Secure Development and Operational Environment for APR1400 Computer-Based I&C Safety Systems

Revision 0

Non-Proprietary

September 2017

REVISION HISTORY

Revision	Date	Page	Description
0	September 2017	All	First Issue

ABSTRACT

This report describes compliance to the secure development and operational environment (SDOE) guidance of RG 1.152 Revision 3 for the APR1400 digital computer-based Safety I&C System. The design features and processes described herein are applicable to all safety systems implemented on the common programmable logic controller (PLC) platform: plant protection system (PPS), engineered safety feature - component control system (ESF-CCS), core protection calculator system (CPCS), and qualified information and alarm system - PAMI (QIAS-P).

As stated in RG 1.152:

> The licensee can provide an SDOE for digital safety systems by (1) designing features that will meet the licensee's secure operational environment requirements for the systems, (2) ensuring that the system is developed without undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely affect the reliable operation of the digital system, and (3) maintaining a secure operational environment for digital safety systems in accordance with the station administrative procedures and the licensee's other programs to protect against unwanted access or changes to these systems.

For item 1, section 3 security design features for computer-based I&C safety systems, describes the built-in security features that prevent unwanted alteration of the system's hardware and software, and the built-in security features that detect and alarm those alterations should they occur. Some features described in this section are generically applicable to all safety systems implemented on the common PLC platform. Other described features are unique to specific systems. In accordance with RG 1.152, this section provides an assessment of the generic and system specific features against postulated threats.

For item 2, section 2 security design processes for development life cycle of computer-based I&C safety systems, describes the generic processes employed during each phase of the software development life cycle that prevent the introduction of unwanted code or detect that code should it be introduced. The processes described in this section are generically applicable to all safety systems implemented on the common PLC platform. Section 2 applies to the following life cycle phases:

- Concepts
- Requirements
- Design
- Implementation
- Test

Sections 2 and 3 describe the processes and security features developed during the concept phase of the safety system development life cycle. The planned security features will be implemented following the planned security processes described for the remaining life cycle phases. In accordance with RG 1.152, Sections 2 and 3 also provide an assessment of those features and processes to ensure they provide

adequate security against postulated threats. Section 2 also describes periodic security re-assessments which will be performed during subsequent life cycle phases to reconfirm the adequacy of the design features and processes, including the effectiveness of the security features and processes against new threats that may arise during the software development life cycle. All security assessments are summarized in Section 4.

Item 3 above, which pertains to maintaining a secure operational environment after equipment delivery to its intended installation location, is addressed through the built-in security features of the safety system, described in Section 3. The security processes applied after equipment delivery are outside the scope of this document, because as stated in RG 1.52:

> Cyber-security and other security controls applied to the latter phases of the life cycle that occur at a licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR Part 50 licensing process and fall under the purview of other licensee programs.

For each safety system implemented on the common PLC platform, this document applies to the entire safety system. This includes the operating system software of the common PLC platform and the application software for each system. Design features and processes are applicable to both, including the engineering development tools used for both, unless specifically noted.

Section 4 summarizes the APR1400 digital computer-based Safety I&C System compliance methods for the key guidance in RG 1.152.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AC	Addressable Constants
APC-S	Auxiliary Process cabinet-Safety
APR1400	Advanced Power Reactor 1400
CIM	Component Interface Module
CPCS	Core Protection Calculator System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DC	Design Certification
ENFMS	Excore Neutron Flux Monitoring System
ESFAS	Engineered Safety Features Actuation Signal
ESF-CCS	Engineered Safety Features – Component Control System
FE	Function Enable
GC	Group Controller
IPS	Information Processing System
MTP	Maintenance and Test Panel
PLC	Programmable Logic Controller
PPS	Plant Protection System
QIAS-N	Qualified Indication & Alarm System-N
QIAS-P	Qualified Indication & Alarm System-P
RDB	Reload Data Block
RTSS	Reactor Trip Switchgear System
SDE	Secure Development Environment
SDL	Serial Data Link
SDN	Safety System Data Network
SOE	Secure Operational Environment
SDOE	Secure Development and Operational Environment
Std.	Standard
USB	Universal Serial Bus
V&V	Verification and Validation

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to describe the design processes and design features of the computer-based safety instrumentation and control (I&C) systems which ensure a secure development and operational environment (SDOE) for the APR1400. In accordance with RG 1.152, this document also provides an assessment of the design processes and design features against postulated threats.

