# Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments

Version 1.0

## Draft Recommended Practice

*February 2007*

# Using Operational Security(OPSEC) to Support a Cyber Security Culture in Control Systems Environments
# Version 1.0
# Draft

Authors: Mark Fabro, Lofty Perch Inc.; Vincent Maio, INL
Contributors: Rita Wells, David Kuipers, Trent Nelson, Heather Rohrbaugh

February 2007

**INL Critical Infrastructure Protection Center**
**Idaho Falls, Idaho 83415**

**Prepared by**
Idaho National Laboratory

# CONTENTS

## Keywords

Control Systems, Operations Security, OPSEC, Security Culture, Cyber Security, Industrial Networks

## Introduction

Information infrastructures across many public and private domains share several common attributes regarding IT deployments and data communications. This is particularly true in the control systems domain. Many organizations use robust architectures to enhance business and reduce costs by increasing the integration of external, business, and control system networks. Data security is often deployed using specialized technologies and is supported by the creation of a cyber security "culture" that is based on policy, guidance, and operational requirements. By using methods of operational security (OPSEC), the security culture empowers management and users to maintain and enhance cyber security by instilling procedures and guidelines into the day-to-day operations.

However, the cyber security strategies required to protect the business domains and the associated security culture that is created to support the security programs may not be easily translated to the control system space. Factors such as operational isolation, legacy networking, and inflexible roles in job activities may not be conducive to creating environments that are rich with cyber security capability, functionality, or interest. As such, guidance is required to help organizations leverage operational security and establish effective, self-sustaining security cultures that will help protect information assets in the control systems architectures.

This document reviews several key operational cyber security elements that are important for control systems and industrial networks and how those elements can drive the creation of a cyber security-sensitive culture. In doing so, it provides guidance and direction for developing operational security strategies including:

- Creating cyber OPSEC plans for control systems
- Embedding cyber security into the operations life cycle
- Creating technical and non-technical security mitigation strategies.

## Audience and Scope

This document is designed for managers and security professionals charged with developing, deploying, and improving the cyber security in their control systems domains. Although designed to be flexible enough to be read and used by system operators and engineers, the material is intended to be used by those that are deploying cyber security programs and creating security-sensitive cultures in control system environments. It is not designed to replace a sector-specific approach to creating a cyber security program, but rather guide interested parties in some of the more common areas requiring special attention. It may be found most appropriate by those that have experience in deploying cyber security programs in modern information

technology (IT) domains and are beginning to address the issues related to deploying cyber security strategies for industrial control architectures. The scope of the material is not technically demanding and can be used to provide a foundation for creating or augmenting existing information resource protection initiatives.

In the interest of brevity, and assuming the general readership will have experience with some IT security aspects, only some generalized standards for cyber security are discussed. The document is designed to address a few of the major issues encountered in developing a cyber OPSEC plan that can contribute to developing a security-sensitized culture. From these baseline standards, the reader is encouraged to investigate other related work and guidance that may be more applicable to their specific sectors. Moreover, it is important to note that as organizations use their own IT security framework as a baseline to create OPSEC in their control domains, other robust sector-specific cyber security initiatives can be used to augment best practices.[1] With more than 40 standards organizations worldwide working on guides that either directly or indirectly impact the security of control systems, readers can use this document as a basis in developing their own OPSEC programs based on other efforts.[2]

## Background

Recently, there has been extensive literature pertaining to potential cyber attacks on control networks by terrorists, nation-states, hackers, and insider threats.[3] These critical systems, many decades old in their technology, are rapidly becoming connected to business networks, to the Internet, and to each other. The security implications are evident, and there is reason for both concern and prudent action.[4] However, many of the industries that may be affected are likely to place cyber security at less than top priority for a variety of reasons: lack of resources for cyber security, the inability to deploy an effective cyber security function, or no substantial evidence of a threat. Additionally, personnel responsible for the cyber security of control systems may have little knowledge to accurately determine which products and actions are most appropriate for their specific control network or how to reduce their cyber risk in the most efficient way. Even once the technology required to protect key control systems has been deployed, the security culture that is required on an operational level to maintain, support, and sustain the defensive strategies may not evolve naturally.

Businesses that operate in a recognized critical infrastructure industry,[5] such as energy, water, transportation, and chemical manufacturing, need to practice due care and diligence on the cyber security of their control system or industrial network. This is no small task as it is a delicate operation to take the right steps to achieve the necessary level of security while balancing issues such as purpose, effectiveness, ease of use, compliance with regulatory requirements, and cost constraints. Ongoing effort and discipline is required during the control

---

[1] The reader is encouraged to review specific cyber security work done by ISA SP99, NIST, NERC, CIDX and other sector-guidance that has been published. More information is at http://www.us-cert.gov/control_systems/csdocuments.html

[2] ISA Intech Magazine, December 2006, page 57 “Power to Security Standards’, Joseph M. Weiss

[3] http://www.us-cert.gov/control_systems/csthreats.html

[4] http://www.us-cert.gov/control_systems/index.html

[5] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

system lifecycle to retain the proper level of operational cyber security, because of the critical need for proper securing of elements associated with control systems (i.e., control room personnel, software applications, equipment, and the overall network environment). Due care requires that management, control system administrators, and control and IT system security officers take proper steps to ensure the control system networks are protected, along with the employees and the public. Due diligence requires that the same individuals have a proactive program to identify the cyber threats, understand and manage the cyber vulnerabilities and other issues pertinent to reducing the cyber security risk to their control systems and associated industrial networks.

In addition to deploying robust security technologies and business planning initiatives, the creation and nurturing of a cyber security culture is critical in protecting corporate assets in the business domain or in the industrial environments that support the core of the business itself. To produce the environment in which a security culture can be created, components in operational security can be developed. This OPSEC plan is not unlike the programs that are now ubiquitously in place for enterprise and IT networks.

