

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

**Process Control
Security Requirements Forum
(PCSRF)**

Security Profile Specification (SPS)

26 August 2002

DRAFT

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

1	Introduction.....	4
4.1	Initiative Purpose	4
4.2	The Purpose of the SPS.....	5
4.3	The Scope of the SPS.....	6
4.4	Application of the SPS.....	7
4.5	Reading this Document.....	9
2	System Definition and Description.....	10
4.1	Section Overview.....	10
4.2	Control System (CS) Definition	10
3	Operational Security Environment	14
4.1	Section Overview.....	15
4.2	Secure Usage and Environment Assumptions	15
4.2.1	A.External_System_Functionality	16
4.2.2	A.Open_Control_System_Access.....	16
4.2.3	A.Network_Connectivity	17
4.2.4	A.Perimeter_Defense	17
4.2.5	A.Remote_Access	17
4.2.6	A.Physical_Security_Sophistication.....	17
4.2.7	A.Accessible_Comm_Medium.....	18
4.2.8	A.Secureable_Comm	18
4.2.9	A.Safety_Dependency	19
4.3	Vulnerabilities.....	19
4.4	Regulatory Mandates & Policy.....	21
4	Security Policy and Control System Mechanism Implementation Objectives	23
4.1	Policy Objectives Governing the Acquisition, Development and Continuous Operation of Control Systems.....	23
4.2.1	DM-PO.Business_Continuity	23
4.2.2	DM-PO.Regulatory_Compliance.....	24
4.2.3	DM-PO.Risk_Assessment	24
4.2.4	DM-PO.Security_System_Verification	24
4.2.5	DM-PO.Migration_Strategy	25
4.2.6	DM-PO.Collaborative_Working_Relationships.....	25
4.2.7	DM-PO.Security_Ownership.....	26
4.2	Control System Functionality Objectives	27
4.2.1	CSO.Non_Interference.....	27
4.2.2	CSO.Security_Override	27
4.2.3	DM-CSO.Access_Control	27
4.2.4	DM-CSO.Communications_Integrity	29
4.2.5	DM-CSO.Control_System_Integrity	30
4.2.6	DM-CSO.Event_Trace.....	30

DRAFT

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

4.2.7 DM-CSO.Intrusion_Detection_Response..... 31
4.2.8 DM-CSO.Operational_Configuration_Integrity..... 32

Process Control System Component Security Profile Specification (SPS) August 2002

1 Introduction

5 *Objective: This section introduces and describes this security specification document in terms of its purpose, content, intended usage and application. The technically focused material introduced in this section will be expanded in the System Definition and Description Section.*

4.1 Initiative Purpose

10 The National Information Assurance Partnership (NIAP – partnership between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST)), as part of the Critical Infrastructure Protection Program, provides technical support and guidance to industry to improve the information technology security posture of the systems and supporting operations that comprise the US national critical
15 information infrastructure. One component of this effort addresses the IT security for the networked digital process control systems used to support industrial applications. The NIST Intelligent Systems Division of the Manufacturing Engineering Laboratory, the NIST Information Technology Laboratory and the NIST Electrical and Electronics Engineering Laboratory are working with industry to incorporate end-to-end security engineering into the life-cycle processes of process control systems and the components
20 that comprise such systems.¹

25 The goal of this effort is the development of security specifications that characterize or establish a *profile* of the security functions and mechanisms that must be implemented into components that comprise process control systems. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF), an industry group organized under the NIAP umbrella. The outcome of this work will be the development and dissemination of best practices and ultimately security standards that will be used in the acquisition, development, and retrofit of industrial control systems.

30 The PCSRF is a working group comprised of representative organizations from the various sectors that make up the US process control industry and the vendors that design, develop, and integrate components and systems for the industry. The PCSRF is working with security professionals to assess the vulnerabilities and establish appropriate

¹ End-to-end security engineering in life-cycle processes refers to defining criteria that establishes a basis for the following activities: definition of acquisition requirements; definition of development and integration requirements; definition of verification processes such as certification and accreditation to ensure that solutions are appropriately matched with the operating environment; and the definition of ongoing assessment and adjustment activities to ensure that the desired level of security is maintained as systems evolve through upgrades and replacements due to either technology changes or changes resulting from new threats in the operating environment.

Process Control System Component Security Profile Specification (SPS) August 2002

35 strategies for the development of policies and countermeasures that the U.S. process
controls industry can employ through a combination of technology and procedural
mechanisms to reduce residual risk to an acceptable level.

40 The requirements specification framework defined by the Common Criteria for
Information Technology Security Evaluation², is being used to document the results of
this effort in the form of Common Criteria Protection Profile security specifications.

4.2 The Purpose of the SPS

45 The process for development of a CC-compliant protection profile involves conducting
the following activities:

- 50 • **Statement of the Security Problem:** Information about the control system, about
vulnerabilities that exist in the technologies employed by the control system and
about the operational context in which the control system is used must be
collected and analyzed. The analysis supports development of a complete and
precise statement of the security problem that is to be solved. The security
problem is stated in terms of threats that must be countered and mandated policies
that must be enforced. The threat and policy statements are made in the context
of assumptions regarding the intended operational environment and intended use
of the control system that is described.
- 55 • **Statement of the Solution to the Security Problem:** The protection
mechanisms³ regarded as necessary and sufficient to address the stated security
problem are identified and described. The protection mechanisms can be stated in
varying degrees of specificity; starting with a high-level statement of objectives,
60 followed by intermediate-level statements of functional and assurance
requirements, and finally low-level statements describing the implemented
functions and assurance measures⁴.
- 65 • **Substantiation of the Solution:** There will be complete traceability between the
statements of the security problem down to the statements of the security solution.