1.2 Scope

The security design processes, design features and corresponding assessments described here-in are applicable to the following computer-based safety I&C systems:

- Plant Protection System (PPS)
- Core Protection Calculator System (CPCS)
- Engineered Safety Features – Component Control System (ESF-CCS)
- Qualified Indication and Alarm System-P (QIAS-P)

2. SECURITY DESIGN PROCESSES FOR DEVELOPMENT LIFE CYCLE OF COMPUTER-BASED I&C SAFETY SYSTEMS

This section describes the processes implemented during each phase of the APR1400 digital computer-based I&C safety system development, that prevent inclusion of unwanted functions in documents, hardware or software code, and to detect those unwanted functions should they be included. Unwanted functions can be included during initial development or through unwanted modifications. This section also assesses the effectiveness of those processes.

These processes are based on the assumption that potential intruders have a detailed knowledge of the safety system, including development tools and development processes. All types of unwanted designs and software code are considered in the assessment of the effectiveness of these processes.

The processes defined in this section are applicable to the common platform and the specific safety system applications. The processes apply to all security related functions, including functions implemented in conventional hardware, and functions implemented in digital software programmable devices such as microprocessors and field programmable gate arrays (FPGA).

This section assesses potential vulnerability of the environment for development life cycle phases, that would introduce unwanted changes in the computer-based safety I&C systems. The following specific vulnerabilities are assessed:

TS

In order to ensure a secure development environment (SDE), the following generic defenses are applicable to the SDE throughout each phase of the computer-based Safety I&C systems development life cycle:

TS

TS

Some examples of defensive measures: (1) Periodic password change procedures, (2) Confirmation of software configuration identifiers for both developed code and software development tools prior to making code changes, and (3) Periodic scanning of software development tools for malicious code.

In addition to these general SDE defenses, additional measure for life cycle phases are described below.

The design team (DT) is responsible for developing, maintaining, and updating the documents, software code of the computer-based I&C system. This process is followed by the review by the independent V&V team (VT). When the documents or software code of the computer-based I&C system are completed by the DT, the independent VT performs review of those documents or software code.

The review also includes verification to ensure that no errors were introduced by developers or by the software development tools. After the reviews of the documents and code, testing of the software is performed.

The review ensures that the SDE requirements are properly reflected. The VT also ensures there have no functions in the referenced documents that are not traceable to the each phase documentation.

Therefore, the review assures that any undesired requirements or data that introduce vulnerabilities are detected and corrected.

Test reports contain reference to the test procedures, the configuration of the test environment and the test results. Opportunity of changes to test results, or not reporting adverse findings documented in the test logs, are excluded by the reviews performed by the VT.

All V&V activities including the documentation of their results are performed in accordance with the software V&V plan.

The documents are managed based on the software configuration management plan. Released documentation is stored and retrieved only from the access controlled electronic environment that prevents any alteration to a configuration controlled item.

These subsequent assessments confirm that the related design features are progressing through the development process, and that no unwanted function has been added.

The following sections describes the use of these SDE defensive measures and assesses their effectiveness for each phase of the development life cycle.

2.1 Concepts Phase

This document reflects the output of the planning process described in BTP 7-14, which is equivalent to the concepts phase of RG 1.152, Position C.2.1. Therefore, the security features and processes described in this document reflect the SDOE product of the concepts phase, which establishes the SDOE licensing basis.

Section 3 describes the security features of the safety system. The sections below describe the security processes (including additional security assessments) required during each subsequent life cycle phase of the system development process, to ensure those security features are implemented correctly and that no unwanted functions are included. Both sections assess the effectiveness of those planned features and processes to mitigate potential threats.

The following generic defenses against undesired software changes are applicable throughout each phase of the software development life cycle process:

TS

TS

These security processes are checked periodically by the Quality Assurance organization, which is independent of the Engineering organization.

2.2 Requirements Phase

During this phase, two kinds of requirements specifications are developed:

- System Requirements Specification (SysRS)

  The SysRS provides overall system configuration, design considerations and operational requirements. The SysRS provides the necessary detail to develop software and hardware specifications. These specifications define performance, functional and Human System Interface (HSI) requirements, and system interfaces. The specifications also define the digital platform and basic architecture of each system using that platform.

- Software Requirements Specification (SRS)

  During this phase, specifications for software are produced. The software specification involves the functions and architecture of the software, including key partitions and interfaces. The functional design is documented primarily in logic diagrams and graphical screen display. The SRS reflects the requirements documented in the SysRS.

Multiple SysRS and SRS are prepared for the common platform and for the various functions of the safety

system (PPS, CPCS, ESF-CCS and QIAS-P).

