

DRAFT

**Control Center Protection Profile
For Industrial Control Systems
Version 0.50**

**Submitted To:
Process Control
Security Requirements Forum
(PCSRF)**

**By:
Digital Bond, Inc.**

February 17, 2004

DRAFT

DRAFT

TABLE OF CONTENTS

1 INTRODUCTION 5

1.1 PROTECTION PROFILE IDENTIFICATION 5

1.2 PROTECTION PROFILE OVERVIEW 5

1.3 ASSURANCE LEVEL 5

1.4 RELATED PROTECTION PROFILES 6

1.5 PROTECTION PROFILE ORGANIZATION 6

2 TARGET OF EVALUATION (TOE) DESCRIPTION 7

2.1 PHYSICALLY REMOTE SYSTEMS 8

2.2 FIELD DEVICES 9

2.3 SECURITY OVERVIEW 9

3 TOE SECURITY ENVIRONMENT 10

3.1 ASSUMPTIONS 10

3.2 THREATS 10

3.2.1 Threats Addressed By The TOE 10

3.2.2 Threats To Be Addressed By Operating Environment 13

4 SECURITY OBJECTIVES 14

4.1 SECURITY OBJECTIVES FOR THE TOE 14

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 17

5 TOE SECURITY REQUIREMENTS 18

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 18

5.1.1 Security Function Policies 18

5.1.2 Security Functional Components 20

5.1.3 Security Audit (FAU) Requirements 22

5.1.4 Cryptographic Support (FCS) Requirements 26

5.1.5 User Data Protection (FDP) Requirements 27

5.1.6 Identification And Authentication (FIA) Requirements 32

5.1.7 Security Management (FMT) Requirements 34

5.1.8 Protection Of The TSF (FPT) Requirements 36

5.1.9 Resource Utilization (FRU) Requirements 39

5.1.10 TOE Access (FTA) Requirements 39

5.2 TOE SECURITY ASSURANCE REQUIREMENTS 40

5.2.1 Configuration Management (ACM) 41

5.2.2 Delivery And Operation (ADO) 43

5.2.3 Development (ADV) 44

5.2.4 Guidance Documents (AGD) 46

5.2.5 Life Cycle Support (ALC) 47

5.2.6 Tests (ATE) 48

5.2.7 Vulnerability Assessment (AVA) 50

6 RATIONALE 52

6.1 RATIONALE FOR TOE SECURITY OBJECTIVES 52

6.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT 56

6.3 RATIONALE FOR SECURITY REQUIREMENTS 56

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS 66

APPENDIX A: ACRONYMS 67

DRAFT

APPENDIX B: DEFINITIONS 68
APPENDIX C: APPROVED CRYPTOGRAPHIC ALGORITHMS 69

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Protection Profile are consistent with those used in Version 2.1 of the Common Criteria [CC]. The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment* and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations are used in this Protection Profile

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define pass-fail criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

Terminology

The terminology used in this Protection Profile is largely defined in the Common Criteria. To aid the reader a number of Common Criteria and ICS specific acronyms are included in Appendix A. Similarly, definitions are included in Appendix B.

1 Introduction

1.1 Protection Profile Identification

Title: Control Center Protection Profile for Industrial Control Systems (ICS)

5 **Sponsor:** Process Control Security Requirements Forum (PCSRF)

Authors: Dale Peterson, Digital Bond, Inc

10 **Criteria Version:** This Protection Profile was developed using Version 2.1 of the Common Criteria.

Protection Profile Version: 0.50

15 **Registration:** <to be provided upon registration>

Keywords: Industrial Control System, Process Control System, SCADA, DCS

1.2 Protection Profile Overview

20 This Control Center Protection Profile for ICS defines the minimum security requirements for an ICS Control Center used to control a critical infrastructure component. A Control Center typically includes real time servers, human-machine interface (HMI) stations for operators, historian servers, a network infrastructure, and any other management components that enable centralized control of the critical infrastructure. A Control Center is a central point for gathering information about the critical infrastructure system, includes programs to analyze and present this information, and issues commands to modify the
25 critical infrastructure system. A large, complex, and geographically dispersed infrastructure system can be operated by a small number of people in a Control Center.

30 The Control Center boundaries are both physical, such as a Control Center room, and logical. A logical boundary could include a Primary Control Center, Backup Control Center, and remote HMI stations. This Protection Profile defines the confidentiality, integrity, and availability requirements for information and communication while inside a physical and logically defined Control Center boundary. The Protection Profile also defines requirements for the import of data from PLCs, RTUs, and other field devices that are outside the TOE.

35 1.3 Assurance Level

The assurance level for this Protection Profile is EAL3.

1.4 Related Protection Profiles

This Protection Profile used a draft of the *System Protection Profile – Industrial Control Systems*, draft Version 0.91 (February 4, 2004), as input.

40 1.5 Protection Profile Organization

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides a general definition of Control Centers used in an ICS.

45 Section 3 describes the expected environment for the TOE, in particular the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. This section then defines the set of threats that are to be addressed by either technical countermeasures in the Target of Evaluation (TOE) or through environmental controls.

50 Section 4 defines the security objectives for both the TOE and the environment in which the TOE resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the TOE.

55

Section 6 provides a rationale to explicitly demonstrate that the IT security objectives satisfy the threats. The section then explains how the set of requirements are complete relative to the objectives; that each security objective is addressed by one or more relevant component requirements.

60

Appendix A contains a list of acronyms used in the Protection Profile.

Appendix B provides definitions for many of the terms used in the Protection Profile.

65 Appendix C contains a list of approved cryptographic algorithms that shall be used to meet functional requirements in Section 5.

2 Target of Evaluation (TOE) Description

70 The TOE for this Protection Profile is an ICS Control Center.

The purpose of an ICS is to control a complex process. An ICS has the following four primary functions:

- Measurement – data generation
- 75 ➤ Acquisition – data collection
- Control – data assessment, information generation and response determination, and automatic or manual response
- Human / Machine Interface (HMI) – processing of inputs from and presentation of information to human operators

80

ICS are used to control critical infrastructure systems such as electric generation and distribution, water treatment and delivery, nuclear power plants, oil and gas pipelines, chemical processing and a wide variety of manufacturing processes.

85 Many of the larger ICS have one or more Control Centers that provide centralized control of the complex process. A Control Center typically consists of:

- Real time servers that are the center of the Control Center. Real time servers communicate with field devices, HMI stations, and historical servers. The majority of the ICS Control Center application is typically performed on the real time server.
- 90 ➤ Historian servers that store historical data. In addition to the audit value of this data, the data may still be used in the operation of the ICS and often can be viewed from an HMI station.
- Local HMI stations used to view ICS information, enter commands, and generally operate and administer the ICS. Local HMI stations are located within the same physical security boundary as the ICS servers.
- 95 ➤ Remote HMI stations can have the same functionality as a local HMI station, but remote HMI stations are not in the same physical security boundary as the ICS servers.
- Other ICS servers such as development servers and decision support servers.
- 100 ➤ Servers to support a network operating system.
- Network infrastructure to facilitate communication between various servers and stations in the Control Center.

105 A Control Center is bounded with both a physical and logical security perimeter that may include multiple locations. These boundaries can be identical if all systems are located in one physical area. Frequently, for both availability and operational issues, the Control Center systems are distributed in more than one physical location, see Figure 2-1.

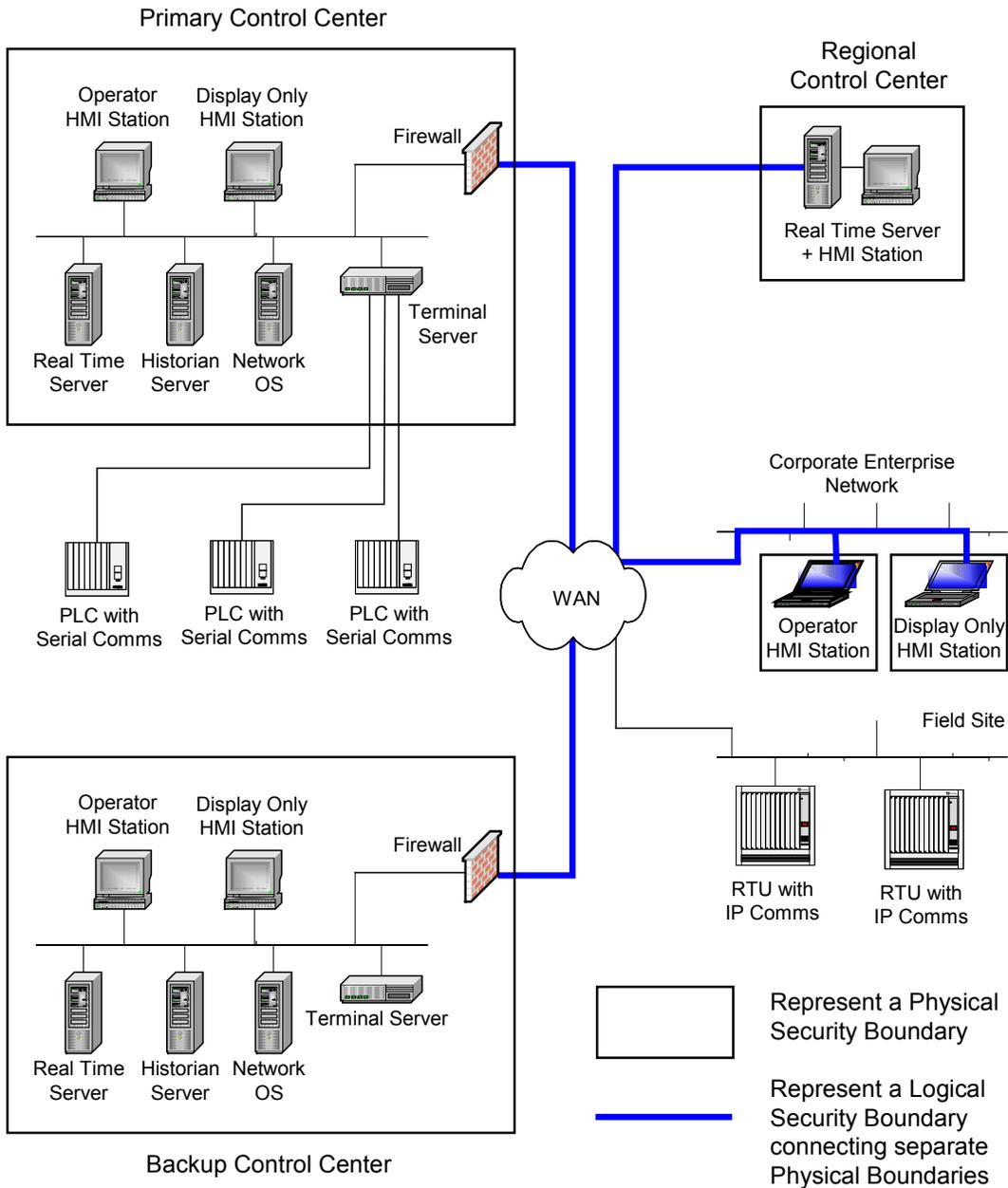


Figure 2-1 TOE and Security Perimeters

110 **2.1 Physically Remote Systems**

One or more systems in the TOE may be in different physical security boundaries. This Protection Profile has addressed this through a logical security boundary and by adding an Information Flow Control Policy, P.Remote_TSF, and accompanying functional requirements for TOE communications outside a physical security boundary.