² Also known as ISO/IEC 15408

³ A protection mechanism may be implemented through a combination of technology based (i.e. computer-based) mechanisms and procedural functions. With regard to computer based mechanisms, they may in turn be implemented in any combination of hardware, software or firmware.

⁴ The low-level statements appear only in a Security Target as the Security Target provides an “as-built” description that includes all implementation details. This differs from a Protection Profile because the Protection Profile serves to “characterize” a potential solution and is therefore absent of implementation details.

Process Control System Component Security Profile Specification (SPS) August 2002

There will also be discussion that substantiates and justifies the decisions made throughout the specification development process to illustrate that the required functionality and assurance measures (i.e., the security solution) are in fact appropriate, necessary and sufficient to solve the stated security problem.

70

This process, once completed, results in a significant amount of information that must then be organized for presentation to support the development and verification activities that follow. The Common Criteria defines a security specification framework (called a Protection Profile) that is a standard template for organizing and related this information.

75

The CC also provides a catalog of criteria to articulate the requirements that describe the security solution in terms of developed functionality and applied assurance measures. This framework also includes PP verification criteria; a set of checks and balances, that allows for verification that the PP document contains information and that it is properly organized and presented⁵.

80

The SPS is not a protection profile. Rather than to work directly within the context of the CC's language and constructs, the PCSRF will focus on developing and documenting requirements using the language of the various process control industry operating domains and in that regard, to generate an intermediate *Security Profile Specification* (SPS) which will be translated into one or more CC-compliant protection profiles after the requirements are validated.

85

One key distinction between the SPS and PP is that a PP focuses exclusively on the security functions and mechanisms. This SPS may include additional information such as safety-critical and performance information. This additional information will help to identify additional security-relevant information that if incorporated into the resultant protection profile will yield a more comprehensive and complete security specification.

90

4.3 The Scope of the SPS⁶

95

This security profile specification defines the security criteria applicable to a Process Control System (hereafter referred to as a Control System (CS)) that is employed in those

⁵ The CC does not contain checks and balances to validate the security problem or solution. In other words, the CC does not address determining that the security problem is an accurate reflection of reality and that the security solution is achievable, cost-effective, meaningful, etc. That effort is left to the organization that drafts the PP document – not the organization the conducts the PP evaluation.

⁶ Notice that the scope as currently defined excludes everything that is not part of the control system. The scope does not exclude interfaces to other systems, but does exclude the processing on those systems. This issue must be revisited as discussion tends to bleed over to include the non-control system components and more specifically, the security issues inherent to those components and their operation.

DRAFT

Process Control System Component Security Profile Specification (SPS) August 2002

industries regarded as a component of the national critical information infrastructure. Candidate industries include the electric utilities, discrete parts manufacturing, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals and mining.

A CS can be characterized as a distributed collection of components that provide the following basic functions to control a complex process:

- Measurement – data collection
- Control – data assessment, information generation and response determination
- Manipulation – response execution
- Human-machine interface – processing of inputs from and presentation of information to human operators

The functions described above are referred to as continuous steady-state functions. The purpose of the SPS is to define what must be done for the control system to remain in a *secure* continuous steady-state. However, such functionality is not enough; there must be corresponding functions that transition the control system from a *secure* dormant state to its *secure* continuous steady-state⁷ and functions that transition the control system from a *secure* continuous steady-state to a *secure* shutdown state. These functions can be categorized as:

- Startup, initial condition or set-point establishment
- System and process behavior management controls, discrete event logging, configuration and component maintenance and changes
- Shutdown, backup and recovery

This specification addresses the above in the context of the security functionality that must be present to enable the continuous secure execution of the control system in governing the process that is being controlled. This specification simply makes an argument for security requirements to address the defined security problem, and in that respect and that respect alone, is a stand-alone document. To fully understand how the defined security functionality relates to the control system in a general sense, this document (and its derivatives) must be developed, applied, and maintained in conjunction with relevant functional, performance, and safety specifications.

4.4 Application of the SPS

⁷ It is likely that can be more than one secure steady-state, for example, an operational state used for day-to-day continuous operation and a maintenance state used for upgrading components.

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

135 This SPS is developed as an intermediate step in crafting a set of CC-compliant PPs. The
SPS will serve to

- 140 a. Support the argument for and establishment of minimal security criteria
that is applicable across all process control industries boundaries
- b. Support the establishment of minimal security criteria applicable in the
context of a single process control industry
- 145 c. Support the development of guidance to the process control industries and
operating facilities for the development of unique security criteria to
support their control system life-cycle.

The PPs derived from this specification may be applied in one or more of the following
roles:

150

Acquisition Vehicle – There are two contexts in which a security specification may serve
the acquisition process:

- 155 a. Statement of required security functionality – In this context, the specification
would serve as the basis for communicating the minimal required security
functionality that must exist in candidate products. The vendor community would
develop components that incorporated the security functionality defined by the
specification.
- 160 b. Criteria to gauge sufficiency of available products – In this context the
specification serves as the basis for determining how close a candidate product
comes to matching the required security functionality.

165 **Verification of Compliance** – There are several contexts in which the security
specification would serve as a basis for determining the correctness of an
implementation:

- 170 • Evaluation at the component level – The evaluation would serve to
substantiate the correctness of the implementation of a well-defined set of
security functions and mechanisms.
- Certification at the system level – The certification would serve to substantiate
the correctness and suitability of the implementation for a well defined set of
security functions within a well-defined operational environment and
175 operational context.