The SysRS and SRS fully document the security design requirements established during the concepts phase, as described in section 3. Requirements applicable to the common digital platform or to the safety system applications are clearly distinguished. These documents are generated by the design team based on peer review, such as design review meetings. TS

The requirements phase includes a SDOE re-assessment to assure that the security requirements established during the concepts phase, which are fully documented in the requirements phase output products, are adequate to address known security threats, including new threats that were not previously identified during the concepts phase. This assessment also reconfirms the adequacy of the output product storage facility described in Section 2.6.

2.3 Design Phase

During the design phase, the Software Design Descriptions (SDD) are created. The SDD provides the necessary system and functional design detail, software specifications and software interface requirements to implement all system functions, including all security features described in Section 3. The SDD reflects the requirements documented in the SRS, which is provided from the system requirements phase. The SDD adds detail, such as setpoints, calculation sequence and electrical specifications. Multiple SDDs are prepared for the common platform and for various functions of the safety system (PPS, CPCS, ESF-CCS and QIAS-P).

TS

All design phase output products, including independent verification reports are versioned, released and controlled, as required by the configuration management plan of the SPM. The secure development and operational environment measures that ensure the final design phase output products are protected from unwanted alteration, after the independent verification and final approval, are described in Section 2.6.

The design phase includes a SDOE re-assessment to assure that the security requirements specified in the requirements phase, which are fully documented in the design phase output products, are adequate to address known security threats, including new threats that were not previously identified during the concepts phase. This assessment also reconfirms the adequacy of the output product storage facility described in Section 2.6.

2.4 Implementation Phase

Software code is created during the implementation phase for the common digital platform and for the application software that is implemented on each target processor of the common platform for each safety system. The software is documented in source code listings and in graphical diagrams that show the interconnection of various common platform software function blocks.

The software code reflects the detailed designs documented in the SDD, which is provided from the design phase. Software is configured in units that represent logical groupings of platform or application functions. Multiple software units are prepared for the common platform and for various functions of the safety system (PPS, CPCS, ESF-CCS and QIAS-P). Software units are tested during the implementation phase.

The software code fully implements the designs established during the design phase, including all

security design features. Software code applicable to the common digital platform or to the safety system applications is clearly distinguished. Software code is generated by the design team based on peer review, such as design review meetings. The software code undergoes formal independent technical review and formal technical management review.

TS

The secure development and operational environment measures that ensure the final implementation phase output products are protected from unwanted alteration, after the independent verification and final approval, are described in Section 2.6.

The implementation phase includes a SDOE re-assessment to assure that the security features documented in the SDDs of the design phase, which are fully documented in the implementation phase output products, are adequate to address known security threats, including new threats that were not previously identified during the concepts phase. This assessment also reconfirms the adequacy of the output product storage facility described in Section 2.6, and the test environment security that will be used in the next life cycle phase.

2.5 Test Phase

During the test phase, common digital platform operating system software is integrated with the common digital platform hardware, and application software is integrated with the common digital platform hardware and software for each system. The test phase covers two types of testing:

- Integration Testing

  This testing confirms that the software modules, which are integrated together with the actual common platform hardware meet the requirements specified in the SRS. The testing looks for errors in the software, errors in the hardware and software interfaces, errors in timing and fail-safe features, errors in handling self-test detected failure conditions, and errors in failure recovery. Integration tests are conducted on multiple units that form a logical test entity or subsystem.

- Validation (Factory Acceptance) Testing (FAT)

  This is a test of the fully integrated hardware and software for a complete system to validate that the system meets the requirements specified in the SysRS. The validation test is conducted with all connected system interfaces, including those that pose security threats. The system testing demonstrates that all requirements in the SysRS function correctly in the final integrated system. FAT is the final test performed by the equipment supplier, prior to delivery of the equipment.

These tests encompass the key security features described in Section 3: (1) physical access control, (2) data communication controls with other systems (3) protection against software alteration, and (4) protection of deterministic performance. The test phase confirms the specific system security requirements, such as key switches and control room alarms. The tests confirm the correct functionality of the integrated system with all interfaces and all peripheral equipment and interfaces. The application level testing also ensures that any standard functions of the common digital platform, that are unused for a particular processor, do not pose security vulnerability.

TS

TS

The secure development and operational environment measures that ensure the final Test Phase output products are protected from unwanted alteration, after the independent verification and final approval, are described in Section 2.6.

The test phase includes a SDOE re-assessment to assure that the security requirements established during the requirements phase, which are fully demonstrated in the test phase output products, are adequate to address known security threats, including new threats that were not previously identified during the concepts phase. This assessment also reconfirms the adequacy of the output product storage facility described in Section 2.6, and the test environment security.

