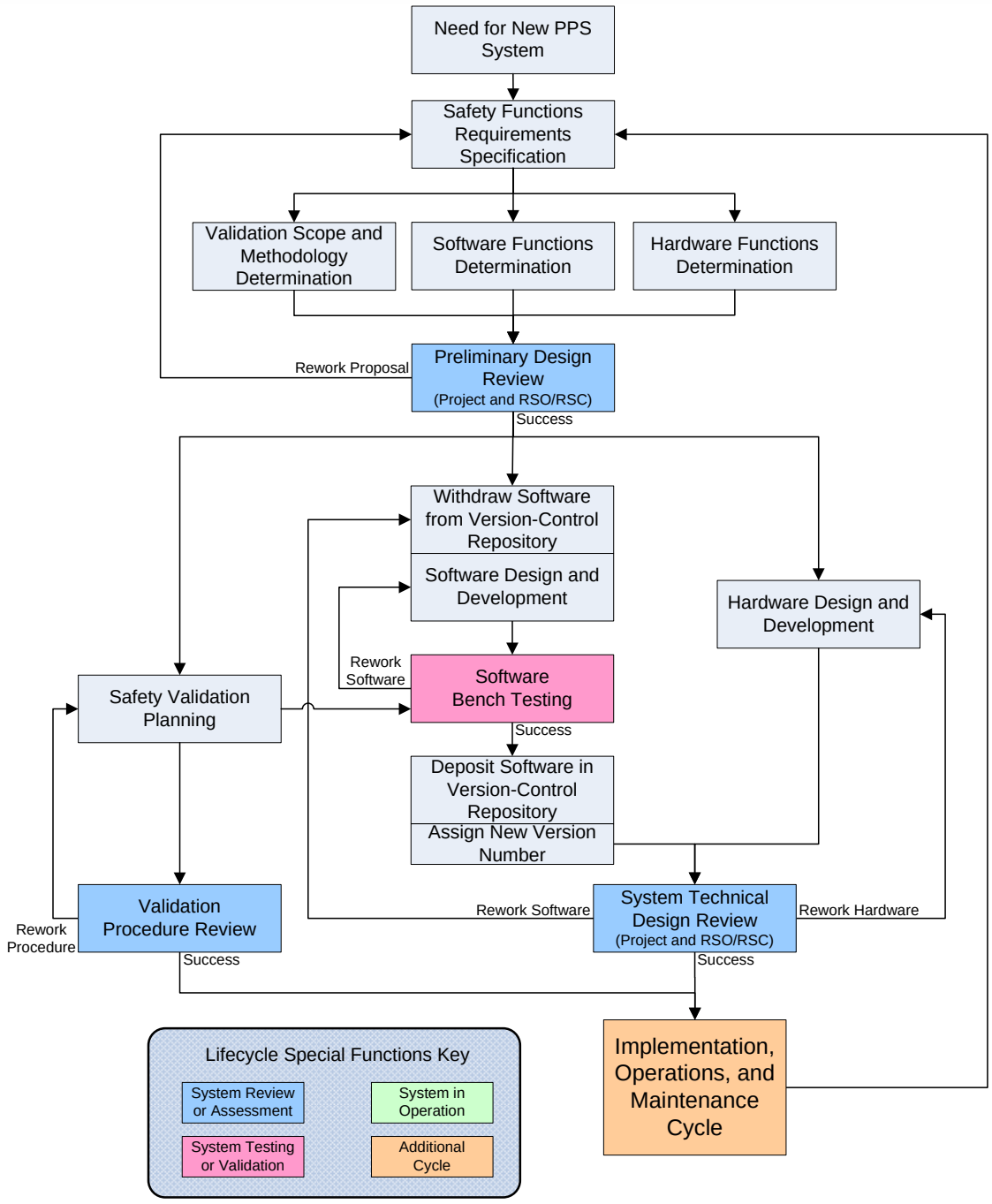

Figure 3: Proposed PLC PPS Development and Review Cycle

2.3 Software Version Control

We propose to use the 'CVS' Concurrent Versions System software, a widely used open-source code, to manage PPS software version control. The file repository and CVS configuration will be managed by an independent software engineer outside of the PPS Group. Concurrent file use will not be allowed. A new version number will be automatically assigned when a revised program is placed in the repository. This version

number will be referenced during the Technical Design Review and during formal Initial Acceptance and Safety Assurance Testing. The version number will also be written on the Pilz PNOZmulti smart card so that it is readily visible when the card is not installed in the PLC.