115 **2.2 Field Devices**

The Control Center communicates with a variety of field devices, including PLCs, IEDs, and RTUs. Field devices are the means to send measured and acquired data back to systems in the Control Center, and the Control Center sends commands and programming to field devices.

120

Field devices are typically outside of the TOE's physical and logical security boundaries, as shown in Figure 2-1. There currently is not a Protection Profile for ICS field devices, so the functional requirements for this communication are covered under FAU_ITC.1. The TOE is required to perform reasonableness testing on the parameters received from a field device and on the amount of information sent from a field device.

125

In the future it is likely a Protection Profile will be developed for ICS field devices that will include cryptographic measures to insure the authenticity and integrity of this information. When a Protection Profile is available the field device communication could be treated as inter-TSF communication and the appropriate functional requirements could be added to this Protection Profile.

130

2.3 Security Overview

Integrity and availability are the two most important security issues for ICS systems and this is reflected in the Protection Profile. Strong authentication of users, authentication of subjects, and authentication of data integrity in transit and at rest are required of all systems in the TOE. A robust and flexible access control system is required that provides both role based and location based access control methods. The majority of the functional requirements address integrity issues.

135

Availability is also extremely important for ICS that control critical infrastructures. While the functional requirements that address availability are smaller in number, they are robust as well. Simply stated, redundancy must be in place so the TOE will function even with multiple failures of critical servers and systems. In the event of loss of operation, there are requirements addressing the secure recovery of data and resumption of TOE operation.

140

145

Confidentiality is a lesser concern in ICS. Functional requirements related to confidentiality are deal primarily with TOE communication outside of a physical security boundary.

1503 TOE Security Environment

This section identifies the following:

- significant assumptions about the TOE's operating environment
- threats to the organization countered by TOE's compliant with this Protection Profile
- 155 - threats requiring reliance on environmental controls to provide sufficient protection

3.1 Assumptions

The following conditions are assumed to exist in the operating environment.

A.User_Physical_Access

160

All users within the physical security perimeter will have access to the HMI and may have access to all other systems except for the control servers.

A.Administrator_Physical_Access

165

All control servers will be in a separate, physically secured area within the physical security perimeter.

A.Separate_Network

170

The control servers will reside on separate networks or subnets that are restricted to only the TOE operations and use.

A.Moderate_Exposure

175

The threat of malicious attacks aimed at discovering and exploiting vulnerabilities is considered moderate.

3.2 Threats

The following threats are addressed either by the TOE or the operating environment.

180 3.2.1 Threats Addressed By The TOE

The threats discussed below are addressed by Protection Profile compliant TOEs. The threat agents are either unauthorized persons, unauthorized IT devices, or disgruntled insiders. These threat agents are generically referred to as an attacker except when a threat is related to a specific threat agent.

185

T.Unauthenticated_Access

190 An attacker may bypass the authentication security controls of the TOE and access the functionality of the TOE including issuing commands, altering data, and changing an application or device configuration.

T.Credential_Cracking

195 An attacker may repeatedly try to guess authentication credentials in order to gain unauthorized access to the functionality of the TOE.

T.Credential_Replay

200 An attacker may record, via electronic or non-electronic means, authentication credentials and replay or reenter the credentials to gain unauthorized access to the functionality of the TOE.

T.Escalation_Of_Privilege

205 A disgruntled insider or attacker, who has already gained limit access, may be allowed to exceed his authorized privileges either by circumventing security or as a result of a lack of granularity in the access control mechanisms.

T.Spoofing

210 An attacker may bypass the information flow control policy and insert unauthorized requests, commands, or code by masquerading as a legitimate user or subject that has already been authenticated.

215 T.Transmitted_Data_Modification

An attacker may modify part or all of an authorized data stream and thereby attack the integrity of the TOE.

220 T.WAN_Data_Compromise

225 An attacker may access a WAN that TOE data must transit to communicate between two physical security boundaries in the TOE. The attacker may eavesdrop or sniff the WAN and recover TOE data for the value of the data or to assist in planning a cyber attack on the TOE.

T.Stored_Data_Modification

230 An attacker may modify part or all of the TOE application and cdata stored in a control server.

T.Data_Replay

235 An attacker may record data communications to a TOE device and replay the recorded data at a later time to fool the TOE device into performing an unauthorized action.

T.False_Communication_Outside_TOE

240 An attacker may send false data or commands from outside the TOE to attack the integrity and availability of the TOE. These data or commands could be modifications of legitimate communication, replayed legitimate communication, or spoofed communication.

T.Audit_Record_Integrity

245 An attacker may cause audit records to be modified or deleted, thus masking an attacker's actions.

T.Audit_Full

250 An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus preventing a record of an attacker's actions.

T.Audit_Accountability

255 An attacker may not be accountable for the actions he conducts because the actions are not recorded in an audit log or the audit log is not reviewed, thus allowing an attacker to escape detection.

T.System_Integrity

An attacker may replace or destroy the applications, configuration information, or system data stored on a device in the TOE to attack the integrity and availability of the TOE.

T.Application_Data_Integrity

265 An attacker may modify or destroy application data including current, real time data, historical data, and audit logs.

T.Information_Storage_Analysis

270 An attacker may access and analyze information stored in a TOE database to plan an attack against the TOE.

T.Communication_Denial_Of_Service

275 An attacker may insert large quantities of information into the communications channel and prevent authentic TOE communication from reaching its destination.

T.Device_Denial_Of_Service

280

An attacker may send large quantities or specially crafted information to a TOE device and cause it to cease its function or be available to perform timely service.

T.Moderate_Exposure

285

A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it controls.

3.2.2 Threats To Be Addressed By Operating Environment

290

The threats discussed below must be countered by procedural measures and administrative methods.

T.Usage

295

The TOE may be inadvertently configured, used, and administered in an insecure manner by authorized persons.

T.Device_Fault

300

A malicious physical attack or natural event may cause a TOE device to cease operation.

T.Communication_Fault

A malicious physical attack or natural event may cause a TOE communication path to cease operation.

3054 Security Objectives

4.1 Security Objectives for the TOE

The following are the IT security objectives for the TOE:

O.Identification

310

The TOE shall uniquely identify the claimed identity of each user.

O.User_Authentication

315

The TOE must authenticate the claimed identity of each user with a two-factor authentication method prior to providing access to any TOE function. The authentication process must not provide any information except for pass or fail.

O.Restricted_Use_Of_Session

320

The TOE must notify users regarding unauthorized use of the TOE and enforce restrictions to limit use of an authenticated session to the authentication user by preventing multiple concurrent sessions and locking a session that has been idle for a period of time defined by a TOE Administrator.

325

O.Access_Control

330

The TOE must provide and enforce an access control capability that allows the TOE Administrator to restrict access and operations to the subjects in the system. The TOE Administrator shall be able to further restrict access by time of day / day of week criteria.

O.Role_Based_Access_Control

335

The TOE must provide a means to place users into roles and make access control decisions based on roles.

The system should support the ability to create and define as many roles as required by the system. At a minimum the roles defined in Table 4.1 must be included in the TOE.

Role	Role Description
Administrator	User who is responsible for deploying, maintaining, and managing the ICS system.
Operator	User who performs regular operations that run the ICS.
Display	User who is allowed to view the status of the system but is not allowed to make any changes to the ICS.

340

O.Subject_Based_Access_Control

The TOE must provide a means to place subjects into a group and assign user or role based access control to the subject group.

345

Application Note: Subject based access control allows a user to be restricted to administering, operating, or viewing a group of subjects that could represent a physical location, type of subject, or any combination that is logical based on an area of responsibility.

350

O.Subject_Authentication

Individual subjects in the TOE must perform mutual authentication prior to communication with another TOE subject or object.

355

O.Command_Authentication

Individual devices in the TOE must authenticate the integrity of all commands and responses sent from another TOE device prior to acting on or storing the data.

360

O.Data_Exchange_Confidentiality

The TOE must protect the confidentiality of TOE data while it is outside of a TOE physical security boundary.

365

O.Replay_Protection

The TOE must identify the replay of any data and prevent action based on the replayed data.

370

O.Reasonableness_Test

The TOE must identify and reject any commands or responses originating outside the TOE that contain unreasonable values or occur at an unreasonable frequency. Any communication that fails this reasonableness test must generate a security alarm.

375

O.Device_Redundancy

The functionality of the TOE must not be compromised if any one device in the TOE is unavailable.

380

O.Communication_Redundancy

The functionality of the TOE must not be compromised if any single communication path is unavailable.

385

O.System_Integrity

390 All devices in the TOE must identify any unauthorized changes to process control applications, process control system and application configurations, and process control data. An alarm must be generated if an unauthorized change has occurred.

O.Secure_State

395 Upon initial start-up of the TOE or recovery from interruption in any part of TOE service, the TOE must not compromise its resources and preserve the secure state of the system.

O.Cryptography

400 The TOE shall employ cryptographic algorithms approved by a recognized security standards body and that have no known vulnerabilities. The key size for all algorithms shall be greater than the capability of any actual exhaustion attack.

O.Audit

405 The TOE must provide the means of recording selected security-relevant events, to assist an Administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave it susceptible to attack. Additionally the events must be recorded in a manner to hold users accountable for any actions they perform that are
410 relevant to security.

O.Audit_Overflow_Protection

415 The audit record shall maintain user accountability of the most recent auditable actions in the event that the maximum capacity of the audit log is reached.

