# System Protection Profile - Industrial Control Systems

## Version 1.0

**Prepared for**

**by**

# Document Control

## Preparation

| Action | Name | Date |
|---|---|---|
| Prepared by: | Ron Melton, Terry Fletcher, Matt Earley | 14 April 2004 |
| Reviewed by: | Murray Donaldson | 14 April 2004 |

## Release

| Version | Date Released | Change Notice | Pages Affected | Remarks |
|---|---|---|---|---|
| 0.91 | 4 Feb 2004 | N/A | All | SPP populated into new structure. Core information chapters (1 to 6) nearing completion. Chapters 7 and 8 (Application Notes & Rationale) under development. |
| 1.0 | 14 April 2004 | N/A | All | First release |

## Distribution List

| Name | Organisation | Title |
|---|---|---|
| Keith Stouffer | NIST | PCSRF Program Manager |
| PCSRF Members | Various | Various |


© Copyright 2004 National Institute of Standards & Technology

# TABLE OF CONTENTS

**DOCUMENT CONTROL** ..... **2**

PREPARATION ..... 2
RELEASE ..... 2
DISTRIBUTION LIST ..... 2

**1 INTRODUCTION** ..... **9**

1.1 SPP IDENTIFICATION ..... 9
1.2 SPP OVERVIEW ..... 9

**2 STOE DESCRIPTION** ..... **13**

2.1 OVERVIEW OF THE SYSTEM TARGET OF EVALUATION (STOE) ..... 13
2.2 SCOPE OF THE STOE ..... 13
2.3 SECURITY FEATURES ..... 15
2.4 FEATURES OUTSIDE OF SCOPE ..... 17

**3 STOE SECURITY ENVIRONMENT** ..... **18**

3.1 SECURE USAGE ASSUMPTIONS ..... 18
3.2 THREATS TO SECURITY ..... 18
*3.2.1 Threats Addressed by the STOE ..... 19*
*3.2.2 Threats Addressed by the Operating Environment ..... 27*
3.3 OVERARCHING ORGANIZATIONAL SECURITY POLICIES ..... 27

**4 RISKS** ..... **29**

4.1 RISK CATEGORIES APPLICABLE TO THE STOE ..... 29
4.2 RISKS TO THE EXTERNAL OPERATING ENVIRONMENT ..... 34

**5 SECURITY OBJECTIVES** ..... **35**

5.1 SECURITY OBJECTIVES FOR THE STOE ..... 35
5.2 SECURITY OBJECTIVES FOR THE EXTERNAL OPERATING ENVIRONMENT ..... 38

**6 IT SECURITY REQUIREMENTS** ..... **39**

6.1 STOE SECURITY FUNCTIONAL REQUIREMENTS ..... 39
*6.1.1 Logon Controls: ..... 42*
*6.1.2 Password Selection ..... 44*
*6.1.3 Authentication Data Protection ..... 45*
*6.1.4 Replay / Reuse ..... 45*
*6.1.5 Session Suspension ..... 46*
*6.1.6 User Accounts and Profiles ..... 46*
*6.1.7 Role based access control ..... 47*
*6.1.8 Controls on RBAC Attributes ..... 48*
*6.1.9 Firewall access control ..... 48*


© Copyright 2004 National Institute of Standards & Technology

*6.1.10 Audit events* ... *49*
*6.1.11 Intrusion detection and response* ... *50*
*6.1.12 Audit trail protection* ... *52*
*6.1.13 Audit trail analysis / review* ... *53*
*6.1.14 TOE Integrity* ... *53*
*6.1.15 Data Authentication* ... *54*
*6.1.16 Data exchange integrity* ... *54*
*6.1.17 Functions required to support dependencies* ... *55*
*6.1.18 Secure Communications Channels* ... *56*
*6.1.19 Management Functions* ... *58*
*6.1.20 Physical Security Requirements* ... *61*
*6.1.21 Security Event Monitoring* ... *61*
*6.1.22 Requirements for interfaces between system components* ... *63*
*6.1.23 Requirements for composability and interoperability between system components* ... *63*
*6.1.24 Configuration requirements* ... *63*
6.2 STOE SECURITY ASSURANCE REQUIREMENTS ... 63
*6.2.1 Configuration Management (ACM)* ... *65*
*6.2.2 Delivery and Operation (ADO)* ... *67*
*6.2.3 Guidance Documents (AGD)* ... *69*
*6.2.4 Life Cycle Support (ALC)* ... *71*
*6.2.5 Security Awareness (ASA)* ... *74*
*6.2.6 System O&M Security Controls (ASC)* ... *74*
*6.2.7 System Architecture (Class ASD)* ... *76*
*6.2.8 Tests (ATE)* ... *80*
*6.2.9 Vulnerability Assessment (AVA)* ... *83*
*6.2.10 Assurance Maintenance (AMA)* ... *85*
6.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT ... 89
6.4 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT ... 89

**7 SPP APPLICATION NOTES ... 90**

7.1 SPP OVERVIEW ... 90
*7.1.1 SPP Purpose* ... *90*
*7.1.2 SPP Structure* ... *91*
*7.1.3 SPP Application* ... *94*
7.2 SPP APPLICATION: RISK MANAGEMENT ... 94
*7.2.1 Risk Management Process* ... *94*
7.3 SPP APPLICATION: SPP ... 96
*7.3.1 Refinement of the Security Environment* ... *97*
*7.3.2 Risk Identification* ... *98*
*7.3.3 Refinement of the Security Objectives* ... *100*
*7.3.4 Refinement of the IT Security Requirements* ... *100*
*7.3.5 Supporting Rationale* ... *100*
7.4 SPP APPLICATION: SST ... 101


© Copyright 2004 National Institute of Standards & Technology

*7.4.1 STOE Summary Specification ..... 101*
*7.4.2 SPP Claims ..... 102*
*7.4.3 Supporting Rationale ..... 102*

**8 RATIONALE ..... 103**

8.1 SECURITY RISKS RATIONALE ..... 103
*8.1.1 All Assets, Threats and Vulnerabilities Addressed ..... 103*
*8.1.2 Security Risks are Sufficient ..... 120*
8.2 SECURITY OBJECTIVES RATIONALE ..... 120
*8.2.1 All Assumptions, Threats and Policies Addressed ..... 120*
*8.2.2 Security Objectives are Sufficient ..... 132*
*8.2.3 Suitability of the Security Objectives to counter identified Risks ..... 132*
*8.2.4 Sufficiency of the Security Objectives to counter identified Risks ..... 137*
8.3 SECURITY REQUIREMENTS RATIONALE ..... 137
*8.3.1 Suitability of the Security Requirements ..... 137*
*8.3.2 Sufficiency of the Security Requirements ..... 143*
*8.3.3 Satisfaction of Dependencies ..... 143*
8.4 RATIONALE FOR EXTENSIONS ..... 143
*8.4.1 Augmentation for Assurance Background Information ..... 143*
8.5 STRENGTH OF FUNCTION CLAIMS ..... 150

**APPENDIX A – ACRONYMS ..... 151**


© Copyright 2004 National Institute of Standards & Technology

# LIST OF TABLES

Table 1 –Scope of the STOE ..... 14
Table 2 – Summary of STOE Security Features ..... 15
Table 3 – Secure Usage Assumptions ..... 18
Table 4 – Threat Agents for the STOE ..... 19
Table 5 – Sources of Vulnerabilities of the STOE ..... 20
Table 6 – Attack Methods against the STOE ..... 21
Table 7 – Assets protected by the STOE ..... 23
Table 8 – Threats countered by the STOE ..... 25
Table 9 – Organizational Security Policies ..... 27
Table 10 – Identified Risk Categories for the STOE ..... 29
Table 11 – Security Objectives for the STOE ..... 35
Table 12 – STOE Security Functional Requirements ..... 39
Table 13 – STOE Security Assurance Requirements ..... 64
Table 14 - Mapping of Assets, Threats and Vulnerabilities to Security Risks ..... 103
Table 15 - Mapping of Security Risks to Assets, Threats and Vulnerabilities ..... 116
Table 16 - Mapping of Assumptions, Threats, and OSPs to Security Objectives ..... 120
Table 17 - Mapping of Security Objectives to Threats, Policies and Assumptions ..... 127
Table 18 - Mapping of Security Risks to Security Objectives ..... 132
Table 19 - Mapping of Security Objectives to Security Risks ..... 134
Table 20 - Mapping of Security Objectives to Security Requirements ..... 137
Table 21 - Mapping of Security Requirements to Security Objectives ..... 139


© Copyright 2004 National Institute of Standards & Technology

# Conventions and Terminology

## Conventions

The notation, formatting, and conventions used in this System Protection Profile are consistent with those used in Version 2.1 of the Common Criteria [CC]. Selected presentation choices are discussed here to aid the System Protection Profile reader. The CC allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 2.1.4 of Part 2 of the CC [CC2] are *refinement, selection, assignment* and *iteration.*

- 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 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.

- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

All operations described above are used in this System Protection Profile. *Italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

## Terminology

The terminology used in the System Protection Profile is that defined in the Common Criteria [CC1, CC2]. A glossary has also been provided in Appendix A – Acronyms.

## References

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

[CC1] Common Criteria Part 1: Introduction and General Model, Version 2.1, CCIB-99-031, August 1999.


© Copyright 2004 National Institute of Standards & Technology

[CC2] Common Criteria Part 2: Security Functional Requirements, Version 2.1, CCIB-99032, August 1999.

[CC3] Common Criteria Part 3: Security Assurance Requirements, Version 2.1, CCIB-99033, August 1999.

[CEM] Common Evaluation Methodology Part 2: Evaluation Methodology, Version 1.0, CEM99/045, August 1999.

# Document Organization

**Section 1** provides the introductory material for the System Protection Profile.

**Section 2** provides general purpose and STOE description.

**Section 3** provides a discussion of the expected environment for the STOE. This section also defines the set of threats that are to be addressed by either the technical, operational or management controls implemented by the STOE or through the environmental controls.

**Section 4** identifies the risks to the STOE that have been derived from the statement of the security environment defined in section 3.

**Section 5** defines the security objectives for both the STOE and the STOE environment.

**Section 6** contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3 [CC2, CC3], respectively that must be satisfied by the STOE.

**Section 7** contains guidance information for SST authors who would like to claim conformance to the SPP.

**Section 8** provides a rationale to explicitly demonstrate that the identified risks to the STOE have been derived from the aspects identified in the security environment. It also demonstrates how the security objectives have been derived from each of the identified risks. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Section 8 also provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the System Protection Profile requirements.

**Appendix A** documents an acronym list to define frequently used acronyms applicable to the STOE.


© Copyright 2004 National Institute of Standards & Technology

# 1 Introduction

This introductory section presents *System Protection Profile (SPP)* identification information and an overview of the SPP.

## 1.1 SPP Identification

This section provides information needed to identify and control this SPP. This SPP targets an **extended Evaluation Assurance Level (EAL) 3** level of assurance for the STOE.

| | |
|---|---|
| **SPP Title:** | System Protection Profile - Industrial Control Systems |
| **SPP Version:** | 1.0 |
| **CC Version:** | Common Criteria for Information Technology Security Evaluation, Version 2.1 Final |
| **SPP Evaluation:** | National Information Assurance Partnership |
| **Author(s):** | National Institute of Standards & Technology |
| **Keywords:** | Industrial Control Systems |

## 1.2 SPP Overview

**SPP Background**

This SPP has been developed as part of the Process Control Security Requirements Forum (PCSRF) sponsored by the National Institute of Standards and Technology (NIST). This SPP is intended to provide an ISO 15408 based starting point in formally stating security requirements associated with industrial control systems (ICS). This SPP includes security functional requirements (SFRs) and security assurance requirements (SARs) that extend ISO 15408 to cover issues associated with systems. These extensions are based on current ISO subcommittee work to extend ISO 15408 to cover the accreditation of systems and the evaluation of system protection profiles and system security targets. These extensions broaden consideration of security controls to include non-technical controls based on procedural and management functions.

**Industrial Process Security**

Continued existence of modern society is dependent on its industry and infrastructure and its ability to control electrical, chemical and mechanical transformations of materials and energy to produce desired results.

Generally, an ICS is a computer-based system(s) used to control industrial processes and physical functions. Industrial control systems automate these control functions allowing for industrial processes that are faster, larger and more complex than non-automated means. The ICS and


© Copyright 2004 National Institute of Standards & Technology

associated systems assure the safe and environmentally acceptable operation of a specific industrial process.

The ultimate goal of an ICS is to assure the specified operational, safety and environmental compatibility of a specified industrial process such as a power plant and its distribution network. The "specified operation" may be "continued operation" or "demand operation." For example, a power plant operation generally is supposed to be continuous while an emergency power generator typically is supposed to operate on demand only. Safety and environmental compatibility means that neither personnel safety, nor the quality of the environment (natural or otherwise) are endangered.

Therefore, the overall security concern for an ICS typically originates from malicious threat agents attempting to disrupt an industrial process such as to interfere with it specified operation (e.g. to create a power outage) or to negatively impact on the environment and/or personnel safety (e.g. exploding a fuel tank or destabilizing chemical process to free noxious gases).

It is worth noting that attempting to capture the requirements of all ICS implementations in a single document is not feasible due to the differences between the processes and the networks deployed across various industries. However, there exists a subset of those security requirements that are applicable to all ICS implementations. This subset is the focus of this SPP.

The SPP has been written in such a way that it may be used as the basis for preparing a System Security Target for a specific ICS or as the basis for a more detailed SPP for a sub-class of ICS such as a Supervisory Control and Data Acquisition System (SCADA). For more discussion of the role of this SPP refer to section 7.1 of the application notes.

**ICS Background**

There are several varieties of ICS, but all consist of the same basic elements. As shown in Figure 1 those components are: the controller, sensors, actuators (or final control elements), and in some cases a human machine interface (HMI) and a remote diagnostics and maintenance capability. These components may be in close physical proximity or they may be distributed with great distances (many miles) between some of the elements) depending on the specific application. In addition to these technical elements ICS include a human element including operators, maintainers and engineers. They also have operating procedures and other non-technical elements.

A simplified view of the operation of an ICS and the function of the elements is as follows. The controller implement control algorithms based on a mathematical model of the process to be controlled and the control objectives. The sensors sense the state of the process through measurement of process parameters such as temperature, pressure, voltage, pH, position, size, etc. The state of the process may change due to external "disturbances", changes in the process inputs such as feed material, or in response to action initiated by the controller. The controller processes the sensor information and, based on the control algorithm and desired state of the process, sends commands to the final control elements which in turn interact with the controlled process to affect changes in its state. The final control elements take many different forms including valves, switches, relays, motors, and so forth depending on the nature of the process under control. The


© Copyright 2004 National Institute of Standards & Technology

HMI provides a means for human operators to monitor the state of the process and the ICS, to interact with the controller to change the control objective and may also include manual control options (for the case of emergency). Similarly there may be a remote diagnostics and maintenance interface to be used in gathering data used for diagnostics, maintenance, emergency procedures or other similar activities.

**Need for an ICS SPP**

Recently, several factors have raised concern about the security of industrial control systems. First, there has been a general trend to replace specialized control devices, particularly controllers and communications elements, with general purpose computer equipment and associated data communications technology. Second, many companies have chosen to interconnect certain parts of their process control networks with their corporate intranet once they have introduced general-purpose equipment into the process control system.

These two factors introduce all of the potential vulnerabilities found in the network computing in general, particularly if there is a path through the corporate intranet to the Internet at large. Third, for ICS that are broadly distributed a variety of communications media are used including the public switched telephone system, wireless communications and the Internet. There are potential security vulnerabilities associated with each of these communications paths. Finally, ICS are key components of much of our national critical infrastructure including the electric power, water and water treatment, oil and gas production and distribution as well as industrial and military manufacturing.

To address these vulnerabilities organizations are primarily installing security retrofits or upgrades to existing their existing ICS. This SPP is intended to provide a basis for these activities as well as the design of new systems. In either case, the security functionality should be implemented based on a risk analysis that determines security requirements based on an assessment of threats, vulnerabilities and impacts.

**System Protection Profile - Industrial Control Systems**

The System Protection Profile for Industrial Control Systems (SPP-ICS) specifies the integrated set of security requirements for industrial control systems. The integrated set of requirements includes requirements for operating policies and procedures, requirements for information technology based system components, requirements for interfaces and interoperability between system components, and requirements for the physical environment and protection of the system.

Because the SPP-ICS represents an integrated view of the requirements, special consideration is given to decomposition of security functionality and assignment of specific security functions to sub-systems or components of the overall integrated system. Likewise, the decomposition or composability of the security functionality is also considered. The goal of this aspect of analysis and design is to define security requirements for subsystems or system components at the lowest possible level while at the same time retaining the required level of assurance and security functionality for the integrated system as a whole.


© Copyright 2004 National Institute of Standards & Technology

As shown in Figure 1 an industrial control system consists of classes of components for the direct control of a process (the controller(s), actuators and sensors) a human machine interface and capabilities for remote diagnostics and maintenance. Although not represented in the diagram, there are also human elements such as operators and non-technical elements such as operating procedures.

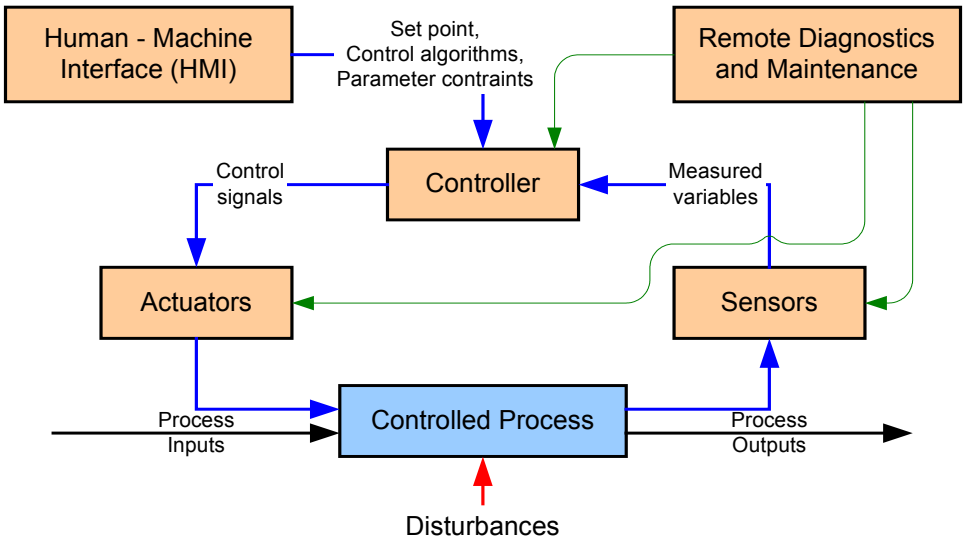


**Figure 1: Generic industrial control system**

This system protection profile is written for a generic industrial control system as a high-level statement of requirements. It provides a starting point for more specific and detailed statements of requirements for industrial control systems focused on a specific industry, company, or component.


© Copyright 2004 National Institute of Standards & Technology

# 2 STOE Description

This section provides context for the STOE evaluation by identifying the system and describing the evaluated configuration.

## 2.1 Overview of the System Target of Evaluation (STOE)

This section describes the security subsystem of the industrial control system. The security subsystem includes both the information technology based components and the non-information technology based elements implemented via policies and operating procedures. Particular attention is given to the interaction and dependencies between the security subsystem and the overall industrial control system.

The STOE focuses on protecting data confidentiality, data integrity and system availability without interfering with safety system functions. Data integrity centers on protecting data flows to and from the controller and the other ICS components or subsystems. The STOE is also intended to protect system availability to assure continuity of operations.

## 2.2 Scope of the STOE

The STOE consists of the security services and procedures, both automated and manual, which are designed to meet the security objectives defined to counter threats to the ICS.

The scope of the STOE is depicted graphically in Figure 2. Boxes with bold red borders depict the primary system security functions. These functions are: user authentication services (including user access control), physical access control, boundary protection, and data / device authentication. User authentication services control access to process control related computer systems including the human machine interface (HMI) and remote diagnostics and maintenance. In addition, user authentication is used by the physical access control system to authenticate personnel for physical access. Data / device authentication is shown as a separate function to emphasize the need for data and command signal authentication. Note that the corporate intranet is in the external environment of the STOE.

The blue lines from actuator to controlled process and from controlled process to sensor indicate that these are physical connections representing the direct interactions that take place. The rest of the diagram depicts logical connections. Security controls based on management and operating procedures are not shown in the figure.


© Copyright 2004 National Institute of Standards & Technology

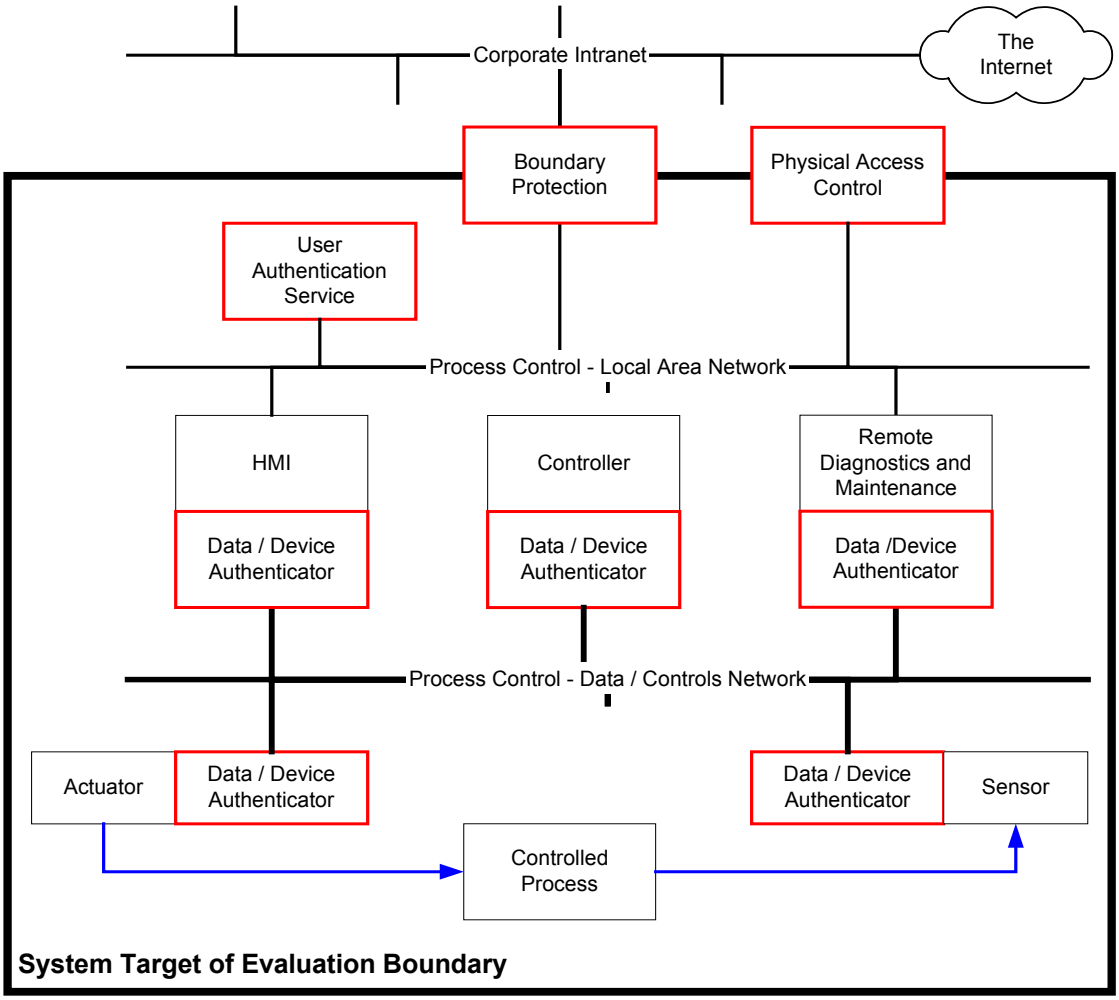


**Figure 2** ***Graphical depiction of System Target of Evaluation***

The scope of the STOE includes the technical and non-technical elements identified in Table 1.