2.4 Software Bench Testing

With some modifications, the established certification cycle of Initial Acceptance Tests, Safety Assurance Tests, and Interlock Checks will continue to be the cornerstone of the safety assurance lifecycle for the PPS at SLAC. However, additional 'Software Bench Testing' will be added to the Development and Review Cycle for the software. Conceptually, this is part of the Initial Acceptance Test as described in *Guidelines for Operations* Guideline 27. The overall approach to testing is described later in the Implementation, Operation, and Maintenance Cycle.

The conduct of software bench testing is less formal than in situ certification procedures, but that does not diminish its importance. Generic types of tests may be specified as part of the overall validation planning.

Testing of safety-related software shall meet the following requirements: testing shall be the main validation method for the software; animation and modeling may be used to supplement the validation activities; the software shall be exercised by simulation of input signals present during normal operations, anticipated occurrences, and undesired conditions requiring system action. For each safety function test, a chronological record of the actions performed, the results of the actions, and any discrepancies between expected and actual results shall be documented.

The tests shall show that all of the specified requirements are correctly performed and that the software does not perform unintended functions. Test cases and their results shall be documented for subsequent analysis and independent assessment; in particular these tests must be available for examination during the System Technical Design Review. The documented results of the software tests shall state either that the software has passed or the reasons for its failure.

2.5 System Technical Design Review

System hardware and software shall be reviewed for conformance with SLAC policy for safety significant systems. The overall system must also be reviewed for conformance with these requirements. This includes reviewing the source code by static methods to ensure conformance to the specified design of the software module, the required coding standards, and the safety requirements.

The System Technical Design Review is planned and facilitated by the LCLS PPS Systems Manager for proposals and revisions prior to commissioning. This responsibility is handed off to the CPE SSRO following successful commissioning of the system. Membership of the review panel is determined by the review facilitator and at a minimum shall include: either the LCLS PPS Systems Manager or the CPE SSRO; the PPS Group

Leader or designee; and a representative from the Accelerator Systems Division, nominally the ADSO.

The RSO will be notified of and invited to all System Technical Design Reviews. The System Technical Design Review Report will be provided to the RSO. Depending upon the scope of the proposed change, the RSO may require an RSC Technical Design Review. Except when new design techniques, technologies or other departures from standard practice are proposed, providing the System Technical Design Review Report to the RSO is typically sufficient for final approval to authorize the implementation of a new or modified system. Regardless, the RSO is authorized to require an RSC Technical Design Review for any proposed system or change.

2.6 Documentation

Details of all modifications shall be documented, including references to the modification request, the results of the impact analysis that assess the impact of the proposed modification on the functional safety and the decisions taken with associated justifications, software configuration history, deviation from normal operations and conditions (if applicable), and all documented information affected by the modification activity.

3.0 Implementation, Operation, and Maintenance Cycle

All maintenance and modifications to the PPS system must conform to the SLAC configuration control policy as defined in *Guidelines for Operations* Guideline 14 "Configuration Control of Radiation Safety Systems" and other SLAC documentation described in Section 1.1 as well as the policies set forth in this document. This cycle is not explicitly defined by SLAC documentation; instead policies and rules for management and work on radiation safety systems are defined. The overall Implementation, Operation, and Maintenance Cycle can be constructed from these rules. Processes described in this cycle are effectively unchanged with the introduction of programmable electronic systems. However, there are changes to many work practices to accommodate new issues relevant to programmable systems.

3.1 Work on Radiation Safety Systems

All maintenance and modifications on existing radiation safety systems, or installation of new systems, must be done under the auspices of a Radiation Safety Work Control Form (RSWCF). Key management personnel must authorize the work. The person responsible for performing the work and the Area Manager describe the scope of work and sign to authorize. Before the work is authorized to begin, Radiation Physics and the operational safety officer (Accelerator Department Safety Office for the main accelerator facility) determine the appropriate safety mitigation to be taken prior to the commencement of work (if any) and the required checkout procedures that must be performed prior to the resumption of operations. The required checkout procedure may vary dramatically depending upon the scope of work. Any PPS modification requires review and approval of the RSO (and also possibly the RSC); testing requirements for any PPS modification

are set during the Preliminary Design Review. Overall system security must be provided in order to ensure that only authorized maintenance and modifications are performed on the system and to ensure compliance with Guideline 14. New work practices and engineering standards that will be implemented to accommodate programmable electronic safety systems with respect to this issue are described later.