O.Security_Event_Analysis

420 The TOE must provide an automated and manual means for an Administrator to analyze the security events in an audit trail to identify and investigate potential security incidents.

O.Recovery_And_Response

425 The TOE must recover from a system outage and securely distribute all system changes within a time period set by the Administrator.

O.EAL

430 The TOE must be tested and shown to be resistant to attackers possessing moderate attack potential.

4.2 Security Objectives for the Environment

O.Physical_Security_Perimeter

435 Physical access inside the TOE physical security perimeter by unauthorized users must be prevented.

O.Outside_Physical_Security_Perimeter

440 The TOE is physically secure inside the physical security perimeter.

O.Logical_Security_Perimeter

445 Logical access to the TOE from outside the TSF control must be restricted to authorized protocols and authorized IP addresses.

O.Environmental_Services_Backup

450 Environmental services, such as power and temperature / humidity controls, that are required for continued operation of the TOE have redundancy to prevent a single point of failure.

O.Usage

455 The TOE is delivered, installed, administered, and operated in a manner that maintains security.

O.Training

460 Authorized users are trained on the TOE related security policies and procedures.

O.Moderate_Exposure

465 The threat of malicious attacks aimed at discovering and exploiting vulnerabilities is considered moderate.

5 TOE Security Requirements

470 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the Common Criteria.

5.1 TOE Security Functional Requirements

475 The functional security requirements for this Protection Profile, summarized in the following table, consist of the following components from Part 2 of the Common Criteria.

480 The statement of the TOE security requirements must include a minimum strength of function level for the TOE security functions. The minimum strength of function level for this Protection Profile is SOF-medium.

Specific strength of function metrics are defined for the following requirements: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FIA_AFL.1, FIA_SOS.2, FIA_UAU.6, FMT_REV.1, FPT_RCV.3, and FTA_MCS.1.

5.1.1 Security Function Policies

485 Several of the functional requirements in Section 5.1 reference Security Function Policies (SFPs). SFPs are named pieces of requirements. They are not organizational policies. The SFPs used by functional requirements in this Protection Profile are listed below:

5.1.1.1 Access Control SFPs

490 *P.Access_Control*

Table 5-1 defines access privileges by role and information type. The P.Access_Control SFP is used in the access control of data and management of security attribute requirements.

Information Type	Role	Function
User Authentication Data	Administrator	Set default, initialize, modify, delete
User Management	Administrator	Add, delete, and modify user and user data; assign and modify role and location membership and other access control parameters
User Role Management	Administrator	Define, modify, and delete roles used in

Information Type	Role	Function
		access control
Location Access Control	Administrator	Define, modify, and delete locations used in access control
Audit Information	Administrator	Read audit information, set and modify storage capacity and other parameters, set analysis rules, archive
Object Management	Administrator	Add, delete, and modify parameters including reasonableness parameters
Object Operation	Administrator, Operator	Display status, modify parameter values
Object Display	Administrator, Operator, Display	Display status
TOE System Maintenance	Administrator	System testing and system testing parameters, installation, upgrades, patches, restoration
Security Attributes	Administrator	set default, modify, delete attributes and response actions
Key Management	Administrator	Set defaults, generate, distribute, destroy, change parameters

495

Table 5-1 Access Control Table

5.1.1.2 Information Flow Control SFPs

P.Internal_TSF: Internal TSF Transfers

500

The information flow control SFP for communication that does not cross a physical security perimeter.

P.Remote_TSF: Remote TSF Transfers

505 The information flow control SFP for communication that remains in the TSF but crosses a physical security perimeter.

P.Outside_TSF: Transfers Outside TSF Control

510 The information flow control SFP between the TSF and systems outside the TSF.

5.1.2 Security Functional Components

Component	Component Name
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit Data Generation
FAU_SAA.1	Potential Violation Analysis
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG.2	Guarantees Of Audit Data Availability
FAU_STG.3	Action In Case Of Possible Audit Data Loss
FAU_STG.4	Prevention Of Audit Data Loss
FAU_CKM.1	Cryptographic Key Generation
FAU_CKM.2	Cryptographic Key Distribution
FAU_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_DAU.1	Basic Data Authentication
FDP_IFC.2	Complete Information Control
FDP_IFF.1	Simple Security Attributes
FDP_ITC.1	Import Of User Data Without Security Attributes
FDP_ITT.1	Basic Internal Transfer Protection
FDP_SDI.1	Stored Data Integrity Monitoring
FIA_AFL.1	Authentication Failures
FIA_ATD.1	User Attribute Definition
FIA_SOS.2	TSF Generation of Secrets

Component	Component Name
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.3	Unforgeable Authentication
FIA_UAU.6	Re-authenticating
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User Identification Before Any Action
FIA_USB.1	User-subject Binding
FMT_MOF.1	Management Of Security Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management Of TSF Data
FMT_MTD.2	Management Of Limits On TSF Data
FMT_REV.1	Revocation
FMT_SMF.1	Specification Of Management Functions
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_FLS.1	Failure With Preservation Of Secure State
FPT_ITT.3	TSF Data Integrity Monitoring
FPT_RCV.3	Automated Recovery Without Undue Loss
FPT_RPL.1	Replay Detection
FPT_RVM.1	Non-bypassability Of The TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Time Stamps
FPT_TRC.1	Internal TSF Consistency
FPT_TST.1	TSF Self Test
FRU_FLT.2	Limited Fault Tolerance
FRU_RSA.1	Resource Allocation
FTA_MCS.1	Basic Limitation On Multiple Concurrent Sessions
FTA_SSL.1	TSF-initiated Session Locking
FTA_SSL.2	User-initiated Locking
FTA_TAB.1	Default TOE Access Banners

Component	Component Name
FTA_TSE.1	TOE Session Establishment

Table 5-2 Security Functional Components

5.1.3 Security Audit (FAU) Requirements

5.1.3.1 Security Audit Automatic Response (FAU_ARP.1)

515

FAU_ARP.1.1

The TSF shall take [an action of generating a real time alarm to the HMI and place an event in the audit log] upon detection of a potential security violation.

5.1.3.2 Audit Data Generation (FAU_GEN.1)

520

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

- (a) Start-up and shutdown of the audit functions;
- (b) All auditable events for the *basic* level of audit;

525

Application Note: The components that have auditable events at the basic level are listed in Table 5-3.

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

530

- (a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- (b) For each audit event type, based on the auditable event definitions of the functional components included in the Protection Profile / Security Target, [the bold refinement text in column two of Table 5-3].

535

Application Note: The type of event shall include one or more security event types to differentiate security events from non-security related events. Multiple security event types may be related to the severity of the security event.

Component	Auditable Events
FAU_ARP.1	Actions taken due to imminent security violations
FAU_SAA.1	Enabling, disabling, and threshold changes of the analysis mechanisms Automated responses by the tool
FAU_SAR.1	Reading of information from the audit records

Component	Auditable Events
FAU_SAR.2	Unsuccessful attempts to read information from the audit records
FAU_SAR.3	The parameters used for the viewing
FAU_STG.3	Actions taken due to exceeding of a threshold
FAU_STG.4	Actions taken due to the audit storage failure
FAU_CKM.1 FAU_CKM.2 FAU_CKM.4	Success and failure of the activity The object attribute(s) and object value(s) excluding any sensitive information (e.g. secret or private keys)
FCS_COP.1	Success and failure, and the type of cryptographic operation. Any applicable cryptographic mode(s) of operation, subject attributes and object attributes
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP
FDP_DAU.1	Successful generation of validity evidence Unsuccessful generation of validity evidence
FDP_IFF.1	All decisions on requests for information flow
FDP_ITC.1	All attempts to import object data
FDP_ITT.1	All attempts to transfer user data, including the protection method used and any errors that occurred
FDP_SDI.1	All attempts to check the integrity of user data, including an indication of the results of the integrity check., if performed
FIA_AFL.1	Reaching an unsuccessful authentication attempt threshold, the action taken, and restoration to the normal state, if appropriate
FIA_SOS.1	Rejection or acceptance by the TSF of any tested two-factor authentication credentials
FIA_UAU.2	All use of the authentication mechanism
FIA_UAU.3	All immediate measures taken and results of checks on the fraudulent data
FIA_UAU.6	All re-authentication attempts
FIA_UID.2	All use of the user identification mechanism, including the user identity provided
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject)
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.

Component	Auditable Events
FMT_MSA.1	All modifications of the values of security attributes.
FMT_MSA.3	Modifications of the default setting of restrictive rules. All modifications of the initial values of security attributes.
FMT_MTD.1	All modifications to the values of the of the TSF data
FMT_MTD.2	All modifications to the limits on TSF data All modifications in the actions to be taken in case of violation of the limits
FMT_REV.1	All attempts to revoke security attributes The success or failure of the revocation
FMT_SMF.1	Use of management functions
FMT_SMR.1	Modifications to the group of users that are part of a role
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the tests
FPT_FLS.1	Failure of the TSF
FPT_ITT.3	The detection of modification of TSF data The action taken following detection of an integrity error
FPT_RCV.3	The fact that a failure or service discontinuity occurred The resumption of the regular operation The type of failure or service discontinuity
FPT_RPL.1	Detected replay attacks
FPT_STM.1	Changes to the time
FPT_TRC.1	Restoring consistency upon reconnection Detected inconsistency between TSF data
FPT_TST.1	Execution of the TSF self tests and the results of the tests
FRU_FLT.2	Any failure detected by the TSF
FRU_RSA.1	Rejection of allocation operation due to resource limits All attempted uses of the resource allocation functions for resources that are under control of the TSF
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions

Component	Auditable Events
FTA_SSL.1 FTA_SSL.2	Any attempts at unlocking an interactive session Locking of an interactive session by the session locking mechanism Successful unlocking of an interactive session
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session

540

Table 5-3 Auditable Events

5.1.3.3 Potential Violation Analysis (FAU_SAA.1)

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

545

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

- (a) Accumulation or combination of [failed login attempts or communication integrity failures from a subject] known to indicate a potential security violation.
- (b) [Communication from a subject or set of subjects that significantly exceeds the expected communication to indicate a potential security violation.
- (c) The potential security violations shall be placed in the audit log and displayed in an alarm display on the HMI.]

550

5.1.3.4 Audit Review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide [authorized Administrators] with the capability to read [all information] from the audit records.