2.6 Document and Software Storage Security Measures

TS

TS

2.7 Security Processes for COTS Software

There are two kinds of commercial off-the-shelf (COTS) software:

- System Software

  This software runs within the operating system of the safety system processors.

- Engineering Tools

  This software is used to create original software in accordance with this SPM, that runs within the safety system processors.

This section describes the processes employed to (1) achieve high assurance that COTS software products are free of unwanted code that could degrade the security of the safety system, and (2) to ensure that any unwanted code that may be introduced into the safety system by the COTS software products is detected and eliminated.

TS

TS

However, even though engineering tools are utilized that have a known history of correct performance and high security, unwanted functions that may be introduced by the tools is prevented or detected by manual verification and validation activities conducted during multiple phases of the software life cycle, as described in Sections 2.3 through 2.5.

3. SECURITY DESIGN FEATURES FOR COMPUTER-BASED I&C SAFETY SYSTEMS

This section describes hardware and software design features that minimize the APR1400 digital computer-based Safety I&C system's susceptibility to inadvertent access and undesirable behavior from connected systems, that could adversely affect the system's safety functions. These are the security design features of the safety system established during the Concept Phase.

The safety system is designed with features that minimize the potential for security vulnerabilities. The system uses a combination of personnel access controls, and hardware and software design features to protect the safety-related software from unauthorized alteration and to protect the safety system's deterministic performance. This is achieved through a combination of features within the common digital platform and features within the system applications. These features protect the system against adverse operation, from either intentional or unintentional sources.

This section describes the design features that prevent unintended changes to hardware or software code, and to detect those unintended changes should they occur. These design features are based on the assumption that potential intruders have a detailed knowledge of the safety system, and that unintended functions can be included during initial development or through unintended modifications. This section assesses the effectiveness of those design features; all types of unwanted changes to designs and software code are considered in the assessment of the effectiveness of these features.

The hardware or software of the safety system can only be altered by physically accessing the safety system. Personnel access to the safety system is controlled. Remote access capability from sources outside the protected area of the nuclear power plant is not implemented for the safety system.

The APR1400 digital computer-based safety I&C systems include various electronic interfaces with other I&C equipment that resides within the protected area of the plant but is outside the divisional boundaries of the safety system. The specific design features of the safety system that allow it to protect itself against potential security threats from outside its divisional boundary are described below. All electronic interfaces are controlled within the protected area of the plant, and all interfaces conform to the interdivisional communications guidance of DI&C ISG-04 "Task Working Group #4: Highly-Integrated Control Rooms Communications Issues Interim Staff Guidance, rev.1". Compliance to ISG-04 assures that any threat from inter-division digital data communication that could adversely affect the safety function is mitigated.

Deterministic behavior is a key attribute of the safety system that ensures predictable performance for all abnormal plant conditions. This section describes the key features of the safety system that achieve deterministic performance, the security design features that protect that performance against external threats, and the security features that ensure any disruption to deterministic performance is detected and alarmed. The methods described below to protect the deterministic performance of the safety system conform to the interdivisional communications guidance of DI&C ISG-04 "Task Working Group #4: Highly-Integrated Control Rooms Communications Issues Interim Staff Guidance, rev.1". Compliance to ISG-04 assures that the deterministic performance of the safety system is protected from threats that may be introduced by inter-division communication interfaces. In addition, the security features and detection methods described above ensure undesired software that affects the deterministic operation of the system is immediately detected. This includes software that may be hidden, and triggered after a plant event or triggered after time in operation.

3.1 Plant Protection System

3.1.1 PPS Potential Operational Environment Vulnerabilities

This section provides an assessment of PPS potential vulnerability to events initiated by unwanted access and undesirable behavior from connected systems, which could adversely affect the system's safety functions.

3.1.1.1 PPS Vulnerability to Unwanted Access

3.1.1.1.1 PPS Vulnerability to Physical Access

TS

Section 3.1.2.1.1 describes system design features that mitigate these physical access vulnerabilities.

3.1.1.1.2 PPS Vulnerability to Logical Access

TS

Section 3.1.2.1.2 describes system design features that mitigate these logical access vulnerabilities.

3.1.1.2 PPS Vulnerability to Non- Deterministic Performance

The vulnerabilities described below have the potential to adversely affect safety I&C system deterministic performance: TS

Section 3.1.2.2 describes system design features that mitigate these potential vulnerabilities to adverse deterministic performance.

3.1.2 PPS Assessment of Design Features for a Secure Operational Environment

This section describes hardware and software design features for a secure operational environment (SOE).