**Table 1 –Scope of the STOE**

| STOE Components | Example Hardware/Software Components |
|---|---|
| **Physical Boundary Protection** | Access control for ICS perimeter and control center security |
| **Logical Boundary Protection** | Firewall and other gateway security devices (e.g. intrusion detection systems) |
| **Data authentication** | Data authentication service performed by ICS components (e.g. authenticators) |
| **Data Confidentiality** | Encryption services, such as link encryption devices between trusted endpoints |


© Copyright 2004 National Institute of Standards & Technology

| STOE Components | Example Hardware/Software Components |
|---|---|
| **User Authentication** | User authentication service, integration with physical access control |
| **Continuity of Operations** | System backup and recovery, backup power, etc |
| **Operating procedures** | System policies and procedures (e.g. backup frequency, password requirements, etc) |
| **Training** | Security awareness & training courses, etc. |
| **Management procedures** | Staff selection criteria, disciplinary measures and other relevant personnel security policies |

## 2.3 Security Features

The STOE provides the following security features:

**Table 2 – Summary of STOE Security Features**

| Feature | Description |
|---|---|
| **Authentication** | Authentication of the following:<br>▪ Financial and business critical information sent from the ICS to external systems<br>▪ Configuration change commands affecting core ICS functions (e.g. control algorithms, set points, limit points etc)<br>▪ Users and services accessing the protected assets (e.g. actuators, control systems, etc) |
| **Confidentiality** | Protection of business, financial and control data from unauthorized disclosure (as determined by risk assessment and approved by the data or system owner), including, but not limited to, appropriate segments within the ICS network. |
| **Integrity** | Protection against the unauthorized modification of the following information:<br>▪ Information flows of a sensitive nature on exposed network segments<br>▪ Internal control data used throughout the ICS<br>▪ ICS operational system configuration |
| **Availability** | Protection against the loss of availability of all critical and major ICS operational systems including, but not limited to, |


© Copyright 2004 National Institute of Standards & Technology

| Feature | Description |
|---|---|
| | ▪ Control servers<br>▪ Primary communications channel (or network)<br>▪ ICS operational system configuration capability |
| **Boundary Protection** | Protection against unauthorized attempts to breech both the physical and the logical boundaries of the ICS. |
| **Access control** | Strict access control for the following:<br>▪ On-site and off-site remote access into the ICS network<br>▪ Externally-visible interfaces of the ICS<br>▪ System resources deemed by the owner(s) as requiring protection<br>▪ Those system functions capable of modifying ICS configuration<br>▪ Critical ICS processes based on state information relevant to that process (e.g. time of day, location, etc) |
| **Backup / Recovery** | Backup mechanisms for critical ICS data and control information to enable timely recovery from system compromises or damage. |
| **Audit** | Entries in the audit log of appropriate ICS components detailing the successful and unsuccessful security relevant activities of users and applications. |
| **Monitoring** | Monitoring and detection of unauthorized activity, unusual activity and attempts to defeat the security capabilities of the ICS, including the deployment of intrusion detection systems (IDS) at critical parts of the ICS infrastructure. |
| **Non-interference with safety critical functions** | Non-interference of ICS security functions and safety-critical functions while maintaining ICS performance. |
| **Self Verification** | Self-tests to verify the configuration and integrity of the security functions of the ICS. |
| **Emergency power** | Emergency power sufficient to allow for graceful shutdown of the ICS and the controlled process in the event that primary and secondary power fail. |
| **Security Plans, Policies & Procedures** | Security plans, policies and procedures covering at least the following areas:<br>▪ Overarching security policy governing the access and necessary protection for all ICS components<br>▪ Security management of the ICS and associated infrastructure<br>▪ Security management roles and responsibilities throughout the |


© Copyright 2004 National Institute of Standards & Technology

| Feature | Description |
|---|---|
| | ICS management infrastructure<br>▪ Documentation of the organizational risk management process and its relationship to ICS systems<br>▪ Business continuity and disaster recovery plans for the ICS<br>▪ Migration Strategy covering the identification, assessment and treatment of new or existing vulnerabilities (in accordance with risk management policy) during the life-cycle of the ICS<br>▪ Policies governing the roles, responsibilities and activities authorized for third parties interfacing with ICS components<br>▪ Policies and the necessary procedures to ensure adherence to identified compliance regulations (e.g. System Audits, Privacy Act, etc) |

## 2.4 Features Outside of Scope

Features outside the scope of the defined STOE:

- General physical protection outside the scope of the ICS
- Enterprise intranet protection
- Protection of "business" information and systems other than that generated by the ICS while it resides within the ICS.
- Primary power sources (e.g. mains generated supply)
- General corporate-level security policies, procedures and training (the STOE will only address ICS specific policies, procedures and training)


© Copyright 2004 National Institute of Standards & Technology

# 3 STOE Security Environment

In order to clarify the nature of the security problem that the STOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the STOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the STOE or its environment is required.
- Any organizational security policy statements or rules with which the STOE must comply.

## 3.1 Secure Usage Assumptions

The following assumptions relate to the operation of the TOE:

**Table 3 – Secure Usage Assumptions**

| Name | Description |
|---|---|
| **A.PHYSICAL_ACCESS** | In accordance with organizational policy physical access controls are applied at designated physical access points throughout the system whose perimeters are defined by the organization, and personnel with authorized access is documented and maintained. Entry to secure areas is controlled and monitored on a periodic basis. |
| **A.COMMS_ACCESS** | In accordance with organizational policy, physical access to communication media, and connections to the media, and services allowed to go over the communications media (e.g., internet access, e-mail) is controlled, as is access to devices that display or output system control information. |
| **A.EXTERNAL** | The ICS network may have connectivity with non-ICS system networks through which Internet connectivity is possible. |
| **A.REMOTE** | Remote access to ICS components may be available to authorized individuals. |

## 3.2 Threats to Security

Threats may be addressed either by the STOE or by its intended environment (for example, using personnel, physical, or administrative safeguards not provided by the STOE). These two classes of threats are discussed separately.

Threats are characterized in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threats agents are described as a combination of expertise, available resources, and


© Copyright 2004 National Institute of Standards & Technology

motivation. Attacks are described as a combination of attack methods, any vulnerabilities exploited, and opportunity.

### 3.2.1 Threats Addressed by the STOE

The following sections document the threat agents, attacks and assets relevant to the STOE. The last section combines all three aspects into a list of threats to be countered by the STOE.

#### 3.2.1.1 Threat Agents

Threats agents are characterized through a combination of expertise, available resources, and motivation. The threat agents relevant to the STOE have been captured below in Table 4.

**Table 4 – Threat Agents for the STOE**

| Threat Agent Label | Description[1] | | | |
|---|---|---|---|---|
| | Threat Agent | Expertise | Resources | Motivation |
| **AGENT.INSIDER** | Trusted employee, contractor, vendor or customer | Low/High | Substantial | Non-malicious |
| **AGENT.EVIL_INSIDER** | Trusted employee, contractor, vendor or customer acting inappropriately | Low/High | Substantial | Malicious |
| **AGENT.PRIOR_INSIDER** | Former trusted employee, contractor, vendor or customer | Low/High | Moderate | Malicious |
| **AGENT.OUTSIDER** | Unauthorized external party | High | Minimal/ Moderate | Malicious |
| **AGENT.NATURE** | Environmental sources of threats such as earthquakes, flood and fire | N/A | Substantial | N/A |

Evil insiders include those legitimate users on the internal ICS network who misuse privileges or impersonate higher-privileged users.

[1] The descriptions for expertise, resources and motivation correspond to those defined for "capability of the attacker", "resources of the attacker", and "intent of the attacker" from Appendix E of NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems.


© Copyright 2004 National Institute of Standards & Technology

Outsiders include those intruders gaining access to the ICS from the Internet, dialup lines, physical break-ins, or from partner (supplier or customer) networks linked to the corporate network.

#### 3.2.1.2 Attacks

Attacks are described as a combination of attack methods, any vulnerabilities exploited, and opportunity.

##### *3.2.1.2.1 Sources of Vulnerability*

The sources of vulnerability applicable to the STOE have been captured below. Please note that these sources of vulnerability should be further refined by the SST author to identify specific vulnerabilities applicable to the their own instantiation of the STOE.

*Editor's note: The table below refers to sources or categories of vulnerabilities applicable to an ICS. It is envisaged that the categories of vulnerabilities listed below will be refined by the SST author as each STOE will have vulnerabilities specific to their own security environment in which the ICS is deployed.*

**Table 5 – Sources of Vulnerabilities of the STOE**

| Vulnerability Label | Vulnerability | Description |
|---|---|---|
| **V.PLAINTEXT** | Use of clear text protocols | The use of clear text protocols and the transmission of business and control data unencrypted over insecure communication channels (e.g. FTP, TELNET). |
| **V.SERVICES** | Unnecessary services enabled on system components | The presence of unnecessary system services on key ICS components and subsystems that may be exploited to negatively impact on system security (e.g. sendmail, finger services). |
| **V.REMOTE** | Remote access vulnerabilities | Uncontrolled external access to the corporate network (e.g. through the Internet) allowing unauthorized entry to the interconnected ICS network. Also includes vulnerabilities introduced through poor VPN configuration, exposed wireless access points, uncontrolled modem access (e.g. through networked faxes) and weak remote user authentication techniques. |
| **V.ARCHITECTURE** | Poor system architecture design leading to weaknesses in system security posture | Business and operational requirements impacting on the effectiveness of deployed or planned security measures to protect the confidentiality, integrity and availability of the ICS and its components. Poor security architecture may also lead to the bypass and tamper of ICS security functions. |


© Copyright 2004 National Institute of Standards & Technology

| Vulnerability Label | Vulnerability | Description |
|---|---|---|
| **V.DEVELOPMENT** | Poor system development practices leading to weakness in system implementation | Lack of quality processes (e.g. configuration management, quality testing) leading to errors in system implementation and third party products such as buffer overflows and errors in control algorithms. |
| **V.NOPOLICIES** | Inadequate system security policies, plans and procedures | Lack of formal system policies, plans and procedures (e.g. weak password policies, no incident response plans, irregular compliance audits, poor configuration management policies and procedures, poor system auditing practices, backup procedures etc). |
| **V.SPOF** | Single Points of Failure | Poor security architecture design leading to one or more single points of failure in the ICS and resulting in system unavailability. |
| **V.NOTRAINING** | Inadequate user training | Inadequate training on system security issues leading to poor user security awareness. |
| **V.3RDPARTY** | Unauthorized access to ICS via 3rd party network | Unauthorized user access to the ICS or its components via a 3rd party network connection. |
| **V.NORISK** | Lack of risk assessment | Inadequate risk assessment activities performed on critical assets leading to a poor understanding of the security posture of the ICS and the security controls needed to counter security risks to the organization. |

### *3.2.1.2.2 Attack Descriptions*

The generic types of attack relevant to the STOE have been captured below. Please note that the referenced vulnerabilities have been defined in the previous section.

**Table 6 – Attack Methods against the STOE**

| Attack Label | Description | | | |
|---|---|---|---|---|
| | Attack | Method | Vulnerabilities | Opportunity[2] |

[2] The description for opportunity relates to whether the attack can be conducted within the ICS network (locally) or outside the protected boundary of the ICS network (remotely).


© Copyright 2004 National Institute of Standards & Technology

| Attack Label | Description | | | |
|---|---|---|---|---|
| | Attack | Method | Vulnerabilities | Opportunity[2] |
| **ATTACK.SNIFF** | Unauthorized traffic analysis | Packet capture tool, keystroke logger etc | V.PLAINTEXT, V.ARCHITECTURE, V.REMOTE, V.3RDPARTY, V.NORISK | Locally & Remotely |
| **ATTACK.REPLAY** | Unauthorized replay of captured traffic | Packet capture tool, keystroke logger etc | V.PLAINTEXT, V.ARCHITECTURE, V.REMOTE, V.3RDPARTY, V.NORISK | Locally & Remotely |
| **ATTACK.SPOOF** | Impersonating an authorized user | Exploitation of weak user authentication mechanism | V.PLAINTEXT, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.3RDPARTY, V.NORISK | Locally & Remotely |
| **ATTACK.DOS** | Overloading the network | Distributed denial of service attack from the Internet causing system downtime | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.3RDPARTY, V.NORISK | Remotely |
| **ATTACK.ERROR** | Operator error | ICS system operator error causing security breach | V.SERVICES, V.NOPOLICIES, V.NOTRAINING, V.NORISK | Locally |
| **ATTACK.SOCIAL** | Social engineering of authorized users | Unsolicited contact with employee with the intent of discovering user credentials or acquiring sensitive information | V.NOPOLICIES, V.NOTRAINING, V.NORISK | Locally & Remotely |
| **ATTACK.VIRUS** | Virus infection of ICS system components | Virus propagation via email system or Internet downloaded content (e.g. Trojan) | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY, V.NORISK | Locally |


© Copyright 2004 National Institute of Standards & Technology

| Attack Label | Description | | | |
|---|---|---|---|---|
| | Attack | Method | Vulnerabilities | Opportunity[2] |
| **ATTACK.DESTROY** | Destruction of ICS control data, business data or configuration information | File deletion on compromised ICS file servers | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK | Locally & Remotely |
| **ATTACK.MODIFY** | Modification of ICS control data, business data or configuration information | File modification on compromised ICS file servers | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK | Locally & Remotely |
| **ATTACK.BYPASS** | Bypass of system security functions and mechanisms | Modification of ICS configurations of components | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NORISK | Locally & Remotely |
| **ATTACK.PHYSICAL** | Compromise of poorly implemented and/or controlled physical security mechanisms | Unauthorized access to physically secured areas housing system assets (e.g. perimeter security breach) | V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK | Locally |
| **ATTACK.NATURE** | Acts of nature causing system unavailability | Environmental occurrences such as earthquake, flood and fire | V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING V.SPOF, V.NORISK | Locally |

#### 3.2.1.3 Assets

Assets protected by the STOE include the following:

**Table 7 – Assets protected by the STOE**

| Asset Label | Asset | Description |
|---|---|---|
| **ASSET.ACTUATOR** | Actuator | One or more devices that receive the controlled variables from the controller and feeds them into the controlled process for action. |


© Copyright 2004 National Institute of Standards & Technology

| Asset Label | Asset | Description |
|---|---|---|
| **ASSET.SENSOR** | Sensor | One or more devices that sense or detect the value of a process variable and generates a signal related to the value (includes the sensing and transmitting parts of the device). |
| **ASSET.CONTROLLER** | Controller | The computer system or components that processes sensor input, executes control algorithms and computes actuator outputs (e.g. Programmable Logic Controllers). |
| **ASSET.HMI** | HMI | The hardware or software through which an operator interacts with a controller, providing a user with a view into the manufacturing process for monitoring or controlling the process. |
| **ASSET.REMOTE** | Remote Diagnostics & Maintenance | The hardware and software devices responsible for diagnostic and maintenance activities performed on the ICS from remote locations (e.g. Remote Terminal Units, pcAnywhere). May also include the communications mechanism or protocol used to access to the ICS (e.g. VPN). |
| **ASSET.COMMS** | Communications Infrastructure | The communications infrastructure used to bridge the control loop within an ICS. Also includes the network protocols and control equipment used to integrate ICS components and subsystems (e.g. Ethernet, wireless, RS-232 etc). |
| **ASSET.CTRLPROCESS** | Controlled Process | The process subject to analysis and control by the ICS (including the inputs and outputs to the process). |
| **ASSET.CTRLINFO** | Process Control Information | The process control information being collected by, processed by, stored on and transmitted to or from the components that constitute the process control network |
| **ASSET.BUSINFO** | Process Control Business Information | The process control business or financial information being created by, processed by, stored on and transmitted to or from the components that constitute the process control network. |


© Copyright 2004 National Institute of Standards & Technology

#### 3.2.1.4 Threat Description

Using the description of the threat agents, attacks and assets captured in the previous sections, each of the threats relevant to the STOE have been characterized below:

**Table 8 – Threats countered by the STOE**

| Threat Label | Threat | Description |
|---|---|---|
| **T.DISCLOSURE** | Unauthorized Information Disclosure | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SOCIAL) to acquire sensitive information (ASSET.COMMS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components. |
| **T.EVIL_ANALYSIS** | Unauthorized Analysis | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SOCIAL) to analyze sensitive information flows (ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) protected by the STOE. |
| **T.EVIL_MODIFICATION** | Unauthorized Modification | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.MODIFY, ATTACK.BYPASS, ATTACK.SNIFF) to modify sensitive information (ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components. |
| **T.EVIL_DESTRUCTION** | Unauthorized Destruction | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.DESTROY, ATTACK.BYPASS) to destroy sensitive information (ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components. |
| **T.CTRL_TAMPER** | Tampering with control components | The tampering of ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) by malicious individuals (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) via the following attacks (ATTACK.MODIFY, ATTACK.BYPASS, ATTACK.PHYSICAL). |
| **T.BAD_COMMAND** | Integrity of Control Commands | An authorized operator (AGENT.INSIDER) accidentally issues bad commands (ATTACK.ERROR) resulting in the modification of controlled ICS processes and components (ASSET.CTRLPROCESS, ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI). |
| **T.SPOOF** | Spoofing legitimate users of the STOE | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SPOOF, ATTACK.SOCIAL) to obtain user credentials (ASSET.REMOTE, ASSET.COMMS) stored on ICS server components to impersonate authorized users. |


© Copyright 2004 National Institute of Standards & Technology

| Threat Label | Threat | Description |
|---|---|---|
| **T.REPUDIATE** | Identity repudiation | An authorized user (AGENT.INSIDER) denies having performed an action (ATTACK.ERROR) on the ICS interactive systems (ASSET.REMOTE, ASSET.COMMS, ASSET.HMI). |
| **T.DOS** | Denial of Service | An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.DESTROY, ATTACK.DOS) that denies service to valid users by making ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) temporarily unavailable or unusable. |
| **T.PRIVILEGE** | Elevation of privilege | An unprivileged individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.ERROR, ATTACK.SNIFF, ATTACK.SPOOF, ATTACK.SOCIAL) to obtain user credentials (ASSET.REMOTE, ASSET.COMMS) stored on ICS server components to elevate privileged access to ICS components for malicious purposes. |
| **T.NO_FAULT_RECORD** | Fault Detection | Faults generated by the system (AGENT.INSIDER) as a consequence of operator error and/or security breach (ATTACK.ERROR) while performing their routine tasks are not detected nor audited on ICS interactive systems (ASSET.REMOTE, ASSET.COMMS, ASSET.HMI) for further analysis and correction. |
| **T.DISASTER** | System Unavailability due to Natural Disaster | A natural disaster (AGENT.NATURE) ceases operation of one or more components of the ICS (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) as a consequence of earthquake, fire, flood or other unpredictable event (ATTACK.NATURE). |
| **T.OUTAGE** | System Unavailability due to Power Outage | A natural disaster, malicious or non-malicious individual (AGENT.NATURE, AGENT.INSIDER, AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) inadvertently (or otherwise) causes a power outage affecting the availability of one or more components of the ICS (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS). |
| **T.INFECTION** | Virus Infection | An individual (AGENT.INSIDER, AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) maliciously or accidentally introduces a virus to the ICS network (ATTACK.VIRUS) causing unnecessary system downtime and corruption of data (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO). |


© Copyright 2004 National Institute of Standards & Technology

| Threat Label | Threat | Description |
|---|---|---|
| **T.PHYSICAL_ACCESS** | Unauthorized physical access | An unauthorized individual (AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.PHYSICAL) to gain physical access to protected ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS). |

### 3.2.2 Threats Addressed by the Operating Environment

This SPP has not identified any threats relevant to the operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to address the threats relevant to the STOE operating environment.

## 3.3 Overarching Organizational Security Policies

This section describes the Overarching Organizational Security Policies (OOSPs) that define the broader context of the organization which support and govern the use of a system. These will form part of the basis for deriving the actual organizational security policies (OSPs) to be included as part of a specific STOE.

The scope of organizational security policy includes both the organizational security policies of the organization that has responsibility for operating the industrial control system as well as those for any external organizations that the industrial control system interacts with. Security related organizational policies include the following:

**Table 9 – Organizational Security Policies**

| Name | Description |
|---|---|
| **P.EVENT** | The organization shall monitor security events to ensure compliance with security policies (e.g. security incident response plan). |
| **P.PERSONNEL** | The organization shall have in place policies, training programs, and reporting and enforcement mechanisms such that personnel know their security role in the organization. |
| **P.INFRASTRUCTURE** | The organization shall provide an organizational structure to establish the implementation of the security program, in which the policies can be established, maintained and enforced throughout the organization. |
| **P.CONFIGURATION** | The organization shall provide management and operational security controls necessary to manage the system's configuration during operations and evaluate and control changes to ensure that the system remains secure. |


© Copyright 2004 National Institute of Standards & Technology

| Name | Description |
|---|---|
| **P.PHYSICAL** | Adequate physical security shall be provided to detect or prevent unauthorized access or connection to the system and its components. |
| **P.POLICY** | The organization and system shall comply with organizational and regulatory policies and controls governing the use of, and implemented by the system to ensure secure operations. |
| **P.ASSETS** | The organization shall provide documentation of the system and its components, to understand the overall security posture. |
| **P.SAFETY** | The organization shall comply with relevant standards to ensure the safety of the system and its operators. |
| **P.NO_INTERFERE** | ICS security controls shall be implemented so as not to impede the minimum required operational capabilities of the ICS, and so as to not impede the safety systems that protect the ICS. |
| **P.BUSINESS** | The ICS shall be operated in accordance with a business continuity policy that addresses the identification of and response to events that adversely affect the ability of the ICS to operate in fulfilling its design goals (e.g. power outages, acts of nature etc). |
| **P.RISK** | The ICS shall be designed, implemented, and operated to meet the risk objectives resulting from a system life-cycle risk management program. The risk management program shall establish a comprehensive and integrated set of risk management goals for issues affecting ICS operation, safety and security. |
| **P.ENVIRONMENT** | The STOE operating environment shall have adequate security controls to counter those threats originating from outside of the defined STOE. The implementation and maintenance of these security controls should be in accordance with organizational security policies similar to those listed in this table and be selected based on the outcomes of a risk assessment. |


© Copyright 2004 National Institute of Standards & Technology

# 4 Risks

The security risks are a further instantiation of the security problem. The element of risk is captured by the SPP to determine the relative importance of the security needs of the STOE and its operating environment. They guide the specification of the security objectives by ensuring that only those security needs seen as critical to the organization are addressed by the STOE or its operating environment.

Each risk is a product of asset value, assessed level of relevant threats, and associated vulnerabilities (as identified in the previous section). It represents the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organization.

Please note that this SPP has not specified the level of risk. Rather, it is intended that the SST author evaluate and prioritize the level of each risk according to their own ICS implementation (based on the combination of the value of each asset to the organization, the impact and probability rating of each threat successfully exploiting the identified vulnerabilities, and the effectiveness of existing security controls). Further guidance on the completion and relevance of this section can be found in chapter 7.

## 4.1 Risk Categories applicable to the STOE

The categories of security risks relevant to the STOE are described in Table 10. The table references the threats, vulnerabilities and assets identified in the previous chapter.

*Editor's Note: At this level of abstraction the SPP has only captured the categories of risk applicable to the generic ICS described by this SPP. It is anticipated that future SPPs and SSTs will identify specific risks relevant to the author's own organizational context, and therefore expand upon the generic risks presented in this chapter.*

**Table 10 – Identified Risk Categories for the STOE**

| Risk Category Label | Risk Category Description | Threats | Vulnerabilities | Assets |
|---|---|---|---|---|
| **RISK.MANAGE** | Risks associated with the security roles and responsibilities applicable to all ICS users, as well as risks associated with the successful implementation of the organizational security policies. | T.BAD_COMMAND,<br>T.REPUDIATE,<br>T.PRIVILEGE,<br>T.NO_FAULT_RECORD, | V.PLAINTEXT,<br>V.SERVICES,<br>V.REMOTE,<br>V.ARCHITECTURE<br>V.NOPOLICIES,<br>V.NOTRAINING,<br>V.3RDPARTY<br>V.NORISK | ASSET.ACTUATOR,<br>ASSET.SENSOR,<br>ASSET.CONTROLLER,<br>ASSET.HMI,<br>ASSET.REMOTE,<br>ASSET.COMMS,<br>ASSET.CTRLPROCESS |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Risk Category Description | Threats | Vulnerabilities | Assets |
|---|---|---|---|---|
| **RISK.SECPOLICY** | Risks associated with the development, endorsement and maintenance of the instruction stipulated by the corporate security policies. | T.BAD_COMMAND, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.RISKMAN** | Risks associated with the management of the risk assessment processes for the ICS. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.COMPLY** | Risks associated with not meeting internal and statutory requirements. | TBD | V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.ASSETCTRL** | Risks associated with asset classification, labelling, media management and accountability. | T.REPUDIATE, T.PRIVILEGE, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Risk Category Description | Threats | Vulnerabilities | Assets |
|---|---|---|---|---|
| **RISK.PERSONNEL** | Risks associated with personnel vetting, security awareness, training, separation of duties and system usage agreements. | T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.PHYSICAL** | Risks associated with unauthorized physical access and/or damage to system components. | T.PHYSICAL_ACCESS | V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS |
| **RISK.ENVIRON** | Risks associated with the effects of natural disasters, such as fire, flood and earthquake. | T.DISASTER | V.ARCHITECTURE V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.EVIL_ACCESS** | Risks associated with the illicit use, modification and destruction of company data or inappropriate access to information.<br>Risks associated with the inability to make individuals accountable for the actions they take when using the systems. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.NEED2KNOW** | Risks associated with the threat to information confidentiality and privacy, unauthorised disclosure and clear desk practices. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.SPOOF, T.PRIVILEGE | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Risk Category Description | Threats | Vulnerabilities | Assets |
|---|---|---|---|---|
| **RISK.INTEGRATE** | Risks associated with the integration of security requirements into the systems development cycle and the selection of third party products. | TBD | V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.NETCOMMS** | Risks associated with the protection of network communications at the logical and physical layers. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.NO_FAULT_RECORD, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.CONNECT** | Risks associated with connections to other IT systems. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.INTERNET** | Risks associated with the use of the Internet and email services both internal and external to the ICS. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.REMOTE** | Risks associated with the connection of remote users to the ICS network. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Risk Category Description | Threats | Vulnerabilities | Assets |
|---|---|---|---|---|
| **RISK.ONLINE** | Risks associated with the delivery of online services, including statutory requirements, security issues and controls, publishing and third-party security. | T.DISCLOSURE, T.DOS, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.OPSMANAGE** | Risks associated with managing system changes, such as changes not approved or audited correctly, lack of consultation with relevant parties, loss of skilled people, and lack of correct documentation.<br>Risks associated with the use of technology for data and system control, including data protection, backup, disaster recovery, inadequate security, and insufficient capacity, etc. | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.IDS** | Risks associated with security auditing, security breach detection and response, incident reporting and forensic evidence requirements. | T.BAD_COMMAND, T.REPUDIATE, T.NO_FAULT_RECORD, | V.SERVICES, V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS |
| **RISK.CONTINUITY** | Risks associated with ensuring the uninterrupted availability of all key business resources required to support essential (or critical) business activities. | T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.DOS, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

## 4.2 Risks to the External Operating Environment

This SPP has not identified any risks relevant to the external operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to mitigate the risks to the STOE external operating environment.