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

4.5 Reading this Document

180 This document is going through its early development stage. The information presented
reflects various viewpoints, issues and concerns as presented by the various stakeholders
from the various process control industries. Through review and tailoring, the goal is for
this document to capture the necessary and relevant information to allow these various
stakeholders to communicate across their individual viewpoints.

185 This document also contains information that provides guidance, raises issues and is
intended to prompt thought and to force resolution by the stakeholders. All such text will
be preceded by the term “Application Note” and will be presented in *an italicized font* to
allow distinguishing the text from the main document text. Over time and as the
document matures, these application notes will change function to be application notes
190 for the end users of the specification: the acquisition users, the vendor community, the
control system integrators, and the control system operational users.

Process Control System Component Security Profile Specification (SPS) August 2002

2 System Definition and Description

195 *Objective: This section defines control system concepts and components. This section
also places the control system in context with its operational environment
to include its interfaces with other systems.*

4.1 Section Overview

200 The intent of this section is to define the components of a control system in an abstract
manner such that the discussion that follows in subsequent sections may be applied
regardless of the physical or technology attributes of specific control system vendor
products. This specification does not focus on the detailed security capabilities of those
systems and their components that exist in the control system facility do not provide
205 control system functionality. Examples of these systems include managerial and office
automation systems. This section does address the security requirements for the
interfaces between the control system and these systems to ensure that such interfaces
have inherent security capabilities to secure the interface communications.

210 *Application Note: The above statement is not absolute – the control system may be defined to
include other systems or components that do not directly provide control
over some process. Broadening the scope control system definition beyond
what is presented above adds complexity to the process of developing the
specification. It is recommended that consideration for expanding the above
215 basis is not made until after consensus is reached in defining those
components that are necessary to minimally define a control system.*

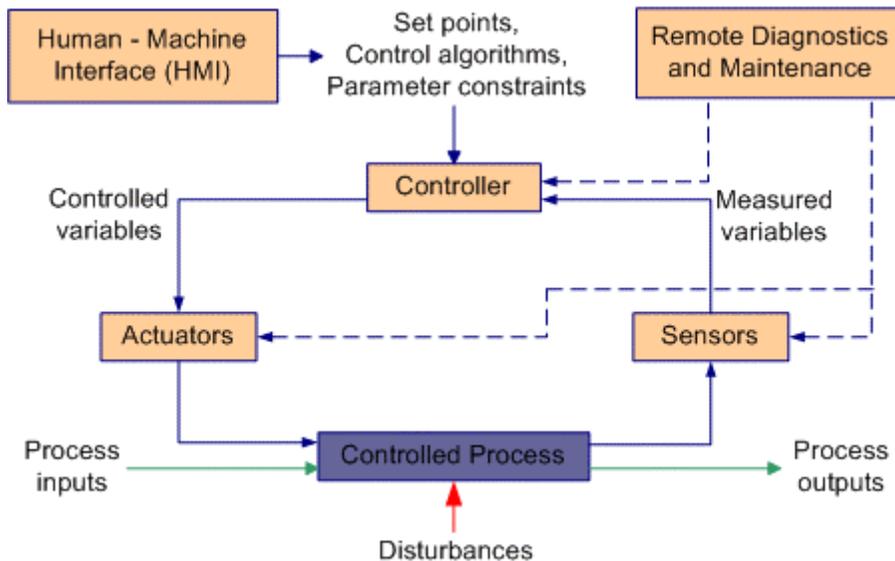
4.2 Control System (CS) Definition ⁸

220 A CS is comprised of a collection of discrete component types that are integrated together
to manage an industrial production, transmission, or distribution process. These
components may be categorized in terms of the fundamental function they provide within
the CS, such as a controller, sensor, transmitter or actuator. These components may be
further characterized in terms of their basis for operation, which may be mechanical,
pneumatic, hydraulic, electrical or electronic means. An additional categorization may be
225 made when these fundamental functions are integrated together to provide multiple
functions within a single physical housing, such as the combining of a sensor and
transmitter function into a single physical unit.

⁸ This section exists for informational purposes to establish a context for the definition of the CS. In that regard the issues of CS system definition are identified so that reviewers can provide comments from a consistent basis. The conclusion that we can ignore the nomenclature of PLC vs. DCS vs. SCADA must be verified as a correct assertion.

Process Control System Component Security Profile Specification (SPS) August 2002

230 The key control components of an industrial control system, including the control loop,
the human machine interface (HMI), and remote diagnostics and maintenance utilities,
are shown in Figure 1. A control loop consists of sensors for measurement, control
hardware, process actuators, and communication of process variables. Measurement
variables are transmitted to the controller from the process variable sensors. The
controller interprets the signals and generates corresponding control signals that it
transmits to the process actuators. This results in new values of the process variables and
235 the sensors transmit revised signals back to the controller. The human-machine interface
allows a control engineer or operator to configure set points, control algorithms and
parameters in the controller. The HMI also provides displays of process status
information, including alarms and other means of notifying the operator of malfunctions.
Diagnostic and maintenance tools often made available via modems and Internet enabled
240 interfaces allow control engineers, operators and vendors to monitor and change
controller, actuator, and sensor properties from remote locations. A typical industrial
system contains a proliferation of control loops, HMIs and Remote Diagnostics and
Maintenance tools built on an array of network protocols. Supervisory level loops and
lower level loops operate continuously over the duration of a process at cycle times
245 ranging on the order of minutes to milliseconds.



