


<div> <u>Large Synoptic Survey Telescope</u></div> <div>Camera System Plan</div>	Document # LCA-139-C	Date Effective	<div>LSST Camera APPROVED</div> <div>Effective Date: 21 Apr 2015</div>
	Author(s) Martin Nordby Jon Thaler	Stuart Marshall Walt Innes	
	Subsystem/Office Systems Integration, Performance and Safety Assurance		
Document Title Camera Hardware Protection Plan			

1. Change History Log

Revision	Effective Date	Description of Changes
A	29 October 2011	Presented at CD-1.
B	24 June 2013	Updated Figure 2; final clean-up for release Added architectural principles and explicit requirements for local protection system implementation; revised architectural schematics Corrected CD-1 date in Revision A entry above. Reviewed under LCN-1024.
C	21 April 2015	Eliminated the Master Permit. Released per LCN-1231.

2. Contents

1.	Change History Log.....	1
2.	Contents	1
3.	Acronyms.....	2
4.	Applicable Documents.....	2
5.	Purpose and Scope	3
6.	Introduction.....	3
7.	Camera Protection Protocol	4
7.1.	Hazard Identification	4
7.2.	Protection Development Methodology	4
7.2.1.	Protection Plan Goal	4
7.2.2.	Protection Protocol Description	5
7.2.3.	Camera Protection Protocol List.....	6
8.	Protection System Architecture	6
8.1.	Architectural Principles	6
8.1.1.	Protection is Handled Locally.....	6
8.1.2.	Protection System Elements are Separable.....	6
8.1.3.	Protection System Definition is All-Encompassing	7
8.1.4.	Protection Does Not Rely on Remotely-Configurable Software	7
8.2.	Architecture and Functional Connectivity	7
9.	Functional Requirements and Capabilities	9
9.1.	Testing and Certification.....	9
9.2.	Overrides and Fault Recovery.....	9
9.2.1.	Start-Up/Shut-Down	9

9.2.2.	Fault Recovery	9
9.2.3.	Troubleshooting and Maintenance	9
10.	Derived Camera and Subsystem Requirements	9
10.1.	Protection System Derived Requirements	10
10.2.	Management of Protection System Firmware	10
10.2.1.	Firmware Validation and Verification	10
10.2.2.	Configuration Control	11

3. Acronyms

CCS	Camera Control System
CPS	Camera Protection System
PHA	Preliminary Hazard Analysis
MPM	Master Protection Module
LPM	Local Protection Module
HCU	Hardware Control Unit
HPU	Hardware Protection Unit
PLC	Programmable Logic Controller
PPE	Personal Protective Equipment
PSAP	Performance and Safety Assurance Plan
SLAC	SLAC National Accelerator Laboratory
SSPP	System Safety Program Plan

4. Applicable Documents

- [1] LCA-138, "Performance and Safety Assurance Plan"
- [2] LCA-31, "System Safety Program Plan"
- [3] LCA-14, "Preliminary Hazard Analysis"
- [4] LCA-15, "Hazard List"
- [5] LCA-140, "Camera Protection Protocol List"
- [6] LCA-48, "Camera System Specification"

5. Purpose and Scope

This document describes all aspects of the Camera Protection System (CPS), including its definition and development, architecture and high-level design, plans for implementation, testing, and certification, and derived functional and implementation requirements. By definition, the CPS includes all systems and components of the Camera that are used to monitor or detect, and actively protect against, prevent, or stop a mishap or a hazard coming to pass, but that is fully independent of Camera Control System (CCS) control, and otherwise not under any software control.

The CPS is comprised of a collection of subsystem hardware including sensors, switches, and programmable logic controllers (PLC's) that work together to provide protection for the Camera. In general, protection functions are handled at the lowest level of control possible—typically at the subsystem device—while cross-subsystem protection is managed by a Master Protection Module. This document provides the overarching methodology, architecture, and requirements that define the system.

Note that the CPS does not address hazards that are mitigated by process controls, administrative procedures, or other “non-active” controls. See Ref. [1], the Performance and Safety Assurance Plan for a description of how these are addressed.