© Copyright 2004 National Institute of Standards & Technology

# 5 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the SPP, is to be addressed. Just as some threats are to be addressed by the STOE and others by its intended environment, some security objectives are for the STOE and others are for its environment. These two classes of security objectives are discussed separately.

## 5.1 Security Objectives for the STOE

The security objectives for the STOE are as described in the following table.

**Table 11 – Security Objectives for the STOE**

| Objective Label | Objective Description |
|---|---|
| **O.PHYSICAL** | The STOE must provide protection at the physical boundaries of the ICS to prevent access to the protected assets by unauthorized users. |
| **O.RISK** | ICS risk assessment shall be conducted throughout the life-cycle of an ICS, such that a documented and approved risk assessment process is conducted initially, and reviewed with each change to the manufacturing process or change to the ICS; and to ensure that changing vulnerabilities do not degrade the security of the ICS. |
| **O.NON_INTERFERENCE** | The ICS security functions shall be implemented in a non-interfering manner such behavior of the ICS functions and safety functions are able to meet their performance constraints. |
| **O.INTERCONNECTIVITY** | ICS security functions shall include the capability to secure interfaces and interconnectivity of ICS related safety systems, as required. |
| **O.DATA_BACKUP** | The STOE must include provisions for ICS data and control information (including executable software and control data) to assure the ability for timely recovery to an operating state if the ICS is compromised or damaged. The data backup procedures should follow industry best practices including (but not limited to) secondary storage locations, testing of recovery procedures, and a back up interval either driven by configuration changes or a specified time interval or a combination of both. |
| **O.DATA_AUTHENTICATION** | The STOE shall authenticate configuration change commands such that configuration (control algorithms, set points, limit points, etc.) cannot be changed unless the origin of the command can be positively established.<br><br>The STOE shall authenticate financial or other business critical information sent from the STOE to external systems. |


© Copyright 2004 National Institute of Standards & Technology

| Objective Label | Objective Description |
|---|---|
| | |
| **O.CONTINUITY** | The ICS shall ensure continuity of operations in accordance with a business continuity policy that addresses a known set of anticipated events that might adversely affect the operational capability of the ICS. |
| **O.MANAGEMENT** | A policy for governing security shall be defined to establish the following:<br>▪ An organization-wide, security management infrastructure<br>▪ Identified roles and responsibilities, together with explicit authority to ensure operational security within the management infrastructure |
| **O.MIGRATION** | The ICS shall have a migration strategy providing the capability to govern the evolution of the control system throughout its security operational life cycle. The migration strategy shall address at a minimum:<br>Assessment of new vulnerabilities and appropriate/necessary mitigating actions to control/reduce new vulnerabilities. This may include maintenance of the current system state (components, configuration, patches, etc).<br>The integration between computer implemented and personnel implemented procedures. |
| **O.COMPLIANCE** | The ICS shall be operated in compliance with relevant governing mandates. |
| **O.3RDPARTY** | Policies governing the roles, responsibilities and activities authorized for individuals not employed by the control system operating organization shall be developed. |
| **O.REMOTE** | The policies shall establish methods for on-site internal, on-site remote, and off-site remote access to control system resources. |


© Copyright 2004 National Institute of Standards & Technology

| Objective Label | Objective Description |
|---|---|
| **O.ACCESS_CONTROL** | The ICS shall provide the capability to grant or deny access to control system resources based upon the action being performed, and the authorizations associated with authorized subjects.<br><br>The ICS shall deny unauthorized agents access to every control system resource.<br><br>The ICS shall require that each agent authorized to use the control system is identified and is provided with credentials to authenticate their identity.<br><br>The ICS must be able to include knowledge of the control system state and/or the controlled process state when making an access control decision.<br><br>The ICS shall include knowledge of time and location in the rules for making an access control decision. |
| **O.SECURE_COMMS** | The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational communications capability.<br><br>The ICS shall provide the capability to allow information flows only between those endpoints authorized by the system. |
| **O.DATA_INTEGRITY** | The ICS shall provide the capability to protect information flows from replay, substitution or modification.<br><br>The ICS shall provide the capability to allow the recipient of an authorized information flow to verify the correctness of the received information. |
| **O.CONFIDENTIALITY** | The ICS shall protect the confidentiality of information determined by the respective owners as requiring protection, including, but not limited to, information related to business, financial and control data. |
| **O.AVAILABILITY** | The ICS shall have continuity of availability for operational capability.<br><br>The ICS shall be capable of continuing operation if a control server is unavailable for any reason.<br><br>The ICS shall be capable of continuing operation if the primary communications channel is unavailable for any reason. |


© Copyright 2004 National Institute of Standards & Technology

| Objective Label | Objective Description |
|---|---|
| **O.SYSTEM_INTEGRITY** | The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational system configuration and capability.<br>The ICS shall provide the capability to restrict access to the functions used to establish and maintain the secure operational configuration of the ICS. |
| **O.SYSTEM_DIAGNOSTICS** | The ICS shall be capable of performing self-tests to verify the configuration and integrity of the security functions of the ICS.<br>The ICS shall provide the capability for self-test to be executed on start-up, at periodic intervals, and on demand. |
| **O.MONITORING** | The ICS shall be capable of detecting unauthorized activity, unusual activity and attempts to defeat the security capabilities of the ICS. |
| **O.AUDIT** | The ICS shall provide the capability to record and maintain event traces that reflect the successful and unsuccessful security relevant activities involving ICS resources. |
| **O.IDS** | The ICS shall be capable of detecting unauthorized activity, unusual activity and attempts to defeat the security capabilities of the ICS.<br>The control system shall be capable of initiating action in response to the detection of a potential violation of the ICS security policy. |

## 5.2 Security Objectives for the External Operating Environment

This SPP has not identified any security objectives relevant to the external operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to address the security needs outside the scope of the STOE.


© Copyright 2004 National Institute of Standards & Technology

# 6 IT Security Requirements

## 6.1 STOE Security Functional Requirements

This section contains the functional requirements for the STOE. This includes system security functional requirements and system security assurance requirements. The requirements are primarily stated as logical requirements and cover information technology related requirements, requirements for system security policies and system security related operating procedures, and integration requirements addressing interfaces and interoperability between security system components. The functional requirements are listed in summary form in the table below.

*Editor's Note: Table 12 and the text below it outline extensions to the functional requirements that is building on ISO system work in concert with NIST work building on security controls.*

**Table 12 – STOE Security Functional Requirements**

| No. | Component | Component Name |
|---|---|---|
| **Class FAU: Audit** | | |
| 1 | FAU_ARP.1 | Security alarms |
| 2 | FAU_GEN.1 | Audit data generation |
| 3 | FAU_GEN.2 | User identity association |
| 4 | FAU_SAA.1 | Potential violation analysis |
| 5 | FAU_SAA.2 | Profile based anomaly detection |
| 6 | FAU_SAA.3 | Simple attack heuristics |
| 7 | FAU_SAA.4 | Complex attack heuristics |
| 8 | FAU_SAR.1 | Audit review |
| 9 | FAU_SAR.2 | Restricted audit review |
| 10 | FAU_SAR.3 | Selectable audit review |
| 11 | FAU_STG.1 | Protected audit trail storage |
| 12 | FAU_STG.2 | Guarantees of audit data availability |
| 13 | FAU_STG.3 | Action in case of possible audit data loss |
| 14 | FAU_STG.4 | Prevention of audit data loss |
| 15 | FAU_SEL.1 | Selective audit |
| **Class FCS: Cryptographic support** | | |


© Copyright 2004 National Institute of Standards & Technology

| No. | Component | Component Name |
|---|---|---|
| 16 | FCS_CKM.4 | Cryptographic key management |
| 17 | FCS_COP.1 | Cryptographic operation |
| **Class FDP: User data protection** | | |
| 18 | FDP_ACC.1 | Subset access control |
| 19 | FDP_ACC.2 | Complete access control |
| 20 | FDP_ACF.1 | Security attribute based access control |
| 21 | FDP_DAU.2 | Data authentication |
| 22 | FDP_IFC.1 | Subset information flow control |
| 23 | FDP_IFC.2 | Complete information flow control |
| 24 | FDP_IFF.1 | Simple security attributes |
| 25 | FDP_UCT.1 | Basic data exchange confidentiality |
| 26 | FDP_UIT.1 | Data exchange integrity |
| 27 | FDP_UIT.2 | Source data exchange recovery |
| **Class FEM Event Monitoring** | | |
| 28 | FEM_EDI.1 | Event Definition and Identification |
| 29 | FEM_EDI.2 | Interaction of System Event Monitoring Components |
| 30 | FDM_EDI.3 | Alarm Audit Requirements |
| 31 | FEM_EDI.4 | Alarm Respoonse |
| **Class FIA: Identification & Authentication** | | |
| 32 | FIA_AFL.1 | Authentication failure handling |
| 33 | FIA_ATD.1 | User attribute definition |
| 34 | FIA_SOS.1 | Verification of passwords |
| 35 | FIA_SOS.2 | TSF generation of passwords |
| 36 | FIA_UAU.1 | Timing of authentication |
| 37 | FIA_UAU.2 | User authentication before any action |
| 38 | FIA_UAU.3 | Unforgeable authentication |
| 39 | FIA_UAU.4 | Single use authentication mechanisms |
| 40 | FIA_UAU.7 | Protected authentication feedback |
| 41 | FIA_UID.1 | Timing of identification |
| 42 | FIA_UID.2 | User identification before any action |


© Copyright 2004 National Institute of Standards & Technology

| No. | Component | Component Name |
|---|---|---|
| **Class FMT: Management of functions in TSF** | | |
| 43 | FMT_MOF.1 | Management of security functions behavior |
| 44 | FMT_MOF.2 | Security function and security policy mapping |
| 45 | FMT_MSA.1 | Management of security attributes |
| 46 | FMT_MTD.1 | Management of TSF data |
| 47 | FMT_MTD.4` | Management of TSF data to policy mapping |
| 48 | FMT_REV.1 | Revocation |
| 49 | FMT_SAE.1 | Time limited authorization |
| 50 | FMT_SMF.1 | Security management functions |
| 51 | FMT_SMR.1 | Security roles |
| 52 | FMT_SMR.2 | Restrictions on security roles |
| 53 | FMT_SMR.4 | Security role to policy mapping |
| **Class FEM: Security event monitoring** | | |
| 54 | FEM_EDI.1 | Event definition and identification |
| 55 | FEM_EDI.2 | Interaction of system event monitoring components |
| 56 | FEM_EDI.3 | Alarm audit requirements |
| 57 | FEM_EDI.4 | Alarm response |
| **Class FPT: Protection of the TSF** | | |
| 58 | FPT_AMT.1 | Abstract machine testing |
| 59 | FPT_FLS.1 | Failure with preservation of secure state |
| 60 | FPT_ITA.1 | Inter-TSF availability within a defined availability metric |
| 61 | FPT_ITC.1 | Inter-TSF confidentiality during transmission |
| 62 | FPT_ITI.1 | Inter-TSF detection of modification |
| 63 | FPT_ITI.2 | Inter-TSF detection and correction of modification |
| 64 | FPT_PHP.1 | Passive detection of physical attack |
| 65 | FPT_PHP.2 | Notification of physical attack |
| 66 | FPT_PHP.3 | Resistance to physical attack |
| 67 | FPT_PHP.4 | Domain definition and alarm response |
| 68 | FPT_RCV.2 | Automated recovery |
| 69 | FPT_RCV.3 | Automated recovery without undue loss |


© Copyright 2004 National Institute of Standards & Technology

| No. | Component | Component Name |
|---|---|---|
| 70 | FPT_RCV.4 | Function recovery |
| 71 | FPT_RCV.5 | Continuous degraded operations |
| 72 | FPT_RPL.1 | Replay detection |
| 73 | FPT_SEP.1 | TSF domain separation |
| 74 | FPT_SSP.1 | Simple trusted acknowledgement |
| 75 | FPT_SSP.2 | Mutual trusted acknowledgement |
| 76 | FPT_STM.1 | Reliable time stamps |
| 77 | FPT_TDC.1 | Inter-TSF data consistency |
| 78 | FPT_TRC.1 | Internal TSF consistency |
| 79 | FPT_TST.1 | TSF testing |
| **Class FCM: Protection of System Configuration** | | |
| 80 | FCM_IDI.1 | Identification information |
| 81 | FCM_IDI.2 | Change requests and actions |
| 82 | FCM_IDI.3 | Authorizations |
| **Class FRU: Resource utilization** | | |
| 83 | FRU_FLT.1 | Degraded fault tolerance |
| 84 | FRU_PRS.1 | Limited priority of service |
| 85 | FRU_PRS.2 | Full priority of service |
| **Class FTP: Trusted path/channels** | | |
| 86 | FTP_ITC.1 | Inter-TSF trusted channel |
| 87 | FTP_TRP.1 | Trusted path |

The following sections contain the functional components from the Common Criteria Part 2 [CC2] (CC) with the operations completed. The standard CC text is in regular font; the text inserted by the System Protection Profile (SPP) author is in accordance with the conventions described in at the beginning of this document.

### 6.1.1 Logon Controls:

#### FIA_UID.1 Timing of identification


© Copyright 2004 National Institute of Standards & Technology

Hierarchical to: No other components.

**FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.**

**FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**
Dependencies: No dependencies

### FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.

**FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.**

**FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**
Dependencies: **FIA_UID.1 Timing of identification**

### FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1

**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.
Dependencies: **FIA_UID.1 Timing of identification**

### FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.

**FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].**

**FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].**
Dependencies: **FIA_UAU.1 Timing of authentication**

### FTP_TRP.1 Trusted path
Hierarchical to: No other components.
**FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.**


© Copyright 2004 National Institute of Standards & Technology

**FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.**

**FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*].**
Dependencies: No dependencies

**FTA_TSE.1 TOE session establishment**
Hierarchical to: No other components.

**FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attributes*].**
Dependencies: No dependencies

### 6.1.2 Password Selection

**FIA_SOS.1 Verification of *passwords***
Hierarchical to: No other components.
**FIA_SOS.1.1 The TSF shall provide a mechanism to verify that *passwords* meet [assignment: *a defined quality metric*].**
Dependencies: No dependencies

**FIA_SOS.2 TSF Generation of *passwords***
Hierarchical to: No other components.
**FIA_SOS.2.1 The TSF shall provide a mechanism to generate *passwords* that meet [assignment: *a defined quality metric*].**
**FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated *passwords* for [assignment: *list of TSF functions*].**
Dependencies: No dependencies

**FMT_SAE.1 Time-limited authorisation**
Hierarchical to: No other components.
**FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*].**
**FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.**
Dependencies: **FMT_SMR.1 Security roles**
**FPT_STM.1 Reliable time stamps**


© Copyright 2004 National Institute of Standards & Technology

### 6.1.3 Authentication Data Protection

**FIA_UAU.7 Protected authentication feedback**
Hierarchical to: No other components.
**FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.**
Dependencies: **FIA_UAU.1 Timing of authentication**
(For passwords)

**FMT_MTD.1Management of TSF data**
Hierarchical to: No other components.
**FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].**
Dependencies: **FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

**FPT_RPL.1 Replay detection**
Hierarchical to: No other components.
**FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: *list of identified entities*].**
**FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected.**
Dependencies: No dependencies

### 6.1.4 Replay / Reuse

**FIA_UAU.3 Unforgeable authentication**
Hierarchical to: No other components.
**FIA_UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.**
**FIA_UAU.3.2 The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.**
Dependencies: No dependencies
**FIA_UAU.4 Single-use authentication mechanisms**
Hierarchical to: No other components.
**FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(*s)].**
Dependencies: No dependencies
---These are targeted to preventing replay attacks from captured control signals---


© Copyright 2004 National Institute of Standards & Technology

### 6.1.5 Session Suspension

**FTA_SSL.1 TSF-initiated session locking**
Hierarchical to: No other components.
**FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:**
**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 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].**
Dependencies: **FIA_UAU.1 Timing of authentication**
**FTA_SSL.2 User-initiated locking**
Hierarchical to: No other components.
**FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session,**
**by:**
**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.2.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].**
Dependencies: **FIA_UAU.1 Timing of authentication**
**FTA_SSL.3 TSF-initiated termination**
Hierarchical to: No other components.
**FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].**
Dependencies: No dependencies

### 6.1.6 User Accounts and Profiles

**FMT_MTD.1Management of TSF data**
Hierarchical to: No other components.
**FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].**
Dependencies: **FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

(User accounts and User profiles)

**FIA_ATD.1 User attribute definition**


© Copyright 2004 National Institute of Standards & Technology

Hierarchical to: No other components.
**FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].**
Dependencies: No dependencies

(Definition of user security attributes contained in a user profile)

### 6.1.7 Role based access control

**FDP_ACC.1 Subset access control**
Hierarchical to: No other components.
**FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].**
Dependencies: **FDP_ACF.1 Security attribute based access control**

**FDP_ACC.2 Complete access control**
Hierarchical to: FDP_ACC.1
**FDP_ACC.2.1** The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] **and all operations among subjects and objects covered by the SFP.**
**FDP_ACC.2.2 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.**
Dependencies: FDP_ACF.1 Security attribute based access control

**FDP_ACF.1 Security attribute based access control**
Hierarchical to: No other components.
**FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].**
**FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].**
**FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].**
**FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**
Dependencies: **FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**


© Copyright 2004 National Institute of Standards & Technology

**FMT_SMR.1 Security roles**
Hierarchical to: No other components.
**FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorized identified roles*].**
**FMT_SMR.1.2 The TSF shall be able to associate users with roles.**
Dependencies: **FIA_UID.1 Timing of identification**

**FMT_SMR.2 Restrictions on security roles**
Hierarchical to: **FMT_SMR.1**
**FMT_SMR.2.1** The TSF shall maintain the roles: [assignment: *the authorized identified roles*].
**FMT_SMR.2.2** The TSF shall be able to associate users with roles.
**FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *a single user account is not assigned the two different roles associated with a two-man rule*] are satisfied.**
Dependencies: **FIA_UID.1 Timing of identification**

Application Note: FDP_ACF.1 may be used to specify that particular operations require two distinct roles to authorize the action. FMT_SMR.2.3 can ensure that a user account cannot be assigned to both roles (as used above). If there is more than one situation requiring implementation of a two-man rule the combination should be iterated for each set of roles.

### 6.1.8 Controls on RBAC Attributes

**FMT_MSA.1 Management of security attributes**
Hierarchical to: No other components.
**FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].**
Dependencies: **[FDP_ACC.1 Subset access control or**
**FDP_IFC.1 Subset information flow control]**
**FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

### 6.1.9 Firewall access control

**FDP_IFC.1 Subset information flow control**
Hierarchical to: No other components.


© Copyright 2004 National Institute of Standards & Technology

**FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].**
Dependencies: **FDP_IFF.1 Simple security attributes**

**FDP_IFC.2 Complete information flow control**
Hierarchical to: FDP_IFC.1
**FDP_IFC.2.1** The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects* and *information*] and **all operations that cause that information to flow to and from subjects covered by the SFP.**
**FDP_IFC.2.2 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.**
Dependencies: **FDP_IFF.1 Simple security attributes**

**FDP_IFF.1 Simple security attributes**
Hierarchical to: No other components.
**FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].**
**FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].**
**FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].**
**FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].**
**FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize information flows*].**
**FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].**
Dependencies: **FDP_IFC.1 Subset information flow control**
**FMT_MSA.3 Static attribute initialization**

### 6.1.10 Audit events

**FAU_GEN.1 Audit data generation**
Hierarchical to: No other components.
**FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:**


© Copyright 2004 National Institute of Standards & Technology

**a) Start-up and shutdown of the audit functions;**
**b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and**
**c) [assignment: *other specifically defined auditable events*].**
**FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:**
**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 PP/ST, [assignment: *other audit relevant information*]**
Dependencies: **FPT_STM.1 Reliable time stamps**

**FAU_GEN.2 User identity association**
Hierarchical to: No other components.
**FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.**
Dependencies: **FAU_GEN.1 Audit data generation**
**FIA_UID.1 Timing of identification**

**FMT_MTD.1Management of TSF data**
Hierarchical to: No other components.
**FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].**
Dependencies: **FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

**FAU_SEL.1 Selective audit**
Hierarchical to: No other components.
**FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:**
**a) [selection: *object identity, user identity, subject identity, host identity, event type*]**
**b) [assignment: *list of additional attributes that audit selectivity is based upon*].**
Dependencies: **FAU_GEN.1 Audit data generation**
**FMT_MTD.1 Management of TSF data**

### 6.1.11 Intrusion detection and response

**FAU_ARP.1 Security alarms**
Hierarchical to: No other components.


© Copyright 2004 National Institute of Standards & Technology

**FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.**
Dependencies: **FAU_SAA.1 Potential violation analysis**

### FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
**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.**
**FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:**
**a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;**
**b) [assignment: *any other rules*].**
Dependencies: **FAU_GEN.1 Audit data generation**

### FAU_SAA.2 Profile based anomaly detection

Hierarchical to: FAU_SAA.1
**FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group*].**
**FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.**
**FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].**
Dependencies: **FIA_UID.1 Timing of identification**

### FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1
**FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the TSP.**
**FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].**
**FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.**
Dependencies: No dependencies

### FAU_SAA.4 Complex attack heuristics


© Copyright 2004 National Institute of Standards & Technology

Hierarchical to: FAU_SAA.3
**FAU_SAA.4.1** The TSF shall be able to maintain an internal representation of the **following event sequences of known intrusion scenarios [assignment: *list of sequences of system events whose occurrence are representative of known penetration scenarios*] and** the following signature events [assignment: *a subset of system events*] that may indicate a potential violation of the TSP.

**FAU_SAA.4.2** The TSF shall be able to compare the signature events **and event sequences** against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].
**FAU_SAA.4.3** The TSF shall be able to indicate an imminent violation of the TSP when **system activity** is found to match a signature event **or event sequence** that indicates a potential violation of the TSP.
Dependencies: No dependencies

### 6.1.12 Audit trail protection

**FAU_STG.1 Protected audit trail storage**
Hierarchical to: No other components.
**FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.**
**FAU_STG.1.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.**
Dependencies: **FAU_GEN.1 Audit data generation**

**FAU_STG.2 Guarantees of audit data availability**
Hierarchical to: FAU_STG.1
**FAU_STG.2.1** The TSF shall protect the stored audit records from unauthorized deletion.
**FAU_STG.2.2** The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.
**FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*].**
Dependencies: FAU_GEN.1 Audit data generation

**FAU_STG.3 Action in case of possible audit data loss**
Hierarchical to: No other components.
**FAU_STG.3.1 The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].**
Dependencies: FAU_STG.1 Protected audit trail storage

**FAU_STG.4 Prevention of audit data loss**


© Copyright 2004 National Institute of Standards & Technology

Hierarchical to: FAU_STG.3
**FAU_STG.4.1 The TSF shall [selection: '*ignore auditable events*', '*prevent auditable events, except those taken by the authorized user with special rights*', '*overwrite the oldest stored audit records*'] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.**
Dependencies: FAU_STG.1 Protected audit trail storage

### 6.1.13 Audit trail analysis / review

**FAU_SAR.1 Audit review**
120 This component will provide authorized users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.
Hierarchical to: No other components.
**FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit records.**
**FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.**
Dependencies: **FAU_GEN.1 Audit data generation**

**FAU_SAR.2 Restricted audit review**
Hierarchical to: No other components.
**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.**
Dependencies: **FAU_SAR.1 Audit review**

**FAU_SAR.3 Selectable audit review**
Hierarchical to: No other components.
**FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *criteria with logical relations*].**
Dependencies: **FAU_SAR.1 Audit review**

### 6.1.14 TOE Integrity

**FPT_PHP.1 Passive detection of physical attack**
Hierarchical to: No other components.
**FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.**
**FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.**


© Copyright 2004 National Institute of Standards & Technology

Dependencies: **FMT_MOF.1 Management of security functions behavior**

**FPT_PHP.2 Notification of physical attack**
Hierarchical to: FPT_PHP.1
**FPT_PHP.2.1** The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
**FPT_PHP.2.2** The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
**FPT_PHP.2.3 For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.**
Dependencies: FMT_MOF.1 Management of security functions behavior

**FPT_PHP.3 Resistance to physical attack**
Hierarchical to: No other components.
**FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.**
Dependencies: No dependencies

### 6.1.15 Data Authentication

**FDP_DAU.2 Data authentication with identity of guarantor**
Hierarchical to: **FDP_DAU.1**
**FDP_DAU.2.1** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*].
**FDP_DAU.2.2** The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information **and the identity of the user that generated the evidence.**
Dependencies: **FIA_UID.1 Timing of identification**

### 6.1.16 Data exchange integrity

**FDP_UIT.1 Data exchange integrity**
Hierarchical to: No other components.
**FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.**
Dependencies: **[FDP_ACC.1 Subset access control, or**


© Copyright 2004 National Institute of Standards & Technology

**FDP_IFC.1 Subset information flow control]**
**[FTP_ITC.1 Inter-TSF trusted channel, or**
**FTP_TRP.1 Trusted path]**

### 6.1.17 Functions required to support dependencies

**FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.**
Dependencies: No dependencies

**FDP_ACF.1 Security attribute based access control**
Hierarchical to: No other components.
**FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].**
Dependencies: **FDP_ACC.1 Subset access control**
**FMT_MSA.3 Static attribute initialization**

**FMT_MSA.1 Management of security attributes**
Hierarchical to: No other components.
**FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].**
Dependencies: **[FDP_ACC.1 Subset access control or**
**FDP_IFC.1 Subset information flow control]**
**FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

**FMT_MSA.3 Static attribute initialization**
Hierarchical to: No other components.
**FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the *SFP*.**
**FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.**
Dependencies: **FMT_MSA.1 Management of security attributes**
**FMT_SMR.1 Security roles**

**FDP_IFC.1 Subset information flow control**
Hierarchical to: No other components.


© Copyright 2004 National Institute of Standards & Technology

**FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].**
Dependencies: **FDP_IFF.1 Simple security attributes**

**FMT_MOF.1Management of security functions behavior**
Hierarchical to: No other components.
**FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].**
Dependencies: **FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

### 6.1.18 Secure Communications Channels

**FPT_ITA.1 Inter-TSF availability within a defined availability metric**
Hierarchical to: No other components.
**FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: *list types of TSF data*] provided to a remote trusted product within [assignment: *a defined availability metric*] given the following conditions [assignment: *conditions to ensure availability*].**
Dependencies: No dependencies

**FPT_ITC.1 Inter-TSF confidentiality during transition**
Hierarchical to: No other components.
**The TSF shall protect all data transmitted from the TSF to a remote trusted product from unauthorized disclosure during transmission.**
Dependencies: No dependencies

**FPT_ITI.1 Inter-TSF detection of modification**
Hierarchical to: No other components.
**FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted product within the following metric: [assignment: *a defined modification metric*].**
**FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted product and perform [assignment: *action to be taken*] if modifications are detected.**
Dependencies: No dependencies.
**FPT_ITI.2 Inter-TSF detection and correction of modification**
Hierarchical to: FPT_ITI.1
**FPT_ITI.2.3 The TSF shall provide the capability to correct [assignment: *type of modification*] of all TSF data transmitted between the TSF and a remote trusted product.**
Dependencies: No dependencies.