250 Figure 1 Key Control Components

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

In a large enterprise, there may be several geographically distributed industrial plants. Enterprise business operations can access plant information over the Internet or in some cases over a wide area network (WAN). The local area network (LAN) of a processing plant services the all of the operations within the plant while the actual control system of the plant sits on what has historically been a somewhat isolated peer-to-peer network. The systems at these levels can be categorized into two primary types of supervisory based control schemes, Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition Systems (SCADA). DCS are used to control large, complex processes such as power plants or refineries, typically at a single site. SCADA systems are used to control (perhaps) less complex, but more dispersed assets where centralized data acquisition is as important as control. Typically distribution operations of water systems, gas pipelines, and electrical transmission lines use SCADA systems. Generic industrial control system network architectures are shown for both DCS and SCADA based control schemes in the Appendices. A glossary of terms describing the components found in the diagram also can be found in the Appendix of this document.

Despite the different nomenclature, the underlying concepts, components, and functions of DCS and SCADA systems are the same. Therefore, the target of this specification is a CS in an abstract sense – it might be a DCS, a SCADA system, some combination of these or other configurations. The CS is characterized by components that record information, monitor information, transmit information, receive information or determine and issue command sequences. The goal of this SPS is to capture the relevant vulnerabilities based upon this abstract representation of the CS. Basing all discussion on that which is fundamental to the problem to be solved may alleviate the difficulty posed by the nomenclature used to define specific components that comprise a CS.

Application Note: This section exists for informational purposes to establish a context for all information presented in subsequent sections of the specification. This section is of utmost importance and it will undergo continuous change as the remainder of the document undergoes change.

In that regard the issues of CS system definition are presented for PCSRF reviewers to comment from a consistent basis. The comments required include confirmation that the preceding paragraphs are accurate and relevant and recommendation for additional material that is missing.

The scope of this security profile specification is therefore limited to the identified components of a CS that provide or utilize functionality characterized as follows:

Application Note: The final text of this section will be based upon the explicit threats and policies defined in the Operational Security Environment section. But, we need to establish context within which we can define the explicit statements.

DRAFT

Process Control System Component Security Profile Specification (SPS) August 2002

295 *So for now, we will focus on the components of the control system and the
functionality that is required to secure those components.*

- **Information Flow**

300 Information flow is the movement of data between two uniquely identifiable points
via a communication medium during which there may be digital pre or post
processing of the data.

305 *Application Note: The focus is on basic movement of data as opposed to focusing on what
type of data comprises the information flow. There may be multiple
information flows over the same physical channel, and if it is necessary
to distinguish between the various types of data and their logical flows,
then the SPS will do so.*

310 *The focus is also not on the form of communication media – e.g., wired,
wireless, unless there are specific criteria that apply only in the context
of a type of communication media.*

315 *Issues of concern are ensuring the correctness (integrity) and
availability of the data within bounds to ensure that there is no
disruption of the process managed by the control system (i.e., the
integrity of the control system process).*

- **Authenticated Access Control**

320 Authenticated access control requires that access to a uniquely identifiable component
by an identifiable agent occurs only if a defined set of rules authorizes the access.

325 *Application Note: An agent is defined as a human entity or active digital entity (process,
message, mobile code, etc.).*

330 *There are two concepts key to this term: 1) the identify of the agent must
be authenticated and 2) there are well defined rules that govern the
decision to grant or deny access.*

335 *This concept has been softened to not require uniquely identifiable
agents since role-based access may be appropriate in some cases. It
may be the case that there are both role-based and individual-based
authenticated access to control system resources.*

Also note that the components must be uniquely identifiable.

Process Control System Component Security Profile Specification (SPS) August 2002

- **Management Controls**

340 Management controls requires the definition of data and functions that support the
operation of the control system. Based upon those definitions, there is also the
definition of management controls and the allocation of authority to invoke the
management controls.

345 *Application Note: This discussion links to the authenticated access controls. From the*
security function standpoint, the access to a control system resource
includes access to the functions that control the behavior of the control
system itself. Therefore, using the authenticated access control
350 *discussion that precedes this, the management controls may be accessed*
by role or by individual.

- **Status Monitoring**

355 Status monitoring is the generation and collection of event information to support
manual and automated processes that maintain CS operation within defined
operational, safety and security parameters.

Application Note: Status monitoring may be used to support detection of possible policy
violations based upon the recorded events. Such would be the case
360 *should intrusion detection-like capability be part of the SPS.*

- **Control System Continuous Operation**

365 Control system continuous operation includes those capabilities that ensure the
integrity and availability of the security functions implemented into the control
system.

Application Note: This is not runtime controls for the operator. This is the self-protection
mechanisms built into the control system to protect itself from trusted
370 *and untrusted users and devices. Some are more esoteric and hidden*
from the user (memory protection domains implemented by the
hardware) but others are more visible (redundancy and fail-over).

3 **Operational Security Environment**

375

Objective: This section describes the security problem that is to be solved in terms of
the operational environment in which the control system will be placed

Process Control System Component Security Profile Specification (SPS) August 2002

and how the control system is intended to be used within that operational environment.

380 4.1 Section Overview

Application Note: The security problem that must be addressed by process control system components and its operational environment is defined in terms of

385 ○ *Assumptions – The assumptions regarding the intended operational environment serve to bound the problem space and problem definition. They are expressed relative to the physical and computer operating environment, the technology employed in control systems and the common and unique aspects of the varying process control industries that will make use of this specification.*

390 ○ *Vulnerabilities – Statement of vulnerabilities are made within the context of the stated assumptions. Vulnerabilities apply to the control system as well as to the systems to which the control system interfaces and the physical procedures that govern the use of the control system. The scope for definition of vulnerabilities should be initially broad-based to prevent pre-mature elimination of a legitimate concern.*

395 ○ *Regulatory Mandates & Policy – Mandates, policies or directives that govern the use and application of control systems are stated since they may require mechanisms to support the enforcement of the criteria. The scope of regulatory constraints to be considered overlaps the scope discussed for identification of vulnerabilities⁹.*

400

4.2 Secure Usage and Environment Assumptions

405 The following assumptions are made regarding the intended use of the CS and the operational environment in which the CS shall be used:

410 *Application Note: This is currently more of an “all-inclusive” list of issues that are relevant but not necessarily appropriate for this specification. We will not be able to answer the question of keep/discard until we get more substance to the document. Note also that some of these statements may be better stated in the form of policy or may be restated in the form of vulnerabilities of the PCS from which we can derive threat statements.*

⁹ This overlap exists because policy statements are supposed to be derived from an assessment of existing vulnerabilities.