The system uses a combination of personnel access controls, as well as hardware and software design features to protect the safety-related software from unwanted alteration and to protect the safety system's deterministic performance. This is achieved through a combination of features within the digital platform and features within the system applications. These features protect the system against adverse operation, from either intentional or unintentional sources.

This section describes the design features that prevent unwanted changes to hardware or software code, and to detect those unwanted changes should they occur. These design features are based on the assumption that potential intruders have a detailed knowledge of the safety system, and that unwanted functions can be included during modifications. This section assesses the effectiveness of those design

features; every type of unwanted changes to designs and software code is considered in the assessment of the effectiveness of these features.

3.1.2.1 PPS Unwanted Access Vulnerability Assessment

3.1.2.1.1 PPS Physical Access Controls Assessment

The hardware or software of the safety system can be altered by physically accessing the safety system, as described in Section 3.1.1.1.1. Each vulnerability described in Section 3.1.1.1.1 is mitigated by one or more specific security features, as shown in each bullet below.

Personnel access to the safety system is controlled by the following:

TS

The physical access controls are sufficient to deter unwanted access to any division of the safety system and to detect and alarm unwanted access. There are four safety divisions, with a minimum of two safety divisions required to perform the safety function. Therefore, three of the four divisions would need to experience unwanted physical access, with no security or operator response to the alarms described above, to adversely affect the safety functions. Since each safety division is physically separated and there are multiple access alarms, it is very unlikely that unwanted access could occur in two divisions concurrently, prior to deterrence through security countermeasures.

3.1.2.1.2 PPS Logical Access Controls Assessment

Logical access to the PPS is controlled by the following:

TS

TS

[redacted]

3.1.2.2 PPS Deterministic Performance Controls Assessment

Deterministic behavior is the key attribute of the PPS that ensures predictable performance for all abnormal plant conditions. This section describes the main features of the PPS that achieve deterministic performance, the security design features that protect the performance against external threats, and the security features that ensure any disruption to the deterministic performance is detected and alarmed.

Deterministic performance is achieved by the following key design features of the PPS operating system, which is unaffected by the application software:

TS

[redacted]

TS

3.2 Core Protection Calculator System

3.2.1 CPCS Potential Operational Environment Vulnerabilities

This section provides an assessment of CPCS potential vulnerability to events initiated by unwanted access and undesirable behavior from connected systems, which could adversely affect the system's safety functions.

3.2.1.1 CPCS Vulnerability to Unwanted Access

3.2.1.1.1 CPCS Vulnerability to Physical Access

TS

TS

.

Section 3.2.2.1.1 describes system design features that mitigate these physical access vulnerabilities.

3.2.1.1.2 CPCS Vulnerability to Logical Access

TS

Section 3.2.2.1.2 describes system design features that mitigate these logic access vulnerabilities.

3.2.1.2 CPCS Vulnerability to Non-Deterministic Performance

The vulnerabilities described below have the potential to adversely affect safety I&C system deterministic performance:

TS

TS

Section 3.2.2.2 describes system design features that mitigate these potential vulnerabilities to adverse deterministic performance.

3.2.2 CPCS Assessment of Design Features for a Secure Operational Environment Assessment

This section describes CPCS hardware and software design features for an SOE. The system uses a combination of personnel access controls, as well as hardware and software design features to protect the safety system from unwanted alteration and to protect the safety system's deterministic performance. This is achieved through a combination of features within the digital platform and features within the system applications. These features protect the system against adverse operation, from either intentional or unintentional sources.

This section describes the design features that prevent unwanted changes to hardware or software code, and to detect those unwanted changes should they occur. These design features are based on the assumption that potential intruders have a detailed knowledge of the safety system, and that unwanted functions can be included during modifications. This section assesses the effectiveness of those design features; every type of unwanted changes to designs and software code is considered in the assessment of the effectiveness of these features.

3.2.2.1 CPCS Unwanted Access Vulnerability Assessment

3.2.2.1 CPCS Physical Access Controls Assessment

The hardware or software of the safety system can be altered by physically accessing the safety system, as described in Section 3.2.1.1.1. Each vulnerability described in Section 3.2.1.1.1 is mitigated by one or more specific security features, as shown in each bullet below.

Personnel access to the safety system is controlled by the following:

TS

TS

The physical access controls are sufficient to deter unwanted access to any division of the safety system and to detect and alarm unwanted access. There are four safety divisions, with a minimum of two safety divisions required to perform the safety function. Therefore, three of the four divisions would need to experience unwanted physical access, with no security or operator response to the alarms described above, to adversely affect the safety functions. Since each safety division is physically separated and there are multiple access alarms, it is very unlikely that unwanted access could occur in two divisions concurrently, prior to deterrence through security countermeasures.

