

## **Process Control Security Environments and Objectives**

Process Control Security Requirements Forum (PCSRF)

(<http://www.isd.mel.nist.gov/projects/processcontrol/>)

### **Introduction**

The NIST Intelligent Systems Division (ISD) of the Manufacturing Engineering Laboratory is working with the Information Technology Laboratory and the Electrical and Electronic Engineering Laboratory to address the information security issues of computer control systems used in the process control industries.

This effort is being carried out through the Process Control Security Requirements Forum (PCSRF), an industry group organized under the National Information Assurance Program (NIAP). NIAP is a joint effort between the National Institute of Standards and Technology and the National Security Agency ([www.niap.nist.gov](http://www.niap.nist.gov)). As part of the Critical Infrastructure Protection Program, NIST and NSA are working to provide technical support and guidance to industry to improve the Nation's security posture. Creation of the PCSRF is one such effort. The PCSRF Focuses on security of the computer control systems used in process industries, including electric utilities, petroleum, pulp & paper, metals & mining, waste, water, chemicals, and pharmaceuticals, with an emphasis on industries considered to be part of the Nation's Critical Infrastructure.

The outcome of this work will be the development and dissemination of standards for process control security. The Process Control Security Requirements Forum (PCSRF), a working group comprised of vendors and users of process control automation, has been established to identify and document the security requirements of the US. Process Controls Industry. The PCSRF is working with security professionals to apply the ISO 15408 Common Criteria methodology to develop Protection Profiles for process control.

This paper presents a description of the different types of process control industries as well as the computer control systems typically used. A security environment for the target of evaluation (TOE) is identified. The environment is formulated by identifying secure usage assumptions, performing a threat analysis of existing systems, and reviewing organizational security policies for the industries. Security objectives of the TOE are then identified using the formulated security environment.

## **Process Control Industries**

Electric Utilities: The electrical power infrastructure is made up of transmission and distribution networks (electric power grid) that create and supply electricity to end-users. The electric power grid is a highly interconnected and dynamic system consisting of thousands of public and private utilities and rural cooperatives. Electric utilities use centralized automation technology incorporating high-speed digital computers, supervisory and control systems, and a variety of communication systems.

Petroleum: Natural gas, crude, refined petroleum, and petroleum-derived fuels represent Oil and Gas substances. The Oil & Gas infrastructure includes the production holding facilities, refining and processing facilities, and transportation devices (including pipelines, ships, trucks, and rail systems) for such substances. Pipelines and distributors make extensive use of computer-based transportation technologies such as valve regulation via communications systems that control gas flow while also providing accounting information contract data, and electronic gas measurement

Pulp & Paper: *(Short write-up needed)*

Metals & Mining: *(Short write-up needed)*

Waste: *(Short write-up needed)*

Water: The water supply infrastructure encompasses water sources, holding facilities, transport systems, the filtration, cleaning and treatment systems and delivery mechanisms that provide for domestic and industrial applications. Water supply systems are primarily utilized for agriculture, industry, business, fire fighting and residential purposes.

Chemical: *(Short write-up needed)*

Pharmaceuticals: *(Short write-up needed)*

## **Process Control Computer Systems**

Real-time computer control systems used in process control applications have many characteristics that are different than traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response. Security is generally not a strong design driver and therefore tends to be bypassed in favor of performance. A corollary is that it is generally not possible to add arbitrary additional code for security measures as a retrofit to existing systems. However, the most egregious examples of problems with process control systems are cases where nothing at all has been done, where generic passwords are left on systems, and where there are no policies or procedures for addressing security issues. Some of these issues can and should be addressed in existing systems without impacting system performance.

Additional security issues arise in the Process Control industry when the IT community thinks they have security under control on the business and administrative side of a company and operations management is often not aware that they have a problem on their side. Yet both sides are increasingly open to the external world through Internet, e-business, and remote diagnostic and maintenance links.