Simply augmenting and migrating a proven cyber security program from the business domain into a control domain is not always the most effective solution. Care must be taken in creating this new OPSEC plan to accommodate some of the domain-specific issues that are found in control system architectures. Figure 1 below is a table illustrating some of the more common IT security elements that would be expected to be found under a cyber OPSEC plan and highlights some of the differences in requirements for a control system:[6]

| SECURITY TOPIC | INFORMATION TECHNOLOGY | CONTROL SYSTEMS |
|---|---|---|
| Anti-virus & Mobile Code Counterfeasures | Common & widely used | Uncommon and difficult to deploy |
| Support Technology Lifetime | 3-5 Years | Up to 20 years |
| Outsourcing | Common & widely Used | Rarely Used |
| Application of Patches | Regular/Scheduled | Slow (Vendor specific) |
| Change Management | Regular/Scheduled | Legacy based – unsuitable for modern security |
| Time Critical Content | Delays are generally accepted | Critical due to safety |
| Availability | Delays are generally accepted | 24x7x365 (continuous) |
| Security Awareness | Good in both private and public sector | Generally poor regarding cyber security |
| Security Testing/Audit | Scheduled and mandated | Occasional testing for outages |
| Physical Security | Secure | Very good but often remote and unmanned |

**Figure 1. Control System Requirements**

[6] PA Knowledge Limited, 2002

The above table clearly illustrates how requirements in each of the IT and control domains can impact security topics required in an OPSEC plan. Mapping an existing IT centric plan into the control domain without proper impact analysis can have negative consequences. As such, key foundations must be prepared in developing the cyber OPSEC plan that can accommodate for these differences. Some core concerns that may be considered in developing a cyber OPSEC plan for control systems are:

How does the need for real time data impact the deployment of security technology? Is latency an acceptable by-product of security technology deployment (i.e., encryption)?

How does the operator community and the associated job specialization impact OPSEC activities?

How does physical security at remote facilities impact access to components for upgrading software and firmware? What about recovery and incident response times?

If there is no testing or staging facility, how can upgrades for security software (i.e., antivirus) be evaluated prior to installation in production environments?

This document introduces some of the more essential cyber security activities that are important for control system OPSEC programs and, as a result, important in creating a cyber security culture. In addition to balancing these activities with normal business operations, these activities must be routine in nature and enable the industrial network and individual computer-based control systems to continue to run reliably and securely. This document is divided into three major sections, all of which focus on developing a control system cyber security culture by addressing key OPSEC ideals:

Section 1: Creating OPSEC Programs: From Management to User

Section 2: Sustaining Cyber Security Culture: Embedding Security into the Operations Life cycle

Section 3: Technical and Non-Technical Solutions

Section 1 covers key issues of administrative management, accountability, and the steps managers can take to create an effective cyber OPSEC program. It reviews the core components of the OPSEC discipline and applies them to the issues of creating an OPSEC program, populating the program with control-sensitive content, establishing management boundaries, and nurturing the program during its lifetime.

Section 2 discusses how cyber security can be embedded into the development and operational life cycle and provide a mechanism for meeting major security objectives in control systems and industrial networks. In doing this, organizations can provide a capability to create and maintain a self-sustaining cyber security capability for the control systems domain that is applicable to managers, operators, and other entities. As such, this second section addresses

issues such as “single points of failure” along with classic IT concepts of using clustering and backups.

Section 3 provides insight into mitigation strategies that cover both the technical and non-technical perspectives. Presenting cyber security in this manner, along with the previous discussion on OPSEC foundations, users will be able to enhance their overall lexicon for cyber security and decide how to present it so that a security culture is supported. Content in this section discusses technical activities for mitigation security issues in the control domain, training and awareness activities, and suggestions for enhancing and growing the cyber OPSEC program. A discussion of attacks and countermeasures is not included, but the reader is encouraged to review existing material at US-CERT regarding cyber attacks and control systems.7

## 1. Creating Cyber OPSEC Programs: From Management to Users

In tandem with a robust cyber security policy, having management create, support, and maintain an effective cyber security program is critical to an overall healthy cyber security posture. There are many cyber security consequences that an industry with an IT enterprise system and automated control network needs to consider, including disclosure of confidential product data, corruption of control data, interruption of services, and physical destruction of the assets under automation control (the latter being a unique aspect of control systems and industrial networks in comparison to IT networks). From a management perspective, the creation and maintenance of a cyber OPSEC program in the control system domain is very similar to traditional IT domains. However, certain nuances and cultural differences can make the management of the cyber security program challenging. Thus, the challenge becomes how to reuse appropriate OPSEC fundamentals from the IT domain in the control systems environment.

To mitigate these issues, managers must be able to instill a program that accounts for the unique needs, capabilities, and operational requirements of those users and operators working in the industrial domain. Such programs often have familiar key components such as:

Generate a cyber OPSEC program for control systems users

Define management responsibilities and cultural considerations

Define OPSEC management boundaries for control systems

Write a cyber security OPSEC policy for control systems

Ensure control system operator/user input on development of the security culture

Implement and monitor a control system OPSEC program

[7] http://www.us-cert.gov/control_systems

## 1.1 Creating the Program

Many organizations that operate in the control systems domain have some operational oversight by a larger corporate or business function. Considering that most modern business entities use up-to-date IT communications infrastructures, it may be assumed they may have (at least at some level) a cyber security program and policy. This does not necessarily mean the program is robust, it just means that on some level some cyber security is being done. This may come in the form of anti-virus, firewalls, and user authentication, all of which are standard security solutions found in most commercial IT solutions. For larger organizations, there may indeed be a dedicated cyber security function that oversees all aspects of cyber OPSEC elements.

When a cyber OPSEC program exists for the traditional IT domain (which is usually the case), the task of creating a cyber OPSEC initiative for a control domain is much easier. Overall, the components of the OPSEC plan are very similar regardless of the domain it is to operate over, which makes it easier for management to "migrate" a proven plan to the control environment. Moreover, in the event there is an existing plan in place for the business domain, it is quite possible that those operating in the control domain have some (but maybe limited) exposure. This, in essence, may make the effort of obtaining senior-level buy-in easier in creating the cyber OPSEC plan, and make the justification easier as well.