6. Introduction

The CPS provides the last and strongest line of a tiered defense against the occurrence of a mishap. The Camera's first defense against a mishap is in the design, analysis, and testing of Camera components. This includes developing a clear understanding of functional requirements, a process by which the design and manufacturing plans are reviewed and approved as meeting those requirements, and verification test plans to ensure that the as-built hardware meets expectations. Second, Camera hardware is protected by a clear monitoring, communication, command, and control system that orchestrates all Camera actions. The CCS actively monitors the condition of all systems within the Camera and compares operating parameters with preset allowable limits. This provides early warning of trends in hardware operation that could result in a mishap, as well as immediate emergency action to prevent a mishap if thresholds are exceeded. Finally, the CPS system includes hardware interlocks and switches, monitored and controlled by Local Protection Modules (LPM's) to set systems to a safe state in the event that CCS controls fail or otherwise do not function as needed.

The CPS is a key functional system of the Camera that provides active mitigation of Camera hazards by preventing a mishap from occurring or stopping one in the process of occurring, thus preventing damage to Camera hardware, insult to the environment, or injury to personnel. The CPS operates completely independent of both global control by the CCS and local control from local Hardware Control Units (HCU's), providing core protection for all elements of the Camera. During normal operation and maintenance of the Camera, the CCS ensures safe monitoring and control of all Camera systems. However, Camera protection activities are intended to be performed regardless of the state of the CCS. Indeed, the CCS may not be functioning normally, not functioning at all, or even functioning at odds with what is needed for protection, but the protection system provides the “safety net” to ensure that no unsafe operations are executed and that systems are either shut down or put in a safe state if a fault occurs, regardless of the condition of the CCS.

7. Camera Protection Protocol

7.1. Hazard Identification

The System Safety Program Plan (SSPP) Ref. [2] defines the methodology by which Camera hazards are captured, defined, and ranked. Part of this process involves identifying the method by which the hazard is mitigated and the means by which the mitigation plans are verified to be in effect. The Camera Preliminary Hazard Analysis (PHA) Ref. [3], adds considerable detail in describing the functional and physical elements of every Camera subsystem device, along with identifying the hazards associated with them. The PHA defines and refers to Ref. [4], the Hazard List, which succinctly lays out every discrete hazard in the Camera, its ranking, mitigation method, and verification plan. This includes hazards associated with the Camera design, operations, and interaction with personnel.

This document, the Camera Hardware Protection Plan, delineates the system by which hazards are mitigated using active controls. The SSPP defines—and the Hazard List enunciates—six mitigation methods, two of which involve active control. They are, in order of decreasing effectiveness:

Eliminate—select a design alternative that removes the hazard altogether

Control—change the design or manufacturing plans to reduce the severity or probability of a harmful outcome, thereby controlling the impact of the hazard

Include a Safety Feature—add a protective feature to the design with the specific purpose of providing static intervention, not requiring active testing

Add a Safety Device—use an active safety device that interrupts the mishap sequence

Add a Warning Device—include an active detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event

Invoke Procedures or Training—incorporate special procedures and training, including the use of personal protective equipment (PPE), or add-on protective barriers or equipment

The CPS addresses those hazards in the Hazard List that have as mitigations a Safety Device or Warning Device, since these involve active monitoring and control—also known as safety functions. Hazards that are mitigated by Eliminating or Controlling them, by introducing a passive safety feature, or by Procedure or Training are not in the domain of the CPS to address. See the PSAP Ref. [2] for details addressing non-active mitigation of hazards.

7.2. Protection Development Methodology

7.2.1. Protection Plan Goal

The following methodology describes the process in developing hardware protection protocols for hazards that have been defined in the Hazard List. It is intended to be used after the SSPP, PHA, and Hazard List process has been used to identify and classify the hazards, and not to bypass that process.