Process Control System Component Security Profile Specification (SPS) August 2002

415 *Some of the assumptions exist simply to highlight issues and invite
discussion. They are not expected to remain in their current form or to
remain at all.*

4.2.1 A.External_System_Functionality

420 This specification does not levy security requirements on system components that
interface with the control system but that are not directly responsible for controlling
the process managed by the control system.

425 *Application Note: This assumption is intended to distinguish between the control system
and some external system that interfaces with the control system. The
security functionality of the external system is not defined by the SPS.*

430 *This assumption does not preclude specifying the security behavior over
the interfaces between the control system and an external system.*

435 *As an example, the security capability of a firewall that protects the
network interfaces between the control system and systems on another
network is not part of the SPS. The interface requirements for
communicating with the firewall are part of the SPS.*

4.2.2 A.Open_Control_System_Access

440 Within a process control facility, control system components may be directly or
indirectly accessible to individuals that are granted access areas in which control
system components are contained.

445 *Application Note: We are assuming that authorization to be in the facility implies that
opportunity exists to access the control system. Such access may be
possible via direct interaction to control system components or via
indirect access via the facility network infrastructure.*

450 *If this assumption is valid then it implies vulnerabilities that must be
addressed through some combination of procedure or mechanism.*

450 *Realize that this assumption may be true only in some cases within a
facility. For example, can we make a distinction between the control
room and other locations within the facility where control system
components reside?*

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

455 **4.2.3 A.Network_Connectivity**

The control system network is integrated with other system networks to include connectivity to the Internet.

460 *Application Note: The implication is that the control system may be accessed via an external internet connection and that internal access to the control system is possible from other facility networks. Again, this is an assumption that if found to be true, must be restated in the form of the vulnerabilities resulting from the decision to network the systems.*

465

4.2.4 A.Perimeter_Defense

470 The control system operations facility will have effective protection mechanisms in place to control access to the control system from a device not located on the control system network.

Application Note: Is this a fair assumption as such protection mechanisms may include firewalls, filtering routers and intrusion detection systems?

475 *An alternative is to address this as a vulnerability and then demand, via policy, that such protection measures are put in place by the organization with responsibility for securing access to the control system.*

480 **4.2.5 A.Remote_Access**

Remote access to control system components is available to product vendor personnel and personnel employed at the process control facility.

485 *Application Note: Again, this is an assumption that implies we have a problem that must be solved. If it is determined that this statement is valid, then the issue is to be addressed as either the vulnerabilities associated with remote access or through policy for secure remote access.*

490 **4.2.6 A.Physical_Security_Sophistication**

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

The degree of physical protection provided to control system components, excluding communication medium, is largely a function of the specific process being controlled and the characteristics of the physical location of the components.

495

Application Note: This assumption, while perhaps truthful, introduces a problem that must be addressed. This is a good statement but it really serves to force the definition of what the degrees of physical protection might be and how they are allocated within an industry.

500

If this SPS were to address all industries, then the statement is valid. But should the SPS be specific to a particular industry, then it is expected for that SPS to have the details of physical protection documented.

505 **4.2.7 A.Accessible_Comm_Medium**

There is no physical protection of control systems communication mediums. There are no security services provided by the communications infrastructure for the control system components.

510

Application Note: There are no expectations for communication mediums to be secure. There are also no expectations that any security may be derived from components that implement the communications infrastructure.

515

This assumption must be validated. Should this assumption hold, then the vulnerabilities resulting from lack of secure communication medium must be stated.

520 **4.2.8 A.Secureable_Comm**

Only the following types of control system communications are addressed by this SPS ...

525

Application Note: Various forms of control system communications have been discussed. It is not practical to put all control system communications in one group and then to try and secure them across-the-board. What is required is the clear statement of the types of control system communication that will be secured. This assumption attempts to do that.

530

At the August PCSRF meeting, there was reservation regarding the content of the following statement:

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

535 *CS components that employ data communications protocols including Ethernet, TCP/IP, FieldBus, RS-232 serial are subject to the criteria contained in this specification.*

The scope of the required protection mechanisms must be clearly stated. Any other protocols or communication medium used by the process control industry for which protection is required must be listed.

540 *This is not an assumption that will be kept. Once assessed, the specific protocols will be incorporated into appropriate policy and threat statements.*

545 **4.2.9 A.Safety_Dependency**

There are security vulnerabilities that if exploited will result in violation of safety criteria¹⁰

550 *Application Note: Although it is agreed that this is a true statement, there was reservation about the statement. The concern must be documented so that this general statement may be interpreted properly within the various industries.*

555 *Better yet – should there be clear distinction made by the various industries, then such should be fully documented as a means of information sharing between the industries.*

560 *Where we can define specific references then we must. Since safety policy and mandated controls are in place – the failure to properly secure the system may result in the inability to maintain safe operations.*

4.3 Vulnerabilities

565 *Application Note: Computer security has not been a priority issue within the control system community. Control systems were designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and employed communications protocols based on proprietary implementations. The adoption of communications protocols based on international standards, applications utilizing Internet technology and commercial off-the-shelf hardware and software by the control system industry has resulted in*
570 *increased exposure and vulnerability to those with intent to disable or*

¹⁰ Reference safety guidance

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

disrupt the operation of control system components. As such, control systems routinely operate within and are susceptible to the same threat environment as the more general enterprise IT business systems.