555

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

560

5.1.3.5 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

565

5.1.3.6 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1

570 The TSF shall provide the ability to perform searches and sorting of audit data based on:

- (a) [the type of audit event
- (b) subject that caused the event
- (c) object acted on by the event
- (d) date and time range]

5.1.3.7 Guarantees Of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2

580 The TSF shall be able to prevent modifications to the audit records.

FAU_STG.2.3

The TSF shall ensure that [one days] audit records will be maintained when the following conditions occur: audit storage exhaustion, failure, and attack.

5.1.3.8 Action In Case Of Possible Audit Data Loss (FAU_STG.3)

FAU_STG.3.1

585 The TSF shall display an alarm on the HMI if the audit trail exceeds 80% of storage capacity.

5.1.3.9 Prevention Of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1

590 The TSF shall overwrite the oldest stored audit records and [display an alarm on the HMI until the audit data loss is stopped] if the audit trail is full.

5.1.4 Cryptographic Support (FCS) Requirements

5.1.4.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1

595 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [from the list of approved algorithms in Appendix C] and specified cryptographic key sizes [of at least 112 bits for symmetric/private key cryptographic algorithms and 1024 bits for asymmetric/public key algorithms] that meet the following standards: [all current
600 NIST standards].

5.1.4.2 Cryptographic Key Distribution (FCS_CKM.2)

FCS_CKM.2.1

605 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [from the list of approved algorithms in Appendix C] that meet the following standards: [all current NIST standards].

5.1.4.3 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1

610 The TSF shall destroy cryptographic keys in accordance with a specified key destruction method [zeroization] that meets the following: [FIPS 140-2 Level 2 for Subscriber/Level 3 for Registration and Certification Authorities].

Application Note: Zeroization shall destroy unencrypted private keys by altering and deleting memory and storage containing the keys.

615 5.1.4.4 Cryptographic Operation (FCS_COP.1)

FCS_COP.1.1

620 The TSF shall perform [digital signatures, message authentication, encryption, and key exchange or negotiation] with a specified cryptographic algorithm [from a list of approved algorithms in Appendix C] and cryptographic key sizes [of at least 112 bits for symmetric/private key cryptographic algorithms and 1024 bits for asymmetric/public key algorithms] that meet the following standards: [all current NIST standards].

5.1.5 User Data Protection (FDP) Requirements

5.1.5.1 Complete Access Control (FDP_ACC.2)

FDP_ACC.2.1

625 The TSF shall enforce the [P.Access_Control SFP] on:

[Subjects: All users in the Administrator, Operator, and Display roles
630 Objects: All stored application data, system and application configuration parameters, system and application files],

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

635 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.5.2 Access Control Functions (FDP_ACF.1)

FDP_ACF.1.1

640 The TSF shall enforce the [P.Access_Control SFP] to objects based on [role, location, and time of day / day of week].

FDP_ACF.1.2

645 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [role, location, time of day / day of week, object status, object parameter boundaries, and TOE status].

FDP_ACF.1.3

650 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [none].

5.1.5.3 Data Authentication With Identity of Guarantor (FDP_DAU.1)

FDP_DAU.1.1

655 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [the following:

- (a) audit logs
- (b) historical data
- 660 (c) application files, system files, data files, and other files required for operation of the TOE.]

FDP_DAU.1.2

The TSF shall provide the [real time servers, historical servers, and Administrators] with the ability to verify evidence of the validity of the indicated information.

665 **5.1.5.4 Complete Information Flow Control (FDP_IFC.2)**

FDP_IFC.2.1 (1)

670 The TSF shall enforce the [P.Internal_TSF SFP] on [all subjects and information within a TOE physical security perimeter] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.1 (2)

675 The TSF shall enforce the [P.Remote_TSF SFP] on [all subjects and information within a TOE logical security perimeter but in two (2) different TOE physical security perimeters] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.1 (3)

680 The TSF shall enforce the [P.Outside_TSF SFP] on [all information received from a source outside the TOE logical security perimeter (outside the TSF)] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2

685 The TSF shall ensure that all operations that cause any information in the TSC to
flow to and from any subject in the TSC are covered by an information flow control
SFP.

5.1.5.5 Simple Security Attributes (FDP_ IFF.1)

FDP_ IFF.1.1 (1)

690 The TSF shall enforce the [P.Internal TSF SFP] based on the following types of
subject and information security attributes:

(a) [subject security attributes:

- source subject identifier
- IP address of source subject
- (ST Assignment: list of additional security attributes)

695

(b) information security attributes:

- transport layer protocol
- IP layer protocol
- (ST Assignment: list of additional information attributes)]

700

FDP_ IFF.1.2 (1)

The TSF shall permit an information flow between a controlled subject and
controlled information via a controlled operation if the following rules hold:

- 705 (a) [the IP address of the source subject is an authorized IP address in the TOE
(b) the transport protocol occurs on the expected port
(c) the data integrity of the information is cryptographically proven as identical to
the data sent by the source subject
(d) the source subject's identity is cryptographically authenticated.]

710

FDP_ IFF.1.3 (1)

The TSF shall enforce the following: [none].

FDP_ IFF.1.4 (1)

715 The TSF shall provide the following: [none].

FDP_ IFF.1.5 (1)

The TSF shall explicitly authorize an information flow based on the following
rules: [none].

720

FDP_ IFF.1.6 (1)

The TSF shall explicitly deny an information flow based on the following rules:

- 725 (a) [the IP address of source subject is not an approved address in the TOE
(b) the transport protocol differs from the expected protocol
(c) the cryptographic data integrity check fails
(d) the identity of the source subject cannot be cryptographically verified]

FDP_IFF.1.1 (2)

The TSF shall enforce the [P.Remote_TSF SFP] based on the following types of subject and information security attributes:

730

(a) [subject security attributes:

- IP address of source subject
- user or system identity
- (ST Assignment: list of additional security attributes)

735

(b) information security attributes:

- transport layer protocol
- IP layer protocol
- (ST Assignment: list of additional information attributes)]

740

FDP_IFF.1.2 (2)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

745

(a) [the IP address of the source subject is an authorized IP address in the TOE

(b) the transport protocol occurs on the expected port

(c) the communication is encrypted from the source subject to the destination

(d) the data integrity of the information is cryptographically proven as identical to the data sent by the source subject

(e) the source subject's identity is cryptographically authenticated]

750

FDP_IFF.1.3 (2)

The TSF shall enforce the following: [none].

FDP_IFF.1.4 (2)

The TSF shall provide the following: [none].

755

FDP_IFF.1.5 (2)

The TSF shall explicitly authorize an information flow based on the following rules: [none].

760

FDP_IFF.1.6 (2)

The TSF shall explicitly deny an information flow based on the following rules:

(a) the IP address of source subject is not an approved address in the TOE

(b) the transport protocol differs from the expected protocol.

(c) the information is not encrypted from the source subject

765

(d) the cryptographic data integrity check fails.

(e) the identity of the source subject cannot be cryptographically verified

FDP_IFF.1.1 (3)

The TSF shall enforce the [P.Outside_TSF SFP] based on the following types of subject and information security attributes:

770

- (a) [subject security attributes:
- IP address of source subject
 - user or system identity
 - (ST Assignment: list of additional security attributes)

775

- (b) information security attributes:
- transport layer protocol
 - IP layer protocol
 - (ST Assignment: list of additional information attributes)]

780

FDP_IFF.1.2 (3)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- (a) the IP address of the source subject is an authorized IP address in the TOE
- (b) the transport protocol occurs on the expected port
- (c) a parameter in the information has a value within the parameters expected boundary

785

FDP_IFF.1.3 (3)

The TSF shall enforce the following: [none].

790

FDP_IFF.1.4 (3)

The TSF shall provide the following: [none].

795

FDP_IFF.1.5 (3)

The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (3)

The TSF shall explicitly deny an information flow based on the following rules:

- (a) [the IP address of source subject is not an approved address in the TOE
- (b) the transport protocol differs from the expected protocol
- (c) the information contains parameters that are outside the minimum or maximum boundaries expected for a parameter field
- (d) the information is greater than a maximum command or response length]

805

5.1.5.6 Import Of User Data Without Security Attributes (FDP_ITC.1)

FDP_ITC.1.1

The TSF shall enforce the [P.Outside_TSF SFP] when importing **object data**, controlled under the SFP, from outside of the TSC.

810

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

815

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:

820

- (a) [all parameters that will be used in the TOE must fall within the expected value boundaries set in the TOE. Parameters falling outside the boundaries shall be discarded].

5.1.5.7 Basic Internal Transfer Protection (FDP_ITT.1)

FDP_ITT.1.1 (1)

825

The TSF shall enforce the [P.Internal_TSF and P.Remote_TSF information flow control SFPs] to prevent *modification* of user and object data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1 (2)

830

The TSF shall enforce the [P.Remote_TSF information flow control SFP] to prevent *modification and disclosure* of user and object data when it is transmitted between physically-separated parts of the TOE.

5.1.5.8 Stored Data Integrity Monitoring (FDP_SDI.1)

FDP_SDI.1.1

835

The TSF shall monitor user and object data stored within the TSC for [corruption or deletion of data] on all objects based on the following attributes: [a cryptographic integrity checksum].

5.1.6 Identification And Authentication (FIA) Requirements

5.1.6.1 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1

840

The TSF shall detect when [five(5)] unsuccessful authentication attempts occur related to [the number of authentication attempts for a user in the last ten (10) minutes].

FIA_AFL.1.2

845

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [disable the account for ten (10) minutes and generate a security event in the audit log].

5.1.6.2 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1

850

The TSF shall maintain the following list of security attributes belonging to individual users:

- (a) [unique userID

- (b) data required to verify authentication credentials
- (c) user roles
- 855 (d) areas of responsibility
- (e) time and day the user is allowed to login to the TOE].

5.1.6.3 TSF Generation Of Secrets (FIA_SOS.2)

FIA_SOS.2.1

860 The TSF shall provide a mechanism to generate that secrets meet [a two-factor authentication requirement].

865 Application note: Two-factor authentication includes two of the following three authentication factors: something you know (such as a password or PIN), something you have (such as a token or smart card), and something you are (such as a fingerprint or hand geometry).

FIA_SOS.2.2

The TSF shall be able to enforce the use of TSF generated secrets for [two-factor authentication].