Most of the security problems in these production and distribution systems occur at higher control and acquisition levels. The systems at these levels can be categorized into two types of computer systems, Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition Systems (SCADA)[1][2][3]. Both systems are similar in that they are high level supervisory control systems that are integrated using similar types of components. Significant difference are the types of networking and communication technologies used because of system geographic dispersion.

Distributed Control Systems (DCS) are used primarily in factories, treatment plants. They have similar functionality to SCADA systems, but the field data gathering or control units are usually located within a more confined area. Communications are typically via local area networks (LAN) making communication amongst the system components faster and more reliable compared to the communication of a SCADA System. Supervisory Control and Data Acquisition Systems (SCADA) are used to monitor and control systems that are Geographically dispersed to the extent that the system cannot be confined to a LAN, but rather must be connected using communication mechanisms such as internet and radio frequency. These networking technologies are normally less reliable than a LAN.

A diagram of a Distributed Control System is shown in Figure 1. DCS systems control an entire factory from the supervisory level down to the lowest actuation and sensing equipment. A DCS is divided into several subsystems, each managed by unique controller, yet all interconnected to form a single entity. Various types of communication networks, both standardized and proprietary, are used to connect the controllers. Systems can often be accessed from as high as the corporate level and as low as the field instrument level via modem communication to the outside world.

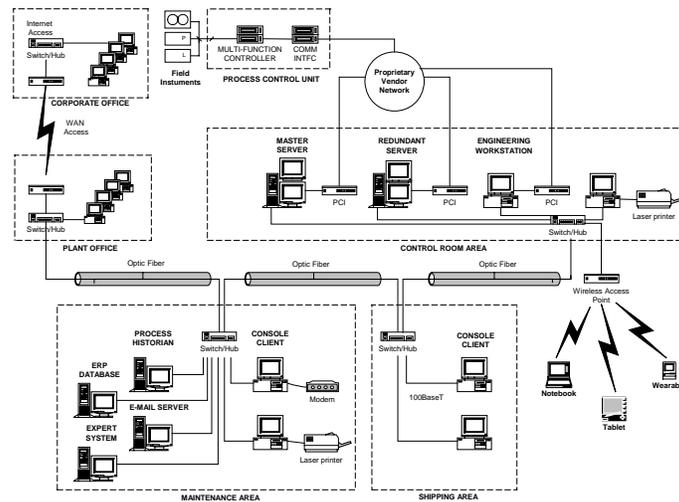
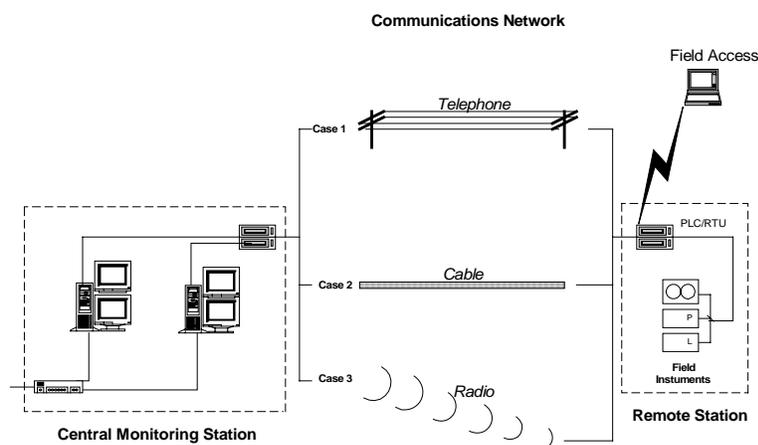


Figure 1 – A Typical DCS

A SCADA System, Figure 2, used to monitor and control geographically dispersed equipment, consists of a Central Monitoring System and one or more Remote Stations. Field instrumentation refers to the sensors and actuators that are directly interfaced to equipment. This instrumentation generates the analog and digital signals that will be monitored by the Remote Station. The Remote Station is installed at the remote site being monitored and controlled by a central host computer. A remote station consists of either a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC) which control equipment actuators and monitor sensors. The communications network is the medium for transporting information from one remote location to another. This is performed using telephone line, cable, or radio frequency. Telephone lines are typically used in place of leased lines due to lower costs and in the usual event that remote sites are not accessible by telephone lines, the use of radio also offers an economical solution. If the remote site is too isolated to be reached directly via a direct radio signal, a radio repeater is used to link the site. The central monitoring houses the master computer(s) and uses a Man Machine Interface (MMI) program to monitor various types of data needed for operation. The CMS collects information gathered by the RTU(s) and generates necessary actions for events detected.