## 1.2 Program Elements

As OPSEC elements can be unique based on the organizational requirements; observing standards such as ISO 27002 (formerly 17799)[8] can provide some directions in ensuring key components are inherent in the cyber security program. These include:

### 1.2.1 Risk Assessment and Treatment

This activity covers the overall and incorporated risk assessment done from an organizational perspective and will include a robust analysis of the control systems domain. In any case, looking at risk as a function of consequence (as opposed to asset value) may allow for easier calculations applicable to control system environments. Elements that are unique to the control domain, such as loss of life, mean time to recovery, and environmental impact can aid in these calculations.

### 1.2.2 Information Security Policy for the Control Domain

This activity involves a thorough understanding of the organization business goals, the role of the control systems in meeting business goals, and the overall dependence on information (cyber) security. It should reflect the needs of the actual users and operators. It needs to be understandable, applicable to the control domain, and produced by the people using it.

[8] ISO Code of Practice for Information Security Management (ISO 17799, 27002) http://www.27000.org/

### 1.2.3 Organization of Information Security (Internal and External)

A management framework needs to be established to initiate, implement, and monitor a security governance structure. Security programs need senior-level approval and support, and wherever possible security functions need to be incorporated into other IT functions in the control environment. External parties are also included in these areas, and security issues and activities with third party or other vendors need to be addressed.

### 1.2.4 Asset Management, Classification, and Control

As organizations require understanding of the information assets they have in their industrial control systems environments, the cyber OPSEC plan needs to be shaped in such a way that those resources are protected appropriately. By the assignment of assets to owners and application of security functions to that ownership, both the issue of asset classification and responsibility are addressed. Information assets in the control domain need to be classified to indicate the degree of protection; the classification should result in appropriate information labeling and assignment to user, operator, and process.

### 1.2.5 Human Resources Security

Organization oversight for access and assignment are required at all times. Allowing Human Resources to assign requirements based on the “joiners, users, or leavers” model empowers a control system business to have a perpetual understanding on user and employee status while they are using control system assets. This model provides for applying security and appropriate care in the protection of assets before the hiring of the user, during the user’s employment, and after the user leaves the organization. Depth of functional resources should also be provided to ensure multiple personnel share responsibility and accountability for the various roles of configuration, monitoring, and operation of control system assets.

### 1.2.6 Physical and Environmental Security

Many control system domains already have an effective physical security apparatus in place. These components, often introduced into the control systems environment prior to the deployment of any IT capability, may require refreshing to accommodate for new security technologies. Such review may cover physical entry control, the creation of secure offices, rooms, facilities, providing physical access controls, and providing protection to minimize risks from fire, electromagnetic radiation, or sabotage. In critical control domains, this may be extended to include providing adequate protection to power supplies and data cables for some of the activities.

Access control and physical access must also include consideration for the installation and management of system-centric media (i.e. software/firmware upgrades) in remote facilities. In many system architectures, the locations where control equipment require servicing are often geographically disperse and may not have appropriate physical security. However, these locations are often accessed by workers, so upgrades or modifications to the resident technology can be performed. This concern for loading and unloading of media into the systems may justify the cross-correlation of cyber activity with physical access, as in many cases the remote facilities are effective connection points into the master control network. As such, logging activities

pertaining to physical access may be cross-referenced with cyber-specific activities to provide a more robust perspective on overall system access. (see 1.2.8)

### 1.2.7 Communications and Operations Management

Accurate documentation of the procedures for the management and operation of all information processing resources in the control systems domain should be established. Core sub components of Communications and Operations Management can include:

- Operational Procedures
    - Change Management
    - Separation of Duties
    - Access to Development Environ
- Backup and Data Retention Activities
- Protection from Malicious Software (Malware) and Attacks
- Third-Part Service Delivery
- Systems Planning and Acceptance
- Network Security and Monitoring
    - Secure Network Management
    - Networks Security Technology
    - Firewalls, Routers, Intrusion Detection

Of particular interest is the network management component. Cyber security requirements for control systems domains require a range of controls that may be different than those found in common IT networks. Measures, such as Defense-in-Depth strategies, can significantly increase overall security posture in these environments.[9] To achieve and maintain security in control system computer networks, special controls should be established to safeguard the confidentiality and integrity of data passing over connected public networks. Special controls may also be required to maintain the availability of the network services.

### 1.2.8 Access Control

Due to the inherent trust and privilege that exists in many control domains, access control needs to be applied to more than just users in the operational environment. To account for the interconnected nature of control systems, as well as the inherent capabilities that many control devices have, many components need to be considered in developing an access control function of a cyber OPSEC plan. To define robust access control, one has to consider:

- Managing user access and user responsibility

- Managing business requirements for access control (which may be very different from those in the corporate domain)

- Monitoring operating system access control

[9] http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

- Directing device access control

- Controlling mobile computing (include remote location activities and media installations).

### 1.2.9 System Acquisition, Development, and Maintenance

To ensure robust security is present in the key systems that operate in control system architectures, security functionality should be inherent in the control technology. Of course, this may be a difficult task to many organizations. When reviewing Figure 1, average support lifetimes are of the order of 20 years, and such durations often "lock" a user into prescribed vendor technologies. As security should ideally be included at the time of inception of a system, many of the critical systems in operation today were designed when robust network or cyber security (beyond a simple vendor-supplied password) was not a requirement.

Information security must be taken into account in the processes for specifying, building/acquiring, testing, and implementing control systems. Issues such as security requirements, valid processing of data, protection of files and cryptographic controls[10] all combine (with others) to create a baseline of key requirements. Moreover, other aspects regarding vendor interaction (coding practices, flaw remediation) should be included.[11]

A strict change control procedure (see Section 3) should be in place to facilitate tracking of changes. Any changes made to the operating system or software packages should be strictly controlled, and the cyber OPSEC plan should reflect this.