3.2 System Testing: Overall Approach

With some modifications, the established certification cycle of Initial Acceptance Tests, Safety Assurance Tests, and Interlock Checks will continue to be the cornerstone of the safety assurance lifecycle for the PPS at SLAC. Additional 'Software Bench Testing,' described previously in this document, has been added during the development cycle of the software, conceptually part of the Initial Acceptance Test as described in *Guidelines for Operations* Guideline 27. Routine annual testing for a static system (no design changes) will continue to be performed with Safety Assurance Tests. An itemized list of the functions tested during Safety Assurance Tests is attached in a draft 'Guidance for SAT procedures' as specified in Guideline 27. This particular version was provided to the RSO following the recent revision of Guideline 27 and was the basis for the recent significant reworking of the PPS testing document set, yet was never formally adopted. Initial Acceptance Tests follow the same general structure, but includes more proof-of-implementation tests of the logic. Safety Assurance Tests are fundamentally looking for broken system components, as opposed to demonstrating successful implementation of the system design.

The testing of software and hardware shall be planned concurrently with system development. The planning of PPS testing shall refer to the criteria, techniques, and tools to be used in the test activities and shall address the evaluation of test results and the corrective actions to be taken.

3.3 Certification Procedures

The development of Initial Acceptance Tests shall be managed by the SSRO with assistance from the PPS Group Leader and the LCLS PPS Systems Manager. These three, plus the CPE and LCLS Controls Managers, and the ADSO, are approvers of the Initial Acceptance Test. Any post-commissioning modifications to the Initial Acceptance Test in order to certify any new functions of the system do not require approval of the LCLS PPS Systems Manager or of the LCLS Controls Manager.

The development of Safety Assurance Tests shall be managed by the SSRO with assistance from the PPS Group Leader and the ADSO. These three, plus the CPE Controls Manager are approvers of the Initial Acceptance Test. Interlock Checks are developed by ADSO and are approved by ADSO and the Operations Group Leader.

The RSO has oversight of the overall design, performance, and testing program for PPS systems at SLAC. Although not required to review and approve every procedure, the RSO is fully authorized to review any procedure and to insist on changes in procedures or

the testing program. The testing program and procedures shall exhibit administrative transparency to allow the RSO to exercise this function.