© Copyright 2004 National Institute of Standards & Technology

**FPT_RCV.5 Continuous secure degraded operations**
Hierarchical to: No other components.
**FPT_RCV.5.1 The TSF shall ensure that [assignment: *security controls and list of failures/service discontinuities*] that continuous degraded operations can occur in a secure state.**
**FPT_RCV.5.2 The functions provided by the TSF to support continuous but degraded operations in event of failure/service discontinuities shall be configurable to support [assignment: *prioritized operations and configurations*].**
**FPT_RCV.5.3 The TSF shall ensure that the transition for recovery from degraded to normal operations [assignment: *list of security controls and configurations*] can be performed in an orderly, consistent and secure state.**

**FPT_SEP.1 TSF domain separation**
Hierarchical to: No other components.
**FPT_SEP.1.1 The TSF shall maintain a security domain for its execution that protects it from interference and tampering from untrusted objects.**
**FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.**
Dependencies: No dependencies.

**FPT_SSP.1 Simple trusted acknowledgement**
Hierarchical to: No other components.
**FPT_SSP.1.1 The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.**
Dependencies: **FPT_ITT.1 Basic internal TSF data transfer protection**
**FTP_SSP.2 Mutual trusted acknowledgement**
Hierarchical to: FPT_SSP.1
**FTP_SSP.2.2 The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.**
Dependencies: FPT_ITT.1 Basic internal data transfer protection.

**FPT_STM.1 Reliable time stamps**
Hierarchical to: No other components.
**The TSF shall be able to provide reliable time stamps for the systems use.**
Dependencies: No dependencies.

**FPT_TDC.1 Inter-TSF basic data consistency**
Hierarchical to: No other components.
**FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted product.**


© Copyright 2004 National Institute of Standards & Technology

**FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.**
Dependencies: No dependencies.

**FTP_ITC.1 Inter-TSF trusted channel**
Hierarchical to: No other components.
**FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.**
**FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, the remote trusted product*] to initiate communication via the trusted channel.**
**FPT_ITC.1.3 The TSF shall initiate communication via trusted channel for [assignment: *list of functions for which a trusted channel is required*].**
Dependencies: No dependencies.

**FTP_TRP.1 Trusted path**
Hierarchical to: No other components.
**FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communications paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.**
**FPT_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communications via the trusted path.**
**FPTTRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication,* [assignment: *other services for which trusted path is required*]].**
Dependencies: No dependencies.

**FDP_ETC.1 Export of user data without security attributes**
Hierarchical to: No other components.
**FDP_ETC. 1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside the TSC.**
**FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.**

### 6.1.19 Management Functions

**FMT_SMF.1 Specification of Management Functions**
Hierarchical to: No other components.


© Copyright 2004 National Institute of Standards & Technology

**FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].**
Dependencies: No Dependencies.

**FMT_MOF.2 Security policy and security function mapping**
Hierarchical to: No other components.
**FMT_MOF.2.1 The TSF shall be capable of performing the following security management**
**functions: [assignment: list of security management functions to be provided by the TSF].**
Dependencies: **No Dependencies**

*<Editor's Note: The remaining management functions are extensions to ISO 15408, that is, they are not found in the ISO standard>*

**FMT_MTD.4 Management of TSF data to policy mapping**
Hierarchical to: No other components.
**FMT_MTD.4.1 The TSF shall restrict the ability to specify the mapping for [assignment: *list of security management functions provided by the TSF*], and [assignment: *list of system security policies*].**
**FMT_MTD.4.2 The TSF shall distinguish between [assignment: *system domains*], [assignment: *security policy governing domain*], and [assignment: *data and its distribution and management*].**
Dependencies: **FMT_MTD.1 Management of TSF data**

FMT_REV.1 Access revocation
Physical and IT access shall be revoked within [assignment: *time span*] for personnel whose employment or contractual relationship is terminated or for personnel who are temporarily not actively involved in process control and operations (for example, workers on strike, workers on a leave of absence, etc.)

**FCS_CKM.1 Cryptographic key generation**
Hierarchical to: No other components.
**FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**
Dependencies: **[FCS_CKM.2 Cryptographic key distribution**
**or**
**FCS_COP.1 Cryptographic operation]**
**FCS_CKM.4 Cryptographic key destruction**


© Copyright 2004 National Institute of Standards & Technology

**FMT_MSA.2 Secure security attributes**

**FCS_CKM.2 Cryptographic key distribution**
Hierarchical to: No other components.
**FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].**
**Dependencies: [FDP_ITC.1 Import of user data without security attributes**
**or**
**FCS_CKM.1 Cryptographic key generation]**
**FCS_CKM.4 Cryptographic key destruction**
**FMT_MSA.2 Secure security attributes**

**FCS_CKM.3.1 Cryptographic key access**
Hierarchical to: No other components
**FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].**
**Dependencies: [FDP_ITC.1 Import of user data without security attributes**
**or**
**FCS_CKM.1 Cryptographic key generation]**
**FCS_CKM.4 Cryptographic key destruction**
**FMT_MSA.2 Secure security attributes**

**FCS_CKM.4 Cryptographic key destruction**
Hierarchical to: No other components.
**FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**
**Dependencies: [FDP_ITC.1 Import of user data without security attributes**
**or**
**FCS_CKM.1 Cryptographic key generation]**
**FMT_MSA.2 Secure security attributes**

**FCS_COP.1 Cryptographic operation**
Hierarchical to: No other componenets.
**FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment:*list of standards*].**
**Dependencies: [FDP_ITC.1 Import of user data without security attributes**
**or**


© Copyright 2004 National Institute of Standards & Technology

**FCS_CKM.1 Cryptographic key generation]**
**FCS_CKM.4 Cryptographic key destruction**
**FMT_MSA.2 Secure security attributes**

FPT_PHP.5 Backup and Restore
The TSF shall include the capability to backup and restore the system configuration including critical programs, controller instructions and parameters, and instructions and parameters for all sensors and actuators. Backups shall be performed [assignment: frequency] and whenever critical operating parameters [assignment: identify the critical operating parameters] are changed.

FPT_PHP.5 Backup and Restore Self-Testing
The TSF backup and restore procedure shall be able to be self-tested during regular operations and planned maintenance. Self-Test to be evoked as part of FPT_TST.1.

### 6.1.20 Physical Security Requirements

*<Editor's Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard >*

PHY_SOB.2 Strength of Boundary Access Control
The TSF shall provide physical access control to critical ICS components including, but not limited to: control room(s), servers, controller, sensors, actuators, and the physical plant under control.

*<Editor's Note: This requirement is included as an example. Physical security requirements should be inserted in this section as appropriate to the specific nature of the target ICS >*

### 6.1.21 Security Event Monitoring

*<Editor's Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard >*

**FEM_EDI.1 Event Definition and Identification**
**Hierarchical to: No other components.**
**FEM_EDI.1.1 the TSF shall provide automated event monitoring for [select: *event identification, name of interface, location,component name and functions,* [assignment*: other event information*].**


© Copyright 2004 National Institute of Standards & Technology

**FEM_EDI.1.2 The TSF shall provide the ability to [assignment: *alarm parameter settings, pre-defined security values*].**
**FEM_EDI.1.3 The TSF shall prescribe the information flow for each event [assignment: *monitored interface/component, monitoring device, information flow from receipt of alarm to its transmittal to end receiver for action*] and categorization of the alarm to the system TSF [assignment: *category and impact of alarm*].**
Dependencies**: FMT_SMF.1 Specification of management functions**
**FMT_SMR.1_Security roles**
**FPT_PHP. FPT_PHP.4 Domain definition and response to alarm**

**FEM_EDI.2 Interaction of system event monitoring components**
Hierarchical to**: FEM_EDI.1 Event definition and identification**
**FEM_EDI.2.1**

**defines the iinteractions of technical and operational and management security controls components that support event monitoring associated with the system environment. Also defines the system environment security controls event monitoring reporting mechanism from either direct or indirect interface with the System technical security controls components that support event monitoring. May be used in conjunction with FPT_PHP.**

**FEM_EDI.3 Alarm audit requirements define the audit requirements for the defined alarms.**

**FEM_EDI.4 Alarm response identifies that the alarm response to authorized pre-defined security event monitoring alarms be obtained and documented; identifies the roles and responsibilities that are defined for receipt of alarm and required action, including any timing constraints (possible roles are specified in FMT_SMR.1); defines security event alarm reporting procedures and mechanisms for the exchange of security event alarm information between the System IT and System environment security controls; and specifies that event alarm audit data be transformed to a specific format to support real-time analysis, and into a different useful format for delivery to authorised users for review (see application notes for FAU_SAA)**

FPT_STM.1 Reliable time stamps
**Hierarchical to: No other components.**
The TSF shall be able to provide reliable time stamps for the systems use.
**Dependencies: No dependencies.**


© Copyright 2004 National Institute of Standards & Technology

### 6.1.22 Requirements for interfaces between system components

*<Editor's Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >*

FPT_PHP.2 Authentication Integration
The TSF shall integrate authentication of user access with authentication for physical access such that user access is not granted for a user not identified by the physical access control as being physically present and such that user access is locked when the physical access control indicates that the user is no longer physically present.

### 6.1.23 Requirements for composability and interoperability between system components

FPT_PHP.4 Domain Definition and Response to Alarm
The TSF shall identify and define the domains, which comprise the system, the physical boundary for each domain, and the security policy(s), which governs each of the domains. The system security alarms may be tailored for the components being governed by the specific domain. The definition for each alarm shall be well defined, to include the alarm threshold, where it is reported, and the requisite system response.

This section documents any requirements specific to security composability that have not

### 6.1.24 Configuration requirements

*<Editor's Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >*

FCM_IDI.1 Configuration Change Requests and Actions
The STOE shall be subject to configuration management with an explicit change control and review process.

## 6.2 STOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements are listed in summary form in Table 13 below, with more detail on the assurance requirements following the Table. The general intent of the assurance requirements and associated system evaluation activities is to confirm that the acceptable level of residual risk as documented in the SPP is achieved in the operational system

The baseline evaluation assurance level (EAL) for Industrial Control Systems is EAL 3+. The "+" indicates that the EAL is as defined in ISO 15408 Part 3 with additional assurance requirements. In this case the additional requirements reflect the assurances associated with design, development, integration, testing and deployment of a system as opposed to a component or product. In addition, because the ICS is a system, a


© Copyright 2004 National Institute of Standards & Technology

combination of technical and operations and management security control elements must be considered.

*<Editor's Note: Table 13 and the text below it outlines extensions to the assurance requirements that are building on ISO system work in concert with NIST work on security controls>*

**Table 13 – STOE Security Assurance Requirements**

| No. | Component | Component Name |
|---|---|---|
| **Class ACM: Configuration management** | | |
| 1 | ACM_CAP.3 | Authorization controls |
| 2 | ACM_SCP.1 | TOE CM Coverage |
| 3 | ACM_OBM.1 | CM Operational Baseline and Maintenance |
| **Class ADO: Delivery and Operation** | | |
| 4 | ADO_DEL.1 | Delivery procedures |
| 5 | ADO_IGS.1 | Installation, generation and start-up |
| 6 | ADO_SIC.1 | Site interoperability check |
| **Class AGD: Guidance documents** | | |
| 7 | AGD_ADM.1 | Administrator guidance |
| 8 | AGD_USR.1 | User guidance |
| 9 | AGD_OCD.1 | System operational configuration definition guidance |
| **Class ALC** | **Life cycle support** | |
| 10 | ALC_DVS.1 | Identification of security measures |
| 11 | ALC_FLR.3 | Systematic flaw remediation |
| 12 | ALC_OPS.1 | Operational security |
| **Class ASA** | **Security awareness** | |
| 13 | ASA_PPG.2 | Verified operational security guidance |
| **Class ASC** | **O&M security** | |
| 14 | ASC_PPO.1 | Verified policy and procedures |
| 15 | ASC_PFA.1 | Asset records confirmation |
| 16 | ASC_OIN.1 | Operational integration |
| **Class ASD** | **System Architecture** | |
| 17 | ASD_SAD.1 | Operational system architecture design |
| 18 | ASD_IFS.1 | Operational system interface functional specification |


© Copyright 2004 National Institute of Standards & Technology

| No. | Component | Component Name |
|---|---|---|
| 19 | ASD_SSD.2 | Subsystem design |
| 20 | ASD_IMP.1 | Implementation representation |
| 21 | ASD_COM.1 | System security concept of operations |
| **Class ATE: Tests** | | |
| 22 | ATE_COV.2 | Analysis of coverage |
| 23 | ATE_DPT.1 | Testing high-level design |
| 24 | ATE_FUN.1 | Functional testing |
| 25 | ATE_IND.2 | Independent testing- sample |
| 26 | ATE_AST.3 | Operational testing policy conformance |
| **Class AVA: Vulnerability Assessment** | | |
| 27 | AVA_SOF.1 | Strength of STOE security function evaluation |
| 28 | AVA_MSU.1 | Examination of guidance |
| 29 | AVA_VLA.1 | Developer vulnerability analysis |
| **Class AMA: Assurance Maintenance** | | |
| 30 | ASA_AMP.1 | Assurance maintenance plan |
| 31 | AMA_EVD.1 | Evidence of assurance maintenance |
| 32 | AMA_SIA.1 | Security impact analysis |

### 6.2.1 Configuration Management (ACM)

#### Authorization Controls (ACM_CAP.3)

Dependencies: ALC_DVS.1 Identification of security measures

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

**ACM_CAP.3.2D** The developer shall use a CM system.

**ACM_CAP.3.3D** The developer shall provide CM documentation.

**ACM_CAP.3.1C** The reference for the STOE shall be unique to each version of the TOE.


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ACM_CAP.3.2C** | The STOE shall be labeled with its reference. |
| **ACM_CAP.3.3C** | The CM documentation shall include a configuration list **and a plan**. |
| **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. |
| **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 have been and are being effectively maintained under the CM system.** |
| **ACM_CAP.3.10C** | **The CM system shall provide measures such that only authorized changes are made to the configuration items.** |
| **ACM_CAP.3.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### STOE CM Coverage (ACM_SCP.1)

Dependencies: ACC_CAP.3 Authorization controls

| | |
|---|---|
| **ACM_SCP.1.1D** | **The developer shall provide a list of configuration items for the TOE.** |
| **ACM_SCP.1.1C** | **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.** |
| **ACM_SCP.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |


© Copyright 2004 National Institute of Standards & Technology

### Operational Baseline & Maintenance (ACM_OBM.1)

Dependencies: ACM_CAP.3 Authorization controls

ACM_SCP.1 TOE CM coverage

**ACM_OBM.1.1D** **The developer/system owner shall use a CM system for the initial/most recent evaluated system, which shall be called the "Baseline".**

**ACM_OBM.1.2D** **The CM system shall track and monitor each change, proposed and actual to the system Baseline, and its evaluation status.**

**ACM_OBM.1.3D** **The CM system shall report the current operational system configuration baseline.**

**ACM_OBM.1.4D** **The developer/system owner shall provide CM documentation of the Baseline system.**

**ACM_OBM.1.1C** **The CM System shall uniquely identify the System TOE Baseline, each associated change, and its evaluation status.**

**ACM_OBM.1.2.C** **The CM Plan shall describe how the system baseline is maintained, and changes to the baseline are tracked and controlled.**

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

## 6.2.2 Delivery and Operation (ADO)

### Delivery Procedures (ADO_DEL.1)

Dependencies: No dependencies.

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

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

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


© Copyright 2004 National Institute of Standards & Technology

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

### Installation, Generation and Start-up Procedures (ADO_IGS.1)

Dependencies: No dependencies.

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

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

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

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

### Site Interoperability Check (ADO_SIC.1)

Dependencies: No dependencies.

**ADO_SIC.1.1D** **The developer shall document procedures necessary to ensure that components and interfaces that comprise the System TOE, especially those to legacy security controls and interfaces can be started up and interoperate in a secure manner.**

**ADO_SIC.1.1C** **The site interoperability check procedures documentation shall describe the steps necessary for verification of secure start-up and interoperation of the System TOE in its environment.**

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

**ADO_SIC.1.2E** The evaluator shall determine that the start-up and interoperability check procedures result in a secure configuration.


© Copyright 2004 National Institute of Standards & Technology

### 6.2.3 Guidance Documents (AGD)

#### Administrator Guidance (AGD_ADM.1)

Dependencies: ASD_SAD.1 Operational System Architecture Design

**AGD_ADM.1.1D** **The developer shall provide administrator guidance addressed to system administrative personnel.**

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

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

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

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

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

**AGC_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.**

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

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

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


© Copyright 2004 National Institute of Standards & Technology

### User Guidance (AGD_USR.1)

Dependencies: ASD_SAD.1 Operational System Architecture Design

**AGD_USR.1.1D** **The developer shall provide user guidance.**

**AGD_USR.1.1C** **The user guidance shall describe the functions and interfaces available to the non-administrator users of the System TOE.**

**AGD_USR.1.2C** **The user guidance shall describe the use of user-accessible security functions provided by the System 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.**

**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 the TOE security environment.**

**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.**

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

### System Operational Configuration Definition Guidance (AGD_OCD.1)

Dependencies: ASD_SAD.1 Operational System Architecture Design

ASD_COM.1 Operational System Security Concept of Operations

**AGD_OCD.1.1D** **The developer/integrator/system owner shall provide configuration guidance that defines the security relevant configuration parameters that support the integration of the system components and that allow the system security functions to implement and enforce the system security concept of operations and associated policies.**

**AGD_OCD.1.1C** **The configuration guidance shall describe the security configuration parameters available to the system integrator or equivalent**


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **users/administrator of the System TOE with that role and responsibility.** |
| **AGD_OCD.1.2C** | **The configuration guidance shall describe the use of security parameters configurable by the TOE to implement and enforce the system security policies.** |
| **AGD_OCD.1.3C** | **The configuration guidance shall contain warnings about configuration accessible functions and privileges that should be controlled in a secure processing environment.** |
| **AGD_OCD.1.4C** | **The configuration guidance shall clearly present all configuration related responsibilities necessary for secure operation of the TOE.** |
| **AGD_OCD.1.5C** | **The user guidance shall be consistent with all other documentation supplied for evaluation.** |
| **AGD_OCD.1.6C** | **The configuration guidance shall describe all security requirements relative to the System environment.** |
| **AGD_OCD.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### 6.2.4 Life Cycle Support (ALC)

#### Identification of Security Measures (ALC_DVS.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ALC_DVS.1.1D** | **The developer shall produce development security documentation.** |
| **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.** |
| **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.** |
| **ALC_DVS.1.1E** | **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.** |


© Copyright 2004 National Institute of Standards & Technology

**requirements for content and presentation of evidence.**

**ALC_DVS.1.2E** **The evaluator shall confirm that the security measures are being applied.**

### Systematic Flaw Remediation (ALC_FLR.3)

Dependencies: No dependencies.

**ALC_FLR.3.1D** The developer shall provide flaw remediation procedures addressed to TOE developers.

**ALC_FLR.3.2D** The developer shall establish a a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

**ALC_FLR.3.3D** The developer shall provide remediation guidance addressed to TOE users.

**ALC_FLR.3.1C** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

**ALC_FLR.3.2C** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

**ALC_FLR.3.3C** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

**ALC_FLR.3.4C** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

**ALC_FLR.3.5C** The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

**ALC_FLR.3.6C** The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

**ALC_FLR.3.7C** The procedures for processing reported security flaws shall provide safeguards that any correction to these security flaws do not introduce any new flaws.


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ALC_FLR.3.8C** | The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE. |
| **ALC_FLR.3.9C** | **The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.** |
| **ALC_FLR.3.10C** | **The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security reports and corrections.** |
| **ALC_FLR.3.11C** | **The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.** |
| **ALC_FLR.3.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### Adequacy of Operational Security Measures (ALC_OPS.2)

| | |
|---|---|
| Dependencies: | ASD_COM.1 Operational System Security Concept of Operations |
| **ALC_OPS.2.1D** | **The developer/integrator/system owner shall produce operations security documentation.** |
| **ALC_OPS.2.1C** | **The operations security documentation shall describe all the physical, procedural, personnel, and other security controls measures that are required to protect the integrity of the System TOE implementation in its operational environment.** |
| **ALC_OPS2.2C** | **The operations security documentation shall provide evidence that these security control measures are in place, followed, and enforced during the operations and maintenance of the System TOE.** |
| **ALC_OPS.2.3C** | **The evidence shall provide support that the security control measures, as implemented, provide the required level of protection to maintain effective security of the System TOE.** |
| **ALC_OPS.2.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ALC_OPS.2.2E** | The evaluator shall confirm that the security controls measures are being applied. |

### 6.2.5 Security Awareness (ASA)

#### Verified Operational Security Guidance (ASA_PPG.2)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ASA_PPG.2.1D** | **The system owner/management shall provide security policy and procedure guidance addressed to [selection: [assignment: *appropriate personnel definition*], *all*] personnel.** |
| **ASA_PPG.2.1C** | **The security policy and procedure guidance shall describe the security policies applicable to the system for the target personnel** |
| **ASA_PPG.2.2C** | **The security policy and procedure guidance shall describe how personnel can obtain the full contents of the security policies applicable to the system for the target personnel** |
| **ASA_PPG.2.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASA_PPG.2.2E** | **The evaluator shall independently verify through [selection: *personnel interviews, sampling the procedures in the security policy and procedure guidance*, [assignment: *other methods*]] the veracity of the contents of the security policy and procedures guidance.** |

### 6.2.6 System O&M Security Controls (ASC)

#### Security Policy, Procedures and Organization (ASC_PPO.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ASC_PPO.1.1D** | **The system owner shall provide operational security documentation.** |
| **ASC_PPO.1.1C** | **The security controls documentation shall describe all the policy, procedural, personnel, and related organisational security controls measures that are necessary to protect the confidentiality and** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **integrity of the operations and maintenance of the System TOE in its operational environment.** |
| **ASC_PPO.1.2C** | **The operations security documentation shall provide evidence that these security controls measures are followed during the operation and maintenance of the System TOE.** |
| **ASC_PPO.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASC_PPO.1.2E** | **The evaluator shall confirm that the security controls are being applied.** |

### Physical, Facility and Assets (ASC_PFA.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ASC_PFA.1.1D** | **The developer/system owner/integrator shall provide documentation for the physical, facility, and assets that comprise the System security controls.** |
| **ASC_PFA.1.1C** | **The security controls documentation shall describe all the physical, facility and assets related security controls measures that are necessary to protect the confidentiality and integrity of the operations and maintenance of the System TOE in its operational environment.** |
| **ASC_PFA.1.2C** | **The operations security documentation shall provide evidence that these physical security controls measures are followed during the operation and maintenance of the System TOE.** |
| **ASC_PFA.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASC_PFA.1.2E** | **The evaluator shall confirm that the physical security controls are being applied effectively.** |

### Operational Integration (ASC_OIN.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ASC_OIN.1.1D** | **The developer/system owner/integrator shall provide operational security documentation.** |
| **ASC_OIN.1.1C** | **The operational system security documentation shall describe the integrated system security controls; to include IT and physical, policy,** |


© Copyright 2004 National Institute of Standards & Technology

**procedural, personnel, and other system security measures that are necessary to protect the confidentiality and integrity of the operations and maintenance of the System TOE in its operational environment.**

**ASC_OIN.1.2C** **The operations security documentation shall provide evidence that the integrated security control measures are followed as part of the operations and maintenance of the System TOE.**

**ASC_OIN.1.3C** **The evidence shall justify the integrated security measures provide the necessary level of protection to maintain the confidentiality and integrity of the System TOE.**

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

**ASC_OIN.1.2E** **The evaluator shall confirm that the integrated system security measures are being applied.**

### 6.2.7 System Architecture (Class ASD)

#### Operational System Architecture Design (ASD_SAD.1)

Dependencies: No dependencies.