### 1.2.10 Incident Management

In the event cyber security incidents occur in the control systems domain, robust reporting activities are required to be in place. Many preexisting templates and frameworks for incident reporting are available, and templates used for reporting in the traditional IT domain can be used. However, care must be taken in developing and deploying incident management and handling tactics for the control systems domain.[12] As an example, many incident response plans require elements of systems shutdown, removal, and forensics analysis. When considering the criticality that is inherent in many industrial applications of control systems, such activities are significantly difficult to achieve if not impossible. As such, new strategies for incident handling and forensics need to be investigated, with an end result being a unique set of control system-specific instructions and actions for security managers.

### 1.2.11 Business Continuity Management

Just as in the business domain, a continuity of operations management process should be designed, implemented, and periodically tested in the control systems environment. It is understandable that many organizations with control systems architectures have Business

[10] http://www.gtiservices.org/security/AGA12Draft3r6.pdf

[11] http://www.msisac.org/scada/

[12] https://forms.us-cert.gov/report/

Continuity Management (BCM) plans in place for the resumption of operations following an interruption due to physical or other non-cyber incidents. However, only recently have organizations begun to consider the BCM activities required to support cyber operations in control system environments; initial efforts have included the translation of existing business domain BCM plans into the control systems domain. Like the business domain, these plans needs to be periodically tested, maintained, and refined based on changing circumstances, operational capabilities, and overall control system architectures. The reader is encourage to research sector-specific work that has been done in this area (i.e., ISA, NERC) and ascertain the applicability to their own environments.

### 1.2.12 Compliance

In many sectors, it is essential that strict adherence is observed to the provision of standards, regulatory guidance, and associated laws. Many best practices are emerging for cyber security in the various control systems domains, such as Energy, and many more are on the horizon.[13] Moreover, as in the IT domain, adherence to laws, trade agreements, intellectual property, and vendor licensing is key to maintaining good OPSEC practices.

# 2. Sustaining Cyber Security Culture: Embedding Security into the Operations Life Cycle

The operations life cycle in control system environments is non-trivial and often requires the integration of many associated functions such as operator activities, business requirements, technology upgrades, vendor support, and perpetual training and awareness as it applies to safety. With that, the interaction of these (and many more) functions creates a delicate and complex environment in which security must be pervasive. Most organization have a security culture, as it relates to the protection of the physical assets of the control domain, but emerging practices that connect these once isolated systems to corporate entities, business partners, and peer sites now require enhancing the security culture to include cyber security.

As mentioned before, the assignment of technology ownership to operators and users can help provide tactical protection of information assets and introduce some cultural activities as it relates to cyber security. However, to help maintain the security function and create a self-perpetuating security capability within the control systems domain, the incorporation of cyber security and an OPSEC program into the system life cycle, as shown in Figure 2, is required. By doing so, cyber security can be introduced at all levels of operations, achieve the pervasiveness required, and provide a good environment for the cyber security culture to grow.

[13] http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

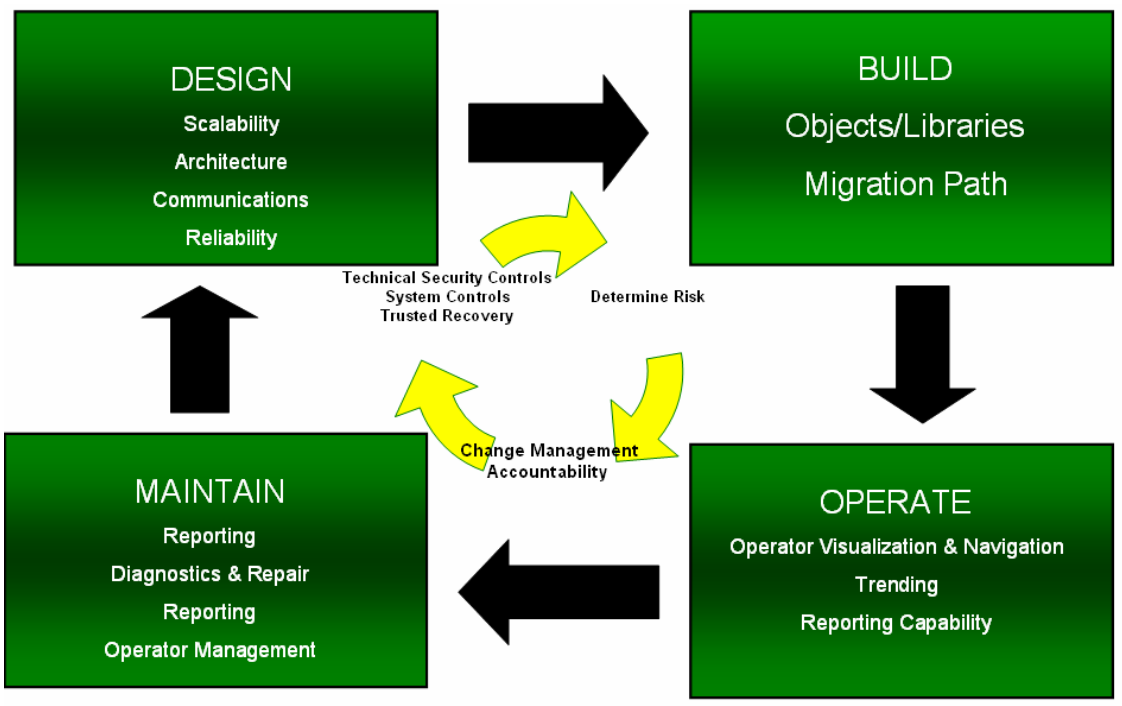


Figure 2. Notional system life cycle with security components.

From the above diagram it is clear to see that there are a number of opportunities to embed cyber security into the life cycle, and like other core life cycle components, security can become part of the common strategy and permeate into the overall operational culture. Recognizing that security is in itself a process rather than a function that is simply done once, organizations have some flexibility in implementing a cyber OPSEC plan into the control systems domain using the life-cycle approach. However, to ensure truly effective security, an OPSEC program must have its foundations as early in the life cycle as possible.