For hazards that involve mitigations with active monitoring and control using a safety or warning device, the goal of the CPS is to prevent a triggering activity from directly resulting in a mishap. Here, a triggering activity could be loss of function, inaction, failure to act, or untimely action performed by a device in the system, as well as a failure of a component or control path. As defined in the SSPP, a mishap is a hazard coming to pass, which could be closely associated with the triggering event or not. The triggering event and mishap could occur in different subsystems or different physical locations, so

an important aspect of the development of the CPS is the identification of hazards that cross subsystems or are less tightly related. This development process is described in the following section.

7.2.2. Protection Protocol Description

For a given hazard, there are six aspects of the protection/prevention process that must be clearly understood to ensure that action taken by the CPS will, in fact, protect against the resulting mishap. These six aspects are described by the following protection methodology:

When a system is in a particular “**pre-condition/state**,” if a “**triggering activity**” occurs, then a “**mishap**” may directly result. To prevent or protect against this from occurring, the CPS uses a “**detection method**,” and if its “**detection threshold/signal**” is exceeded or tripped then a “**protective action**” is taken.

The following describes each of these aspects and their role in the protection protocol for the CPS. For a given protection protocol, these six aspects could be distributed over multiple subsystems or fully contained within a single subsystem. However, all hazards that result in identified mishaps are treated alike and protection protocols managed at the Camera level. Actual implementation of the detection and protection aspects is performed by subsystem hardware, as well as the control of the protocol actions.

7.2.2.1. *Pre-Condition/State*

Not all activities (loss/inaction/failure/action) are inherently hazardous at all times, and some may actually be beneficial or required in some states, but hazardous in others. The pre-condition or state defines the state in which a particular activity presents a hazard to some part of the system.

7.2.2.2. *Triggering Activity*

A triggering activity is a loss of function, inaction, failure to act, or action that leads to a mishap occurring. There may be more than one activity that leads to a particular mishap, and a given activity may produce more than one mishap, so all combinations need to be identified. Note that while this is closely related to the actual mishap, it is usually not identically the same. For example, a triggering activity could be the failure of a clamp mechanism, but the actual mishap is the dropping and damage of the component being supported by the clamp.

7.2.2.3. *Mishap*

A mishap is a hazard that comes to pass, an accident, or an unplanned event or series of events resulting in death, injury, system damage, loss of or damage to equipment or property, or insult to the environment. As detailed in Ref. [2] the SSPP and Ref. [4] the Hazard List, mishaps have an associated probability of occurrence and severity, which may affect the design of the protective measures.

7.2.2.4. *Detection Method*

The method(s) by which the pre-condition, and either the triggering activity or the incipient mishap is detected. This likely involves a sensor or other instrument monitoring the hardware, but may also include monitoring the aliveness of the controller.

7.2.2.5. *Detection Threshold/Signal*

This is the signal produced or the threshold exceeded by the monitoring or detection method. This could be a binary open/close signal, or an analog signal that exceeds a preset limit. The simpler the signal is to interpret, the less complexity involved in processing it by the LPM that is driving it.

7.2.2.6. *Protective Action*

The protective or preventive action taken to avoid the mishap from occurring. This also includes stopping or otherwise suspending action or putting the system in a safe but non-functioning state that requires subsequent operator intervention.

7.2.3. Camera Protection Protocol List

When hazards on the Hazard List are identified as requiring mitigation with active control, the above protection protocols are delineated to characterize how the protection fits into the overall CPS architecture. The result of this protocol development is then added to the Camera Protection Protocol List, Ref. [5]. This List explicitly tallies both the six aspects of the protection protocol described above, and the subsystem responsible for providing that aspect of protection. The List is then used to aggregate functionalities by subsystem device to clarify responsibilities of each of the device protection elements in the CPS.

The List is really an analysis tool to break down the mitigation process into discrete tasks associated with the six elements of the protection protocol; then assigning responsibilities to subsystems. It is the originating document for both Camera system and subsystem requirements, which appear in their respective specifications.

8. Protection System Architecture

8.1. **Architectural Principles**

The protection system architecture and functional capabilities, and the ensuing requirements, are predicated on four key principles.