575

It is a difficult task to define a single cohesive set of vulnerabilities applicable to all process control industries. While there is commonality of equipment used in different process control industries and the same equipment can essentially be used for any application in any industry, there is variation in how the control strategy of a specific control system is configured. Even within a single process control industry, the variation in methods of operations, equipment and technology employed, and control strategy used tends to skew assessment perspectives. This results in focus given to a single control system “at hand” rather than to address the problem at a higher and more abstract level.

580

585

In response to this, the following approach is used to collect information for definition of across-the-board vulnerabilities:

590

- *Each representative process control industry will characterize the vulnerabilities in their operating environment based on an abstract view of the control system they operate. This abstract view is intended to reduce the complexity inherent to the various technologies and communications mediums that exist in a control system. The abstract view will be based on a characterization of the control system in terms of its components and communication mediums employed.*

595

600

- *The result of the individual process control industry efforts to identify vulnerabilities will be analyzed and then consolidated into a comprehensive statement of vulnerabilities. The anticipated output of this consolidation would be the following:*

605

- *Statement of vulnerabilities common across all process control industries*
- *Statement of vulnerabilities unique to a single process control industry*
- *Statement of vulnerabilities that are unique to local decisions for employing and operating control system components*

610

The identification of vulnerabilities to which a control system is exposed requires consideration of the following factors:

615

- Intended operational environment of the control system

DRAFT

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

- Purpose, function and use of the control system
- Technology employed in control system components
- Communication medium employed to network control system components
- Human agents with intent to disrupt, destroy or incapacitate control system operation
- 620 • Natural disaster events that may disrupt, destroy or incapacitate control system operation

The following statements provide a characterization of the vulnerabilities that may be exploited for the intent of disrupting or otherwise preventing a control system from accomplishing its designed intent.

- 625 • Information flows between control system components are subject to interception and analysis.
- Information flows between control system components are subject to interception and replay.
- 630 • Information flows between control system components are subject to interception and modification and replacement.
- 635 • Information flows between control system components may be inserted.
- Executable code may be uploaded to a control system component.
- Control system components with responsibility for supervisory or control functionality have a security failure mode with safety-critical implications.
- 640 • A control system component with responsibility for supervisory or control functionality is unable to detect actual control system component failure or degraded mode operation. The inability to detect such a state may be due to the lack of state, trend-indicating, or other information that conveys the status of control system component integrity.
- 645

Application Note: The above statements are a first cut at characterizing general vulnerabilities in an abstract manner. Each statement should be considered in the context of a specific industry and in terms of each major component type that is integrated into a control system.

650

4.4 Regulatory Mandates & Policy

Application Note: Policy statements establish mandatory constraints imposed by governmental, industry-specific or other controlling entities with respect to:

655

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

660

- *Certification and accreditation criteria*
- *Limitations and constraints on the operations of the control system*
- *Safety-critical policy that has security implications*
- *Others ...*

This section should contain relevant material from actual policies rather than abstract statements of what should be stated in policy.

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

**4 Security Policy and Control System Mechanism
Implementation Objectives**

665

Objective: This section provides a high-level statement of the needs that must be met by a compliant control system. The statement is made in terms of the physical and procedure needs as well as the computer-based mechanisms that must be designed, developed and integrated into the control system.

670

This section documents the Policy Objectives (PO) and Control System Objectives (CSO) that must be met by a compliant control system.

4.1 Policy Objectives Governing the Acquisition, Development and Continuous Operation of Control Systems

675

These policies have been defined based upon analysis of the information collected through interaction with individual control system industries. The information reflected is tagged to indicate the source industry (e.g., DM-PO). Statements without industry tags are based on input not specific to any one industry (e.g., PO). The tags used are¹¹:

680

- DM-PO – Discrete Parts Manufacturing

4.2.1 DM-PO.Business_Continuity

685

- A control system business continuity policy shall be defined to identify, plan for and respond to events effecting the continuous operations of an installed control system.

690

Application Note: The policy should address knowing what can happen, what the implications are when something happens, and what to do when those events happen. These issues are largely outside the scope of detailed security criteria (other than fail-secure, automatic recovery) and are also largely enforced through non-technology-based procedural means. The connection to the security criteria is in the need for total system certification testing which would include the verification of any mechanisms of the control system that support the business continuity policy.

695

¹¹ Only one tag because we have interacted with only one process control industry to-date.

**Process Control System Component Security Profile Specification (SPS)
August 2002**

700 **4.2.2 DM-PO.Regulatory_Compliance**

- The control system shall be operated in compliance with relevant governing mandates.

705 *Application Note: The issue of ensuring compliance with regulatory mandates requires*
identification of such mandates and the assessment of how to incorporate
the appropriate language in the requirements spec to ensure that such
710 *compliance may be demonstrated. Specifically, issues governing*
electronic information, signatures, etc. exist (21 CFR Part 11?), and
there may be others. More information is required to understand the
scope and context of such regulatory material.

4.2.3 DM-PO.Risk_Assessment

- 715
- Risk assessment shall be conducted such that:
 - The control system general operating environment and application of security technology is periodically updated,
 - The results of the risk assessment are relevant to and are applied throughout the control system life cycle process,
 - A documented and approved risk assessment process is followed.
- 720

725 *Application Note: The issue is that the risk assessment activity must be done on a*
periodic basis and the results utilized throughout the system
development and operational life-cycles.