**Figure 2 A Typical SCADA System**

### Secure Usage Assumptions

This is a description of the security aspects of the environment in which the TOE will be used. Information such as physical, connectivity, and personnel issues pertaining to the environment.

### Threat Analysis

The introduction of Internet based information technology within the process controls industry has increased vulnerabilities and threats to the industries computer systems. Centralized operation and remote maintenance of industry systems conducted freely over public telecommunication networks opens the door for threatening organizations to tamper with this critical infrastructure. DCS and SCADA systems that operate on commercial off-the-shelf

## DRAFT

hardware and software, combined with connections to other company networks, allow for simplified invasion and possibly devastation of company manufacturing and distribution systems. Threats to these infrastructures could come from numerous sources: hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters.

The following discussions of industry process control systems attempts to identify possible threats to systems based on known vulnerabilities and their associated risks:

*(Industry input needed)*

To look at the threats associated with DCS and SCADA systems, we have mapped some common threats associated with Real Time (RT) computer systems [4], listed in Figure 3, to the example DCS and SCADA system diagrams. Threats are mapped in accordance with the key networking interfaces on the diagrams.

	<b>Term/Threat</b>	<b>Description</b>
1	Authorization Violation	A person authorized to use a system for one purpose used it for another, unauthorized purpose.
2	Bombs (Logic or Time)	A bomb is a type of Trojan Horse used to release a virus, worm, or another form of attack. It imposes a delay between preparation and activation. A time bomb is set to go off at a specific date and time. A logic bomb is triggered by any combination of conditions, such as particular input transaction or change in a file.
3	Browsing	Browsing is the result of attempts by either a legitimate user or an intruder to access information to which read access is neither authorized nor intended.
4	Bypassing Controls	An attacker exploits system flaws or security weaknesses.
5	Data Modifications	Valid information is altered, replaced with false information, or deleted such that it serves to deceive an authorized individual or entity.
6	Denial of Service	Legitimate access to information or other resources is deliberately impeded.
7	Eavesdropping	Information is revealed from monitored communications.
8	Illegitimate Use	A resource is used by an unauthorized person or in an unauthorized way.
9	Information Leakage	Information is disclosed or revealed to an unauthorized person or entity either through carelessness or for money or favors.
10	Intercept / Alter	A communicated data item is changed, deleted, or substituted while in transit.
11	Interference Database Query Analysis	Database query analysis refers to any process in which an unauthorized individual or entity is able to gain knowledge of sensitive or protected information based on data for which they are either allowed to receive, or by being notified of denied access to information.
12	Masquerade	An entity (person or system) pretends to be a different entity.
13	Physical intrusion	An intruder gains access by circumventing physical controls.
14	Replay	A captured copy of a legitimately communicated data item is retransmitted for illegitimate purposes.
15	Repudiation	A party to a communication exchange later falsely denies that the exchange took place.
16	Resource	A resource (e.g., access port) is deliberately used so heavily that service to other users is