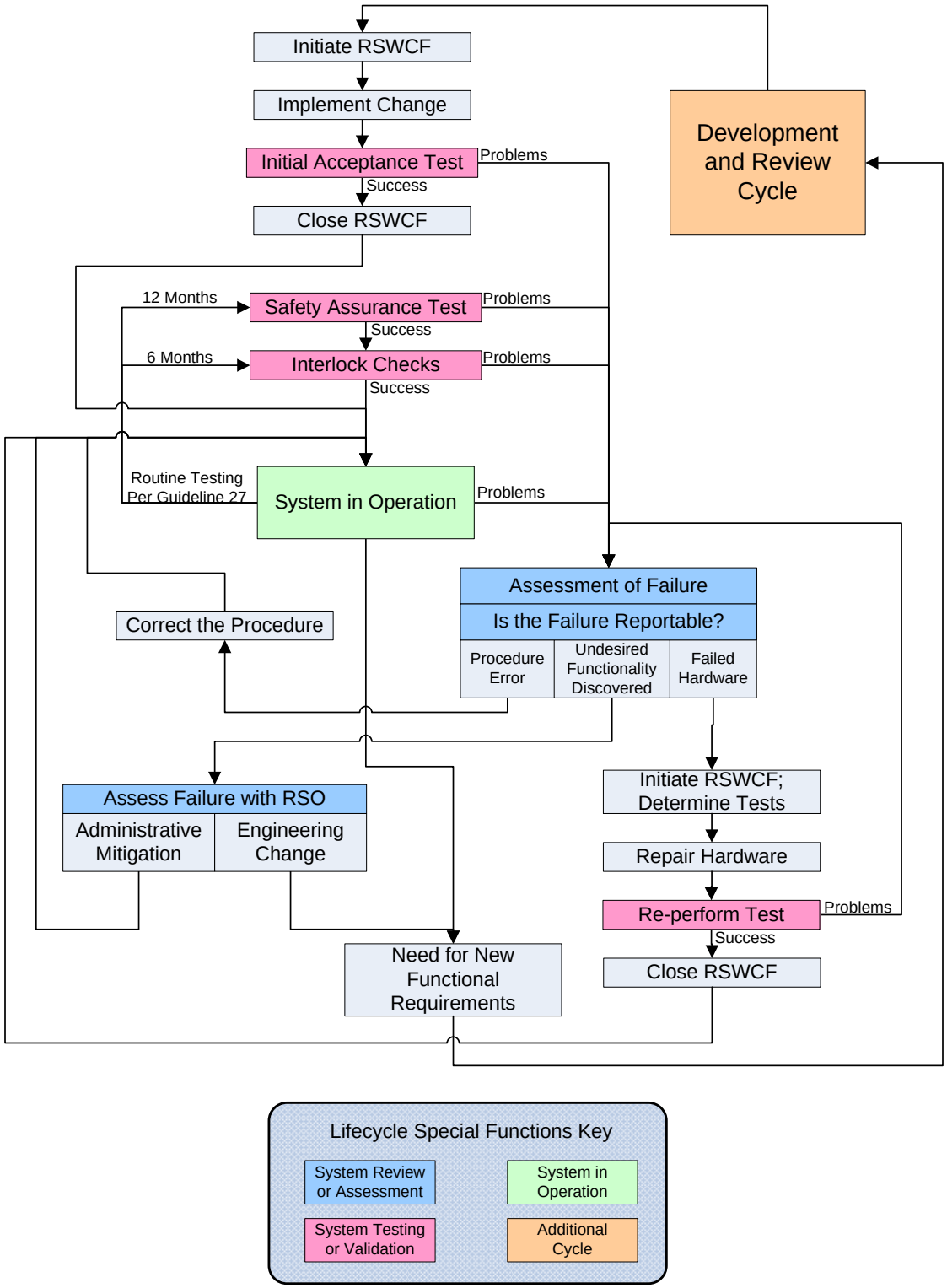

Figure 4: Proposed PLC PPS Implementation, Operation, and Maintenance Cycle

3.4 Failures: Testing and Operational

On occasion the PPS will not perform as desired. These failures can be the result of either a procedural error, failed hardware, or the discovery of undesired functionality. Regardless of cause, all failures of the PPS need to be carefully analyzed. Initial assessment of PPS failures and irregularities is typically done by the Accelerator Operations Group staff when the system is in operation or by the PPS Group when the system is under test. Following initial assessment, one or more of the actions below will be followed. It is the responsibility of the LCLS PPS Systems Manager to assure that proper assessment and correction of PPS failures take place for a new system undergoing commissioning; this is the responsibility of the ADSO for a commissioned system.

1. Any compromise of necessary and required performance of the PPS or discovery of undesired functionality should be brought to the immediate attention of the RSO and Facility Manager for Occurrence Reporting consideration. In some situations, impaired systems *may* be permitted to operate per Guideline 23 “Safety System Deficiency Reviews and Continued Operations.”
2. Hardware failures typically render the system safe (if this is not the case, see item 1 above). The cause of the failure is assessed, a plan of repair and subsequent testing is devised, and under the authorization of a RSWCF the repair is made and the system is tested as prescribed in the RSWCF (or retested if the failure is revealed during routine system testing). If satisfactory results are not obtained, the failure and/or repair strategy needs to be re-assessed.
3. Procedural errors are a common source of ‘failures.’ These typically are not real system failures but may appear as such initially. Operations procedural errors must be analyzed and corrected by the ADSO. PPS testing procedure errors are initially assessed by the SSRO and PPS Group Leader and may escalate to require ADSO approval before operations resume. In practice, any procedural test deviation is escalated to ADSO, and minor typographical and status errors are not. Because of test procedure complexity and length, minor errors are common. During commissioning, the LCLS PPS Systems Manager will also be consulted in addition to ADSO. Again, any safety compromise due to a procedural error is subject the consideration of bullet 1 above.