3.2.2.1.2 CPCS Logical Access Controls Assessment

Logical access to the CPCS is controlled by the following:

TS

TS

3.2.2.2 CPCS Deterministic Performance Controls Assessment

Deterministic behavior is the key attribute of the CPCS that ensures predictable performance for all abnormal plant conditions. This section describes the key features of the CPCS that achieve deterministic performance, the security design features that protect the performance against external threats, and the security features that ensure any disruption to the deterministic performance is detected and alarmed.

Deterministic performance is achieved by the following key design features of the CPCS operating system, which is unaffected by the application software:

TS

TS

3.3 Engineered Safety Features – Component Control System

3.3.1 ESF-CCS Potential Operational Environment Vulnerabilities

This section provides an assessment of ESF-CCS potential vulnerability to events initiated by unwanted access and undesirable behavior from connected systems, which could adversely affect the system's safety functions.

3.3.1.1 ESF-CCS Vulnerability to Unwanted Access

3.3.1.1.1 ESF-CCS Vulnerability to Physical Access

TS

[ ]

Section 3.3.2.1.1 describes system design features that mitigate these physical access vulnerabilities.

3.3.1.1.2 ESF-CCS Vulnerability to Logical Access

TS

[ ]

Section 3.3.2.1.2 describes system design features that mitigate these susceptibilities.

3.3.1.2 ESF-CCS Vulnerability to Non-Deterministic Performance

The vulnerabilities described below have the potential to adversely affect safety I&C system deterministic

performance:

TS

Section 3.3.2.2 describes system design features that mitigate these potential vulnerabilities to adverse deterministic performance.

3.3.2 ESF-CCS Assessment of Design Features for a Secure Operational Environment

This section describes hardware and software design features for a secure operational environment.

The system uses a combination of personnel access controls, as well as hardware and software design features to protect the safety-related software from unwanted alteration and to protect the safety system's deterministic performance. This is achieved through a combination of features within the digital platform and features within the system applications. These features protect the system against adverse operation, from either intentional or unintentional sources.

This section describes the design features that prevent unwanted changes to hardware or software code, and to detect those unwanted changes should they occur. These design features are based on the assumption that potential intruders have a detailed knowledge of the safety system, and that unwanted functions can be included during modifications. This section assesses the effectiveness of those design features; every type of unwanted changes to designs and software code is considered in the assessment of the effectiveness of these features.

3.3.2.1 ESF-CCS Unwanted Access Vulnerability Assessment

3.3.2.1.1 ESF-CCS Physical Access Controls Assessment

The hardware or software of the safety system can be altered by physically accessing the safety system, as described in Section 3.3.1.1.1. Each vulnerability described in Section 3.3.1.1.1 is mitigated by one or more specific security features, as shown in each bullet below.

Personnel access to the safety system is controlled by the following:

TS

The physical access controls are sufficient to deter unwanted access to any division of the safety system and to detect and alarm unwanted access. There are either two or four ESF-CCS divisions (depending on the electro-mechanical plant systems), with a minimum of one or two safety divisions, respectively, required to perform the safety function. Therefore, two or three of the two or four divisions, respectively, would need to experience unwanted physical access, with no security or operator response to the alarms described above, to adversely affect the safety functions. Since each safety division is physically separated and there are multiple access alarms, it is very unlikely that unwanted access could occur in two or three divisions concurrently, prior to deterrence through security countermeasures.

3.3.2.1.2 ESF-CCS Logical Access Controls Assessment

Logical access to the ESF-CCS is controlled by the following:

TS

3.3.2.2 ESF-CCS Deterministic Performance Controls Assessment

Deterministic behavior is the key attribute of the ESF-CCS that ensures predictable performance for all abnormal plant conditions. This section describes the main features of the ESF-CCS that achieve

deterministic performance, the security design features that protect the performance against external threats, and the security features that ensure any disruption to the deterministic performance is detected and alarmed.

Deterministic performance is achieved by the following key design features of the digital platform operating system, which is unaffected by the application software:

TS

TS

TS

3.4 Qualified Indication And Alarm System-P

3.4.1 QIAS-P Potential Operational Environment Vulnerabilities

This section provides an assessment of QIAS-P potential vulnerability to events initiated by unwanted access and undesirable behavior from connected systems, which could adversely affect the system's safety functions.