5.1.6.4 User Authentication Before Any Action (FIA_UAU.2)

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.6.5 Unforgeable Authentication (FIA_UAU.3)

FIA_UAU.3.1

875 The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2

880 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

5.1.6.6 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1

885 The TSF shall re-authenticate the user under the conditions [when the user has been idle for ten (10) minutes].

5.1.6.7 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1

The TSF shall provide only

- 890 (a) [the number of characters typed, without displaying the actual typed characters, when a password or PIN is entered

(b) a message that indicates “authentication failed” when the authentication failed.]

5.1.6.8 User Identification Before Any Action (FIA_UID.2)

FIA_UID.2.1

895 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.6.9 User-subject Binding (FIA_USB.1)

FIA_USB.1.1

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

900 **5.1.7 Security Management (FMT) Requirements**

5.1.7.1 Management Of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1

The TSF shall restrict the ability to determine the behavior of, disable, enable, or modify the behavior of the functions:

- 905 (a) [user roles
(b) TOE system configuration and maintenance
(c) TOE application configuration and maintenance
(d) TOE database and other required application configuration and maintenance
(e) auditing]

910 to [the Administrator role].

5.1.7.2 Management Of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1

915 The TSF shall enforce the [P.Access_Control SFP] to restrict the ability to change default, modify, or delete the security attributes [that are restricted to the Administrator role in Table 5-1] to [the Administrator role].

5.1.7.3 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1

920 The TSF shall enforce the [P.Access_Control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow [the Administrator role] to specify alternative initial values to override the default values when an object or information is created.

925 **5.1.7.4 Management Of TSF Data (FMT_MTD.1)**

FMT_MTD.1.1

The TSF shall restrict the ability to *change default, modify, delete, and clear* the [audit trail specified in FAU_GEN.1, system files, application files, and real time application information] to [Administrators].

930 **5.1.7.5 Management Of Limits On TSF Data (FMT_MTD.2)**

FMT_MTD.2.1

The TSF shall restrict the specification of the limits for [audit trails specified in FAU_GEN.1] to [Administrators].

935 ***FMT_MTD.2.2***

The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits:

- (a) [overwrite the oldest stored audit records
- (b) display an alarm on the HMI stations]

940 **5.1.7.6 Revocation (FMT_REV.1)**

FMT_REV.1.1

The TSF shall restrict the ability to revoke security attributes associated with the *users, subjects, and other objects* within the TSC to [the Administrator role].

945 ***FMT_REV.1.2***

The TSF shall enforce the rules [within fifteen (15) minutes of the revocation].

5.1.7.7 Specification of Management Functions

FMT_SMF.1

The TSF shall be capable of performing the following security management functions:

- 950 (a) [maintenance (deletion, modification, addition) of the audit analysis rules (FAU_SAA)
- (b) maintenance (deletion, modification, addition) of the group of users with read access to audit records (FAU_SAR)
- 955 (c) maintenance of the parameters that control the audit storage capacity (FAU_STG)
- (d) management of changes to cryptographic key attributes (FCS_CKM)
- (e) assignment or modification of objects for which data authentication may apply (FDP_DAU)
- 960 (f) management of the attributes used to make explicit access based decisions (FDP_IFF)
- (g) modification of the additional control rules used for import (FDP_ITC)
- (h) management of the threshold for unsuccessful authentication attempts (FIA_AFL)
- 965 (i) management of actions to be taken in the event of an authentication failure (FIA_AFL)

- (j) management of the user identities (FIA_UID)
- (k) management of default subject security attributes (FIA_USB)
- (l) management of the time interval for abstract machine testing (FPT_AMT)
- 970 (m) management of the mechanism used to provide the protection of data in transit between different parts of the TSF (FPT_ITT)
- (n) management of who can access the restore capability within the maintenance mode (FPT_RCV)
- 975 (o) management of the list of actions that need to be taken in case of replay (FPT_RPL)
- (p) management of the time (FPT_STM)
- (q) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular time interval, or under specified conditions (FPT_TST)
- 980 (r) specifying maximum limits for a resource for individual users and subjects by an administrator (FRU_RSA)
- (s) management of the maximum allowed number of concurrent user sessions by an administrator (FTA_MCS)
- 985 (t) specification and modification of the default time of user inactivity after which lock-out occurs for an individual user (FTA_SSL)
- (u) management of the events that should occur prior to unlocking the session (FTA_SSL)
- (v) maintenance of the banner by the authorized administrator (FTA_TAB)
- (w) management of the session establishment conditions (FTA_TSE)]

990 **5.1.7.8 Security Roles (FMT_SMR.1)**

FMT_SMR.1.1

The TSF shall maintain the roles [Administrator, Operator, and Display].

FMT_SMR.1.2

995 The TSF shall be able to associate users with roles.

5.1.8 Protection Of The TSF (FPT) Requirements

5.1.8.1 Abstract Machine Testing (FPT_AMT.1)

FPT_AMT.1

1000 The TSF shall run a suite of tests during initial start-up, periodically during normal operation, and at the request of an authorised user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.8.2 Failure With Preservation Of Secure State (FPT_FLS.1)

FPT_FLS.1.1

1005 The TSF shall preserve a secure state when the following types of failures occur:
[forced reboot, TOE application hanging, TOE system hanging, and absence or loss
of available of computing memory or storage].

5.1.8.3 TSF Data Integrity Monitoring (FPT_ITT.3)

FPT_ITT.3.1

1010 The TSF shall be able to detect modification of data, substitution of data, re-ordering of data, and deletion of data for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2

1015 Upon detection of a data integrity error, the TSF shall take the following actions:
(a) [discard the packet containing the data
(b) request the packet be resent
(c) generate an event in the audit log]

5.1.8.4 Automated Recovery Without Undue Loss (FPT_RCV.3)

FPT_RCV.3.1

1020 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.3.2

1025 For [unexpected shutdowns, media failures, and system integrity failures], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3

1030 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [15 minutes of operational information] for loss of data or objects within the TSC.

FPT_RCV.3.4

1035 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

5.1.8.5 Replay Detection (FPT_RPL.1)

FPT_RPL.1.1

1040 The TSF shall detect replay for the following entities: [service requests and service responses].

FPT_RPL.1.2

1045 The TSF shall perform [discarding the replayed request or response, generating an alarm to the HMI display, and terminating the TCP session with the subject or object that was the source of the replay] when replay is detected.

5.1.8.6 Non-bypassability Of The TSP (FPT_RVM.1)

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed.

1050 **5.1.8.7 TSF Domain Separation (FPT_SEP.1)**

FPT_SEP.1.1

The TSF shall maintain a security domain for its execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

1055 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.8.8 Time Stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

1060 **5.1.8.9 Internal TSF Consistency (FPT_TRC.1)**

FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

1065 ***FPT_TRC.1.2***

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [ST assignment: list of SFs dependent on TSF data replication consistency].

1070 **5.1.8.10 TSF Testing (FPT_TST.1)**

FPT_TST.1.1

The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, and at the request of the authorized user to demonstrate the correct operation of the TSF.

1075

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

1080 ***FPT_TST.1.3***

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.9 Resource Utilization (FRU) Requirements

5.1.9.1 Limited Fault Tolerance (FRU_FLT.2)

1085

FRU_FLT.2.1

The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [any failure of a single system type or any combination of multiple single system type failures].

1090

Application note: The TOE shall have redundancy for all systems. The TOE shall be fault tolerant even if one of every type of system has failed at the same time since each system shall be redundant.

5.1.9.2 Maximum Quotas (FRU_RSA.1)

1095

FRU_RSA.1.1

The TSF shall enforce maximum quotas on the following resources: [memory, processing power, and data storage] that *an individual user or subject* can use *simultaneously*.

5.1.10 TOE Access (FTA) Requirements

5.1.10.1 Basic Limitation On Multiple Concurrent Sessions (FTA_MCS.1)

1100

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2

1105

The TSF shall enforce, by default, a limit of [one(1)] session per user.

5.1.10.2 TSF-initiated Session Locking (FTA_SSL.1)

FTA_SSL.1.1

The TSF shall lock an interactive session after [ten (10) minutes] by:

1110

- (a) clearing or overwriting display devices, making the current contents unreadable;
- (b) disabling any activity of the user's data access / display devices other than unlocking the session.

FTA_SSL.1.2

1115

The TSF shall require the following events to occur prior to unlocking the session: [two-factor authentication by the user that was locked out].

5.1.10.3 User-initiated Locking (FTA_SSL.2)

FTA_SSL.2.1

The TSF shall allow user-initiated locking of the user's own interactive session, by:

- 1120 (a) clearing or overwriting display devices, making the current contents unreadable;
(b) disabling any activity of the user's data access / display devices other than unlocking the session.

1125 ***FTA_SSL.2.2***
The TSF shall require the following events to occur prior to unlocking the session: [two-factor authentication by the user that was locked out].

5.1.10.4 Default TOE Access Banners (FTA_TAB.1)

1130 ***FTA_TAB.1.1***
Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

5.1.10.5 TOE Session Establishment (FTA_TSE.1)

1135 ***FTA_TSE.1.1***
The TSF shall be able to deny session establishment based on [location, time of day, day of week, and user role].

5.2 TOE Security Assurance Requirements

The requirements in this support specific objectives or are selected to be consistent with EAL3. These assurance components are summarized in Table 5-4.

Assurance Class	Assurance Components	
Class ACM: Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Class ADO: Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence documentation
Class AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Class ALC: Life cycle support	ALC_DVS.1	Identification of security measures
Class ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Class AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

1140

Table 5-4 Assurance Requirements: EAL3

5.2.1 Configuration Management (ACM)

5.2.1.1 Authorization Controls (ACM_CAP.3)

Developer action elements:

1145

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a configuration management (CM) system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

- 1150 ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.
- ACM_CAP.3.2C The TOE shall be labeled with its reference.
- ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.
- 1155 ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.
- ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.
- 1160 ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.
- ACM_CAP.3.7C The CM plan shall describe how the CM system is used.
- ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
- ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM systems.
- 1165 ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.
- Evaluator action items:
- 1170 ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 TOE CM Coverage (ACM_SCP.1)

Developer action elements:

- 1175 ACM_SCP.1.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

- 1180 ACM_SCP.1.1C The CM documentation shall show that the CM system as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.
- ACM_SCP.1.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

1185 ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery And Operation (ADO)

5.2.2.1 Delivery Procedures (ADO_DEL.1)

1190 Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

1195 ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

1200 ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Installation, Generation, And Start-up Procedures (ADO_IGS.1)

Developer action elements:

1205 ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

1210 ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1215 ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development (ADV)

5.2.3.1 Informal Functional Specification (ADV_FSP.1)

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

1220

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

1225

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

1230

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1235

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 Security Enforcing High-level Design (ADV_HLD.2)

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

1240

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

1245

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

1250

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the

supporting protection mechanisms implemented in that hardware, firmware, or software.