In the control system environments, some elements require special attention due to the nature of industrial control systems (i.e., vendor specificity) and their subtle differences from their standard IT counterparts, which can make incorporation of cyber security into the phases a challenge. Yet, regardless of the level of effort, it has been proven that an after-the-fact approach to cyber OPSEC usually costs more in terms of time and money and renders security an unfavorable aspect in the opinions of operators, engineers, and managers. This in itself can impact the cyber security culture in a negative way and should be avoided. Proactive inclusion of cyber security into all operational aspects is indeed an element of an OPSEC best practice.

When control system hardware, software, and cyber security products are evaluated for specific levels of assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process. Operational assurance concentrates on a specific industrial control system network product's architecture, embedded features, and functionality, which enable an industry customer to continually obtain the necessary level of protection when using the product. Examples of operational assurances examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when and if the product

experiences unexpected circumstances. Currently, several initiatives are underway to guide the owner/operator community in the strategic procurement of security-sensitive control systems.[14]

Life-cycle assurance pertains to how the control system product was developed and how assurances were maintained during its development. Scalability, architecture, communications, and reliability are the foundations of the design phase. Traditionally, reliability has been the area of concentration that has accounted for the system's ability to maintain operations over a long period of time and under certain conditions. As such, the culture that has been developed as it pertains to system security is one that is tied to availability of the systems, as well as to the reliably of the system to perform its function. Measures are taken to protect the system in this regard and often do not include consideration for cyber security. This view has evolved with little or no cyber consideration, and so the life cycle activities that address reliability need to be expanded to include cyber security.

Each stage of the product's life cycle may have standards and expectations it must fulfill before it can be deemed "trusted." Examples of life-cycle assurance standards are design specifications, clipping-level configurations, unit and integration testing, configuration management, and trusted distribution. Control system vendors that are looking to achieve a high security rating for its products will have each of these issues evaluated and tested; it is clear that effective relationships between users and vendors need to be in place to ensure cyber security (as part of the overall cyber OPSEC plan) is indeed part of the system design process.

Clearly, there will be commercial technologies and strategies that can be used to support a cyber OPSEC plan and protect control system information assets. But recognizing that proactive mitigation activities have the best return on investment, the implementation of cyber security earlier on is part of a successful overall approach. The following sections address several of these types of operational assurance and life cycle assurance issues not only as they pertain to control system product evaluation, but also as they pertain to a critical infrastructure or industry's responsibilities once the products are implemented. Using the phases of Design, Build, Operate, and Maintain, components supporting cyber OPSEC can strategically be inserted into the overall cycle. This results in cyber security being present to a capillary level and can thus induce a more cyber-sensitive security culture.

## 2.1 Clipping Levels

In both the Design and Operational phases, organizations using industrial systems may be able to set predefined thresholds for the number of specific errors that will be allowed before an activity is considered irregular. In many control domains, deviations from the normal operational activity are rare. In most cases, network activity and communications can be monitored, and as such the behavior of the communications environment can be predicted. Data traffic or activity that is outside of this normal threshold can be set to initiate activities that investigate the anomaly. The threshold that is defined is often referred to as a 'clipping' level, and once that level is exceeded and an alarm is triggered.

[14] http://www.msisac.org/scada/

Providing detection and notification of a cyber security irregular event or activity within the control systems domain is in essence similar to the historical meaning (i.e., irregular event monitoring). The cyber security threshold is a baseline for cyber-related activities that are considered as normal for a control system before alarms are raised. Like the clipping level associated with monitoring normal operating activities, a cyber security clipping level will trigger alarms associated with irregular activity associated with user and cyber activities.

To accommodate for what may be a large number of events, contemporary intrusion detection systems (IDS) may be used to track these activities and behavior patterns because it would be too overwhelming for an individual to continually monitor stacks of audit logs and properly identify certain activity patterns. The goal of using clipping levels is to augment the overall situation awareness that can alert mangers to problems before damage occurs and to be alerted if a possible cyber-related attack is underway. Moreover, results from these observations can provide input to the mitigation strategies that are either technical or non-technical in nature and provide data points for ascertaining more accurate asset behaviors and thus, the risk to those systems. The reader is encouraged to review more in-depth discussions of security technologies for the control system domain.[15]

## 2.2 Configuration, Access, and Change Management

As communications networks inside these domains become connected and entities such as peers and business networks connect to the control domain to collect operational data, strategies to account for the protection of the information resources need to be deployed. It is in the cyber OPSEC plan that the organization can address these issues and provide guidance in key areas such as Asset Management and Operations Management.

One area that deserves special attention within this management enclave, related to the Maintenance phase of the system life cycle, is Change Control. Organizations operating industrial systems will most likely have a change control policy as it relates to the Maintenance phase of the system life cycle, but may not apply the change management practices to the actual automated processes. This policy is usually applicable to the changing of major system components such as communications systems, operator interfaces, diagnostic tools, and others that relate to overall system reliability. As systems become connected, extensions to traditional change control processes are required to accommodate for the required protection of the information assets that are networked or are critical to safety and process control. Components of the change control include: how changes take place within a facility; who can make the changes within a control system network; how the changes are approved; how the changes are documented and communicated to other control system users and other employees; and how the changes are backed up to support system restoration.

Without these policies in place, control system users can make changes that others do not know about and may not have been approved. Although it is uncommon for changes at the industrial level to go undocumented (such as upgrading field devices or swapping in a new human-machine interface [HMI]), last-minute changes to the cyber infrastructure may be made out of necessity and can go undocumented and have negative effects. As seen above as an

[15] http://csrp.inl.gov/

element in Communications and Operations Management, these procedural OPSEC elements have a key role in supporting security culture. Yet, it cannot go without mention that change control is intimately connected to both the Design and Operate phases as well, requiring that testing and evaluation are done prior to instantiating changes into an industrial production environment (see Section 2.2.1 below).

Heavily regulated industries, such as pharmaceuticals and energy, have very strict guidelines regarding what specifically can be done to their control systems and industrial networks and at exactly what time and under which conditions. These guidelines are intended to avoid problems that could impact downstream partners and, ultimately, the users of the product. Without strict controls and guidelines on changes, vulnerabilities can inadvertently be introduced into an industrial control systems network. Additionally, without change control, auditing the changes after implementation is a very complicated task. A well-structured change management process should be put into place to aid administrators. This process should be laid out in the change control policy. Although the types of changes vary, a standard list of procedures can help keep the process manageable and ensure that it is carried out in a predictable and repeatable manner.