3.4.1.1 QIAS-P Vulnerability to Unwanted Access

3.4.1.1.1 QIAS-P Vulnerability to Physical Access

TS

Section 3.4.2.1.1 describes system design features that mitigate these physical access vulnerabilities.

3.4.1.1.2 QIAS-P Vulnerability to Logical Access

TS

Section 3.4.2.1.2 describes system design features that mitigate these susceptibilities.

3.4.1.2 QIAS-P Vulnerability to Non-Deterministic Performance

The vulnerabilities described below have the potential to adversely affect safety I&C system deterministic performance:

TS

Section 3.4.2.2 describes system design features that mitigate these potential vulnerabilities to adverse deterministic performance.

3.4.2 QIAS-P Assessment of Design Features for a Secure Operational Environment Assessment

This section describes hardware and software design features for a secure operational environment.

The system uses a combination of personnel access controls, as well as hardware and software design features to protect the safety system from unwanted alteration and to protect the safety system's deterministic performance. This is achieved through a combination of features within the digital platform and features within the system applications. These features protect the system against adverse operation, from either intentional or unintentional sources.

This section describes the design features that prevent unwanted changes to hardware or software code, and to detect those unwanted changes should they occur. These design features are based on the assumption that potential intruders have a detailed knowledge of the safety system, and that unwanted functions can be included during modifications. This section assesses the effectiveness of those design features; every type of unwanted changes to designs and software code is considered in the assessment of the effectiveness of these features.

3.4.2.1 QIAS-P Unwanted Access Vulnerability Assessment

3.4.2.1.1 QIAS-P Physical Access Controls Assessment

The hardware or software of the safety system can be altered by physically accessing the safety system, as described in Section 3.4.1.1.1. Each vulnerability described in Section 3.4.1.1.1 is mitigated by one or more specific security features, as shown in each bullet below.

Personnel access to the safety system is controlled by the following:

TS

TS

The physical access controls are sufficient to deter unwanted access to any division of the safety system and to detect and alarm unwanted access. The QIAS-P consists of two independent divisions to perform required functions. There are two QIAS-P divisions, with a minimum of one division required to perform the safety function Therefore, two divisions would need to experience unwanted physical access, with no security or operator response to the alarms described above, to adversely affect the safety functions. Since each safety division is physically separated and there are multiple access alarms, it is very unlikely that unwanted access could occur in two divisions concurrently, prior to deterrence through security countermeasures.

3.4.2.1.2 QIAS-P Logical Access Controls Assessment

Logical access to the QIAS-P is controlled by the following:

TS

TS

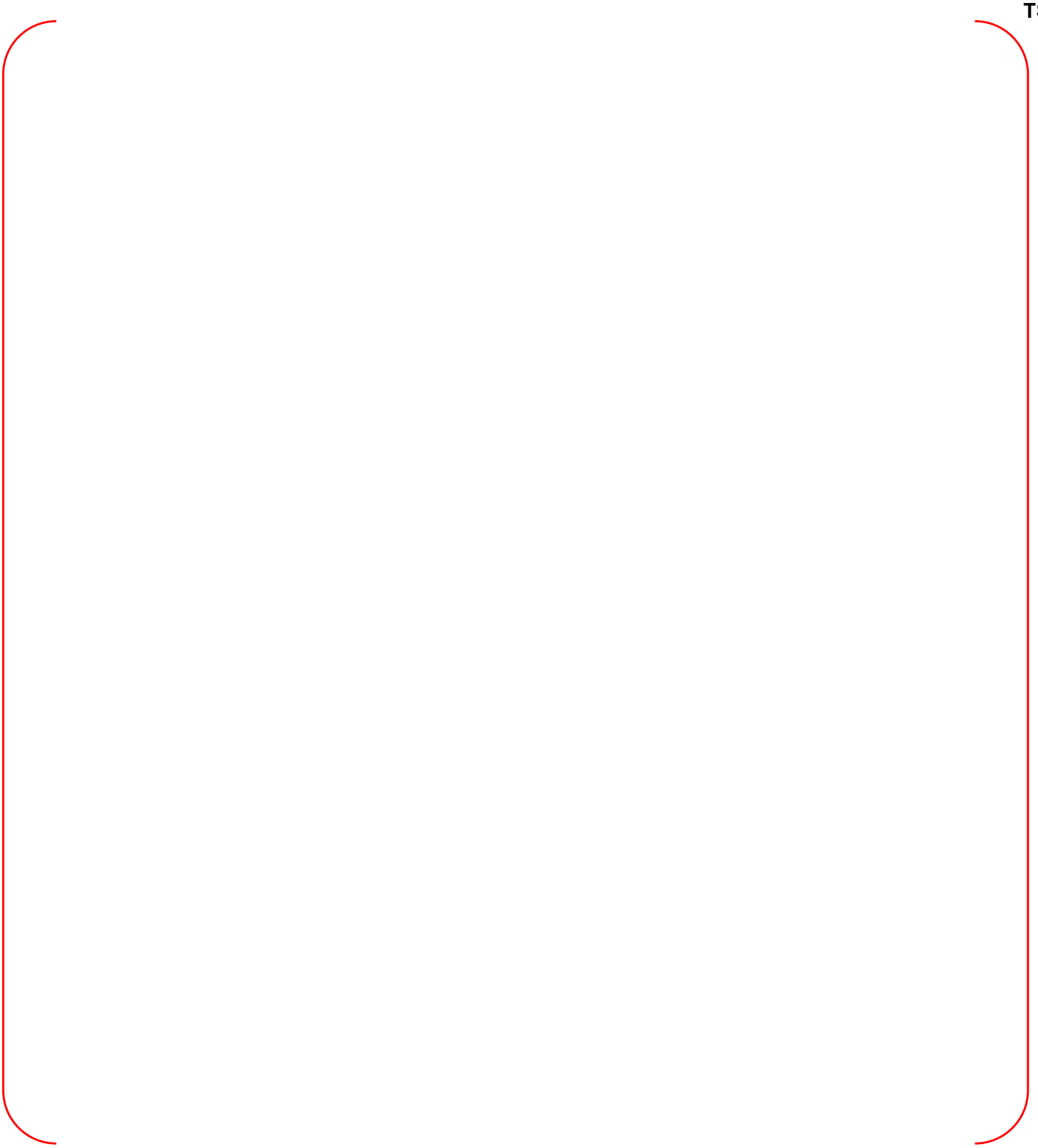
3.4.2.2 QIAS-P Deterministic Performance Controls Assessment