4.2.4 DM-PO.Security_System_Verification

- 730
- The control system components and control system as an integrated unit shall undergo verification analysis and testing to ensure that the control system
 - Meets its design specification
 - Is properly installed and integrated
 - Is properly configured per operational policies
- 735

Application Note: The issue is what must be done to determine that the solutions being sought actually serve to solve the problem. This is not a

Process Control System Component Security Profile Specification (SPS) August 2002

740 *specification development issue – this is an issue regarding the
establishment of a strategy within which one such activity is the
development, validation and verification of the specification.*

4.2.5 DM-PO.Migration_Strategy

- 745 • A migration strategy shall be developed to govern the evolution of the control
system throughout its operational life-cycle. The migration strategy shall address
at a minimum:
- 750 1. Definition and continuous maintenance of the current system state
(components, configuration, etc).
- 755 2. The integration between computer implemented and personnel implemented
procedures
- 755 • A verification plan shall be developed to ensure
- that the migration strategy is being executed properly
 - that the migration strategy is accurately defined
- 760 • The migration strategy shall be refined in response to findings during the
execution of the verification plan.

*Application Note: The issue is that there must be a process followed to take a system from
a given operational state to some other operational state. Several
implications are found in this statement:*

- 765 • *determining that the migration to a new system is necessary
(outside the scope of stating security criteria but related to the
criteria since the decision to go/no go may factor in cost of a
specific migration)*
- 770 • *defining the process of then doing the requirements engineering
(amongst other things) within the bounds established by the
process*

4.2.6 DM-PO.Collaborative_Working_Relationships

- 775 • Policies governing the roles, responsibilities and activities authorized for
individuals not employed by the control system operating organization shall be
developed.

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

- 780
- The policies shall establish methods for on-site internal, on-site remote and off-site remote access to control system resources.

785

Application Note: This issue was presented in the context of on-site presence by contractors, vendors and other third parties and having clearly defined roles, responsibilities and having these individuals being held responsible for their actions (i.e., liability). The ensuing discussion focused on the need for well-defined rules for interaction with business partners and the need for ramifications that are enforced should the rules be violated. The discussion touched on policy for collaboration agreements (ISAs, MOUs) and included security training and awareness, and philosophies on distributed vice centralized access arrangements.

790

A related issue is the establishment of business rules for technology-based interactions between all parties that support the operation of the control system.

795

4.2.7 DM-PO.Security_Ownership

- 800
- A policy governing security shall be defined to establish the following:
 - an organization-wide security management infrastructure
 - identified roles with authority and responsibility to operate within the infrastructure
- 805
- The policy shall define a single office with responsibility for the security of all control system and non-control system computer resources and the personnel authorized to manage those resources.

810

Application Note: In response to the question “Who owns security on the floor” the response was varied and in fact, no one really owns security. This is an organizational and structure issue and has to do with the enforcement of whatever rules are put in place for the secure operation of the control system.

815

There is a need for restructuring management to ensure there is a single authority with responsibility for all computer operations, and to remove the top-level distinction between control and IT systems.

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

4.2 Control System Functionality Objectives

820 These following Control System Objectives (CSO)) have been defined based upon
analysis of the information collected through interaction with individual control system
industries. These objectives establish the high-level statement of functional security
requirements that are to be met through combinations of hardware, software and
825 firmware-based security technology. Each objective is tagged (e.g., DM-CSO) to
indicate the source industry. Where no tag exists (e.g., CSO), the objective is not specific
to any one industry. The tags used are:

- DM-CSO – Discrete Parts Manufacturing

830 **4.2.1 CSO.Non_Interference**

- The control system security functions shall be implemented in a non-interference
manner such that behavior of the primary control system functions and safety
functions are able to meet their performance constraints.

835

*Application Note: This had been captured as part of the intrusion detection and response
objective. However, the scope of this objective must govern all the
security functions implemented on the control system.*

840 **4.2.2 CSO.Security_Override**

- The control system shall provide the capability for the controlled bypass of
security mechanisms in those instances where security policy enforcement
conflicts with the continued safe operation of the control system.

845

*Application Note: This objective requires that designed over-ride mechanisms be in place
to ensure that a safety-critical state is not created or an existing safety-
critical state is not worsened due to security protection mechanisms. The
controlled aspect of the objective means that the security policy includes
850 the ability to override the security enforcement mechanism. Where
possible, specific detail regarding the bounds and conditions for this
override capability should be stated.*

4.2.3 DM-CSO.Access_Control

855

DRAFT

**Process Control System Component Security Profile Specification (SPS)
August 2002**

- The control system shall provide the capability to grant or deny access to control system resources based upon the authorizations associated with authorized agents.

860

Application Note: If this does not apply to the entire control system then the relevant parts must be explicitly stated. The agent is a human or technology-based entity.

- The control system shall deny unauthorized agents access to every control system resource.

865

Application Note: Between the first and second statements we have the standard “that which is not explicitly granted is explicitly denied” approach to stating access policy.

870

- The control system shall require that each agent authorized to use the control system is identified and is provided with credentials to authenticate their identity.

875

Application Note: Per discussion at the August PCSRF this statement has been softened to not make unique identification mandatory. Alternatives include a configurable capability to assign a unique identity and appropriate credentials to each agent, or to require a role-based/function based authentication capability.

880

The distributed and autonomous nature of control systems and their devices requires that device access be addressed in terms of both the human-to-control system access mode and in the component-to-component access mode in the absence of human intervention.

885

The essential issue is: Who can do what, where, and under what circumstances (role dependent, system state dependent)?