Reporting requires interaction, and as organizations map a change control policy to the industrial domain, opportunity is presented to create an environment that will foster a security culture. Wherever possible, organizations should create working groups and outreach teams to ensure effective and timely reporting of changes to the information infrastructure. The following subsections are examples of elements that should be part of any industrial system change control policy that impacts network communications, security, or information-based processes.

### 2.2.1 Request for A Change to Take Place

Requests should be presented to an individual or group that is responsible for approving control system changes and overseeing the activities of changes that take place within a control system environment.

### 2.2.2 Approve the Change

The individual requesting the change must justify the reasons and clearly show the benefits and possible pitfalls of the control system change. Sometimes the requester is asked to conduct more research and provide more information before the change is approved.

### 2.2.3 Document the Change

Once the change is approved, it should be entered into a change log. The log should be updated as the process continues toward completion.

### 2.2.4 Test and Present Results

The control system change must be fully tested to uncover any unforeseen results. Depending on the severity of the change, the change and implementation may need to be presented to a change control committee. Unlike IT networks, changes to industrial networks and their control systems cannot simply be tested 24-hours-a-day, 7-days-a-week, and 365-days-a-

year, similar to most industries. Test beds are occasionally needed to validate the change prior to scheduling an outage for incorporation of the change to the actual production control system.

### 2.2.5 Implement Schedule

Once the control system change is fully tested and approved, a schedule should be developed that outlines the projected phases of the change being implemented and the necessary milestones. These steps should be fully documented and progress should be monitored.

### 2.2.6 Report change to management

A full report summarizing the control system change should be submitted to management. This report can be submitted on a periodic basis to keep management up to date and ensure their continual support. These steps usually apply to large changes that take place within an industrial facility. These types of changes are usually expensive and can have lasting effects on critical information infrastructures or control systems. However, smaller changes should also go through some type of change control process.

If a control system local area network server needs to have a patch applied, it is good practice to have it tested on a non-production server, have the approval of the control system department manager or network administrator, and have both backup and back out plans in place in case the patch causes some negative effects. It is also critical that the operations department create approved back out plans before implementing changes to systems or the network.

Upgrading field technology with current versions of software or firmware is a change management challenge. One of the key issues in maintaining an effective security posture in control system domains is ensuring that key devices are operating with the most recent and up-to-date software or firmware. Yet for many installations, maintaining accurate records of how upgrades are administered is a tremendous task, especially if the number of devices requiring upgrades is significant. Changes to control systems and industrial networks are critical to successful OPSEC programs, especially in large dynamic environments. Changes to control software configurations and network devices can take place in automation environments. Keeping all of these details properly organized is essential. Revision control, or the function that ensures the proper version of the firmware or software is installed, is a core component in ensuring effective, robust, and secure operations.

Numerous changes can take place in a control systems environment, some of which are:

- New control hardware, end device, server, computer, or any hardware additions to the control or SCADA LANs are installed, including sensors and control devices
- New applications and operating system platforms are installed
- Different configurations are implemented
- Patches and updates are installed
- New technologies and processes are integrated

- Policies, procedures, and standards are updated
- New regulations and requirements are implemented
- New networking devices, such as temporary or new remote control LAN access devices are integrated into the network-wire or wireless system
- Additional internal and external data connections are added for user access of components, applications and data

## 2.3 System Controls

Similar to IT networks, system controls are also part of OPSEC for industrial networks. Within the operating systems of some of the specific control system components (Human-Machine Interface computer [HMI], Front-End Processor [FEP]), certain controls must be in place to ensure instructions are being executed in the correct security context. Most operating systems have mechanisms that restrict the execution of certain types of instructions allowing them to occur only when the operating systems of the control system components are in a privileged or supervisory state. This protects the overall security and state of the control system and helps to ensure it runs in a stable and predictable manner.

As such, operational procedures must be developed that indicate what constitutes the proper operation of a control system and a control system resource. This would include a system startup and shutdown sequence, error handling, and restoration from a known and reliable source. If a specific control program needs to send instructions to hardware devices in the field, the request is usually passed off to a process of higher privilege. This is an integral part of the operating system's architecture, and the determination of what processes can submit certain types of instructions is based on the operating system's control tables. Many input/output instructions are defined as privileged and can be executed only by the operating system itself. When a user program needs to send input/output information, it must notify the system's core, which normally contains privileged processes that work at the inner rings of the system. These processes, called system services, authorize either the user program processes to perform these actions (and temporarily increase their privileged state) or the system's processes are used to complete the request on behalf of the user program.

## 2.4 Trusted Recovery

When an operating system or application, such as an HMI or FEP, crashes or fails in the control system environment, it should not put the control system in any type of insecure state. During the standard development and Design phase, control systems are generally designed to fail "safe" and not incur damage to the system. However, as new and more robust systems are introduced into the control system landscape, the need for recovery of the system with full integrity is required. When reviewing some modern cyber attack vectors, one of the key components of attack include the forced failure and rebooting of a compromised system, thus allowing any malicious code to impact the function of the information resource attacked. Thus, as part of the cyber OPSEC plan that addresses how systems will fail and recover (which may

span several components), the Design and Maintain phases are used to incorporate safeguards as they relate to recovery.

In general, how a control system component's operating system responds to a type of failure can be of value to the user/operator, and an understanding of what failures mean can contribute to an overall better understanding of cyber security in the control systems domain. Moreover, an effective cyber OPSEC plan that includes training, response, and management practices as applied can reduce system downtime and increase overall security posture.

System failures may be classified as one of the following:

- System reboot
- Emergency system restart
- System cold start

A *system reboot* takes place after the system shuts itself down (or is forced to shutdown) in a controlled manner in response to a trusted computing base (TCB) failure. Also, if the system finds inconsistent object data structures in its environment or if there is not enough space in some critical tables to perform key tasking, a system reboot may take place. The reboot often releases resources and returns the control system component to a more stable and safer state.