8.1.1. Protection is Handled Locally

Hardware protection functions are handled within the subsystem of the hardware, to the greatest extent possible. The Master Protection Module (MPM) is used only to adjudicate protection protocols between elements of different subsystems and provide system-wide functions. Otherwise, all protection functionality is the responsibility of the subsystem Local Protection Module (LPM).

8.1.2. Protection System Elements are Separable

Local Protection Modules and all protection system elements should be separable and stand-alone in three key ways. First, local protection must function fully independent of the MPM and any system-level support or functionality. This ensures that local protection fully functions during stand-alone sub-assembly testing. Thus, system safety is maintained during stand-alone testing and engineering states when the subsystem is operating autonomous of camera control.

Second, local protection elements must be separable from elements of the control system. This ensures that the control system is not relied upon for any functionality of the protection system. Thus, the state

of the control system and its constituent elements has no bearing on the integrity and performance of the protection system. Note that this includes independence from CCS controlled power supplies and power-up sequencing. Local protection elements are expected to be fully functioning and directly connected to un-switched line power.

Third, the local protection system and its constituent elements must be testable and certified completely separate of both the control system and the MPM. This vastly simplifies the testing and certification process, since it is not contingent on the potentially large number of permutations of control and protection system states. It also simplifies the certification of the overall protection system, since interfaces between LPM's become very well defined and relatively simple. The goal of this is to streamline the certification process and minimize invalidation of the certification because of changes to control system elements during routine servicing or maintenance.

8.1.3. Protection System Definition is All-Encompassing

Any sensor, device, or electronics used in executing functions needed for the protection of camera hardware is, by definition, part of the protection system. Thus, the functionality and requirements levied on protection system elements apply to all such devices. This suggests that it is not feasible for components to be used both for protection and control functions. This flows from the principle of separability, since any shared use or cross-strapping of components would introduce dependencies between the protection and control systems. These dependencies must be explicitly avoided.

8.1.4. Protection Does Not Rely on Remotely-Configurable Software

No part of the protection system should be affected by configuration changes to elements controlled by software that can be re-configured remotely. This follows from earlier principles, since any re-configuration would break certification and introduce dependencies with the software and host electronics. This principle applies both to software used for direct protection logic as well as that used for communication.

8.2. **Architecture and Functional Connectivity**

Six local protection zones have been identified, which correspond with six functional elements needing protection. These functional elements are:

- Exchange System—including the Carousel, Auto Changer, and Filter Loader as well as the supervisor that controls interaction between them

- Shutter—Shutter mechanism, which includes two blade sets

- Power Management—low-voltage AC-DC and DC-DC transformers and voltage regulation system providing power at discrete voltages for the Raft Towers and other systems

- Camera Body—purge environmental control system as well as access-control hatches and monitoring of rigid-body motions of the Camera

- Cryostat—vacuum, thermal, and environmental control of the Cryostat

- Refrigeration System—compressors and ancillary equipment on the ground, providing high-pressure refrigerant for cooling components in the Cryostat

While these six protection zones do not encompass all hardware within the Camera, they include all monitoring and control needed to protect the Camera against all hazards listed in the Protection Protocol List.

The Master Protection Module (MPM) implements protocols that require monitoring in one protection element and action taken in another.

The MPM and local functional elements must operate completely independent of the CCS and its local controllers. However, the two systems are interconnected to a limited extent. Figure 1 shows a generic subsystem device, along with its control elements and protection elements.

On the control side, the local Hardware Control Unit (HCU) communicates with the CCS using the Camera Ethernet bus, then converts high-level commands to low-level instructions which are sent on to the Local Device Controller (LDC) and the hardware device or actuator. Part of the HCU control function involves monitoring of sensors on the hardware for feedback control, status, and health.