**ASD_SAD.1.1D** **The developer/integrator shall provide an architecture description.**

**ASD_SAD.1.1C** **The architecture description shall identify the system in terms of its subsystems and critical components and the interfaces and interconnects between the subsystems and critical components.**

**ASD_SAD.1.2C** **The architecture description shall identify the super-systems that interact with the system and the interfaces and interconnects between the system and the super-systems.**

**ASD_SAD.1.3C** **The architecture description shall describe the purpose of the identified subsystems, critical components, interconnects and interfaces of the system.**

**ASD_SAD.1.4C** **The architecture description shall describe the purpose of the identified interconnects and interfaces from the system to super-systems and shall describe the services from and provided to the super-systems.**

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


© Copyright 2004 National Institute of Standards & Technology

requirements for content and presentation of evidence.

**ASD_SAD.1.2E** **The evaluator shall determine that the architecture description is consistent with the interface functional specification.**

### Operational System Interface Functional Specification (ASD_IFS.1)

Dependencies: No dependencies.

**ASD_IFS.1.1D** **The developer/integrator shall provide an interface functional specification.**

**ASD_IFS.1.1C** **The interface functional specification shall describe the operational system security functions.**

**ASD_IFS.1.2C** **The interfaces functional specification shall be internally consistent.**

**ASD_IFS.1.3C** **The interface functional specification shall identify and describe all the external system security function interfaces, including the behaviour of those interfaces.**

**ASD_IFS.1.4C** **The interface functional specification shall cover all the system security functions.**

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

**ASD_IFS.1.2E** **The evaluator shall determine whether the interface functional specification is a complete instantiation of the system security functional requirements.**

### Subsystem Design Allocation (ASD_SSD.2)

Dependencies: ASD_SSD.1 Subsystem design.

**ASD_SSD.2.1D** **The developer/integrator shall provide a subsystem design.**

**ASD_SSD.2.1C** **The subsystem design shall be internally consistent.**

**ASD_SSD.2.2C** **The subsystem design shall allocate the portion of the SSF to each represented subsystem in terms of minor and major subsystems.**


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ASD_SSD.2.3C** | **The subsystem design shall describe the security functionality provided by each subsystem.** |
| **ASD_SSD.2.4C** | **The subsystem design shall identify all hardware, firmware, and software required by the SSF allocated to the subsystem.** |
| **ASD_SSD.2.5C** | **The subsystem design shall allocate the portion of the SSF to each represented subsystem in terms of minor and major subsystems.** |
| **ASD_SSD.2.6C** | **The subsystem design shall identify the interfaces to the subsystem security functions**. |
| **ASD_SSD.2.7C** | **The subsystem design shall describe the interfaces to each subsystem, in terms of their purpose and method of use of the effects, exceptions and error messages.** |
| **ASD_SSD.2.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASD_SSD.2.2E** | **The evaluator shall determine whether the subsystem design is a complete instantiation of the operational system security functional requirements.** |

### Implementation Representation (ASD_IMP.1)

Dependencies: No dependencies..

| | |
|---|---|
| **ASD_IMP.1.1D** | **The developer/integrator shall provide an implementation representation of the system design.** |
| **ASD_IMP.1.1C** | **The implementation representation shall be internally consistent.** |
| **ASD_IMP.1.2C** | **The implementation representation identify the system functionality, and the system components that when integrated provide that functionality to the operational system.** |
| **ASD_IMP.1.3C** | **The implementation representation shall describe the security functionality provided by the integration of each component in terms of its specific configuration requirements.** |
| **ASD_IMP.1.4C** | **The implementation representation shall identify any hardware, firmware, and software integration and configuration issues, as identified, prior to, or during the operational system evaluation, that will need to be revisited.** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ASD_IMP.1.5C** | **The implementation representation shall identify the integrated components and their required configuration to the system security functions**. |
| **ASD_IMP.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASD_IMP.1.2E** | **The evaluator shall determine whether the implementation representation is a complete instantiation of the integrated operational system security functional requirements.** |

### Operational System Security Concept of Operations (ASD_COM.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ASD_COM.1.1D** | **The system owner/management shall provide a system operations policy documents.** |
| **ASD_COM.1.2D** | **The system owner/integrator shall incorporate system policy enforcement requirements and capabilities into the policy documents provided by the system management, and provide the system operations policy documents with the system enforcement capabilities, and their bounds.** |
| **ASD_COM.1.1C** | **The system concept of operations and enforcement documents subsystem shall be internally consistent.** |
| **ASD_COM.1.2C** | **The operational system operations policy documents shall identify the system capabilities for enforcement of information flow across the operational system interconnects within the operational system boundaries.** |
| **ASD_COM.1.3C** | **The operational system operations policy documents shall identify the system capabilities for enforcement of information flow across the operational system interconnects to external operational systems.** |
| **ASD_COM.1.4C** | **The operational system operations policy documents shall identify the system capabilities for enforcement of local and remote access to the operational system.** |
| **ASD_COM.1.5C** | **The operational system operations policy documents shall identify the system capabilities for enforcement of access to operational system resources based upon access mediation rules.** |
| **ASD_COM.1.6C** | **The operational system operations policy documents shall identify the modes of operation provided by the system, and the enforcement** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **mechanisms to provide secure operations in each of the identified system modes of operation.** |
| **ASD_COM.2.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ASD_COM.2.2E** | **The evaluator shall determine whether the system design is a complete instantiation of the operational system security concept of operations in support of the operational mission.** |

### 6.2.8 Tests (ATE)

#### System Security Controls Testing (ATE_AST.3)

| | |
|---|---|
| Dependencies: | AGD_OCD.1 System operational configuration definition.<br>AGD_USR.1 User guidance<br>ASD_IFS.1 System interface functional definition<br>ASD_IMP.1 Implementation representation |
| **ATE_AST.3.1D** | **The developer/integrator shall provide evidence of test verification planning.** |
| **ATE_AST.3.2D** | **The developer/integrator shall provide an analysis of level of detail of integrated security controls testing.** |
| **ATE_AST.3.3D** | **The developer shall provide test documentation and the the System TOE for testing.** |
| **ATE_AST.3.1C** | **The analysis of the security controls verification shall demonstrate that the correspondence between the security controls as identified in the SST and the tests identified in the test documentation is complete.** |
| **ATE_AST.3.2C** | **The level of detail analysis shall show that the integrated security controls tests identified in the test documentation are able to sufficiently demonstrate that the system security controls integrated into the System TSF operates in accordance with its high level design.** |
| **ATE_AST.3.3C** | **The level of detail analysis shall show that the integrated security controls tests identified in the test documentation are able to sufficiently demonstrate that the system security controls integrated into the System TSF; and are a correct implementation.** |
| **ATE_AST.3.4C** | **The System TOE shall be suitable for testing.** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **ATE_AST.3.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **ATE_AST.3.2E** | **The evaluator shall test a subset of the system TSF to confirm that the system TOE operates as specified in its intended operational environment.** |

### Analysis of Coverage (ATE_COV.2)

| | |
|---|---|
| Dependencies: | ASD_IFS.1 System interface functional definition<br>ATE_FUN.1 Functional testing |
| **ATE_COV.2.1D** | **The developer/integrator shall provide an analysis of the test coverage.** |
| **ATE_COV.2.1C** | **The analysis of 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.** |
| **ATE_COV.2.2C** | **The analysis of the test coverage shall demonstrate tha the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.** |
| **ATE_AST.3.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### Testing: high-level design (ATE_DPT.1)

| | |
|---|---|
| Dependencies: | ASD_IFS.1 System interface functional definition<br>ATE_FUN.1 Functional testing |
| **ATE_DPT.1.1D** | **The developer/integrator shall provide an analysis of the depth of testing.** |
| **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.** |
| **ATE_DPT.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |


© Copyright 2004 National Institute of Standards & Technology

### Functional Testing (ATE_FUN.1)

| | |
|---|---|
| Dependencies: | No dependencies. |
| **ATE_FUN.1.1D** | **The developer/integrator shall test the TSF and documents the results.** |
| **ATE_FUN.1.2D** | **The developer/integrator shall provide test documentation.** |
| **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.** |
| **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.** |
| **ATE_FUN.1.5C** | **The test results from the developer/integrator execution of the tests shall demonstrate that each test security function behaved as specified.** |
| **ATE_FUN.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### Independent testing – sample (ATE_IND.2)

| | |
|---|---|
| Dependencies: | AGD_USR.1 User guidance<br>ASD_IFS.1 System interface functional definition<br>ATE_FUN.1 Functional testing |
| **ATE_IND.2.1D** | **The developer/integrator/system owner shall provide the TOE for testing.** |
| **ATE_IND.2.1C** | **The TOE shall be suitable for testing.** |
| **ATE_IND.2.2C** | **The developer/integrator/system owner shall provide an equivalent set of resources to those that were used in the developer/integrator/system owner's functional testing of the TSF** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| **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. |
| **ATE_IND.2.3E** | **The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.** |

### 6.2.9 Vulnerability Assessment (AVA)

#### Examination of Guidance (AVA_MSU.1)

| | |
|---|---|
| Dependencies: | ADO_IGS.1 Installation, generation, and start-up procedures<br>AGD_USR.1 User guidance<br>ASD_IFS.1 Operational System Interface Functional Specification |
| **AVA_MSU.1.1D** | **The developer/integrator shall provide guidance documentation.** |
| **AVA_MSU.1.1C** | **The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.** |
| **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.** |
| **AVA_MSU.1.4C** | **The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).** |
| **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**. |


© Copyright 2004 National Institute of Standards & Technology

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

### Strength of TOE security function evaluation (AVA_SOF.1)

| | |
|---|---|
| Dependencies: | ASD_SSD.2 Subsystem design allocation<br>ASD_IFS.1 Operational system interface functional specification<br>ASD_COM.1 Operational system security concept of operations |
| **AVA_SOF.1.1D** | **The developer/system owner/integrator shall perform a strength of TOE security function analysis for each mechanism identified in the SST as having a strength of TOE security function claim.** |
| **AVA_SOF.1.1C** | **For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the SPP/SST.** |
| **AVA_SOF.1.2C** | **For each mechanism with a 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 the SPP/SST.** |
| **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/System owner vulnerability analysis (AVA_VLA.1)

| | |
|---|---|
| Dependencies: | ASD_SSD.2 Subsystem design allocation<br>ASD_IFS.1 Operational system interface functional specification<br>ASD_COM.1 Operational system security concept of operations<br>AGD_USR.1 User guidance |
| **AVA_VLA.1.1D** | **The developer/system owner shall perform a vulnerability analysis.** |
| **AVA_VLA.1.2D** | **The developer/system owner shall provide vulnerability analysis documentation** |
| **AVA_VLA.1.1C** | **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways n** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **which a user can violate the TSP.** |
| **AVA_VLA.1.2C** | **The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.** |
| **AVA_VLA.1.3C** | **The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment of the TOE.** |
| **AVA_VLA.1.1E** | **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.** |
| **AVA_VLA.1.2E** | **The evaluator shall conduct penetration testing, building on the developer/system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed**. |

## 6.2.10 Assurance Maintenance (AMA)

### Assurance Maintenance (AMA_AMP.1)

Dependencies: No dependencies.

| | |
|---|---|
| **AMA_AMP.1.1D** | **The developer/integrator shall provide an AM Plan.** |
| **AMA_AMP.1.1C** | **The AM Plan shall contain or reference a brief description of the TOE including the security functionality it provides.** |
| **AMA_AMP.1.2C** | **The AM Plan shall identify the certified version of the system TOE, and shall reference the evaluation results..** |
| **AMA_AMP.1.3C** | **The AM Plan shall reference the TOE component categorization report for the certified version of the TOE.** |
| **AMA_AMP.1.4C** | **The AM Plan shall define the scope of changes to the STOE that are covered by the plan.** |
| **AMA_AMP.1.5C** | **The AM Plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.** |
| **AMA_AMP.1.6C** | **The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **of the next re-evaluation of the TOE.** |
| **AMA_AMP.1.7C** | **The AM Plan shall identify the individual(s) who will assume the role of developer/system owner security analyst for the system TOE.** |
| **AMA_AMP.1.8C** | **The AM Plan shall describe how the developer/system owner security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.** |
| **AMA_AMP.1.9C** | **The AM Plan shall describe how the developer/system owner security analyst role will ensure that all developer/integrator actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.** |
| **AMA_AMP.1.10C** | **The AM Plan shall justify why the identified developer/system owner security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.** |
| **AMA_AMP.1.11C** | **The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.** |
| **AMA_AMP.1.1E** | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| **AMA_AMP.1.2E** | The evaluator shall confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with the proposed changes to the TOE. |

### TOE component categorization report (AMA_CAT.1)

| | |
|---|---|
| Dependencies: | **ACM_CAP.2 Configuration items** |
| **AMA_CAT.1.1D** | **The developer/system owner shall provide a system TOE component categorization report for the certified version of the system TOE.** |
| **AMA_CAT.1.1C** | **The TOE component categorization report shall categorize each component of the system TOE, identifiable in each TSF representation from the most abstract to the least abstract, according to its relevance to security; system TOE component categorization must indicate whether the component is TSP-enforcing or non-TSP** |


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **enforcing.** |
| **AMA_CAT. 1.2C** | **The system TOE component categorization report shall describe the categorization scheme used, so that it can be determined how to categorize new components introduce into the system TOE, and also when to re-categorize existing system TOE components following changes to the system TOE or its security target.** |
| **AMA_CAT. 1.3C** | **The system TOE component categorization report shall identify any tools used in the development *or operational* environment that, if modified, will have an impact on the assurance that the system TOE satisfies its security target.** |
| **AMA_CAT. 1.1E** | **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.** |
| **AMA_CAT. 1.2E** | **The evaluator shall confirm that the categorization of system TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version.** |

### Evidence of maintenance process (AMA_EVD.1)

| | |
|---|---|
| Dependencies: | AMA_AMP.1 Assurance maintenance process |
| | AMA_SIA.1 Sampling of security impact analysis |
| **AMA_EVD.1.1D** | **The developer/system owner security analyst shall provide AM documentation for the current version of the TOE.** |
| **AMA_EVD.1.1C** | **The AM documentation shall include a configuration list that comprises the current version of the TOE.** |
| **AMA_EVD.1.2C** | **The configuration list shall describe the configuration items that comprise the current version of the TOE.** |
| **AMA_EVD.1.3C** | **The AM documentation shall provide evidence that the procedures documented or referenced in the AM Plan are being followed.** |
| **AMA_EVD.1.4C** | **The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.** |
| **AMA_EVD.1.1E** | **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.** |
| **AMA_EVD.1.2E** | **The evaluator shall confirm that the procedures documented or referenced in the AM Plan are being followed.** |


© Copyright 2004 National Institute of Standards & Technology

**referenced in the AM Plan are being followed.**

**AMA_EVD.1.3E** **The evaluator shall confirm that the security impact analysis for the current version of the TOE is consistent with the configuration list.**

**AMA_EVD.1.4E** **The evaluator shall confirm that all changes documented in the security impact analysis for the current version of the TOE are within the scope of changes covered by the AM Plan.**

**AMA_EVD.1.5E** **The evaluator shall confirm that functional testing has been performed on the current version of the Toe, to a degree commensurate with the level of assurance being maintained.**

### Sampling of security impact analysis (AMA_SIA.1)

Dependencies: AMA_CAT.1 TOE component categorization report

**AMA_SIA.1.1D** **The developer/system owner security analyst shall, for the current version of the TOAE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version.**

**AMA_SIA.1.1C** **The security impact analysis shall identify the certified TOE from which the current version of the TOE was derived.**

**AMA_SIA.1.2C** **The security impact analysis shall identify all new and modified TOE components that are categorised as TSP-enforcing.**

**AMA_SIA.1.3C** **The security impact analysis shall, for each change affecting the security target or TSF representations, briefly describe the change and any effects it has on lower representation levels.**

**AMA_SIA.1.4C** **The security impact analysis shall, for each change affecting the security target or TSF representations, identify all IT security functions and all TOE components categorised as TSF enforcing that are affected by the change.**

**AMA_SIA.1.5C** **The security impact analysis shall, for each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change.**

**AMA_SIA.1.6C** **The security impact analysis shall for each applicable assurance requirements in the configuration management (ACM), life cycle support (ALC), delivery and operation (ADO), and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact**


© Copyright 2004 National Institute of Standards & Technology

| | |
|---|---|
| | **on assurance.** |
| **AMA_SIA.1.7C** | **The security impact analysis shall for each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable.** |
| **AMA_SIA.1.1E** | **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.** |
| **AMA_SIA.1.2E** | **The evaluator shall confirm, by sampling that the security impact analysis documents changes to an appropriate level of detail, together with appropriate justifications that assurance has been maintained in the current version of the TOE.** |

## 6.3 Security Requirements for the IT Environment

The STOE has no requirements for the external IT environment, other than those stipulated by the organizational security policies (refer to section 3.3).

## 6.4 Security Requirements for the Non-IT Environment

The STOE has no requirements for the external non-IT environment, other than those stipulated by the organizational security policies (refer to section 3.3).


© Copyright 2004 National Institute of Standards & Technology

# 7 SPP Application Notes

This section of the document contains supporting information that will be useful in developing more focused system protection profiles (SPPs) or system security targets (SSTs) for specific classes of industrial control systems, for example SCADA systems, or for specific applications of industrial control systems.

## 7.1 SPP Overview

### 7.1.1 SPP Purpose

A System Protection Profile provides an implementation-independent set of security requirements for a category of one or more systems. Unlike a traditional Protection Profile (PP) that focuses on the IT security requirements for a product, a SPP also captures management and operational security requirements to ensure the overall effectiveness of a system's security regime. Collectively, these requirements are referred to as the technical, operational and management security requirements of a system.

The term *system* is defined as the combination of physical, personnel, procedures and processes (derived from the operational and management security requirements) integrated with technology-based functions and mechanisms (derived from the technical security requirements), applied together to establish an acceptable level of residual risk in a defined operational environment.

This SPP has documented the minimum set of security requirements applicable to a generic industrial control system. However, while this document has attempted to model a "generic" ICS, it is acknowledged that not all security requirements will apply to all ICS instantiations. Where compliance to a set of security requirements for a specific ICS is required, another SPP should be written to address specific industry needs. A discussion of this relationship between the SPP-ICS and further SPPs and SSTs follows.

As shown by Figure 3 below, the SPP-ICS can be viewed as a high-level object in an object-class hierarchy. In this case, the high-level object is the SPP-ICS and lower-level objects can take the form of one or more SPPs or SSTs.


© Copyright 2004 National Institute of Standards & Technology

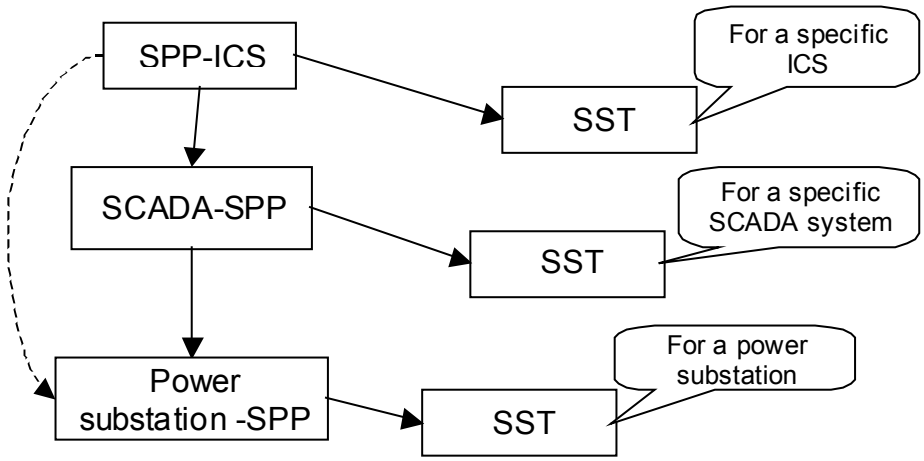


**Figure 3 - Relationship between SPP-ICS and other potential SPP's and SST's**

In the case of a lower-level SPP, one may use the security requirements in the SPP-ICS as a baseline for further refinement. The end result will produce an SPP addressing the security needs of a particular ICS type (e.g. SCADA). Alternatively, an SST author may claim compliance to the SPP-ICS by writing an SST based on the SPP-ICS. In this latter case, the SST author should be aware that further refinement is still required to claim conformance. Such refinements for either a lower-level SPP or a compliant SST have been discussed later in this section.

Regardless of how the SPP-ICS is applied, the SPP-ICS has been developed to be flexible and scalar in nature. That is, the SPP-ICS may be refined to address an entire ICS system, or be refined to address the security needs of specific subsystems commonly used in the process control industry.

Finally, it is envisaged that the SPP-ICS will be used to help ensure interoperability between process control systems, provide for a consistent implementation of security controls across systems and maintain a level of confidence in the security functions and mechanisms used to protect ICS systems and their related assets.

### 7.1.2 SPP Structure

The structure of the SPP-ICS has been developed following the specification of protection profiles defined by the Common Criteria. However, as the SPP-ICS is a *system* PP, the authors have extended the specification to incorporate several differences unique to systems that are not typically found in product-based protection profile specifications. These differences, and their relationships to the main elements defined by the SPP-ICS, have been captured below in Figure 4.

A discussion of each of the elements and their interrelationships in the SPP-ICS is provided below. Please note that each of these elements correspond to a different chapter in the SPP-ICS.


© Copyright 2004 National Institute of Standards & Technology

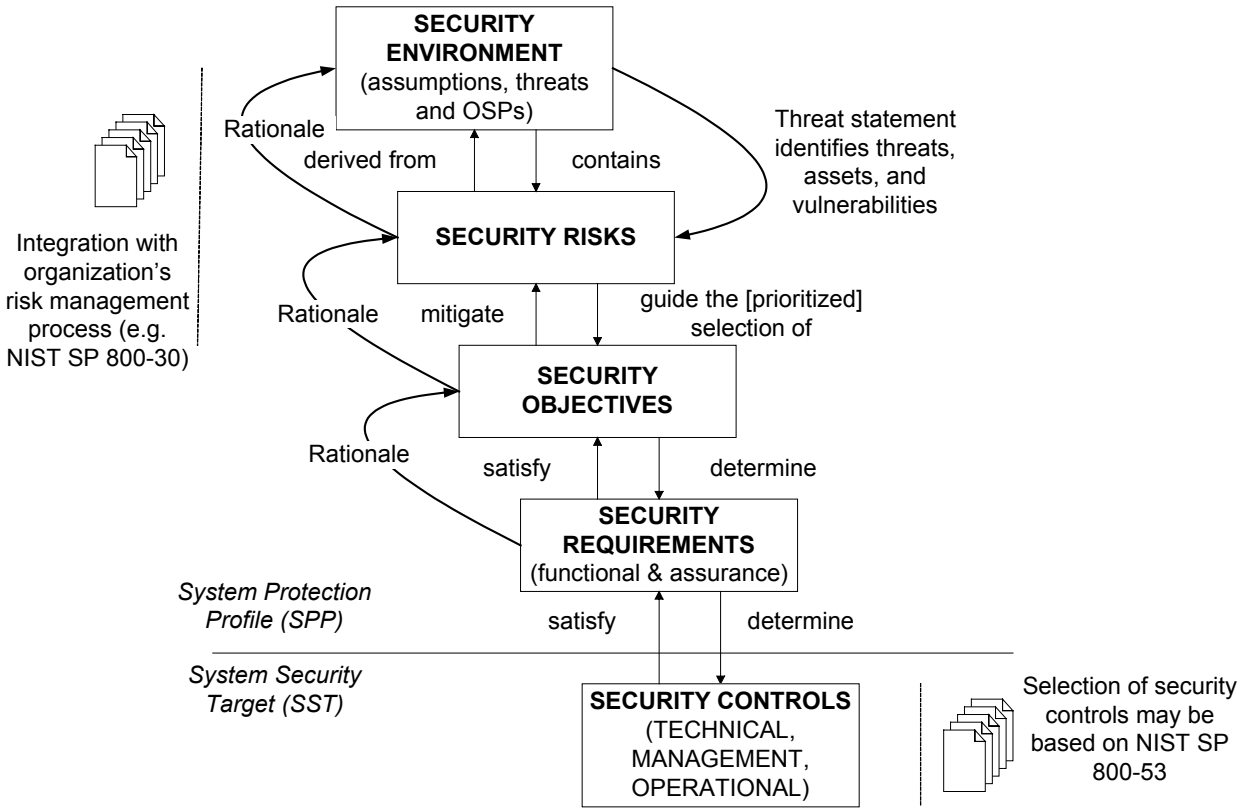


**Figure 4 – SPP-ICS Structure**

#### 7.1.2.1 Security Environment (Chapter 3)

The security environment describes the security aspects of the ICS operational environment. As for any CC-based specification, the SPP-ICS contains a statement of the assumptions, threats and organizational security policies applicable to the STOE. However, the SPP-ICS has expanded the definition of threats to include the following attributes:

- **Threat Agents** conducting an attack against the assets protected by the STOE. A threat agent is characterized by the following:
  - The level of **expertise** of the agent
  - The **resources** available to the agent to stage the attack
  - The **motivation** of the agent
- An **attack** which is characterized by the following:
  - The **method** used by the threat agent to perform the attack
  - The **vulnerabilities** exploited to gain access to the protected assets
  - The window of **opportunity** open to the threat agent to conduct the attack
- The **asset** (protected by the STOE) that is subject to the attack

This approach to specifying the threats reduces ambiguity. It also allows the SST author to thoroughly understand the nature of the threat so that a variety of security controls can be deployed to counter the threat.