- 1255 ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
- 1260 ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
- 1260 ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- 1265 ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.
- Evaluator action items:
- 1265 ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

1270 **5.2.3.3 Informal Correspondence Demonstration (ADV_RCR.1)**

Developer Action elements:

- 1275 ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

- 1280 ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

- ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1285 **5.2.4 Guidance Documents (AGD)**

5.2.4.1 Administrator Guidance (AGD_ADM.1)

Developer action elements:

AGD_ADM..1D The developer shall provide administrator guidance addressed to system administrative personnel.

1290 Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

1295 AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

1300 AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

1305 AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

1310 AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

1315 Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 User Guidance (AGD_USR.1)

1320 Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

- | | | |
|------|--------------|---|
| | AGD_USR.1.1C | The user guidance shall describe the functions and interfaces available to non-administrative users of the TOE. |
| 1325 | AGD_USR.1.2C | The user guidance shall describe the use of user-accessible security functions provided by the TOE. |
| | AGD_USR.1.3C | The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. |
| 1330 | AGD_USR.1.4C | The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment. |
| 1335 | AGD_USR.1.5C | The user guidance shall be consistent with all other documentation supplied for evaluation. |
| | AGD_USR.1.6C | The user guidance shall describe all security requirements for the IT environment that are relevant to the user. |

Evaluator action elements:

- | | | |
|------|--------------|--|
| 1340 | AGD_USR.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
|------|--------------|--|

5.2.5 Life Cycle Support (ALC)

5.2.5.1 Identification Of Security Measures (ALC_DVS.1)

1345 Developer action elements:

- | | | |
|--|--------------|---|
| | ALC_DVS.1.1D | The developer shall produce development security documentation. |
|--|--------------|---|

Content and presentation of evidence elements:

- | | | |
|------|--------------|---|
| 1350 | ALC_DVS.1.1C | The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. |
| 1355 | ALC_DVS.1.2C | The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE. |

Evaluator action items:

- 1360 ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.6 Tests (ATE)

5.2.6.1 Analysis Of Coverage (ATE_COV.2)

1365 Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

1370 ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

1375 ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1380 5.2.6.2 Testing: High-level Design (ATE_DPT.1)

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

1385 ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

1390 ATE_DPT1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 Functional Testing (ATE_FUN.1)

Developer action elements:

- 1395 ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

- 1400 ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
1405 ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
1410 ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

- 1415 ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.4 Independent Testing – Sample (ATE_IND.2)

Developer action elements:

- 1420 ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

- 1420 ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

Evaluator action elements:

- 1425 ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

1430 ATE_IND.2.3E The evaluator shall execute a sample of testes in the test documentation to verify the developer test results.

5.2.7 Vulnerability Assessment (AVA)

5.2.7.1 Examination Of Guidance (AVA_MSU.1)

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

1435 Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure of operational error), their consequences and implications for maintaining secure operation.

1440 AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

1445 AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

1450 AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

1455 AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.2.7.2 Strength Of TOE Security Function Evaluation (AVA_SOF.1)

Developer action elements:

1460 AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the Security Target as having a strength of the TOE security function claim.

Content and presentation of evidence elements:

1465 AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function shall show that it meets or exceeds the minimum strength level defined in this Protection Profile.

1470 AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in this Protection Profile.

Evaluator action elements:

1475 AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

Developer Vulnerability Analysis (AVA_VLA.1)

Developer action elements:

1480 AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

1485 Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

1490 AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1495 AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 Rationale

1500 6.1 Rationale For TOE Security Objectives

- 1505 O.Identification This security objective is required to counter threats: T.Escalation_Of_Privilege and T.Audit_Accountability. Unique identification will allow the access control mechanism to be granular and prevent inadvertent escalation of privilege. A unique userID is required to hold users accountable for their actions.
- 1510 O.User_Authentication This security objective is required to counter threats: T.Credential_Cracking and T.Credential_Replay. The two-factor authentication objective will prevent common threats against systems that use only a fixed password for authentication.
- 1515 O.Restricted_Use_Of_Session This security objective is required to counter threats: T.Unauthenticated_Access by limiting the time an unattended system can be used by an attacker and T.Credential_Replay will be ineffective if the user has a current session.
- 1520 O.Access_Control This security objective is required to counter threats: T.Unauthenticated_Access, T.Escalation_Of_Privilege, T.Stored_Data_Modification, T.Audit_Record_Integrity, T.System_Integrity, T.Application_Data_Integrity, and T.Information_Storage_Analysis. This objective first prevents an attacker from gaining access without valid credentials or raising the privilege of valid credentials. The remainder of the threats are addressed by limiting access and access type through the access control system.
- 1530 O.Role_Based_Access_Control This security objective is required to counter threats: T.Escalation_Of_Privilege, T.Stored_Data_Modification, T.Audit_Record_Integrity, T.System_Integrity, T.Application_Data_Integrity, and T.Information_Storage_Analysis. This objective is a refinement of O.Access_Control that allows an Administrator to put similar users into roles and provide access control to the role.
- 1535 O.Subject_Based_Access_Control This security objective is required to counter threats: T.Escalation_Of_Privilege, T.Stored_Data_Modification, T.Audit_Record_Integrity, T.System_Integrity,

1540		T.Application_Data_Integrity, and T.Information_Storage_Analysis. This objective is a refinement of O.Access_Control that allows an Administrator to control access by subject or groups of subjects. It is very useful when users are allowed access rights to a particular subject or set of subjects.
1545	O.Subject_Authentication	This security objective is necessary to counter threats: T.Spoofing, T.Communication_Denial_Of_Service, and T.Device_Denial_Of_Service. By authenticating both communicating parties the TOE will not accept false information from spoofing attacks and will recognize false communication that may be part of a denial of service attack.
1550	O.Command_Authentication	This security objective is necessary to counter threats: T.Spoofing, T.Transmitted_Data_Modification, T.Communication_Denial_Of_Service, and T.Device_Denial_Of_Service. The objective requires the data in transmitted packets to be authenticated. False or modified packets that would be part of the four threats listed above would be discarded.
1555		
1560	O.Data_Exchange_Confidentiality	This security objective is necessary to counter the T.WAN_Data_Compromise threat. The objective requires encrypting the data when in transit outside a TOE physical security boundary. Encrypted data does not provide any information to the attacker.
1565	O.Replay_Protection	This security objective is necessary to counter threats: T.Credential_Replay, T.Data_Replay, T.Communication_Denial_Of_Service, and T.Device_Denial_Of_Service. The objective directly addresses the two replay threats, and the objective addresses an attacker replaying data as part of a denial of service attack.
1570	O.Reasonableness_Test	This security objective is necessary to counter threats: T.Data_Replay, T.False_Communication_Outside_TOE, T.System_Integrity, T.Communication_Denial_Of_Service, and T.Device_Denial_Of_Service. Data received from outside the TOE does not contain security attributes, so this objective is the only means in the TOE to address T.False_Communication_Outside_TOE. Identifying false data will assist in addressing the other threats by identifying and eliminating possible attacks.
1575		

	O.Device_Redundancy	This security objective is necessary to directly counter T.Device_Denial_Of_Service.
1580	O.Communication_Redundancy	This security objective is necessary to directly counter T.Communication_Denial_Of_Service. It will assist in countering T.Device_Denial_Of_Service by providing an alternate network connection when a device's network interface is unavailable.
1585	O.System_Integrity	This security objective is necessary to counter threats: T.Stored_Data_Modification, T.Audit_Record_Integrity, and T.System_Integrity. All three threats are addressed by preventing and identifying unauthorized changes to different types of stored data on the TOE.
1590	O.Secure_State	This security objective is necessary to counter T.System_Integrity when an attacker attempts to compromise the system integrity during the start-up process prior to all security measures being available.
1595	O.Audit	This security objective is necessary to counter almost all of the threats in this Protection Profile. The information provided by this objective will be used to identify and investigate security incidents and is required to support O.Security_Event_Analysis
	O.Audit_Overflow_Protection	This security objective is necessary to directly counter T.Audit_Full.
1600	O.Security_Event_Analysis	This security objective is necessary to counter almost all of the threats in this Protection Profile. This objective will allow an Administrator to identify and investigate most security incidents and uses data from O.Audit.
1605	O.Recovery_And_Response	This security objective is necessary to counter threats: T.System_Integrity, T.Communication_Denial_Of_Service, and T.Device_Denial_Of_Service in a system with redundancy.
1610	O.EAL	This security objective is necessary to counter the threat: T.Moderate_Exposure because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing moderate attack potential.

	T.Unauthenticated_Access	T.Credential_Cracking	T.Credential_Replay	T.Escalation_Of_Privilege	T.Spoofing	T.Transmitted_Data_Modification	T.WAN_Data_Comprromise	T.Stored_Data_Modification	T.Data_Replay	T.False_Communication_Outside_TOE	T.Audit_Record_Integrity	T.Audit_Full	T.Audit_Accountability	T.System_Integrity	T.Application_Data_Integrity	T.Information_Storage_Analysis	T.Communication_Denial_Of_Service	T.Device_Denial_Of_Service	T.Moderate_Exposure
O.Identification				X									X						
O.User_Authentication		X	X																
O.Restricted_Use_Of_Session	X		X		X														
O.Access_Control	X			X				X			X			X	X	X			
O.Role_Based_Access_Control				X				X			X			X	X	X			
O.Subject_Based_Access_Control				X				X			X			X	X	X			
O.Subject_Authentication					X												X	X	
O.Command_Authentication	X				X	X											X	X	
O.Data_Exchange_Confidentiality							X												
O.Replay_Protection			X						X								X	X	
O.Reasonableness_Test									X	X					X		X	X	
O.Device_Redundancy																		X	
O.Communication_Redundancy																	X	X	
O.System_Integrity								X			X			X					
O.Secure_State														X					
O.Audit	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
O.Audit_Overflow_Protection												X							
O.Security_Event_Analysis	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
O.Recovery_And_Response														X			X	X	
O.EAL																			X

Table 6-1 Summary of Mapping Between Threats and Security Objectives for the TOE

6.2 Rationale For Security Objectives For The Environment

1615

	T.Usage	T.Device_Fault	T.Communication_Fault
O.Physical_Security_Perimeter		X	X
O.Outside_Physical_Security_Perimeter		X	X
O.Logical_Security_Perimeter		X	X
O.Environmental_Services_Backup		X	X
O.Usage	X		
O.Training	X		

Table 6-1 Summary of Mapping Between Threats and Security Objectives for the Environment

6.3 Rationale For Security Requirements

1620 Table 6-3 maps this Protection Profile’s objectives to the security requirements that support them. Table 6-4 is the identical information with the reverse mapping.