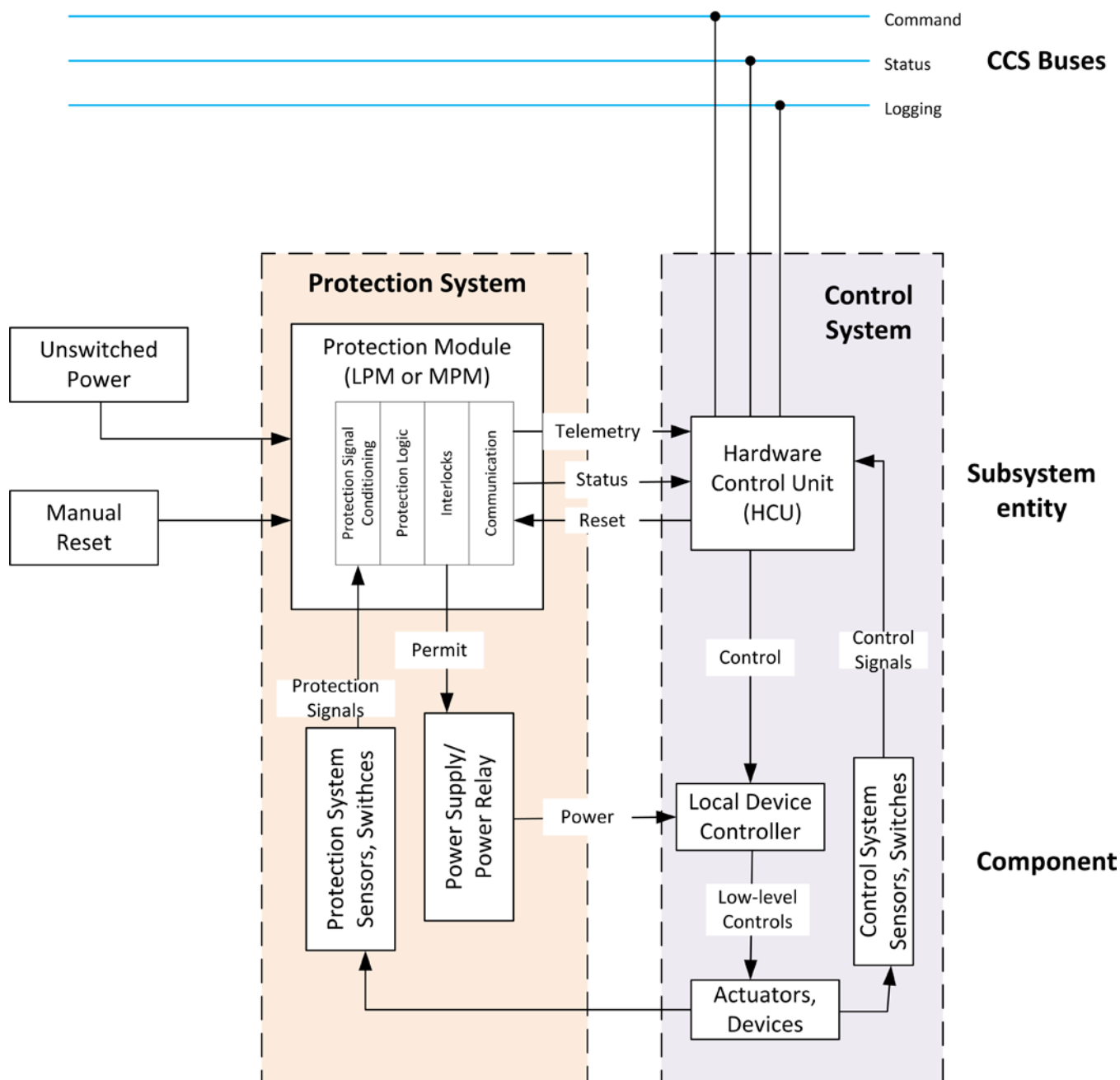


Figure 1: Interrelationship between CCS and CPS elements for a generic functional subsystem.

On the protection side, the protection module (LPM or MPM) controls and monitors the protection system sensors and switches within the hardware and generates interlock permit signals. Note that the mechanism for protection system control is through interlocks on the actuator power. This is the only low-level connectivity allowed between the protection and control systems. If a sensor is needed both for protection interlock and control, then by definition it is considered a protection system sensor.