*Emergency system restarts* often takes place after a system failure happens in an uncontrolled manner; the cause of which may be anything from a core operation failing to work or a lower-privileged user process attempting to access memory segments that are restricted. The system may see this as an insecure activity that it cannot properly recover from without rebooting. When this happens, the system enters a maintenance mode and recovers from the actions taken and then is brought back online in a consistent and stable state.

A *system cold start* takes place when an unexpected activity happens and the regular recovery procedure cannot recover the system to a more consistent state. The system and user objects may remain in an inconsistent state while the control system attempts to recover itself. Intervention may be required by the control system user or administrator to restore the system.

From an OPSEC perspective, having the capability to monitor key file structures for integrity as well as functionality is advantageous. Moreover, for systems with a high level of observed "uptime," unscheduled restarts could be indicative of a serious security issue. The cyber OPSEC plan should have instruction and guidance on how these incidents are observed and reported, and can be deployed as new operational reporting standards or augmentations to existing operator reporting practices. In either case, cyber security applicability to traditional recovery may help contribute to a positive cyber security culture being developed and will support the overall reliability of the control system information architecture. Like all failures and reboots, the cause of these should be investigated as there may be security issues requiring immediate attention.

Modern control system domains have redundancy built in, with back up networks and key resources mirrored to accommodate for any catastrophic failure. Often, in the case of networked

infrastructures, facilities have secondary ready-to-go systems known as 'hot standbys' that are resident online information and control systems assets that are ready to come online in the event of primary system failure. Key to operations (and cyber security) is ensuring that these secondary systems are fully compliant with current configurations and, if needed, can become operational with the exact same configuration and system upgrades as the primary system. This way, if an event requiring a switch-over to the redundant system is required, operation can and will be maintained as if the main system was still online. Unfortunately, many organizations do not ensure key secondary systems are upgraded and configured to the same cyber security standards. There have been instances where secondary systems have been vulnerable.[16]

Having an OPSEC plan in place to instruct users on how to manage and report these issues not only provides effective cultural impact, but also provides inputs to key life-cycle phases such as Maintain and Design. In addition, observations and reporting can be used to support a better understanding of cyber risk and mitigation activities.

## 3. Technical and Non-technical Solutions

Programs that are designed to protect information and information assets have often referenced the three "pillars" of cyber security: Confidentiality, Integrity, and Availability (C-I-A). In this model, availability is one of the foundational and in most cases, highest priority objectives when applied to control systems. Whether this is correct, it is indeed a result of historically non-cyber security cultures having to make system uptime the primary operational activity. As these systems are seen converging with open networks and utilizing cyber resources to allow operations to be more efficient, the other two priorities of confidentiality and integrity become just as important.

Ensuring that the C-I-A model of cyber security is implemented is not enough to provide assurances to modern environments, and it has become clear that effective cyber security culture needs to be a by-product of both technical and non-technical activities. Working to reduce overall cyber security risk in an environment is not a function of technology and policy alone. Like the historical culture that protected physical assets and prevented access to operations centers, the modern security culture for control systems needs to include cyber security. Network and resource availability often is not fully appreciated until it is gone, especially for a control system operation.

Existing robust IT security programs provide capabilities an organization can reuse in its control systems domain and enhance the cyber OPSEC initiatives in the control system environments. These capabilities are often a blend of technical and non-technical solutions that reside outside of the life cycle function and contribute to the ongoing cyber security OPSEC process that nurtures a supporting cyber security culture. Overall, there are several key mitigation strategies that can support the cyber OPSEC initiative, but they can also have a considerable impact on developing a rich cyber security culture. These components include administrative activities, user accountability, countermeasures for single points of failure, and security awareness training.

[16] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf, January 26, 2007

## 3.1 Administrative Activities

### 3.1.1 Separation of Duties

Administrative management is an important, but often overlooked aspect of the OPSEC program in control systems and their associated industrial networks. One aspect of administrative management is the mitigation of threats that are already inherent in the operational domain, such as the trusted insider.

Traditional principles, such as the concept of "separation of duties" ensures that one person acting alone cannot compromise the critical infrastructure or industry's security via its control system. In short, such a practice forces collusion between coworkers and ensures no single person can act alone to carry out an attack. Many organizations currently have such practices in place to mitigate internal threats and it is a common deterrent to malicious activities that can be sourced internally to the operational domain. But it must be noted that in the case of cyber security, the risk is extended to the outside attacker as well. Moreover, the risk is extended due to either the trusted insider working with an external attacker (by providing information or access) or the attacker is a trusted insider using external access to carry out an attack.

Historically, and usually only dealing with attacks sourced in the physical domain, separation of duties would increases the overall level-of-effort a single person must extend to execute an attack and be successful. Operationally, high-risk activities involving critical assets under automotive control (e.g., a high-node substation, high-frequency railroad switches, or chlorine tank at a waste water treatment facility) were broken up into different parts and distributed to different individuals or departments.

But in the modern control environment, these core activities are directed by computer systems, often with programs and processes overseen by a single individual. Moreover, the computing resources in themselves can often be changed, updated, or used by single actors with nefarious intent. As such, the concept of a separation of duties that has historically been prominent in protecting critical operations in the physical domain needs to be extended to the cyber resources. But like other aspects within the cyber OPSEC plan, the separation of duties must not hinder the efficiency of carrying out the automated control function and a fine balance of security and business functionality must be maintained.