3.5 Field Changes: Procedures and Hardware

In the course of commissioning a new system, implementing a modification to an existing system, or execution of testing procedures, it is often necessary to make field changes.

The SSRO and PPS Group Leader review all testing procedures as part of the close-out process prior to signing completion of testing on the Beam Authorization Sheet. Minor editorial changes are authorized at this time. If the field changes involve any unexpected results or spontaneous rewriting of portions of the testing procedure, ADSO is involved in this authorization. The LCLS PPS Systems Manager will also be necessary to authorize procedural field changes for a system undergoing commissioning.

Field changes to hardware are handled with a similar escalatory structure. Minor notation errors in prints such as cross connect identifications can be authorized by the PPS Group

Leader. Any actual change in circuit configuration in order to achieve the desire functionality shall be brought to the attention of the SSRO and ADSO before the system is brought into operation. This will also include the LCLS PPS Systems Manager for a system undergoing commissioning. If the change is more than minor, or if additional expertise is needed to review the change, a formal review will be conducted before the system is brought into operation. In all cases, any such changes will be released in 'as-built' drawings.

3.6 New PLC-Relevant Issues and Work Practices

The following sections describe new issues presented by the proposed PLC-based PPS and the new work practices and controls implemented to address them.

3.6.1 Program Storage Security

The Pilz PLC programs are stored on 'smart cards.' These smart cards cannot be written to once the cards have been 'finalized.' This provides assurance that the program cannot be changed by unqualified persons. The Pilz PLC also has a check-sum feature to continuously confirm that the program has not been corrupted or inadvertently altered. The check-sum is determined upon compilation of the program and is automatically written to the smart card. Upon power up of the Pilz PLC, the program is loaded from the smart card and is immediately compared to the check-sum. The program will not initialize and run if there is no match. If the check-sum does not match during a periodic check during operation, the PLC shuts down to a safe state.

When a smart card is finalized, the version number will be physically written on the card. This will avoid possible confusion and help assure that the proper software version is installed in the proper PLC. Also, the program can be retrieved via the Pilz PLC RS232 port. This port is not part of the system architecture, so equipment needs to be taken to the rack and connected in order to perform this action. This connection can also allow writing to non-finalized smart cards.

3.6.2 Version checking

Software is continuously verified against unintended changes with the checksum feature. An incorrect checksum will result in a safe shut-down of the system. Core safety functionality of the system (hardware and software) is confirmed annually during Safety Assurance Testing. Initial Acceptance Tests and Safety Assurance Tests are written for a specific version of software. A check that the proper version of the software is running in the PLC will be included in these procedures, although the exact method is not yet determined at this time. An indirect check, such as cross-referencing the available checksum to a version number may be utilized.

3.6.3 Physical Access Security

The proposed PLC-based PPS systems will exploit current SLAC system security practices. These practices alone will not provide adequate system security, but are a necessary part of the overall system security. The PPS PLCs, and associated

equipment such as I/O modules, will be situated in locked racks. This will restrict access to this equipment to a small group of authorized persons (members of the CPE PPS Group, and the Operations Group/ADSO). Cabling to field devices will be run in conduit or armored cable. Field devices such as keybanks and annunciators will also be locked to restrict access. Other devices potentially vulnerable to damager or tampering, such as microswitches and emergency off buttons, will be subject to the standard practice of operator interlock checks following periods of potential damage (i.e. long periods of Permitted Access and/or high levels of activity).

3.6.4 Network Access Security

The proposed PLC system architecture provides protection against unauthorized access to PPS safety-critical functions via network connections. A brief discussion of the system PLC architecture is necessary to demonstrate this.

All ‘safety-critical’ functions and logic are contained within or controlled by a pair of ‘safety certified’ Pilz PNOZmulti PLCs. Safety-Critical functions are functions such as sensing the stopper and door positions, knowledge of the access state, search ‘set’ status, and emergency off buttons. Other non safety-critical functions, such as keybank releases, door releases, and status reporting to the controls network, are performed by a single Allen Bradley ControlLogix PLC. All commands to the PPS are routed through this PLC.

Communications from the Pilz PLCs to the Allen Bradley PLC is via DeviceNet, a serial data communications network, and is one direction only. Communications from the Allen Bradley PLC to the Pilz PLCs is through discreet digital signals only. The Pilz PLCs can only accept this form of input in this system architecture (the RS232 port can accept input, but is not utilized in this system architecture). Both of these communications networks are completely contained inside a locked PPS rack.