890

The implications are that it is insufficient to say – “we want role-based access control” without going the next step of characterizing the types of roles and types of accesses. It need not be detailed but it must be more than “give me access control”. Also, the question of where are the access control rules to be applied must be addressed.

895

- The control system must be able to include knowledge of the control system state and/or the controlled process state when making an access control decision.

Application Note: The idea of incorporating control system or controlled process state into the access control decision was presented. This illustrates why

DRAFT

Process Control System Component Security Profile Specification (SPS) August 2002

900 *it is insufficient to state access control requirements in terms of*
abstract statements, and illustrates one way in which an access
control capability can be tailored to address control system specific
issues. State information (the state of the machine, the state of the
905 *process) plus who you are, where are you, what role you have, what*
are you trying to do, what have you done) may all factor into the
decision to grant/deny an access or operation request.

910 *The essential issue: Allowing the policy enforcement mechanism to*
be aware of state information. The needs and capabilities of the
various process industries are likely to differ in this context. This is
a good discussion topic since the first step is to determine if such a
need is credible for a particular industry.

- 915 • The control system shall include knowledge of time and location in the rules for
making an access control decision.

920 *Application Note: Preventing unscheduled access by an individual or process to a*
system resource illustrates the need for a wider scope policy to not
just establish roles and access rights but to also define access in
terms of location and time of day.

925 *A full scope addressing of this issue would also include component-*
to-component access rules to prevent automated access by a device
outside the bounds defined as normal access times or normal access
locations.

4.2.4 DM-CSO.Communications_Integrity

- 930 • The control system shall provide the capability to allow information flows only
between authenticated and authorized endpoints.
- The control system shall provide the capability to protect information flows from
replay, substitution or modification.
- 935 • The control system shall provide the capability to allow the recipient of an
authorized information flow to verify the correctness of the received information.

940 *Application Note: Although these statements were based on a focus on wireless*
technology, there must be effective security over any communications
channel regardless of the technology employed.

Process Control System Component Security Profile Specification (SPS) August 2002

Unless and until specific vulnerabilities of wireless mediums are determined to be significantly different than that of wired mediums, there is nothing different in the way the general requirements for networked information flow, integrity and authentication etc. are specified.

945

4.2.5 DM-CSO.Control_System_Integrity

950

- The control system shall provide the capability to restrict access to the functions used to establish and maintain the secure operational configuration of the control system.

955

- The control system shall be capable of performing self-tests to verify the configuration and integrity of the security functions of the control system.

- The control system shall provide the capability for self-test to be executed on startup, at periodic intervals, and on demand.

960

- The control system shall do <what> once an integrity test fails.

Application Note: This is the standard issue of ensuring the protection of the functions and data associated with establishing and maintaining the integrity of the system.

965

4.2.6 DM-CSO.Event_Trace

- The control system shall provide the capability to record and maintain event traces that reflect the successful and unsuccessful security relevant activities involving control system resources.

970

Application Note: The specific discussion focused on audit and there are some considerations that must be addressed, such as, what does audit mean in a control system context (i.e., what type of activity and what types of events are recorded) there were no unique issues brought up. This issue is closely related to the Control Systems Intrusion Detection System (CIDS) issue since the detection capability might utilize event traces as a means to detect potential policy violations.

975

Note the key phrase – security relevant activities.

980

Process Control System Component Security Profile Specification (SPS) August 2002

4.2.7 DM-CSO.Intrusion_Detection_Response

- The control system shall be capable of detecting potential violations of a nominal use control system policy.
- The control system shall be capable of initiating action in response to the detection of a potential violation of a nominal use control system policy.

Application Note: There was discussion regarding need for proactive response to an attack. Proactive response to an attack is considered as meaning automatic response to an attack, that is, without human intervention. Discussion of intrusion detection system (IDS) capabilities often occurs in the absence of a statement of the norm; an IDS needs to know what is normal to detect the abnormal.

The need for capabilities to monitor activity on the control network and to detect activity that is beyond 'nominal' requires 'nominal' must be defined. By defining the norm a policy may then be established and only then will it be possible to detect potential violations of policy (i.e., an intrusion). The next step would be to define policy for the response to the potential intrusion.

A misconception in terms of IDS application is its use as a "policy enforcement mechanism" to catch violators of system use policies (e.g., if I have legitimate access to the system and legitimately install software and that software does something bad to my system – I cannot assume that the IDS is able to detect the behavior and respond to it).

There are then two lower-level issues:

- *Within what constraints is the detection component to operate? The detection process will consume bandwidth and cycles – so how much budget will be allocated to such processes?*
- *What types of response capabilities are desired? There is this overwhelming notion that the process does not stop – so, what effective response can be had with a process control system should a "potential" violation be detected? The issue is that of response to a potential false alarm. Significant trust in the accuracy and validity of the control IDS is necessary.*

**Process Control System Component Security Profile Specification (SPS)
August 2002**

1025 **4.2.8 DM-CSO.Operational_Configuration_Integrity**

- The control system shall provide the capability to determine the current configuration of a control system resource.
- The control system shall provide the capability for a controlled update to the current configuration of a control system resource.
- The control system shall provide the capability to restrict the use of the controlled update function.

1035

Application Note: In response to comments at the August PCSRF this is changed from “Runtime” to “Operational” configuration integrity. The concept of a “maintenance state” within which these capabilities will be accessible may have to be defined.

1040

The problems of runtime configuration management include having specific runtime CM capabilities and defining and enforcing a policy for use of those capabilities.

1045

Configuration control in the runtime environment has the aspects of restricting the ability to modify the installed baseline, determining the installed base and verifying correctness of the installed base.