The HCU receives telemetry from the LPM and can use the conditioned sensor information for its control, but “sharing” of signals is not permitted. The HCU monitors the status of all signals from the LPM, as well as the status of any permit signals emitted by the LPM. These are communicated back to the CCS and the control room, so that protection status is always available. Note that this is a monitoring function only. The MPM and LPMs are hosted on Hardware Protection Units (HPUs), which are typically PLCs. Multiple LPMs may be hosted on one HPU.

9. Functional Requirements and Capabilities

9.1. Testing and Certification

CPS elements include the LPM or MPM and the HPU that hosts it, as well as the protection system sensors and switches and the power supply switches or relays. This system must be certified to perform as required to protect against all known fault conditions. This certification of CPS functionality needs to be included in subsystem test plans.

Each protection system is a stand-alone unit requiring only external power to fully function. This must function during off-line or unit testing of the subsystem assemblies and be re-certified if any part of the protection system is disturbed or the logic changed.

The protection functions of an HPU must be recertified whenever firmware is reloaded.

9.2. Overrides and Fault Recovery

9.2.1. Start-Up/Shut-Down

ALL elements of each protection system must be fail-safe for sudden or controlled loss of power.

At subsystem entity start-up, the protection system HPU must come up first.

Hardware Control Units must come up in idle or quiescent state.

9.2.2. Fault Recovery

Trips may not be cleared until the triggering fault is corrected. Fault latches are normally reset via the CCS.

9.2.3. Troubleshooting and Maintenance

TBD: What overrides are necessary to allow for maintenance and repair. What overrides, if any, are permissible during operations? What is the procedure for activating and tracking them?

10. Derived Camera and Subsystem Requirements

10.1. Protection System Derived Requirements

The following requirements on hardware, component selection, and subsystem functionality are derived from the protection principles and plans described in this document. These requirements are distributed in Ref. [6] the Camera System Specification and subsystem specifications, calling this document as the source.

Each HPU shall have a power source separate from that powering local HCU and non-protection elements.

Local HPU power shall be unswitched (“always on”).

Local protection system elements shall be in a safe state when powered up and shall be fail-safe from sudden or controlled loss of power.

The HPU shall provide a master status signal and status of all inputs and all permit/inhibit signals to the local HCU for monitoring and communication to the CCS.

Sensors and switches shall not be shared by control and protection systems.. Splitting of the unamplified signal, cross-strapping of the conditioned signal to both the HPU and HCU, and using the HCU or other non-protection system hardware is expressly prohibited

Protection system signals that are needed as part of the control system functionality shall be read out and conditioned within the HPU only, then sent to the HCU as telemetry.

Telemetry and status information communicated from the HPU to the local HCU shall be isolated to ensure that HCU problems do not affect performance of the HPU. This could include opto-isolation.

HPU protection logic shall rely solely on binary switching logic and/or locally-coded programming logic only. Control by remotely-loadable software or software hosted on the local HCU is expressly prohibited.

Communication among protection system elements (e.g.: from sensors to the HPU) shall not use publish/subscribe protocols nor any network shared by elements that are not part of the protection system. By definition, hardware and protocols used for communication between protection system elements are themselves part of the protection system.

Protection system hardware components shall be implemented such that the protection function has a SIL rating of 2 per Ref. IEC 61508.

Protection system hardware components, including wiring, connectors, and boards, shall be fail-safe from loss of function. Thus, failure of a component shall result in the dropping of a permit signal and never result in a bypassing or lack of protection functionality.

Protection system hardware components and assemblies shall have the same reliability as other single-failure point components in the subsystem. Since the subsystem can only be operated when the protection system is functioning properly, it must exhibit the same reliability as other key components in the subsystem, to reduce the likelihood of downtimes.

10.2. Management of Protection System Firmware

10.2.1. Firmware Validation and Verification

Tests must validate that the firmware/local software performs as required for all possible states.

10.2.2. Configuration Control

Firmware/software must be under configuration control to prevent inadvertent use of untested software.