DRAFT

	Exhaustion	disrupted.
17	Sabotage	Common examples of sabotage include: destroying hardware or facilities, planting logic bombs that destroy programs or data (see malicious software), entering data incorrectly, crashing systems, deleting data, holding data hostage, and changing data.
18	Scavenging	Scavenging refers to the process of searching through system residual information or generally available information to find and acquire sensitive data in order to violate information confidentiality.
19	Spying	Spying is defined as direct covert visual or auditory observation of private information as it is being displayed or entered into a computer or related system with the intention of violating information confidentiality.
20	Service Spoofing	A bogus system or system component aims to dupe legitimate users or system into voluntarily giving up sensitive information.
21	Sniffers	Sniffing is the process of monitoring data traffic, usually on a network, in order to collect information that could be used for unauthorized access. Sniffer attacks often involve the use of network monitoring tools called sniffers.
22	Substitution	Substitution is the introduction of unauthorized, potentially malicious, components into the system.
23	Terrorism	Terrorism by an individual or organization, when used in a deliberate way can adversely affect the actions and policies of states and organizations.
24	Theft	A security-critical item, e.g., a token or identity card, is stolen.
25	Traffic Analysis	Information is leaked to unauthorized entities, through observation of communications traffic patterns.
26	Trap Door / Back Door	A Trap Door is a hidden mechanism contained in the software that allow developers, or anyone else knowing the secret, to bypass normal access controls. The mechanism is built into the software by its designer.
27	Trojan Horse	A Trojan Horse is an apparently useful program containing a hidden code fragment, that performs hidden functions and exploiting the privileges of the user.
28	Tunneling	Another way to defeat safeguards is to attack below the level of the safeguard. For example, if there is access control on files, attack the disk sectors where the file is stored. If an application transaction has strict controls, attack the transaction program object module. An attack that goes “under” the controls in this way is called a Tunneling attack.
29	Unauthorized Access Violations of Permission	Violation of permission refers to authorized individuals or entities who exceed their system privileges by executing functions that they are not authorized to perform.
30	Unauthorized Access Piggybacking	Piggybacking (also known as tailgating) is a masquerading technique within a computer system or communication facilities connected to a computer system. The technique covertly uses facilities of computer access and processing.
31	Virus	A virus is a program that attaches itself to a host program so that when the host is executed, the virus will execute. When executed the virus tries to copy itself (or a modified version of itself) to some other host program. Then the virus typically carries out its mission or payload.
32	Worm	A worm is a self-replicating program that is self-contained and does not require a host program. It makes a copy of itself and causes the copy to execute. Unlike viruses, worms don’t usually modify other programs. Worms may be used to destroy data or they may be used to tie up network resources, causing a loss of communication within the network.