All communications to and from the Controls Network and MCC is through the Allen Bradley PLC. Status is reported to the Controls Network with TCP/IP data packets. In this presently proposed system architecture, any input to the PPS comes from a 32 bit digital output module and is accepted by an Allen-Bradley digital input module; only discreet digital I/O data can be transmitted over this connection. In future systems, the discreet digital communication may be abandoned and two-way communication implemented via TCP/IP. This in principle may leave the Allen-Bradley PLC vulnerable to tampering via network access by a skilled and knowledgeable individual. However, these concerns are in fact operational since all critical safety functionality is contained within the Pilz PNOZmulti PLCs. A safety analysis of Allen-Bradley failures is contained in the LCLS Injector Vault PPS Engineering Implementation document.

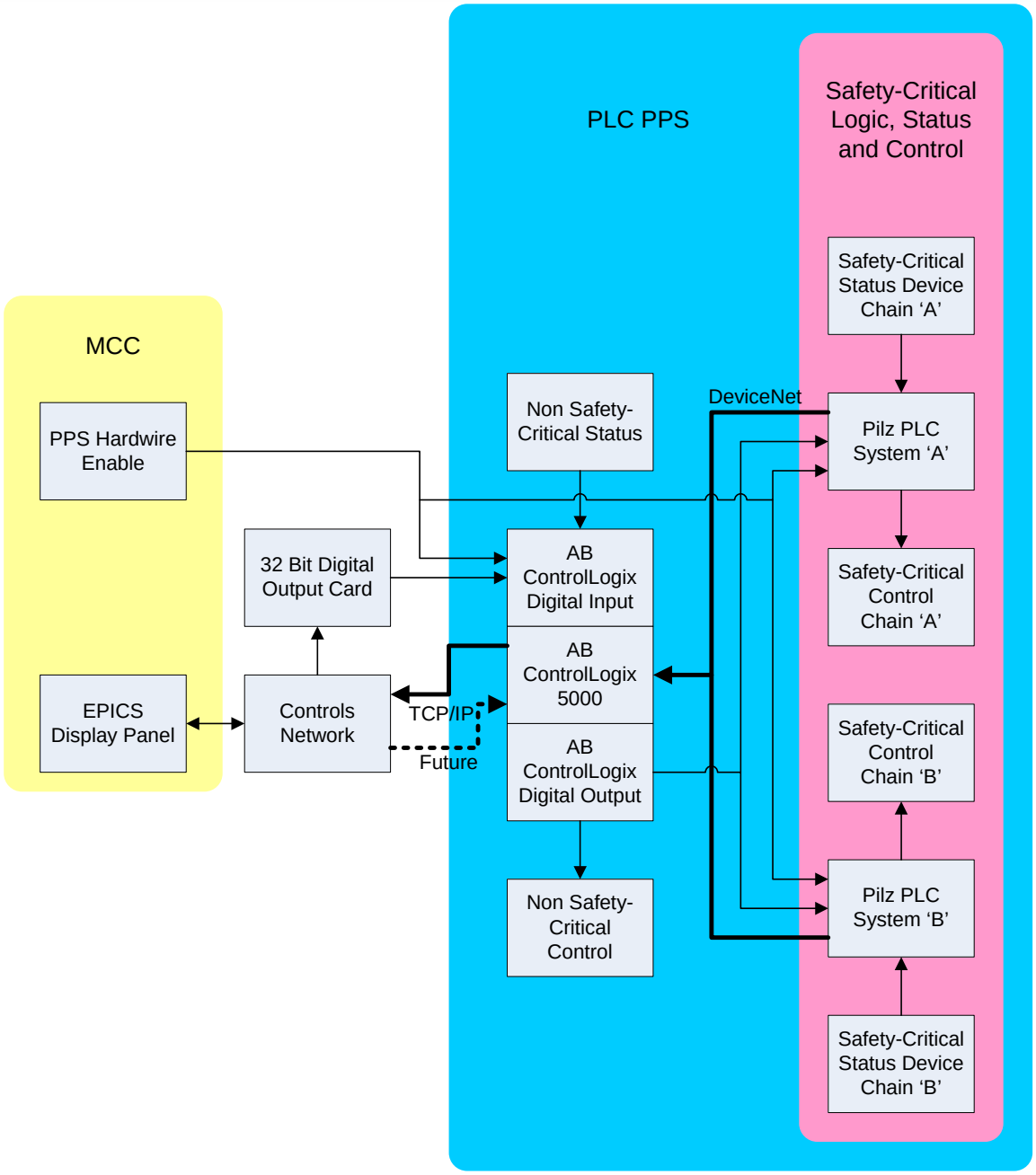

Figure 5: Proposed PLC PPS System Architecture

Additional protections restricting communications permissions to the PPS are also taken. Control commands can only be sent to the PPS from accounts that have 'PPS privilege;' this is generally set only for a set of specific workstations at MCC. While the account privileges are not part of the configuration-controlled system, the practice does provide added security assurance. In addition, and control command sent to the PPS must also be accompanied by the 'PPS Hardwire Enable.' There are two Hardwire Enable switches physically located at MCC.

3.7 Limited Applicability to Allen-Bradley PLC

As previously mentioned in Section 3.6.4 above, functions contained within the Allen-Bradley PLC are considered non safety-critical. However, proper control and utilization of the PPS depends upon proper operation of the Allen-Bradley PLC. As such, all formal development, review, and configuration control processes as described in this document will be applied to the Allen-Bradley PLC. However, it is intended to seek permission to waive or weaken the unauthorized access requirement of Guideline 14 with respect to network access to the Allen-Bradley once it is successfully demonstrated that the system continues to maintain full redundant protection from prompt radiation for all possible failures of the unit. A safety analysis of Allen-Bradley failures is contained in the LCLS Injector Vault PPS Engineering Implementation document.

Guideline for Safety Assurance Tests

Aug 30, 2002

1) Interlock Checks: Proper operation and reporting of door and gate microswitches, keybank microswitches and keybanks, Emergency Off buttons and Emergency Entry/Exit mechanisms shall be confirmed.