Deterministic behavior is a key attribute of the QIAS-P that ensures predictable performance for all abnormal plant conditions. This section describes the key features of the QIAS-P that achieve deterministic performance, the security design features that protect the performance against external threats, and the security features that ensure any disruption to the deterministic performance is detected and alarmed.

Deterministic performance is achieved by the following key design features of the QIAS-P operating system, which is unaffected by the application software

TS

TS



4 RG 1.152 COMPLIANCE SUMMARY

This section summarizes compliance to the key guidance in RG 1.152 Revision 3, Section C.2 Regulatory Position. Key excerpts of the guidance are included, along with the method of compliance for the APR1400 digital computer-based safety I&C systems.

4.1 Concepts Phase (Section C.2.1)

In the concepts phase, the licensee should identify digital safety system design features required to establish a secure operational environment for the system.

TS

From here, “3.X” indicates an abbreviated way of referring to Sections 3.1, 3.2, 3.3, and 3.4.

The licensee should assess the digital safety system’s potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system’s life cycle that could degrade its reliable operation.

TS

The licensee should not allow remote access to the safety system.

TS

4.2 Requirements Phase (Section C.2.2)

4.2.1 System Features

The licensee should define the functional performance requirements and system configuration for a secure operational environment.

TS

The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system’s SDOE feature.

TS

.

Requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

TS

[ ]

4.2.2 Development Activities

During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.

TS

[ ]

4.3 Design Phase (Section C.2.3)

4.3.1 System Features

The safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description.

TS

[ ]

The safety system design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the safety system should address how this software will not challenge the secure operational environment for the safety system. Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle.

TS

[ ]

4.3.2 Development Activities

During the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

TS

[ ]

4.4 Implementation Phase (Section C.2.4)

4.4.1 System Features

The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

TS

[ ]

4.4.2 Development Activities

The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system.

TS

[ ]

The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system.

TS

[ ]

COTS systems … the developer should ensure that the features within the operating system do not compromise the required design features of the secure operational environment so as to degrade the reliability of the digital safety system.

TS

[ ]

4.5 Test Phase (Section C.2.5)

4.5.1 System Features

The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items…Each system design feature of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the safety system's reliability.

TS

[ ]

4.5.2 Development Activities

The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.

TS

[ ]

5 REFERENCES

1. R.G. 1.152, Rev.03, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

2. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

3. APR1400-Z-J-NR-14003-P, Rev. 1, "Software Program Manual" KHNP, 2017.

4. APR1400-Z-J-NR-14001-P, Rev.1, "Safety I&C System," KHNP, 2017.

5. APR1400-Z-J-NR-1 4012-P, Rev.1, "Control System CCF Analysis," KHNP, 2017.