**Figure 3 Common RT Computer System Threats**

DRAFT

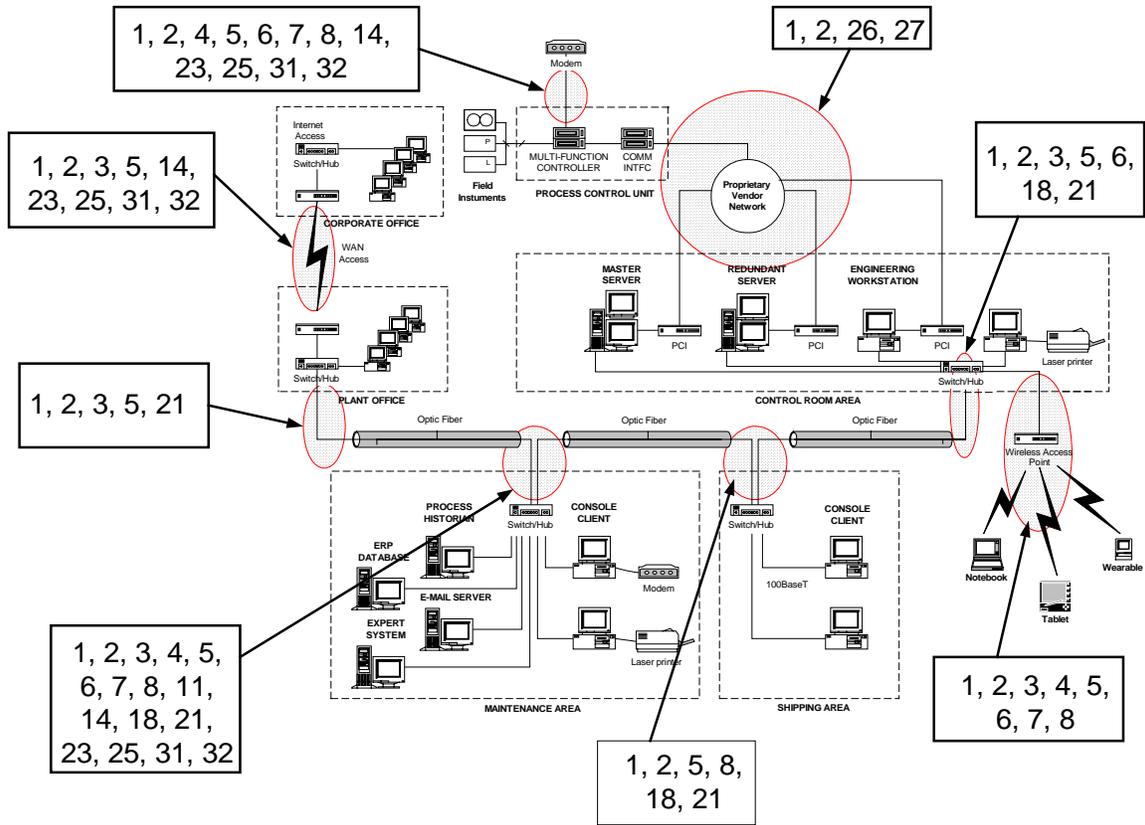


Figure 4 - DCS Threat Mapping

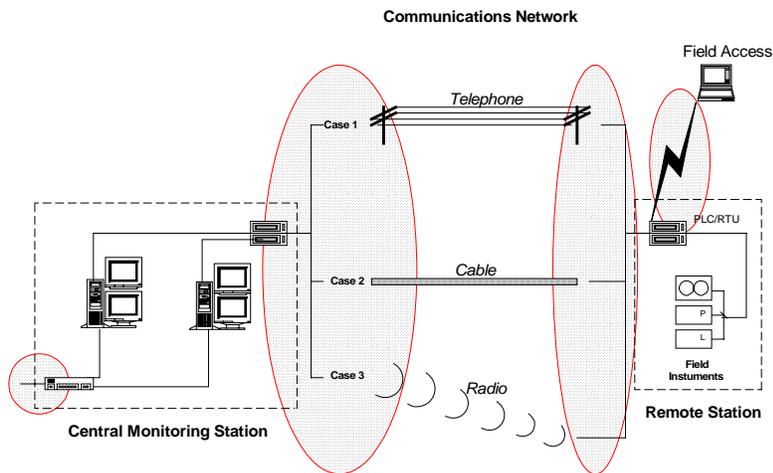


Figure 5 SCADA Threat Mapping

## **Organizational Security Policies**

Drafting the security policy for the process controls industry should begin with a compilation of written policies related to security and a survey of informal policies applied by users.

*(Industry Input Needed)*

## **Security Environment**

*(Need much more info.)*

## **Security Objectives**

The RT requirements of these systems must be taken into account when considering security objectives for these threats since the lower levels of these systems control critical processes. Miniscule interrupts in a time critical process due to a security problem could result in total process failure.

## **References**

1. George D. Jelatis, "Information Security Primer", Secure Computing Corporation, for EPRI
2. Micrologic Systems Inc., "SCADA Primer",  
<http://www.micrologic.com.ph/primers/scada.htm>
3. Natural Gas Information and Educational Resources, <http://www.naturalgas.org>
4. Dr. Sam Bowser, "Real Time (RT) Security Strawman – (draft)",  
The Aerospace Corp., for The Open Group RT Forum Security Group.
5. B. Schneier and A. Shostack, "Breaking Up Is Hard To Do:  
Modeling Security Threats for Smart Cards", Counterpane Internet Security Web Site,  
<http://www.counterpane.com/smart-card-threats.html>