© Copyright 2004 National Institute of Standards & Technology

#### 7.1.2.2 Security Risks (Chapter 4)

The security risks are a further instantiation of the security problem. The element of risk is captured by the SPP-ICS to determine the relative importance of the security needs of the STOE and its operating environment. They also guide the specification of the security objectives by ensuring that only those security needs seen as critical to the organization are addressed by the STOE or its operating environment.

Each risk is a product of asset value, assessed level of relevant threats, and associated vulnerabilities (as identified by the security environment). It represents the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organization responsible for the ICS.

Please note that the SPP-ICS has only listed the categories of risks applicable to a generic ICS. Guidance on the identification of the risks within these categories can be found in section 7.3.2.1.

#### 7.1.2.3 Security Objectives (Chapter 5)

The security objectives are a concise statement of the intended response to the security problem. In order to ensure a cost-effective system design, the inclusion of any security objective should be based on the outcomes of a risk assessment. For the purposes of the SPP-ICS, it is assumed that the owner of the ICS has a well-developed risk management process capable of identifying the risks to the ICS assets. Once identified, the risks should be prioritized and the organization's management should determine how best to treat those risks of high importance. Once this has been decided, any treatment strategies (including the specification of additional security controls needed to mitigate the risk) should be represented in the statement of the security objectives.

#### 7.1.2.4 Security Requirements (Chapter 6)

The security requirements define both the functional and assurance security requirements that the STOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives. Once specified, the security requirements then determine the selection of security controls required to ensure the protection of the STOE assets.

The SPP-ICS has included security functional requirements and security assurance requirements that extend ISO 15408 to cover issues associated with systems. These extensions are based on current ISO subcommittee work to extend ISO 15408 to cover the accreditation of systems and the evaluation of system protection profiles and system security targets. These extensions broaden consideration of security controls to include non-technical controls based on procedural and management functions.

#### 7.1.2.5 Security Controls

The selection of appropriate security controls is driven by the specification of the STOE security requirements. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. Please note that the


© Copyright 2004 National Institute of Standards & Technology

selection of security controls is not performed during an SPP. Rather, the selection of controls is left to the discretion of the SST author (refer to section 7.4.1.1 for guidance).

### 7.1.3 SPP Application

As discussed above, the SPP-ICS has been developed to capture the "generic" security needs of the process control industry. In doing so, it is expected that the SPP-ICS will be updated as it is applied in practice. This may include further instantiations of the SPP-ICS to address the needs of specific ICS types, such as those related to SCADA systems.

## 7.2 SPP Application: Risk Management

Risk management is recognized as an integral part of good management practice. It is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making to meet the business needs of an organization.

Generally, information security risk management methods and techniques are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful.

The risk management process involves establishing the context, identifying, analyzing, evaluating, treating, communicating and monitoring of risks. Each of these stages of the process should be performed in parallel to the SPP or SST development.

Importantly, the risk management process should be applied at all stages in the life cycle of a product or system. The following section has been included to equip the SPP reader with a brief understanding of the risk management process. The terminology defined in the next section is used throughout the remainder of the application notes.

### 7.2.1 Risk Management Process

Several forms of the risk management process for IT systems have been adopted by industry (e.g. NIST Special Publication 800-30). Many of these processes follow a common approach in addressing information security risk in systems. A summary of the approach includes the following steps (as illustrated by Figure 5):

#### 7.2.1.1 Context Establishment

Establishes the strategic, organizational and risk management context in which the rest of the process will take place. Includes characterizing the system with respect to its boundaries, functions, data criticality and data sensitivity.

#### 7.2.1.2 Risk Identification

Identify what, where and how things can arise as the basis for further analysis.


© Copyright 2004 National Institute of Standards & Technology

#### 7.2.1.3 Risk Assessment

Assessment of risks enables an organization to determine which risks can be accepted and which risks require controls to reduce them. ISO 17799 and NIST Special Publication 800-53 establish a code of practice for selecting information security controls.

##### *7.2.1.3.1 Risk Analysis*

Determine the existing controls and analyze risks in terms of impact and likelihood in the context of these controls. The analysis should consider the range of potential impact and how likely those impacts are to occur. Impact and likelihood are typically combined to produce an estimated level of risk.

Analysis of risks depends on the following factors:

- The nature of the business information and systems
- The business purpose for which the information is going to be used
- The environment in which the system is used and operated
- The protection provided by the controls in place.

##### *7.2.1.3.2 Risk Evaluation*

Compare estimated levels of risk against pre-established criteria. This enables risks to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.

#### 7.2.1.4 Risk Treatment

Accept and monitor low-priority risks. For other risks, develop and implement a specific risk management plan with the ultimate goal of reducing the level of risk down to an acceptable level (through the application of one or more technical, management or operational controls). The resultant risk (after security controls have been applied) is referred to as the residual risk.

Options for risk treatment (which are not necessarily mutually exclusive or appropriate in all circumstances), include the following:

- Risk Avoidance: risks can be avoided by deciding not to process with the activity likely to generate the risk (where this is practicable)
- Reduction of Likelihood: the likelihood of occurrence of risk events may be reduced by reducing threats or vulnerabilities through the application of security controls
- Reduction of Impact: the impacts of risk events may be reduced by reducing threats or vulnerabilities through the application of security controls or modification of the assets at risk in some other way
- Risk Transference: transfer the risk (in whole or part) to other parties (e.g. insurance agencies)
- Risk Retention: after unacceptable risks have been reduced or transferred, residual risks may be retained


© Copyright 2004 National Institute of Standards & Technology

#### 7.2.1.5 Monitor and review

Monitor and review the performance of the risk management system and changes that might affect it. Monitor residual risks in accordance with a risk management plan.

#### 7.2.1.6 Communicate and consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

The following figure illustrates the logical flow of the risk management process:

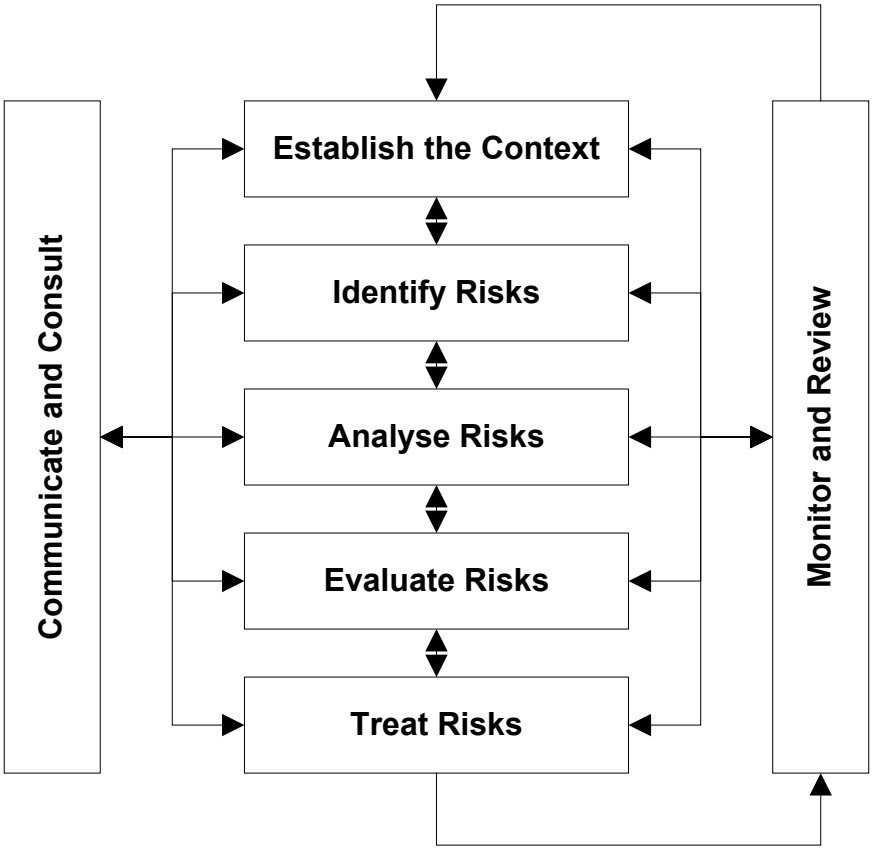


**Figure 5 – Overview of the Risk Management Process**

Please note that the risk management process outlined above should not replace an organization's own risk management methodology. This model has only been included to illustrate the relationship of the main elements of the risk management process to the SPP-ICS.

## 7.3 SPP Application: SPP

This section provides guidance on how to refine the SPP-ICS into further SPP's for specific ICS systems (e.g. SCADA systems).


© Copyright 2004 National Institute of Standards & Technology

### 7.3.1 Refinement of the Security Environment

#### 7.3.1.1 Assumptions, Threats and OOSPs

Due to the high-level nature of the SPP-ICS, it was difficult to specify detailed assumptions for a generic ICS implementation, as the operational environment is relatively diverse amongst the different process industry sectors. Using the included assumptions as a guide, the SPP author should make a concerted effort to ensure that the assumptions about the security aspects of the environment and/or the manner in which the STOE is intended to be used are clearly defined.

Conversely, the statement of threats in the SPP-ICS covers a broad range of threats against the confidentiality, integrity and availability of the STOE. It is noted that not all of these threats may be applicable to the STOE. The SPP author should first seek to confirm whether all of the threat components (i.e. threat agent, the attack and asset) are applicable to their operational environment. Organizations with a well-developed risk management process will have a better indication of whether or not these variables are applicable to their ICS' operational environment. Therefore, it is recommended that the validation of threats be performed against the results of previous risk assessments, security audits etc that have previously identified and assessed the types of threats relevant to the ICS.

The overarching organizational security policies (OOSPs) common to most organizations within the process industry have been included in the SPP. The SPP author should ensure that these cover both the security policies of the organization with responsibility of operating the ICS, as well as those for any external organizations interfacing with the ICS.

#### 7.3.1.2 System Assets

The system assets protected by the STOE include:

- Physical and logical components of the ICS itself (e.g. actuator, controller, HMI, etc)
- Remote diagnostics and maintenance services and supporting mechanisms
- Communications Infrastructure services and technology
- The process subject to control by the ICS
- Process control information
- Process control business or financial information

These asset groupings address the most critical parts of any ICS. However, they are generic in nature and should be refined in accordance with the ICS type. For example, a SCADA implementation may warrant the explicit definition of the Central Monitoring System (CMS) and the components housed within the control room.

Example asset categories that should be considered when developing a specific SPP include:

- Information assets: databases and data files, voice records, image files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;


© Copyright 2004 National Institute of Standards & Technology

- Paper documents: contracts, guidelines, company documentation, documents containing important business or financial data;
- Software assets: application software, system software, development tools and utilities;
- Physical assets: computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, accommodation;
- Marketing assets: company image and reputation; and
- Services: computing and communications services, other technical services (heating, lighting, power, air-conditioning).

#### 7.3.1.3 Vulnerability and Threat Analysis

A vulnerability and/or threat analysis is typically performed during the risk analysis stage of a risk assessment. The SPP author should use the results of any vulnerability or threat analyses applicable to the ICS to confirm the list of vulnerabilities and threats in the SPP-ICS, and refine the definitions as appropriate. Threats and vulnerabilities not applicable to the STOE operating environment may be removed from the SPP. Please note that a relationship exists between a vulnerability and a threat. The SPP author should exercise caution when removing a threat to ensure that it's corresponding vulnerability is still exploitable by another threat.

### 7.3.2 Risk Identification

#### 7.3.2.1 Identification of Risks to the System

The SPP-ICS has only focused on the categories of risks applicable to a generic ICS. The SPP author should use each category as a guide when performing risk identification. The following categories of risk have been included:

- Management of the security infrastructure (RISK.MANAGE)
- Development and implementation of Security Policies (RISK.SECPOLICY)
- Management of the risk assessment process (RISK.RISKMAN)
- Compliance with internal, legal and statutory requirements (RISK.COMPLY)
- Asset classification and control (RISK.ASSETCTRL)
- Personnel security (RISK.PERSONNEL)
- Physical security (RISK.PHYSICAL)
- Impact of natural disasters (RISK.ENVIRON)
- Illegal access to ICS components (RISK.EVIL_ACCESS)
- Confidentiality of information (RISK.NEED2KNOW)
- Integration of security requirements (RISK.INTEGRATE)
- Protection of network communications (RISK.NETCOMMS)
- Connection of IT systems (RISK.CONNECT)
- Use of Internet and email services (RISK.INTERNET)


© Copyright 2004 National Institute of Standards & Technology

- Remote access to the ICS network (RISK.REMOTE)
- Delivery of online services in support of ICS operation (RISK.ONLINE)
- Operational management (RISK.OPSMANAGE)
- Monitoring and detection of security breeches (RISK.IDS)
- Continuity of ICS operations (RISK.CONTINUITY)

Obviously, not all of the categories will apply to all ICS types. For example, RISK.REMOTE will not apply to those organizations that do not allow users to connect remotely to the ICS. The technique used by the SPP author to identify the risks (and other risk-related activities) should be in accordance with the organization's risk management policy.

Once the risk identification is complete, the SPP author may then complete the risk analysis by determining the level of risk (following the risk assessment process adopted by the organization). Once the risks have been evaluated and prioritized the SPP author should obtain management endorsement so that treatment strategies for the critical and other important risks can be developed and captured in the SPP. After the risks and their treatment strategies have been endorsed, the SPP author has a set of risks capable of guiding the selection of the security objectives (see next section). The treatment strategies may also be used to guide the selection of security controls in an SST (refer to section 7.4.1).

#### 7.3.2.2 Prior Risk Assessment

Ideally, a risk assessment should be performed prior to SPP development. However, tight schedules and economic constraints may prevent this from happening in practice. Therefore, one cannot always assume that a risk assessment has been conducted, nor assume that the allocation of security controls (which are selected to meet the security requirements) for the system has been prioritized in accordance with the organization's security and/or risk management policies.

Assuming that a risk assessment has been conducted, the results of the risk assessment can be used to help refine the various sections of the SPP-ICS, including:

- The system context of the risk assessment can be used to help refine the STOE description, including the boundaries and security features implemented by the system (defined in chapter 2 of the SPP-ICS)
- The results of the risk analysis, such as threat and vulnerability assessments, can be used to ensure that all the relevant threats to the assets have been captured in the STOE operational environment (defined in chapter 3 of the SPP-ICS)
- The security requirements for confidentiality, integrity and system availability defined by the risk assessment can be used to extract a set of requirements to be met by the system that are consistent with the business needs of the organization (defined in chapter 6 of the SPP-ICS)
- The security objectives of the system can be refined by focusing on the greatest areas of risk, or those residual risks that need to be monitored in accordance with the organizational risk management plan (defined in chapter 5 of the SPP-ICS)


© Copyright 2004 National Institute of Standards & Technology

As can be seen from the above points, there are significant advantages in having a risk assessment conducted prior to SPP development. Therefore, the SPP author should ensure that the results of previous risk assessments are used as input during the development of the SPP.

### 7.3.3 Refinement of the Security Objectives

The security objectives in the SPP-ICS have been selected based on the needs of the process control industry. However, as mentioned in section 7.3.2.1, the set of security objectives should be driven by the organizational [prioritized] need to mitigate identified risk. Ideally, the SPP author can reference previous risk assessments to determine the risks considered critical to the secure operation of the STOE and the protection of its assets. These risks should be used to determine the selection of the security objectives.

The SPP author may refine, modify or remove any security objective that does complement the security functionality supported by the ICS, provided that all of the risks corresponding to that objective have been satisfied by another security objective. Further, the SPP author should not feel obligated to keep those security objectives that do not contribute to the mitigation of the identified risks.

In the scenario that an identified risk to the organization is not mitigated by an STOE security objective, the SPP author may defer the treatment of that risk to the STOE external operating environment. The external operating environment is defined as everything outside the scope and boundary of the STOE, as defined by the STOE Description. Specification of security objectives on the external operating environment will differ for each ICS implementation given the diverse nature of the process control industry.

### 7.3.4 Refinement of the IT Security Requirements

A significant number of security assurance and functional requirements have been included in the SPP-ICS. This is due to the complicated nature of system security specification. However, not all requirements will be relevant to every ICS implementation. Therefore, the SPP author should use discretion when selecting the requirements for their STOE, and be guided by the security objectives (which are, in turn, guided by the identified risks to the system). Specifying too many security requirements may result in a costly and time-consuming process should the STOE undergo formal evaluation or security audit against the SPP security requirements.

The SPP author should also ensure that all operations on the security functional requirements have been completed.

### 7.3.5 Supporting Rationale

#### 7.3.5.1 Security Risks Rationale

The security risks rationale is an extension to the standard PP specification. It is included in the SPP-ICS to demonstrate that the identified risks of the STOE are relevant to the security problem. This is achieved by extracting the identified threats, vulnerabilities and assets from the security environment and mapping them to one or more risk categories. If at least one asset, threat and vulnerability combination can map to one or more risk categories then the security risks are an accurate and complete representation of the security problem.


© Copyright 2004 National Institute of Standards & Technology

As mentioned in section 7.3.2.1, the SPP author should use the risk categories as guidance to complement the risk identification phase of the ICS risk assessment. Once the risk identification is complete, the SPP author should ensure that every risk is a product of the threat, vulnerability and asset combination. This may also require modification to the security environment to ensure consistency between the SPP sections.

Please note that arguments for the sufficiency of the security risks addressing the identified threats, vulnerabilities and assets should also be completed in the security risks rationale.

#### 7.3.5.2 Security Objectives Rationale

The security objectives rationale has also been extended to cover the integration of risk. Specifically, the security objectives rationale must demonstrate that the security objectives are sufficient to meet the identified risks to the STOE. This is achieved by showing that at least one risk maps to one or more security objectives.

Please note that arguments for the sufficiency of the security objectives mitigating the identified risks to the STOE should also be completed in the security objectives rationale.

## 7.4 SPP Application: SST

This section provides guidance on how to claim conformance to the SPP-ICS for specific ICS systems. Please note that the guidance for "SPP Application: SPP" in section 7.3 is also relevant to an SST. Therefore, this section has only focused on those areas of an SST not already addressed by the previous section.

### 7.4.1 STOE Summary Specification

#### 7.4.1.1 Selection of Controls

Security controls are included in the SST to satisfy the security functional and assurance requirements. It is beyond the scope of this document to provide guidance on the selection of security controls. However, it is strongly recommended that the SPP author refer to 'pre-defined' libraries or catalogues of security controls to ensure that an adequate selection of technical, management and operational controls are included in the SST. Recommended security control catalogues include ISO 17799 and NIST Special Publication 800-53.

It is worth noting that the term 'security control' is equivalent to the term 'security function' used by the CC. However, whereas the focus on the CC is to specify IT-based security functions (aka TOE security functions), the application of the CC to systems has also introduced the notion of non-IT security functions to ensure the correct management and operation of the STOE. For the sake of consistency with other industry standards (e.g. NIST Special Publications 800-53 and 800-30), security functions should be referred to as security controls in an SST. In addition, security controls should be categorized as either technical, management or operational in nature.


© Copyright 2004 National Institute of Standards & Technology

#### 7.4.1.2 Selection of Assurance Measures

The assurance measures are included in the SST to satisfy the security assurance requirements. SST authors should note that the assurance requirements (and the functional requirements) included in the SPP-ICS are an extension to the CC to address the security needs of systems. Therefore, the selection of assurance measures is likely to be derived (in part) from management and operational security controls.

### 7.4.2 SPP Claims

#### 7.4.2.1 Conformance to the SPP-ICS

SST authors should note that conformance to the SPP-ICS requires a significant amount of refinement to the existing SPP-ICS content. This is because in an SPP not all aspects of the operational environment are known, and as a consequence a risk analysis cannot be completed (only the categories of risk have been identified in the SPP-ICS). Therefore, it is recommended that SST authors refine the SPP content prior to developing the SST content. Guidance on how to refine the SPP has been included throughout this chapter.

### 7.4.3 Supporting Rationale

Application guidance on the completion and/or refinement of the rationale has been included in section 7.3.5. However, since security controls are only relevant to an SST, additional guidance is provided below.

#### 7.4.3.1 STOE Summary Specification Rationale

In a product evaluation, the ST author must demonstrate that the IT security functions contribute to the satisfaction of one or more security functional requirements. While the approach is identical for an STOE, the following points should be noted:

- IT security functions are referred to as security controls in an STOE.
- Security controls are classified as either technical, management or operational in nature. All three types of security controls are usually required to satisfy a security requirement, although this is left to the discretion of the SST author.


© Copyright 2004 National Institute of Standards & Technology

# 8 Rationale

## 8.1 Security Risks Rationale

The purpose of this rationale is to demonstrate that the identified security risks are suitable, that is they are sufficient to address the security needs, and that they are necessary, ie, there are no redundant security risks.

### 8.1.1 All Assets, Threats and Vulnerabilities Addressed

The need to demonstrate that there are no redundant security risks is satisfied as follows:

- The first section (Table 14) shows that all of the assets, threats to security, and vulnerabilities have been addressed.
- The second section (Table 15) shows that each security risk addresses at least one assumption, policy, and threat combination.

**Table 14 - Mapping of Assets, Threats and Vulnerabilities to Security Risks**

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| A.ACTUATOR | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.REMOTE<br>R.OPSMANAGE<br>R.CONTINUITY |
| T.BAD_COMMAND | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.OPSMANAGE<br>R.IDS |
| V.PLAINTEXT | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.ASSETCTRL<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.CONTINUITY |
| A.SENSOR | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.IDS<br>R.ONLINE<br>R.CONTINUITY |
| T.REPUDIATE | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.IDS |
| V.SERVICES | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.IDS<br>R.CONTINUITY |
| A.CONTROLLER | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.IDS<br>R.ONLINE<br>R.CONTINUITY |
| T.PRIVILEGE | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE |
| V.REMOTE | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.CONTINUITY |
| A.HMI | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.RISKMAN<br>R.COMPLY<br>R.PERSONNEL<br>R.PHYSICAL |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.IDS<br>R.ONLINE<br>R.CONTINUITY |
| T.NO_FAULT_RECORD | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NETCOMMS<br>R.CONNECT<br>R.ONLINE<br>R.OPSMANAGE<br>R.IDS |
| V.ARCHITECTURE | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| A.REMOTE | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| T.INFECTION | R.SECPOLICY<br>R.RISKMAN<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.CONTINUITY |
| V.NOPOLICIES | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| A.COMMS | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.ONLINE<br>R.CONTINUITY |
| T.DISCLOSURE | R.RISKMAN<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE |
| V.NOTRAINING | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| A.CTRLPROCESS | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.ASSETCTRL<br>R.PERSONNEL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| T.EVIL_ANALYSIS | R.RISKMAN<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.OPSMANAGE<br>R.EVIL_ACCESS<br>R.NEED2KNOW |
| V.3RDPARTY | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| A.CTRLINFO | R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.CONTINUITY |
| T.PHYSICAL_ACCESS | R.PERSONNEL<br>R.PHYSICAL<br>R.NETCOMMS<br>R.OPSMANAGE<br>R.CONTINUITY |
| V.NORISK | R.MANAGE<br>R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.ONLINE<br>R.OPSMANAGE<br>R.IDS |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.CONTINUITY<br>R.PERSONNEL<br>R.PHYSICAL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>C.CONNECT<br>R.INTERNET<br>R.REMOTE |
| A.BUSINFO | R.SECPOLICY<br>R.RISKMAN<br>R.COMPLY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.ENVIRON<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.INTERNET<br>R.OPSMANAGE<br>R.ONLINE<br>R.CONTINUITY |
| T.DISASTER | R.RISKMAN<br>R.PERSONNEL<br>R.ENVIRON |
| V.SPOF | R.RISKMAN<br>R.PERSONNEL |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.ENVIRON<br>R.EVIL_ACCESS<br>R.INTEGRATE<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTER.ONLINE<br>R.OPSMANAGE<br>R.CONTINUITY |
| T.EVIL_MOD | R.RISKMAN<br>R.EVIL_ACCESS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.OPSMANAGE |
| T.EVIL_DESTRUCTION | R.RISKMAN<br>R.EVIL_ACCESS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.OPSMANAGE<br>R.CONTINUITY |
| T.CTRL_TAMPER | R.RISKMAN<br>R.EVIL_ACCESS<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.OPSMANAGE<br>R.CONTINUITY |
| T.SPOOF | R.RISKMAN<br>R.PERSONNEL |


© Copyright 2004 National Institute of Standards & Technology

| Asset/Threat/Vulnerability Label | Associated Security Risk |
|---|---|
| | R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.OPSMANAGE |
| T.DOS | R.RISKMAN<br>R.EVIL_ACCESS<br>R.NETCOMMS<br>R.CONNECT<br>R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.CONTINUITY |


© Copyright 2004 National Institute of Standards & Technology

Table 15 shows that there are no unnecessary IT security risks.