2) Stopper Enable Keyswitch Tests: These tests confirm proper operation of the Stopper Enable Keyswitches. Stoppers that protect the area under test are pulled out/turned on, and the action of disabling them withdraws the Stopper Permits causing them to fall into their fail-safe state. Status indicating the presence or absence of Stopper Permits should be available and checked at this time so they can be used to simply additional tests. For the few stoppers that do not fail-safe, inability to pull out stoppers when permits are disabled should be verified.

3) Stopper Permit Redundancy Tests: The functionality described above shall be confirmed true for the interruption of each Stopper Permit independently.

4) Loss of Stopper IN Status: For Stoppers whose function is to prevent beam from entering a downstream area, it shall be demonstrated that a loss of IN status on either chain inhibits beam entering the area under test, therefore also rendering downstream areas safe.

5) Electrical Hazard Redundancy Tests: It shall be demonstrated that each Electrical Hazard requires both Electrical Hazard Permits in order to remain ON.

6) Security Fault: It shall be demonstrated that Stopper Permits, Electrical Hazard Permits, and Search Status are lost when there is a loss of security in the area under test.

7) Access State Tests: The presence or absence of the appropriate permits as a function of access state shall be verified. This not only includes Stopper Permits and Electrical Hazard Permits, but also appropriate keybank releases (keybank release permits), loss of search with a transfer to Permitted Access, inability to bail to unsafe states with keybanks not complete, inability to bail out of No Access with ‘Stopper IN’ summary not complete, and verification of audio-visual warnings. Proper operation of access annunciators and yellow/magenta lights should also be checked.

8) RASK Tests: Special protection for electrical hazard testing provided by some PPS areas shall be confirmed. This includes prevention of key releases when in Controlled Access with RASK mode, ability to bail to Restricted Access and the inability to bail to No Access when in RASK mode, and the presence of Electrical Hazard Permits only when enabled from Emergency Off RASK keyswitches in the tunnel.

9) Emergency Off Test: It shall be demonstrated that the activation of an Emergency Off Button results in the loss of Searched status and the loss of other appropriate Permits.

10) Burn Through Monitor Tests: It shall be demonstrated that faults of Burn Through Monitor switches result in appropriate actions.

11) Beam Shut-Off Ion Chamber Tests: It shall be demonstrated that faults of Beam Shut-Off Ion Chambers result in appropriate actions.