The rationale for the SOF is based on the moderate attack potential identified in this Protection Profile.

Objectives	Requirements
O.Identification	FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_SMF.1

Objectives	Requirements
O.User_Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.2, FIA_UAU.2, FIA_UAU.3, FIA_UAU.7, FMT_SMF.1, FTA_SSL.1, FTA_SSL.2
O.Restricted_Use_Of_Session	FIA_UAU.6, FMT_SMF.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2, FTA_TAB.1
O.Access_Control	FAU_SAR.2, FDP_ACC.2, FDP_ACF.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_SMF.1, FPT_SEP.1, FTA_TSE.1
O.Role_Based_Access_Control	FAU_SAR.2, FDP_ACC.2, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_SMF.1, FMT_SMR.1, FTA_TSE.1
O.Subject_Based_Access_Control	FAU_SAR.2, FDP_ACF.1, FMT_SMF.1, FTA_TSE.1
O.Subject_Authentication	FDP_IFC.2 (1 and 2), FDP_IFF.1 (1 and 2), FDP_ITT.1 (1 and 2)
O.Command_Authentication	FDP_IFC.2 (1 and 2), FDP_IFF.1 (1 and 2), FDP_ITT.1 (1 and 2), FPT_ITT.3, FPT_TRC.1
O.Data_Exchange_Confidentiality	FDP_IFC.2 (2), FDP_IFF.1 (2), FDP_ITT.1 (2)
O.Replay_Protection	FAU_GEN.1, FIA_UAU.3, FMT_SMF.1, FPT_RPL.1
O.Reasonableness_Test	FDP_IFC.2 (3), FDP_IFF.1 (3), FDP_ITC.1, FMT_SMF.1
O.Device_Redundancy	FRU_FLT.2
O.Communication_Redundancy	FRU_FLT.2
O.System_Integrity	FAU_STG.2, FAU_STG.3, FDP_DAU.1, FDP_SDI.1, FMT_SMF.1, FPT_RCV.3, FPT_SEP.1, FRU_RSA.1
O.Secure_State	FDP_DAU.1, FDP_SDI.1, FMT_MSA.3, FMT_SMF.1, FPT_AMT.1, FPT_FLS.1, FPT_ITT.3, FPT_RCV.3, FPT_RVM.1, FPT_TST.1, FRU_RSA.1
O.Cryptography	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FMT_SMF.1
O.Audit	FAU_GEN.1, FDP_DAU.1, FPT_STM.1

Objectives	Requirements
O.Audit_Overflow_Protection	FAU_STG.4, FMT_MTD.2, FMT_SMF.1, FRU_RSA.1
O.Security_Event_Analysis	FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FIA_AFL.1, FMT_SMF.1, FPT_RPL.1
O.Recovery_And_Response	FMT_SMF.1, FMT_REV.1, FPT_RCV.3, FPT_TRC.1

1625

Table 6-3 Summary of Mappings Between TOE Security Objectives and TOE Security Functions

Requirements	Objectives
FAU_ARP.1	O.Security_Event_Analysis
FAU_GEN.1	O.Replay_Protection, O.Audit
FAU_SAA.1	O.Security_Event_Analysis
FAU_SAR.1	O.Security_Event_Analysis
FAU_SAR.2	O.Access_Control, O.Role_Based_Access_Control, O.Subject_Based_Access_Control
FAU_SAR.3	O.Security_Event_Analysis
FAU_STG.2	O.System_Integrity
FAU_STG.3	O.System_Integrity
FAU_STG.4	O.Audit_Overflow_Protection
FAU_CKM.1	O.Cryptography
FAU_CKM.2	O.Cryptography
FAU_CKM.4	O.Cryptography
FCS_COP.1	O.Cryptography
FDP_ACC.2	O.Access_Control, O.Role_Based_Access_Control
FDP_ACF.1	O.Access_Control, O.Role_Based_Access_Control, O.Subject_Based_Access_Control
FDP_DAU.1	O.System_Integrity, O.Secure_State, O.Audit
FDP_IFC.2 (1 and 2)	O.Subject_Authentication, O.Command_Authentication
FDP_IFC.2 (2)	O.Data_Exchange_Confidentiality
FDP_IFC.2 (3)	O.Reasonableness_Test
FDP_IFF.1 (1 and 2)	O.Subject_Authentication, O.Command_Authentication

Requirements	Objectives
FDP_IFF.1 (2)	O.Data_Exchange_Confidentiality
FDP_IFF.1 (3)	O.Reasonableness_Test
FDP_ITC.1	O.Reasonableness_Test
FDP_ITT.1 (1)	O.Subject_Authentication, O.Command_Authentication
FDP_ITT.1 (2)	O.Subject_Authentication, O.Command_Authentication, O.Data_Exchange_Confidentiality
FDP_SDI.1	O.System_Integrity, O.Secure_State
FIA_AFL.1	O.User_Authentication, O.Security_Event_Analysis
FIA_ATD.1	O.Identification, O.User_Authentication
FIA_SOS.2	O.User_Authentication
FIA_UAU.2	O.User_Authentication, O.Access_Control
FIA_UAU.3	O.User_Authentication, O.Replay_Protection
FIA_UAU.6	O.Restricted_Use_Of_Session
FIA_UAU.7	O.User_Authentication
FIA_UID.2	O.Identification, O.Access_Control
FIA_USB.1	O.Identification
FMT_MOF.1	O.Role_Based_Access_Control
FMT_MSA.1	O.Role_Based_Access_Control
FMT_MSA.3	O.Secure_State, O.Role_Based_Access_Control
FMT_MTD.1	O.Role_Based_Access_Control
FMT_MTD.2	O.Audit_Overflow_Protection
FMT_REV.1	O.Role_Based_Access_Control, O.Recovery_And_Response
FMT_SMF.1	O.Identification, O.User_Authentication, O.Restricted_Use_Of_Session, O.Access_Control, O.Role_Based_Access_Control, O.Subject_Based_Access_Control, O.Replay_Protection, O.Reasonableness_Test, O.System_Integrity, O.Secure_State, O.Cryptography, O.Audit_Overflow_Protection, O.Security_Event_Analysis, O.Recovery_And_Response
FMT_SMR.1	O.User_Authentication
FPT_AMT.1	O.Secure_State
FPT_FLS.1	O.Secure_State

Requirements	Objectives
FPT_ITT.3	O.Command_Authentication, O.Secure_State
FPT_RCV.3	O.System_Integrity, O.Secure_State, O_Recovery_And_Response
FPT_RPL.1	O.Replay_Protection, O.Secure_Event_Analysis
FPT_RVM.1	O.Secure_State
FPT_SEP.1	O.Access_Control, O.System_Integrity
FPT_STM.1	O.Audit
FPT_TRC.1	O.Command_Authentication, O.Recovery_And_Response
FPT_TST.1	O.Secure_State
FRU_FLT.2	O.Device_Redundancy, O.Communication_Redundancy
FRU_RSA.1	O.System_Integrity, O.Secure_State, O_Audit_Overflow_Protection
FTA_MCS.1	O.Restricted_Use_Of_Session
FTA_SSL.1	O.User_Authentication, O.Restricted_Use_Of_Session
FTA_SSL.2	O.User_Authentication, O.Restricted_Use_Of_Session
FTA_TAB.1	O.Restricted_Use_Of_Session
FTA_TSE.1	O.Access_Control, O.Role_Based_Access_Control, O.Subject_Based_Access_Control

Table 6-4 Summary of Mappings Between TOE Security Functions and TOE Security Objectives

1630

O.Identification

The TOE must uniquely identify the claimed identity of each user.

1635

Coverage Rationale: O.Identification is provided by FIA_ATD.1, FIA_UID.2, FIA_USB.1, and FMT_SMF.1. FIA_ATD.1 directly requires a unique userID and meets the objective. FIA_UID.2 and FIA_USB.1 require a unique userID prior to any action and binds the unique userID to a unique subject, respectively. FMT_SMF.1 is the related management requirement.

1640

O.User_Authentication

The TOE must authenticate the claimed identity of each user with a two-factor authentication method prior to providing access to any TOE function. The authentication process must not provide any information except for pass or fail.

1645

1650 Coverage Rationale: O.User_Authentication is provided by FIA_AFL.1, FIA_ATD.1, FIA_SOS.2, FIA_UAU.3, FIA_UAU.7, FMT_SMF.1, FTA_SSL.1, and FTA_SSL.2. FIA_SOS.2 requires two-factor authentication for all users, and FIA_ATD.1 requires the TSF to maintain the authentication credentials with each user. FIA_UAU.2 enforces user authentication prior to any user actions on the TOE. FIA_UAU.3 requires the TSF to prevent forgery and reuse of the credentials, which can be addressed through most two-factor authentication systems. FIA_UAU.7 provides the coverage for the last sentence with regard to limiting information provided during authentication. The remaining requirements address user authentication problems and management.

O.Restricted_Use_Of_Session

1660 The TOE must notify users regarding unauthorized use of the TOE and enforce restrictions to limit use of an authenticated session to the authentication user by preventing multiple concurrent sessions and locking a session that has been idle for a period of time defined by a TOE Administrator.

1665 Coverage Rationale: O.Restricted_Use_Of_Session is provided by FIA_UAU.6, FMT_SMF.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2, and FTA_TAB.1. FTA_TAB.1 requires a banner regarding unauthorized use. FIA_UAU.6 and FTA_SSL.1 require an idle timeout with a default setting of ten minutes. FTA_MCS.2 limits concurrent sessions by a userID and sets the default at one session. All idle lockouts require two-factor authentication to unlock the session. FMT_SMF.1 relates to the management of this objective.

1670

O.Access_Control

1675 The TOE must provide and enforce an access control capability that allows the TOE Administrator to restrict access and operations to the subjects in the system. The TOE Administrator shall be able to further restrict access by time of day / day of week criteria.