**Table 15 - Mapping of Security Risks to Assets, Threats and Vulnerabilities**

| Risk Category Label | Threats | Vulnerabilities | Assets |
|---|---|---|---|
| **RISK.MANAGE** | T.BAD_COMMAND, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS |
| **RISK.SECPOLICY** | T.BAD_COMMAND, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.RISKMAN** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.COMPLY** | TBD | V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Threats | Vulnerabilities | Assets |
|---|---|---|---|
| **RISK.ASSETCTRL** | T.REPUDIATE, T.PRIVILEGE, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.PERSONNEL** | T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.PHYSICAL** | T.PHYSICAL_ACCESS | V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS |
| **RISK.ENVIRON** | T.DISASTER | V.ARCHITECTURE V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.EVIL_ACCESS** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Threats | Vulnerabilities | Assets |
|---|---|---|---|
| **RISK.NEED2KNOW** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.SPOOF, T.PRIVILEGE | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.INTEGRATE** | TBD | V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.NETCOMMS** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.NO_FAULT_RECORD, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.CONNECT** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.INTERNET** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

| Risk Category Label | Threats | Vulnerabilities | Assets |
|---|---|---|---|
| **RISK.REMOTE** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.ONLINE** | T.DISCLOSURE, T.DOS, T.NO_FAULT_RECORD, T.INFECTION | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.OPSMANAGE** | T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |
| **RISK.IDS** | T.BAD_COMMAND, T.REPUDIATE, T.NO_FAULT_RECORD, | V.SERVICES, V.NOPOLICIES, V.NOTRAINING, V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS |
| **RISK.CONTINUITY** | T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.DOS, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS | V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK | ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO |


© Copyright 2004 National Institute of Standards & Technology

### 8.1.2 Security Risks are Sufficient

Due to the generic nature of this SPP and the need for additional refinement of the sources of risks and identified assets, threats and vulnerabilities, sufficiency arguments have not been included. SPP/SST authors should note that additional rationale is required in order to demonstrate that the risks are sufficient to address the security needs (refer to the application notes for guidance).

## 8.2 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are suitable, that is they are sufficient to address the security needs, and that they are necessary, ie, there are no redundant security objectives.

### 8.2.1 All Assumptions, Threats and Policies Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (Table 16) shows that all of the secure usage assumptions, threats to security, and organizational security policies have been addressed.
- The second section (Table 17) shows that each security objective counters at least one assumption, policy, or threat.

**Table 16 - Mapping of Assumptions, Threats, and OSPs to Security Objectives**

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| A.PHYSICAL_ACCESS | O.PHYSICAL<br>O.INTERCONNECTIVITY<br>O.CONTINUITY<br>O.REMOTE<br>O.ACCESS_CONTROL<br>O.MONITORING<br>O.AUDIT<br>O.IDS<br>O.RISK |
| T.DISCLOSURE | O.RISK<br>O.INTERCONNECTIVITY<br>O.DATA_AUTHENTICATION<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.REMOTE<br>O.COMPLIANCE<br>O.ACCESS_CONTROL<br>O.SECURE_COMMS |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.DATA_INTEGRITY<br>O.CONFIDENTIALITY |
| P.EVENT | O.PHYSICAL<br>O.RISK<br>O.INTERCONNECTIVITY<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.REMOTE<br>O.ACCESS_CONTROL<br>O.SECURE_COMMS<br>O.AVAILABILITY<br>O.MONITORING |
| A.COMMS_ACCESS | O.PHYSICAL<br>O.INTERCONNECTIVITY<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.REMOTE<br>O.ACCESS_CONTROL<br>O.AVAILABILITY |
| T.EVIL_ANALYSIS | O.PHYSICAL<br>O.INTERCONNECTIVITY<br>O.DATA_INTEGRITY<br>O.3RDPARTY<br>O.REMOTE<br>O.SYSTEM INTEGRITY<br>O.MONITORING<br>O.AUDIT |
| P.PERSONNEL | O.PHYSICAL<br>O.MANAGEMENT<br>O.3RDPARTY |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.ACCESS_CONTROL<br>O.DATA_INTEGRITY<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.IDS<br>O.AUDIT |
| A.EXTERNAL | O.INTERCONNECTIVITY<br>O.CONTINUITY<br>O.MIGRATION<br>O.COMPLIANCE<br>O.3RDPARTY<br>O.SECURE_COMMS<br>O.DATA_INTEGRITY<br>O.AVAILABILITY<br>O.MONITORING |
| T.EVIL_MODIFICATION | O.PHYSICAL<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.REMOTE<br>O.SECURE_COMMS<br>O.DATA_AUTHENTICATION<br>DATA_INTEGRITY |
| P.INFRASTRUCTURE | O.RISK<br>O.NON_INTERFERENCE<br>O.DATA_BACKUP<br>O.ACCESS_CONTROL<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.MIGRATION<br>O.COMPLIANCE<br>O.IDS |
| A.REMOTE | O.PHYSICAL |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.ACCESS_CONTROL<br>O.CONFIDENTIALITY<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.REMOTE<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.IDS |
| T.EVIL_DESTRUCTION | O.DATA_INTEGRITY<br>O.ACCESS_CONTROL<br>O.MONITORING<br>O.3RDPARTY<br>O.REMOTE<br>O.AVAILABILTIY |
| P.CONFIGURATION | O.PHYSICAL<br>O.INTERCONNECTIVITY<br>O.DATA_AUTHENTICATION<br>O.MANAGEMENT<br>O.MIGRATION<br>O.SYSTEM_INTEGRITY |
| T.CTRL_TAMPER | O.PHYSICAL<br>O.DATA_AUTHENTICATION<br>O.ACCESS_CONTROL<br>O.SECURE_COMMS<br>O.DATA_INTEGRITY<br>O.SYSTEM_INTEGRITY<br>O.SYSTEM_DIAGNOSTICS<br>O.MONITORING |
| P.PHYSICAL | O.PHYSICAL<br>O.INTERCONNECTIVITY<br>O.ACCESS_CONTROL<br>O.SECURE_COMMS |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.REMOTE<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.IDS |
| T.BAD_COMMAND | O.NON_INTERFERENCE<br>O.DATA_AUTHENTICATION<br>O.SECURE_COMMS<br>O.DATA_INTEGRITY<br>O.CONFIDENTIALITY<br>O.AVAILABILITY<br>O.SYSTEM_INTEGRITY<br>O.SYSTEM_DIAGNOSTICS |
| P.POLICY | O.RISK<br>O.NON_INTERFERENCE<br>O.DATA_BACKUP<br>O.DATA_AUTHENTICATION<br>O.ACCESS_CONTROL<br>O.CONFIDENTIALITY<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.MIGRATION<br>O.COMPLIANCE<br>O.3RDPARTY<br>O.REMOTE<br>O.IDS<br>O.AUDIT |
| T.SPOOF | O.DATA_AUTHENTICATION<br>O.ACCESS_CONTROL<br>O.CONFIDENTIALITY<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.REMOTE |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.SYSTEM_INTEGRITY |
| P.ASSETS | O.RISK<br>O.MIGRATIOON<br>O.COMPLIANCE |
| T.REPUDIATE | O.DATA_AUTHENTICATION<br>O.ACCESS_CONTROL<br>O.DATA_INTEGRITY<br>O.MANAGEMENT |
| P.SAFETY | O.NON-INTERFERENCE<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.MIGRATION<br>O.COMPLIANCE<br>O.3RDPARTY<br>O.REMOTE<br>O.SYSTEM_DIAGNOSTICS |
| T.DOS | O.CONTINUITY<br>O.3RDPARTY<br>O.REMOTE<br>O.ACCESS_CONTORL<br>O.SECURE_COMMS<br>O.AVAILABILITY<br>O.AUDIT |
| P.NO_INTERFERE | O.NON_INTERFERENCE<br>O.MANAGEMENT<br>O.MIGRATION<br>O.COMPLIANCE |
| T.PRIVILEGE | O.DATA_AUTHENTICATION<br>O.MIGRATION<br>O.3RDPARTY<br>O.REMOTE |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.ACCESS_CONTROL<br>O.DATA_INTEGRITY<br>O.CONFIDENTIALITY<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.IDS |
| P.BUSINESS | O.DATA_BACKUP<br>O.CONTINUITY<br>O.MANAGEMENT<br>O.MIGRATION<br>O.AVAILABILITY |
| T.NO_FAULT_RECORD | O.SYSTEM_DIAGNOSTICS<br>O.MONITORING<br>O.AUDIT<br>O.IDS |
| P.RISK | O.RISK<br>O.MANAGEMENT<br>O.MIGRATION |
| T.DISASTEER | O.CONTINUITY<br>O.MANAGEMENT<br>O.MIGRATION<br>O.AVAILABILTIY |
| P.ENVIRONMENT | O.PHYSICAL<br>O.RISK<br>O.NON_INTERFERENCE<br>O.MANAGEMENT<br>O.CONTINUITY<br>O.MIGRATION<br>O.SYSTEM_INTEGRITY<br>O.AVAILABILTIY |
| T.OUTAGE | O.AVAILABILITY |


© Copyright 2004 National Institute of Standards & Technology

| Threat/Policy/Assumption Label | Associated Security Objective |
|---|---|
| | O.CONTINUITY<br>O.NON_INTERFERENCE<br>O.DATA_BACKUP |
| T.INFECTION | O.INTERCONNECTIVITY<br>O.DATA_BACKUP<br>O.DATA_AUTHENTICATION<br>O.3RDPARTY<br>O.REMOTE<br>O.SECURE_COMMS<br>O.DATA_INTEGRITY<br>O.SYSTEM_INTEGRITY<br>O.MONITORING |
| T.PHYSICAL_ACCESS | O.PHYSICAL<br>O.RISK<br>O.INTERCONNECTIVITY<br>O.3RDPARTY<br>O.REMOTE<br>O.ACCESS_CONTROL<br>O.SYSTEM_INTEGRITY<br>O.MONITORING<br>O.AUDIT<br>O.IDS |

Table 17 shows that there are no unnecessary IT security objectives.

**Table 17 - Mapping of Security Objectives to Threats, Policies and Assumptions**

| Security Objective | Threats | Policies | Assumptions |
|---|---|---|---|
| **O.PHYSICAL** | T.EVIL_ANALYSIS,<br>T.EVIL_MOIDIFICATION,<br>T.CONTROL_TAMPER,<br>T..PHYSICAL_ACCESS | P.EVENT,<br>P.PERSONNEL,<br>P.CONFIGURATION,<br>P.PHYSICAL<br>P.ENVIRONMENT | A.PHYSICAL_ACCESS<br>A.COMMS_ACCESS,<br>A.REMOTE, |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Threats | Policies | Assumptions |
|---|---|---|---|
| **O.RISK** | T.DISCLOSURE,<br>T.PHYSICAL_ACCESS | P.EVENT,<br>P.INFRASTRUCTURE<br>P.POLICY,<br>P.ASSETS<br>P.RISK,<br>P.ENVIRONMENT | A.PHYISCAL_ACCESS |
| **O.NON_INTERFERENCE** | T.OUTAGE | P.INFRASTRUCTURE<br>P.POLICY,<br>P.SAFETY,<br>P.NO_INTERFERE,<br>P.ENVIRONMENT | |
| **O.INTERCONNECTIVITY** | T.DISCLOSURE<br>T.EVIL_ANALYSIS<br>T.INFECTION<br>T.PHYSICAL_ACCESS | P.EVENT<br>P.CONFIGURATION,<br>P.PHYSICAL | A.PHYSICAL_ACCESS<br>A.COMMS_ACCESS,<br>A.EXTERNAL |
| **O.DATA_BACKUP** | T.OUTAGE,<br>T.INFECTION | P.POLICY,<br>P.BUSINESS, | |
| **O.DATA_AUTHENTICATION** | T.DISCLOSURE,<br>T.EVIL_MODIFICATION,<br>T.CTRL_TAMPER<br>T.BAD_COMMAND<br>T.SPOOF<br>T.REPUDIATE<br>T.PRIVILEGE<br>T.INFECTION | P.CONFIGURATION,<br>P.POLICY | |
| **O.CONTINUITY** | T.DOS,<br>T.DISASTER<br>T.OUTAGE | P.EVENT,<br>P.INFRASTRUCTURE<br>P.POLICY,<br>P.BUSINESS,<br>P.ENVIRONMENT | **A.PHYSICAL_ACCESS,**<br>**A.COMMS_ACCESS,**<br>**A.EXTERNAL** |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Threats | Policies | Assumptions |
|---|---|---|---|
| **O.MANAGEMENT** | T.DISCLOSURE,<br>T.SPOOF,<br>T.REPUDIATE<br>T.DISASTER | P.EVENT,<br>P.PERSONNEL,<br>P.INFRASTRUCTURE<br>P.CONFIGURATION,<br>P.POLICY<br>P.SAFETY<br>P.NO_INTERFERE<br>P.BUSINESS<br>P.RISK<br>P.ENVIRONMENT | **A.COMMS_ACCESS,**<br>**A.REMOTE,** |
| **O.MIGRATION** | T.PRIVILEGE<br>T.DISASTER | P.INFRASTRUCTURE<br>P.CONFIGURATION<br>P.ASSETS<br>P.SAFETY<br>P.NO_INTERFERE<br>P.BUSINESS<br>P.RISK<br>P.ENVIRONMENT | **A.EXTERNAL;** |
| **O.COMPLIANCE** | T.DISCLOSURE | P.INFRASTRUCTURE<br>P.POLICYP.ASSETS<br>P.SAFETY<br>P.NO_INTERFERE | **A.EXTERNAL** |
| **O.3RDPARTY** | T.DISCLOSURE<br>T.EVIL_ANALYSIS<br>T.EVIL_DESTRUCTION<br>T.SPOOF<br>T.DOS<br>T.PRIVILEGE<br>T.INFECTION<br>T.PHYSICAL_ACCESS | P.EVENT<br>P.PERSONNEL<br>P.POLICY<br>P.SAFETY | **A.COMMS_ACCESS**<br>**A.EXTERNAL**<br>**A.REMOTE** |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Threats | Policies | Assumptions |
|---|---|---|---|
| **O.REMOTE** | T.DISCLOSURE<br>T.EVIL_ANALYSIS<br>T.EVIL_MODIFICATION<br>T.EVIL_DESTRUCTION<br>T.SPOOF<br>T.DOS<br>T.PRIVILEGE<br>T.INFECTION<br>T.PHYSICAL_ACCESS | P.EVENT<br>P.PHYSICAL<br>P.POLICY<br>P.SAFETY | **A.PHYSICAL_ACCESS**<br>**A.COMMS_ACCESS**<br>**A.REMOTE** |
| **O.ACCESS_CONTROL** | T.EVIL_DESTRUCTION<br>T.CTRL_TAMPER<br>T.SPOOF<br>T.REPUDIATE<br>T.DOS<br>T.PRIVILEGE<br>T.PHYSICAL_ACCESS | P.EVENT<br>P.PERSONNEL<br>P.INFRASTRUCTURE<br>P.PHYSICAL<br>P.POLICY | **A.PHYSICAL_ACCESS**<br>**A.COMMS_ACCESS**<br>**A.REMOTE** |
| **O.SECURE_COMMS** | T.DISCLOSURE<br>T.EVIL_MODIFICATION<br>T.CTRL_TAMPER<br>T.BAD_COMMAND<br>T.INFECTION | P.EVENT<br>P.PHYSICAL | **A.EXTERNAL** |
| **O.DATA_INTEGRITY** | T.DISCLOSURE<br>T.EVIL_ANALYSIS<br>T.EVIL_MODIFICATION<br>T.EVIL_DESTRUCTION<br>T.CTRL_TAMPER<br>T.BAD_COMMAND<br>T.REPUDIATE<br>T.PRIVILEGE<br>T.INFECTION | P.PERSONNEL | **A.EXTERNAL** |
| **O.CONFIDENTIALITY** | T.DISCLOSURE<br>T.BAD_COMMAND<br>T.SPOOF<br>T.PRIVILEGE | P.POLICY | **A.REMOTE** |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Threats | Policies | Assumptions |
|---|---|---|---|
| **O.AVAILABILITY** | T.BAD_COMMAND<br>T.DOS<br>T.DISASTER<br>T.OUTAGE | P.EVENT<br>P.BUSINESS<br>P.ENVIRONMENT | **A.COMMS_ACCESS**<br>**A.EXTERNAL** |
| **O.SYSTEM_INTEGRITY** | T.EVIL_ANALYSIS<br>T.EVIL_MODIFICATION<br>T.CTRL_TAMPER<br>T.BAD_COMMAND<br>T.SPOOF<br>T.PRIVILEGE<br>T.INFECTION<br>T.PHYSICAL_ACCESS | P.PERSONNEL<br>P.CONFIGURATION<br>P.PHYSICAL<br>P.ENVIRONMENT | **A.REMOTE** |
| **O.SYSTEM_DIAGNOSTICS** | T.CTRL_TAMPER<br>T.BAD_COMMAND<br>T.NO_FAULT_RECORD | P.SAFETY | |
| **O.MONITORING** | T.EVIL_ANALYSIS<br>T.EVIL_MODIFICATION<br>T.EVIL_DESTRUCTION<br>T.CTRL-TAMPER<br>T.PRIVILEGE<br>T.NO_FAULT_RECORD<br>T.INFECTION<br>T.PHYSICAL_ACCESS | P.EVENT<br>P.PERSONNEL | **A.PHYSICAL_ACCESS**<br>**A.EXTERNAL**<br>**A.REMOTE**<br>**P.PHYSICAL** |
| **O.AUDIT** | T.EVIL_ANALYSIS<br>T.DOS<br>T.NO_FAULT_RECORD<br>T.PHYSICAL_ACCESS<br>T.OUTAGE | P.PERSONNEL<br>P.POLICY | **A.PHYSICAL_ACCESS** |
| **O.IDS** | T.PHYSICAL_ACCESS<br>T.NO_FAULT_RECORD<br>T.PRIVILEGE<br>T.DOS | P.POLICY<br>P.PHYSICAL<br>P.INFRASTRUCTURE<br>P.PERSONNEL | **A.REMOTE**<br>**A.PHYSICAL_ACCESS** |


© Copyright 2004 National Institute of Standards & Technology

### 8.2.2 Security Objectives are Sufficient

Due to the generic nature of this SPP and the need for additional refinement of the identified security objectives, assumptions, threats and organizational security policies, sufficiency arguments have not been included. SPP/SST authors should note that additional rationale is required in order to demonstrate that the security objectives are sufficient to address the security needs (refer to the application notes for guidance).

### 8.2.3 Suitability of the Security Objectives to counter identified Risks

The purpose of this section is to show that the security objectives are suitable to address the identified security risks. Table 18 and Table 19 show that each security objective is necessary, that is, each security risk is addressed by at least one security objective and vice versa.

**Table 18 - Mapping of Security Risks to Security Objectives**

| Security Risk | Security Objectives |
|---|---|
| R.MANAGE | O.DATA_AUTHENTICATION<br>O.MANAGEMENT<br>O.3RDPARTY<br>O.AUDIT |
| R.SECPOLICY | O.DATA_AUTHENTICATION<br>O.REMOTE<br>O.AVAILABILITY<br>O.DATA_BACKUP<br>O.3RDPARTY<br>O.RISK<br>O.MANAGEMENT<br>O.COMPLIANCE |
| R.RISKMAN | O.RISK<br>O.DATA_INTEGRITY<br>O.ACCESS_CONTROL |
| R.COMPLY | O.COMPLIANCE |
| R.ASSETCTRL | O.MANAGEMENT<br>O.MIGRATION |
| R.PERSONNEL | O.MANAGEMENT<br>O.RISK<br>O.ACCESS_CONTROL |


© Copyright 2004 National Institute of Standards & Technology

| Security Risk | Security Objectives |
|---|---|
| | O.MIGRATION |
| R.PHYSICAL | O.PHYSICAL |
| R.ENVIRON | O.CONTINUITY<br>O.AVAILABILITY |
| R.EVIL_ACCESS | O.DATA_INTEGRITY<br>O.SECURE_COMMS<br>O.ACCESS_CONTROL<br>O.SYSTEM_INTEGRITY |
| R.NEED2KNOW | O.CONFIDENTIALITY<br>O.ACCESS_CONTROL |
| R.INTEGRATE | O.3RDPARTY<br>O.MIGRATION<br>O.NON_INTERFERENCE |
| R.NETCOMMS | O.SECURE_COMMS<br>O.ACCESS_CONTROL<br>O.DATA_AUTHENTICATION |
| R.CONNECT | O.INTERCONNECTIVITY<br>O.COMPLIANCE<br>O.DATA_AUTHENTICATION<br>O.REMOTE |
| R.INTERNET | O.COMPLIANCE<br>O.MONITORING |
| R.REMOTE | O.3RDPARTY<br>O.REMOTE<br>O.DATA_INTEGRITY<br>O.MONITORING<br>O.DATA_AUTHENTICATION |
| R.ONLINE | O.DATA_AUTHENTICATION<br>O.INTERCONNECTIVITY<br>O.MONITORING |


© Copyright 2004 National Institute of Standards & Technology

| Security Risk | Security Objectives |
|---|---|
| | O.AUDIT<br>O.REMOTE |
| R.OPSMANAGE | O.SYSTEM_INTEGRITY<br>O.SYSTEM_DIAGNOSTICS<br>O.MONITORING<br>O.NON_INTERFERENCE<br>O.DATA_AUTHENTICATION<br>O.RISK<br>O.MANAGEMENT<br>O.MIGRATION<br>O.CONFIDENTIALITY |
| R.IDS | O.IDS<br>O.MONITORING<br>O.AUDIT |
| R.CONTINUITY | O.CONTINUITY<br>O.INTERCONNECTIVITY<br>O.AVAILABILITY<br>O.DATA_BACKUP |

**Table 19 - Mapping of Security Objectives to Security Risks**

| Security Objective | Security Risks |
|---|---|
| O.PHYSICAL | R.PHYSICAL |
| O.RISK | R.SECPOLICY<br>R.RISKMAN<br>R.PERSONNEL<br>R.OPSMANAGE |
| O.NON_INTERFERENCE | R.INTEGRATE<br>R.OPSMANAGE |
| O.INTERCONNECTIVITY | R.CONNECT<br>R.ONLINE<br>R.CONTINUITY |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Security Risks |
|---|---|
| O.DATA_BACKUP | R.SECPOLICY<br>R.CONTINUITY |
| O.DATA_AUTHENTICATION | R.MANAGE<br>R.SECPOLICY<br>R.NETCOMMS<br>R.CONNECT<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE |
| O.CONTINUITY | R.ENVIRON<br>R.CONTINUITY |
| O.MANAGEMENT | R.MANAGE<br>R.SECPOLICY<br>R.ASSETCTRL<br>R.PERSONNEL<br>R.OPSMANAGE |
| O.MIGRATION | R.ASSETCTRL<br>R.INTEGRATE<br>R.OPSMANAGE |
| O.COMPLIANCE | R.SECPOLICY<br>R.COMPLY<br>R.CONNECT<br>R.INTERNET |
| O.3RDPARTY | R.MANAGE<br>R.SECPOLICY<br>R.INTEGRATE<br>R.REMOTE |
| O.REMOTE | R.SECPOLICY<br>R.CONNECT<br>R.REMOTE<br>R.ONLINE |


© Copyright 2004 National Institute of Standards & Technology

| Security Objective | Security Risks |
|---|---|
| O.ACCESS_CONTROL | R.RISKMAN<br>R.PERSONNEL<br>R.EVIL_ACCESS<br>R.NEED2KNOW<br>R.NETCOMMS |
| O.SECURE_COMMS | R.EVIL_ACCESS<br>R.NETCOMMS |
| O.DATA_INTEGRITY | R.RISKMAN<br>R.EVIL_ACCESS<br>R.REMOTE |
| O.CONFIDENTIALITY | R.NEED2KNOW<br>R.OPSMANAGE |
| O.AVAILABILITY | R.SECPOLICY<br>R.ENVIRON<br>R.CONTINUITY |
| O.SYSTEM_INTEGRITY | R.OPSMANAGE<br>R.EVIL_ACCESS<br>R.OPSMANAGE |
| O.SYSTEM_DIAGNOSTICS | R.OPSMANAGE |
| O.MONITORING | R.INTERNET<br>R.REMOTE<br>R.ONLINE<br>R.OPSMANAGE<br>R.IDS |
| O.AUDIT | R.MANAGE<br>R.ONLINE<br>R.IDS |
| O.IDS | R.IDS |


© Copyright 2004 National Institute of Standards & Technology

### 8.2.4 Sufficiency of the Security Objectives to counter identified Risks

Due to the generic nature of this SPP and the need for additional refinement of the sources of risk and the identified security objectives, sufficiency arguments have not been included. SPP/SST authors should note that additional rationale is required in order to demonstrate that the security objectives are sufficient to counter the identified security risks (refer to the application notes for guidance).

## 8.3 Security Requirements Rationale

### 8.3.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are suitable to meet the security objectives. Table 20 and Table 21 show that each security requirement is necessary, that is, each security objective is addressed by at least one security requirement and vice versa. Note that some objectives are partially satisfied by the STOE and partially satisfied by the IT environment. Security Objectives for the STOE are satisfied by security functional and assurance requirements. Security Objectives for the Environment are satisfied by IT requirements for the environment.

**Table 20 - Mapping of Security Objectives to Security Requirements**

| Security Objectives | Security Requirements |
|---|---|
| O.Boundary_Protection | FPT_PHP.1, FPT_PHP.2, FPT_PHP.3<br>FPT_PHP.4, PHY_SOB.1 |
| O.Risk | AVA_VLA.2<br>AMA_AMP.1<br>AMA_EVD.1 |
| O.Non_Interference | FTP_ITC.1 FTP_TRP.1, FPT_SEP.1<br>AVA_MSU.2 |
| O.Data_Backup | FDP_UIT.2, FPT_RCV.2, FPT_RCV.3, FPT_RCV.4, FPT_FLS.1, FPT_AMT.1, FPT_TST.1 |
| O.Data_Authentication | FIA_UAU.3, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FDP_DAU.2, FMT_MTD.1, FMT_SMR.1, FPT_RPL.1 |
| O.Continuity | P.Business_Continuity<br>FRU_FLT.1, FPT_FLS.1, FPT_RCV.5<br>FMT_SMF.1 |
| O.Verify | ATE_FUN.1, ATE_IND.2, ATE_AST.1, ADO_IGS.1, FPT_AMT.1, FPT_TST.1 |


© Copyright 2004 National Institute of Standards & Technology

| Security Objectives | Security Requirements |
|---|---|
| | ADO_IGS.1, FPT_AMT.1, FPT_TST.1 |
| O.Ownership | FMT_SMR.1, FMT_SMR.2, FMT_MOF.1, FMT_MOF.2, FMT_REV.1, FMT_SMF.1, P.Personnel, P.Infrastructure |
| O.Migration | P.Assurance_Maintenance<br>P.Personnel |
| O.Compliance | P.Policy_Procdures |
| O.Collaborate | P.Policy_Procedures |
| O.Access_Control | FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_UAU.1, FIA_UAU.2, FIA_UID.2, FMT_REV.1, FMT_MOF.2, FIA_AFL.1, FTP_TRP.1, FTA_TSE.1, FIA_SOS.1, FIA_SOS.2, FMT_SAE.1, FPT_STM.1, FPT_SEP |
| O.Comms_Integrity | FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_ITI.2, FPT_RCV.5, FPT_RPL.1, FPT_SSP.1, FPT_SSP.2, FPT_STM.1, FPT_TDC.1, FTP_ITC.1, FTP_TRP.1 FPT_TST.1, FDP_ETC.1, FDP_ETC.2, FDP_ITC.1, FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_IFF.1, FCS_COP.1, FCS_CKM.4, FMT_MOF.1, |


© Copyright 2004 National Institute of Standards & Technology

| Security Objectives | Security Requirements |
|---|---|
| O.Available | FPT_FLS.1, FPT_TRC.1, FPT_ITA.1, FRU_FLT.1, FRU_PRS.1, FRU_PRS.2 |
| O.Control_Integrity | FMT_MSA.1, FPT_TST.1, FPT_AMT.1, FPT_FLS.1 |
| O.Event_Monitor | FAU_ARP.1, FAU_SAA.1, FAU_SAA.2<br>FAU_SAA.3, FAU_SAA.4, FAU_SEL.1<br>FPT_ITI.1, FPT_ITI.2<br>FEM_EDI.1, FEM_EDI.2, FEM_EDI.3, FEM_EDI.4, FAU.GEN.1, FAU_GEN.2<br>FPT_TDC.1, FMT_SMF.1, FMT_SMR.1 |
| O.Event_Log | FAU_GEN.1, FAU_GEN.2, FAU_SEL.1<br>FAU_SAR.1, FAU_SAR.2, FAU_SAR.3,<br>FAU_STG.1, FAU_STG.2, FAU_STG.3, FAU_STG.4, FPT_STM |
| O.IDS | FAU_ARP.1 FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4, FPT_ITI.1, FPT_ITI.2, FEM_EDI.1, FEM_EDI.2 |

**Table 21 - Mapping of Security Requirements to Security Objectives**

| Requirements | Objective |
|---|---|
| FAU_ARP.1 | O.Event_Monitor |
| FAU_GEN.1 | O.Event_Monitor |
| FAU_GEN.2 | O.Event_Monitor |
| FAU_SAA.1 | O.Event_Monitor |
| FAU_SAA.2 | O.Event_Monitor |
| FAU_SAA.3 | O.Event_Monitor |
| FAU_SAA.4 | O.Event_Monitor |
| FAU_SEL.1 | O.Event_Monitor |
| FCS_CKM.4 | O.Comms_Integrity |
| FCS_COP.1 | O.Comms_Integrity |


© Copyright 2004 National Institute of Standards & Technology

| Requirements | Objective |
|---|---|
| FDP_ACC.1 | O.Access_Control |
| FDP_ACF.1 | O.Event_Monitor |
| FSP_DAU.2 | O.Data_Authentication |
| FDP_ETC.1 | O.Comms_Integrity |
| FDP_ETC.2 | O.Comms_Integrity |
| FDP_IFF.1 | O.Comms_Integrity<br>O.Access_Control |
| FDP_ITC.2 | O.Comms_Integrity |
| FDP_UCT.1 | O.Comms_Integrity |
| FDP_UIT.1 | O.Comms_Integrity |
| FDP_UIT.2 | O.Comms_Integrity<br>O.Data_Backup |
| FEM_EDI.1 | O.Event_Monitor |
| FEM_EDI.2 | O.Event_Monitor |
| FEM_EDI.3 | O.Event_Monitor |
| FEM_EDI.4 | O.Event_Monitor |
| FIA_AFL.1 | O.Access_Control |
| FIA_SOS.1 | O.Access_Control |
| FIA_SOS.2 | O.Access_Control |
| FIA_UAU.1 | O.Access_Control |
| FIA_UAU.2 | O.Access_Control |
| FIA_UAU.3 | O.Data_Authentication |
| FIA_UAU.4 | O.Data_Authentication |
| FIA_UAU.7 | O.Data_Authentication |
| FIA_UID.1 | O.Data_Authentication |


© Copyright 2004 National Institute of Standards & Technology

| Requirements | Objective |
|---|---|
| FIA_UID.2 | O.Access_Control |
| FMT_MOF.1 | O.Comms_Integrity<br>O.Ownership |
| FMT_MOF.2 | O.Access_Control<br>O.Ownership |
| FMT_MSA.1 | O.Control_Integrity |
| FMT_MTD.1 | O.Data_Authentication |
| FMT_REV.1 | O.Ownership |
| FMT_REV.2 | O.Access_Control |
| FMT_SAE.1 | O.Access_Control |
| FMT_SMF.1 | O.Event_Monitor<br>O.Ownership<br>O.Continuity |
| FMT_SMR.1 | O.Event_Monitor<br>O.Ownership<br>O.Data_Authentication |
| FMT_SMR.2 | O.Ownership |
| FPT_AMT.1 | O.Control_Integrity<br>O.Verify<br>O.Data_Backup |
| FPT_FLS.1 | O.Control_Integrity, O.Data_Backup<br>O.Available<br>O.Continuity |
| FPT_ITA.1 | O.Available |
| FPT_ITC.1 | O.Comms_Integrity |
| FPT_ITI.1 | O.Event_Monitor |
| FPT_ITI.2 | O.Event_Monitor |


© Copyright 2004 National Institute of Standards & Technology

| Requirements | Objective |
|---|---|
| FPT_PHP.1 | O.Boundary_Protection |
| FPT_PHP.2 | O.Boundary_Protection |
| FPT_PHP.3 | O.Boundary_Protection |
| FPT_PHP.4 | O.Boundary_Protection |
| FPT_RCV.2 | O.Data_Backup |
| FPT_RCV.3 | O.Data_Backup |
| FPT_RCV.4 | O.Data_Backup |
| FPT_RPL.1 | O.Comms_Integrity<br>O.Data_Authentication |
| FPT_SEP.1 | O.Non-Interference<br>O.Comms_Integrity |
| FPT_SSP.1 | O.Comms_Integrity |
| FPT_SSP.2 | O.Comms_Integrity |
| FPT_STM.1 | O.Comms_Integrity<br>O.Access_Control |
| FPT_TDC.1 | O.Event_Monitor |
| FPT_TRC.1 | O.Available |
| FPT_TST.1 | O.Control_Integrity<br>O.Verify<br>O.Data_Backup |
| FRU_FLT.1 | O.Available<br>O.Continuity |
| FRU_PRS.1 | O.Available |
| FRU_PRS.2 | O.Available |
| FTA_TSE.1 | O.Access_Control |
| FTP_ITC.1 | O.Comms_Integrity<br>O.Non-Interference |


© Copyright 2004 National Institute of Standards & Technology

| Requirements | Objective |
|---|---|
| FTP_TRP.1 | O.Comms_Integrity<br>O.Access_Control<br>O.Non-Interference |

### 8.3.2 Sufficiency of the Security Requirements

Due to the generic nature of this SPP and the need for additional refinement of the sources of risk and the identified security objectives, sufficiency arguments have not been included. SPP/SST authors should note that additional rationale is required in order to demonstrate that the security objectives are sufficient to counter the identified security risks (refer to the application notes for guidance).

### 8.3.3 Satisfaction of Dependencies

Due to the generic nature of this SPP and the need for additional refinement of the security requirements, a dependency analysis has not been included. SPP/SST authors should note that a dependency analysis is required in order to show that the dependencies between the security requirements have been addressed by the SPP/SST (refer to the application notes for guidance).

## 8.4 Rationale for Extensions

### 8.4.1 Augmentation for Assurance Background Information

This section provides the rationale for the inclusion of the explicit system assurance requirements, as noted in Table 18. An overview for each class will address from a security controls perspective, the contribution to system security provided by the noted assurance component(s).

#### 8.4.1.1 Class ASA: Security awareness

The need to communicate the security responsibilities expected of personnel can be supported with the development of complete and consistent documentation describing those expectations. Although, the ISO/IEC 15408 Part 3 AGD class could easily be interpreted to include the procedural security functions as well as the IT security functions, the provider and focus of the documentation is different. In a systems context, the usage documentation will contain specifics about the system that product documentation cannot.

The security policy and procedures documents class, PPD, provides the requirements for documentation describing security expectations, procedures and policies for personnel accessing the assets. The component(s) in this class are used to gain confidence that personnel are informed of those procedural expectations so that the security can be maintained.

#### 8.4.1.2 Class ASC System operational and management security controls


© Copyright 2004 National Institute of Standards & Technology

The ASC class is closely derived from the technical security control based assurance ASD class. Operational security is concerned with the physical, policy, procedural, personnel, and other organisational security control measures that are used in the operational environment to protect the STOE; as well as support its business function. For instance System support of degraded operations, as part of continuing business operations in response to natural or man-made events (see PBC in section 4). Management security is concerned with the provision of management and infrastructure support enable the operational security controls and technical security controls to effectively be used. The objective of this activity is to assess the completeness, accuracy, and usability of the system operational and management security controls components of the system, and to verify that the security and operational policies, procedures, organization and physical assets support the system security requirements that are allocated to them. This is achieved through examination of the policies and procedures and physical system control security attributes, and any associated design and configuration documentation. The latter becomes especially important if there is a direct interface to the IT part of the system security. This may also include observation and interviews with personnel to gain insight to the strength of the organization security infrastructure. As noted above, the PPD class will also contribute to confidence gained that personnel are informed of the system security related procedures.

#### 8.4.1.3 Class ACM: Configuration Management

The objective of Configuration Management during evaluation is to provide assurance that the evaluator has the correct version of all system components for the other evaluation activities. It applies therefore to measures within the development environment, not the operational environment. When the operational system is deployed, configuration management is a series of system capabilities allowing operational decision makers to control the configuration and changes to it. The most recent evaluation evolves to be the baseline, and will be maintained as such by the organization. Any proposed modifications, bug fixes, or system capability upgrades/enhancements will be controlled and evaluated against the most recent evaluated baseline, and that baseline will be updated accordingly. Additionally, operational and maintenance security controls will also be updated as necessary to respond to the changing threat and operational environment. These too will be evaluated from a system security impact perspective and changes will be controlled accordingly, as part of the system security configuration.

#### 8.4.1.4 Class ADO: Delivery and operation

The purpose of the system delivery and operation activity is to judge the adequacy of the documentation of the procedures used to ensure:

- That the system components can be delivered to the operating organization without modification;
- That the system can be accepted by the operating organization and that it is put under configuration control;
- That the system components can be installed, generated and started into an initial secure configuration that verifies interoperability between components;
- That the system can be configured to enforce the policies that govern day-to-day operations.


© Copyright 2004 National Institute of Standards & Technology

- Site interoperability can be ensured, such that the security relevant system, subsystem, external and component interfaces that comprise the System TOE, especially those to legacy security controls can be started up, and interoperate in a secure manner in the intended operational environment

The ADO_IGS documentation shall be used to assure that the system transition incorporating the patch, upgrade, or new components into the operational environment can be conducted transparently and without disruption to system availability and integrity.

#### 8.4.1.5 Class ASD: System Architecture, Design and Configuration Documentation

The ASD assurance class is closely derived from the ADV class in ISO/IEC 15408 Part 3. However, the necessary development and integration information appropriate for systems is different enough from those in the current status that it was determined that a separate class was appropriate avoid confusion.

The purpose of this class is to assess the completeness, coherency and consistency of the system architecture, design and operational configuration documentation and to verify that the system architecture, design and configuration reflect the security requirements allocated to the various subsystems and components of the system. This is achieved through examination of increasingly refined descriptions of the System Security Function (SSF) architecture, design and configuration documentation.

This class is closely related to the ADV assurance class for product design abstractions. However, because so many changes are needed to meet the needs of system level design, a complete new class is added. This may be merged at a later time with ADV but for now the differences are viewed significant enough that a new class is warranted.

#### 8.4.1.6 Class AGD Guidance documents

The purpose of the guidance document family is to judge the adequacy of the documentation describing the integration and operational use of the system. Such documentation includes that aimed at system integrators, trusted administrators and non-administrative users whose incorrect actions could adversely affect the security behaviour and characteristics of the system, as well as that aimed at normal users whose incorrect actions could adversely affect the ability of the system to provide the required protection capabilities for their own data.

Therefore, the AGD activity is closely related to the processes and procedures defined by the operational security requirements. The user and administrator guidance includes information regarding the technology aspects of the system as well as the operational and human processes of the system.

There are additional types of users in a distributed system, and their roles and responsibilities extend beyond the traditional user and administrator categories required user documentation.


© Copyright 2004 National Institute of Standards & Technology

Each of the user roles need to know both the technical and management and operational security controls needed to accomplish their business mission.

One of these users may be external systems that are considered outside the STOE. The critical issue is that if there is a component that interfaces with the STOE but for whatever reason the component is not part of the STOE, then it is necessary to:

a) Define the interfaces between the STOE and the external component;
b) Define the security properties, if any, that are provided by or that are provided across the interfaces,
c) Define how the STOE and external component will authenticate themselves to each other;
d) Define the secure method by which the STOE and the external component will communicate such that a security policy is enforced;
e) Define the security agreement between the parties with responsibility for operating the STOE and the external component to establish the business rules that govern how that interface is to be used and maintained over time.
f) Define the security relevant configuration parameters that allow implementation, integration, and enforcement of system security policies.

The guidance documents family applies to those functions and interfaces which are related to the security of the system as a whole. In principle, the notion of providing users 'all information necessary to maintain the security...' applies directly to system evaluations. However, in practice, a product administrator guide will provide instructions on how to change settings; in a system context the values to be set are decided so the administrator guidance will instruct on exactly how to configure the system to optimize security in its distributed environment. In addition, it could be that the AGD components cover all the evidence of security controls that require that users be made aware of policies and procedures because they provide the information required for the user to securely operate within and as part of the system.

It is often wrongly assumed that there would only be one guidance document for the system administrator, while in fact there could be multiple pieces of guidance for different administrator roles. This is particularly true in a distributed system context where different portions of the system may be administered and maintained by completely different roles. This may also apply to the operational user guidance - different types of users may be issued different guidance documents. In addition, the system integrator is considered a user of the system and requires detailed integration and check-out procedural guidance to ensure that any given component/product is securely integrated into the system.

#### 8.4.1.7 Class ALC Life cycle support

The purpose of the life-cycle support class is to judge the adequacy of the procedures used during the integration and operational life-cycle of the system. These procedures include the security measures used throughout system development (i.e., integration), the life-cycle model used by the integrator, and the tools used by the integrator throughout the life-cycle of the system.

The process of life cycle support is much more extensive, and increasingly important in a system context. This is due to the composition of a system being a collection of various products that are


© Copyright 2004 National Institute of Standards & Technology

integrated together to support business operations and security requirements that protect those operations. The system, which may be widely distributed, requires procedures to monitor and track the system from its inception as an operational entity, until it is securely retired from the organisation. System security controls need to be evaluated at regular intervals; and the system components tracked both from a parts obsolescence perspective, related supportability aspects, and modifications to increase functionality, replace obsolete parts, take advantage of more efficient technology, add a interface to another system, and respond to a new or different threat environment. In this regard, following the STOE's initial verification and authorisation for operation, ALC becomes inherently tightly coupled to AMA. ALC aspects may be considered more of a local issue, where the system is monitored for maintenance and performance. An example being that a bug may be found, or an obsolete part notification might be received from a vendor, or a software end of support life notice. These issues would be handled more informally with the vendor or by the system IT department. They may also be contractual obligations that drive the organisation's response, and the vendor's requirements. Whereas upgrading the STOE for a new capability, adding an interface, or response to a new threat, would be more broad brushed, and have a potentially greater impact on the System's security contribution, both from technical security and operational and management security controls perspective. The Life Cycle Development plan and procedures and the Assurance Maintenance Plan should complement and support each other. Any proposed or actual change would still require an impact analysis to ensure that the change will not have a negative impact to either system performance or functionality for business or security support.

As with ACM, once the system has been received and enters day-to-day operations, the system has to be entered into the organisation's configuration management and life cycle support systems. The system integrator then may play a prominent role in the day-to-day maintenance of the system in support of its operations. ALC and its product and development focused activities, would then literally transform to operations related activities that, in turn would closely track and support AMA activities.

As such, from operations assurance perspective, it is proposed that one family be introduced, ALC_OPS, from which the system would transition to (from ALC_DEV), following its introduction into day-to-day operations. ALC_FLR while germane for systems, the general responsibility becomes more organisation focused, with system integrator, or organisation IT personnel playing a larger role, and developer responsibilities being more contractual in nature. The premise for systems is that following the established procedure in the operational environment should provide greater confidence that evaluation results remain sound. However, the flaw correction and related information will still be subject to the impact analysis and evaluation process defined in AMA, as part of the continuous monitoring and change process.

#### 8.4.1.8 Class ATE Test

The purpose of this family is to verify that the system components, when installed, integrated and configured in accordance with the system architecture and system configuration evidence, meet the security functional requirements specified in the SST and are effective in enforcing the system security concept of operations. System architecture, integration and design documentation aid in test development and execution. This is accomplished by determining that the SSF has been


© Copyright 2004 National Institute of Standards & Technology

configured as specified by the configuration specification, tested against the relevant architecture and design evidence, by performing a sample of the developer's tests, and by independently testing a subset of the SSF.

The term 'test campaign' is used to denote the entirety of the test activities performed.

A system presents the following issues that are addressed by the test campaign:

a) Physical distribution of the system components;
b) Whether or not the system components have been evaluated. In the case where the component is evaluated, the differences between the evaluated configuration and the configuration of the component when used in the system context raises issues;
c) The impact of the specific operational environment and its contribution to assurance;
d) Achieving secure integration of system components through development of specialized functionality;
e) Varying levels of assurance allocated to different physical or logical components of the system.

The system evaluation test criteria accommodates the need for a flexible test campaign that provides for the following:

a) the availability of evaluated products and evidence about the products,
b) the degree of assurance desired for the various parts of the system,
c) the existence of specialised functionality to integrate components into the system and the degree of assurance required for that specialised functionality.
d) the specific configuration decisions that enable the system to implement the system security requirements and system security concept of operation.

#### *8.4.1.8.1 ATE_AST: AST Family - Testing the operational and management security controls*

System testing must address the operational and management security controls of the system in addition to the technical security control portion. The system introduces concerns for maintaining the system configuration on a day-to-day basis in response to a changing environment and the need for repeated vulnerability assessments to ensure that the system continues to provide effective countermeasures. This class addresses the testing of the operational and management security controls aspects of system security, and verifies its contribution to system security. The test effort is primarily two-fold; the first tests that there is a well-documented mapping of the policy, applicable procedures personnel and physical attributes of the organisation to the system TSF. Second that there is a testable, clear and unambiguous communications medium to status, exchange and report security information among the various security controls of the System.

### 8.4.1.9 Class AVA Vulnerability analysis


© Copyright 2004 National Institute of Standards & Technology

The purpose of the vulnerability assessment activity is to determine the existence and exploitability of flaws or weaknesses in the system as configured for, and implemented in its intended environment. This determination is based upon analysis performed by the developer and the evaluator, with inputs from the consumer; and is supported by evaluator testing.

Inherently, the AVA activity is closely related to the system security policy and procedures, physical security measures, personnel security, and having security infrastructure in place to effectively counter any system vulnerabilities. The system strength of security function encompasses all security controls aspects to ensure that the system remains secure and any breaches can be effectively countered.

The notion of vulnerability assessment is greatly expanded in a system context, due to the added complexity when compared to a product. The added system complexity not only can increase the vulnerability access points, but it also can increase potential ways to counter a vulnerability. This is because system security measures can be more robust because of the systems approach, which inherently encompasses a broader type set. Additionally, the system also encompasses operational and management security controls aspects, such as physical boundary monitoring, auditing mechanisms, and more extensive and better training of personnel to create a broader corporate atmosphere of security awareness. The vulnerability assessment activity should be conducted throughout the system life cycle to ensure that the security controls change, as needed, and remain effective in the changing threat environment.

#### 8.4.1.10 Class AMA Assurance maintenance

The purpose of the assurance maintenance activity is to assure that the system will continue to maintain its security assurance baseline as changes are made to the system itself or to its environment. Such changes may include new threats or vulnerabilities, changes to the system or environment that can have a security impact, changes in personnel, and modifications or changes to the system's external interfaces. This activity includes both technical and operational and management security controls elements.

The notion of assurance maintenance is pronounced in a system context because of the typical system complexity and incorporation of the mix of security controls features. Therefore, any change/modification/upgrade to any of the security components of the system will require an analysis to determine the impact to secure system operation itself; and to determine if an unrelated feature may have to be modified to contribute to system security, due to those changes.

The assurance maintenance activity is an ongoing activity that is applicable to any changes in the system environment that may impact security, throughout the system life cycle. These changes could range from a new facility intrusion detection system, to the addition of a new emergency generator that will be used by the system, to an additional external interface that the system must exchange data with. And in fact, an additional external interface to the system, would involve the definition of that interface, any new vulnerabilities that could be introduced via that interface, and both technical and operational and management security controls related documentation would necessarily need to be updated, driven by the system need to accommodate the new interface.


© Copyright 2004 National Institute of Standards & Technology

A change in the operational environment itself will necessitate an evaluation of security aspects of the system security baseline, and how best to accommodate that change. That change may be all-inclusive and impact the system as a whole, or it may impact a single domain of the system. In the latter case, existing system components may be able to accommodate the security aspects of the change, or by just tweaking the configuration to accommodate security aspects of the operational environment. There needs to be a change mechanism in place and documented in

AMA for a product is typically a developer function. However, that role will necessarily shift to the system owner for a system. This is due primarily to the interaction of technical and operational security controls of the system, especially when considering the operational security policies and procedures that will govern human behavior, which typically tends to evolve over time. The length and breadth of security controls system components, which includes event monitoring, augments system security but also necessarily increases the role of the system owner in support of this function.

## 8.5 Strength of Function Claims

This SPP does not include any strength of functions claims.


© Copyright 2004 National Institute of Standards & Technology

# Appendix A – Acronyms

| | |
|---|---|
| CC | Common Criteria |
| EAL | Evaluation Assurance Level |
| ICS | Industrial Control System |
| IT | Information Technology |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| PP | Protection Profile |
| PSF | Procedural, Policy, Personnel & Physical Security Functions |
| SF | Security Function |
| SFP | Security Function Policy |
| SOF | Strength of Function |
| SP | Special Publication |
| SPP | System Protection Profile |
| ST | Security Target |
| SST | System Security Target |
| STOE | System Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | Technical Security Functions |
| SSF | System Security Functions |
| TSFI | TSF Interface |
| TSP | TOE Security Policy |


© Copyright 2004 National Institute of Standards & Technology