1680 Coverage Rationale: O.Access_Control is provided by FAU_SAR.2, FDP_ACC.2, FDP_ACF.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_SMF.1, FPT_SEP.1, and FTA_TSE.1. FDP_ACC.2 and FDP_ACF.1 require the P.Access_Control SFP that meets this objective. FTA_TSE.1 also facilitates access control by time of day / day of week. FIA_UAU.2, FIA_UID.2, and FIA_USB.1 integrate the user authentication process into access control. FAU_SAR.1 covers access control to audit records. FPT_SEP.1 restricts tampering of the TSF by unauthorized users. FMT_SMF.1 addresses the management for this objective.

1685

O.Role_Based_Access_Control

1690

The TOE must provide a means to place users into roles and make access control decisions based on roles.

1695 The system should support the ability to create and define as many roles as required by the system. At a minimum the roles defined in Table 4.1 must be included in the TOE.

1700 Coverage Rationale: O.Role_Based_Access_Control is provided by FAU_SAR.2, FDP_ACC.2, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_SMF.1, FMT_SMR.1, and FTA_TSE.1. FDP_ACC.2 and FDP_ACF.1 require the P.Access_Control SFP that meets this objective. FMT_MOF.1 specifically requires user roles be used to restrict the ability to act on functions in the TOE. FMT_SMR.1 specifically addresses the management of roles. FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2 and FMT_SMF.1 cover other related management for this objective. FAU_SAR.2 covers access to audit records.

O.Subject_Based_Access_Control

1710 The TOE must provide a means to place subjects into a group and assign user or role based access control to the subject group.

1715 Coverage Rationale: O.Subject_Based_Access_Control is provided by FAU_SAR.2, FDP_ACF.1, FMT_SMF.1, and FTA_TSE.1. FDP_ACF.1 and FTA_TSE.1 meet this requirement directly. FAU_SAR.2 covers access to audit records, and FMT_SMF.1 relates to the management of this objective.

O.Subject_Authentication

1720 Individual subjects in the TOE must perform mutual authentication prior to communication with another TOE subject or object.

1725 Coverage Rationale: O.Subject_Authentication is provided by FDP_IFC.2 (1 and 2), FDP_IFT.1 (1 and 2), and FDP_ITT.1 (1 and 2). These requirements address and define two informational flow control SFPs, P.Internal_TSF and P.Remote_TSF. These SFPs require the source subject's identity to be cryptographically authenticated and therefore meet this objective.

O.Command_Authentication

1730 Individual devices in the TOE must authenticate the integrity of all commands and responses sent from another TOE device prior to acting on or storing the data.

1735 Coverage Rationale: O.Command_Authentication is provided by FDP_IFC.2 (1 and 2), FDP_IFT.1 (1 and 2), FDP_ITT.1 (1 and 2), FPT_ITT.3, and FPT_TRC.1. These requirements address and define two informational flow control SFPs, P.Internal_TSF and P.Remote_TSF. These SFPs require the data integrity be

verified through a cryptographic integrity check for all commands and responses, including replication and other system communication.

1740

O.Data_Exchange_Confidentiality

The TOE must protect the confidentiality of TOE data while it is outside of a TOE physical security boundary.

1745

Coverage Rationale: O.Data_Exchange_Confidentiality is provided by FDP_IFC.2 (2), FDP_IFF.1 (2), and FDP_ITT.1 (2). These three functional requirements relate to the P.Remote TSF information flow control SFP. FDP_IFC.2 assigns the SFP. FDP_IFF.1 (2) requires encryption for all communication from source to destination. FDP_ITT.1 (2) enforces the SFP to prevent disclosure of information.

1750

O.Replay_Protection

The TOE must identify the replay of any data and prevent action based on the replayed data.

1755

Coverage Rationale: O.Replay_Protection is provided by FAU_GEN.1, FIA_UAU.3, FMT_SMF.1, and FPT_RPL.1. FPT_RPL.1 directly addresses this objective. FAU_GEN.1 indicates audit records may help identify replay. FIA_UAU.3 deals with replay of user authentication credentials, and FMT_SMF.1 addresses the management requirements for this objective.

1760

O.Reasonableness_Test

The TOE must identify and reject any commands or responses originating outside the TOE that contain unreasonable values or occur at an unreasonable rate. Any communication that fails this reasonableness test must generate a security alarm.

1765

Coverage Rationale: O.Reasonableness_Test is provided by FDP_IFC.2 (3), FDP_IFF.1 (3), FDP_ITC.1, and FMT_SMF.1. The third iteration of FDP_IFC.2 and FDP_IFF.1 is for the P.Outside_TSF information flow control policy and requires a check of parameters to insure values are reasonable prior to acceptance. FDP_ITC.1 essentially repeats the reasonableness test requirement for the generic "import of user data".

1770

Application Note: If a Protection Profile is developed for Field Devices, this reasonableness test for imported user data could be converted to an inter-TSF transfer of data with strong cryptographic requirements. Since neither the field device Protection Profile nor products with the cryptographic capabilities exist, this Protection Profile made communication with field devices a separate information flow control policy based primarily on a reasonableness test.

1775

1780

O.Device_Redundancy

1785 The functionality of the TOE must not be compromised if any one device in the TOE is unavailable.

Coverage Rationale: O.Device_Redundancy is provided directly by FRU_FLT.2.

1790 ***O.Communication_Redundancy***

The functionality of the TOE must not be compromised if any single communication path is unavailable.

1795 Coverage Rationale: O.Communication_Redundancy is provided directly by FRU_FLT.2.

O.System_Integrity

1800 All devices in the TOE must identify any unauthorized changes to process control applications, process control system and application configurations, and process control data. An alarm must be generated if an unauthorized change has occurred.

1805 Coverage Rationale: O.System_Integrity is provided by FAU_STG.2, FAU_STG.3, FDP_DAU.1, FDP_SDI.1, FMT_SMF.1, FPT_RCV.3, FPT_SEP.1. and FRU_RSA.1. FAU_STG.2 and FAU_STG.3 identify unauthorized changes to audit records and generate the appropriate alarm. FDP_DAU.1 more broadly covers the TOE application and application data for the same issues, and FDP_SDI.1 actively monitors the data for system integrity faults. FPT_RCV.3 and FPT_SEP.1 address using system integrity controls to securely recover from failures. FRU_RSA.1 places limits on resources to prevent system integrity failures. FMT_SMF.1 covers management requirements related to this objective.

O.Secure_State

1815 Upon initial start-up of the TOE or recovery from interruption in any part of TOE service, the TOE must not compromise its resources and preserve the secure state of the system.

1820 Coverage Rationale: O.Secure_State is provided by FDP_DAU.1, FDP_SDI.1, FMT_MSA.3, FMT_SMF.1, FPT_AMT.1, FPT_FLS.1, FPT_ITT.3, FPT_RCV.3, FPT_RVM.1, FPT_TST.1, and FRU_RSA.1. A large number of requirements overlap to provide a secure state and start-up and all other times. However, FPT_FLS.1 and FPT_RCV.3 directly address this objective.

1825 ***O.Cryptography***

The TOE shall employ cryptographic algorithms approved by a recognized security standards body and that have no known vulnerabilities. The key size for all algorithms shall be greater than the capability of any actual exhaustion attack.

1830 Coverage Rationale: O.Cryptography is provided by FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, and FMT_SMF.1. The FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, and FCS_COP.1 functional requirements specify NIST standard algorithms and sufficiently large keys sizes for strength of function. FMT_SMF.1 covers the management issues for this objective.

1835

O.Audit

1840 The TOE must provide the means of recording selected security-relevant events, to assist an Administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave it susceptible to attack. Additionally the events must be recorded in a manner to hold users accountable for any actions they perform that are relevant to security.

1845 Coverage Rationale: O.Audit is provided by FAU_GEN.1, FDP_DAU.1, and FPT_STM.1. FAU_GEN.1 provides the requirements to generate the audit records that include information identifying the user or subject that initiated the event. FDP_DAU.1 verifies the integrity of the audit records and identifies potential attacks and misconfiguration. FPT_STM.1 provides time stamps that are crucial for audit records.

1850

O.Audit_Overflow_Protection

1855 The audit record shall maintain user accountability of the most recent auditable actions in the event that the maximum capacity of the audit log is reached.

1860 Coverage Rationale: O.Audit_Overflow_Protection is provided by FAU_STG.4, FMT_MTD.2, FMT_SMF.1, FRU_RSA.1. FAU_STG.4 requires the TSF to overwrite the oldest stored audit records which meets the “most recent auditable actions” portion of the objective. FMT_MTD.2, FMT_SMF.1, and FRU_RSA.1 all provide a means for an Administrator to configure the capacity of the audit records.

O.Security_Event_Analysis

1865 The TOE must provide an automated and manual means for an Administrator to analyze the security events in an audit trail to identify and investigate potential security incidents.

1870 Coverage Rationale: O.Security_Event_Analysis is provided by FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FIA_AFL.1, FMT_SMF.1, and FPT_RPL.1. FAU_ARP.1, FAU_SAA.1, and FIA_AFL.1 cover the automated security event analysis, and FAU_SAR.1 and FAU_SAR.3 cover the manual security event analysis. FPT_RPL.1 specifically addresses identification of replay. FMT_SMF.1 covers the management issues for this objective.

1875

O.Recovery_And_Response

The TOE must recover from a system outage and securely distribute all system changes within a time period set by the Administrator.

- 1880 Coverage Rationale: O.Recovery_And_Response is provided by FMT_SMF.1, FMT_REV.1, FPT_RCV.3, and FPT_TRC.1. FPT_RCV.3 directly addresses the recovery objective. FMT_SMF.1 covers the management of recovery settings. FMT_REV.1 requires configuration changes be distributed within fifteen (15) minutes to all systems and addresses the response objective. FPT_TRC.1 directly
- 1885 addresses the replication issues for distributed components in the TOE.

6.4 Rationale for Assurance Requirements

The assurance level for this Protection Profile is EAL3.

- 1890 EAL3 is applicable in those circumstances where developers of users require a moderated level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering. As such, EAL3 is appropriate for ICS Control Centers.

Appendix A: Acronyms

1895

CM Configuration Management
DCS Distributed Control System
EAL Evaluation Assurance Level
HMI Human Machine Interface

1900

ICS Industrial Control System
PCSRF Process Control Security Requirements Forum
SCADA Supervisory Control And Data Acquisition
SFP Security Function Policies
TOE Target of Evaluation

1905

TSF TOE Security Functions
TSP TOE Security Policies

1910

Appendix B: Definitions

<<pending>>

1915

Appendix C: Approved Cryptographic Algorithms

<<pending>>