Each control system operator's role needs to have a complete and well-defined job description, and cyber security personnel should use these job descriptions when assigning control system access rights and permissions for specific control system operations. This may assume that the organization has a dedicated cyber security management team—a luxury that many small to medium size entities do not have. In addition, it needs to be recognized that in some cases the concept of separation of duties is simply not feasible, as the operations environment is administered remotely by a managed services entity or a peer site. Yet, in these cases, due diligence should dictate that the operators have access to only the control network resources required to carry out their tasks. For instance, to help define OPSEC parameters and instill cultural component, a control system configuration specialist/engineer should not be the only person to test their own configuration and any associated programmed code. Another person with a different job and agenda, who has familiarity with the control systems and the assets the

code is automating, should perform functionality and integrity testing on the original engineer's configuration. This should be done because the original configuration programmer may have a biased and narrow view of what the control program is to accomplish, and he/she may only test functions and input values for certain situations.**User Accountability**

Control system user access to resources must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to information assets. A user's access attempts while using a specific control system resource need to be properly monitored, audited, and logged. The individual user ID needs to be included in the audit logs to enforce individual responsibility. Each user should understand his responsibility when using control system and industrial network resources and be accountable for their actions. If user activities were not captured and reviewed, it would be difficult to determine if control system users have excessive privileges or if there has been unauthorized access.

Audit and function logs often contain too much cryptic or mundane information to be interpreted manually. This is why some products are now available that parse logs specific to control system hardware and report important findings. Logs should be monitored and reviewed, through either manual or automatic methods, to uncover suspicious activity and to identify an industrial network environment that is shifting away from its original baselines. This is how control system security administrators can be warned of problems before occurrence of security incidents. When monitoring, control system network administrators need to ask certain questions about the control system users, their actions, and their current level of access. Consider the following examples:

Are users accessing control data information and performing control system tasks that are not necessary for their job description? The answer indicates whether users' rights and permissions need to be reevaluated and possibly modified.

Are repetitive mistakes being made? The answer would indicate whether control system users need further training or system functionality needs to be modified.

Do too many users have rights and privileges to sensitive restricted control data or resources? The answers would indicate whether access rights to the control system and industrial network data and resources need to be reevaluated, whether the number of individuals accessing them needs to be reduced, and/or whether the extent of their access rights should be modified. User access to data should be removed promptly upon termination of need.

## 3.2 Addressing Single Points of Failure

In modern control environments, the convergence of the control technology with open networking and computing services often results in accelerated business capabilities and more granular control over the industrial architectures. However, in these activities, single points of failure can be created as a result of accelerated requirements or unique demands set by management, peer organizations, or even the vendors providing the industrial technology. These single points-of-failure often pose high potential risk to a control network. If a device fails, a large segment or even the entire industrial network is negatively affected. Devices that could represent single points of failure are firewalls, routers, network access servers, T1 lines,

switches, bridges, hubs, various control system computers, and authentication servers. The best defenses against being vulnerable to these single points of failure are proper maintenance, regular backups, and redundancy.

Multiple paths should exist between routers in case one router goes down, and dynamic routing protocols should be used so that each router will be informed when a change to the network takes place. An uninterruptible power supply (UPS) and redundant array of inexpensive disks (RAID), or other redundant fault tolerant backup method, should also be in place and properly configured. The UPS should be able to provide a clean and steady power source to the crucial systems and resources on the control network. RAID provides fault tolerance for hard drives and can improve system performance. Breaking up the data and writing it across several disks so that different disk heads can work simultaneously to retrieve the requested information provides redundancy and speed. Control data is also spread across each disk (called parity) so if one disk fails, the other disks can work together and restore the critical control and configuration data.

### 3.2.1 Fault Tolerance and Clustering

Clustering is widely used in IT networks as a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system for use in the enterprise network as well as the control or SCADA LAN. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which provides immunity to faults and improves performance.

If one of the systems within the cluster fails, processing continues since the other systems pick up the load. This is more appealing than having a secondary control system data historian server that waits in the wings in case a primary server fails. When clustering is used, all systems are used to process requests and none sits idle in the background waiting for another to fail.

### 3.2.2 Backups

Backing up control system software and having industrial network backup hardware devices are two large parts of control system and industrial network availability. Organizations need to be able to restore critical control data in many different scenarios, including if a hard drive fails, a computer resource fails, a physical disaster takes place, or some type of software corruption renders in-use data unavailable. The overarching security policy (one that has used OPSEC components) should be developed that indicates what data gets backed up, how often it is backed up, and how these processes should occur. This practice and the corresponding specifics of the OPSEC plan can be reused from preexisting (and proven) policies and directives. However, as in other cyber OPSEC components, practices need to be tuned and created to accommodate for the nuances and requirements of the control systems domain.

If control system users have important information on their workstations, the operations department needs to develop a method that indicates that backups include certain directories on users' workstations, or that users move their critical control data to a server at the end of each shift to ensure it gets backed up. Backups may occur once or twice a week, every day, or every

hour depending on the criticality and the dynamics of the asset under control. It is up to the organization to determine this routine and readers are encouraged to review sector-specific guidance if it is available. Generally, the more frequent the backups, the more time will be dedicated to the process; therefore, a balance is needed between backup costs and the actual risk of potentially losing critical control data. Again, such cyber OPSEC procedures will be unique to every organization, with many having to address issues related to a small support staff or entirely outsourced security and data recovery management functions.

Inherent with the need for backup documentation, data storage media, and physical separation of the backed up media from the operational system is the process for restoration of part or all of a control system after loss due to hardware, software or facility malfunction. Restoration processes and procedures should be documented to the extent needed to recover the systems in accordance with requirements defined in the OPSEC plan to ensure the system is recovered in the same state it was in prior to loss.

## 3.3 Training and Awareness

The cyber OPSEC plan is not complete without security training and awareness. Often considered one of the more difficult aspects of building a successful OPSEC plan, creating and maintaining an effective outreach program for user and operators is critical to both the culture and the self-sustaining nature of the program. To provide cyber security training into the control system domain, key areas of concentration are required to help bridge the user and operator's perspective on traditional physical security and new emerging issues in cyber security. Although this task may appear daunting at first, proven success in sector-specific training can be leveraged to allow an organization to create robust, accurate, and timely outreach content.

Using a standard framework for developing training content, best practices usually indicate that training must be received prior to any access to information resources. Many operators and users currently have access to the information domain, therefore control systems training must be relevant to existing operations and practices including cyber security elements. As it pertains to users and operators, cyber security training should:

- Be a requirement set forth by senior management
- Be a condition of employment and a mandatory requirement prior to any system access being assigned
- Be updated and provided at least annually, with all new hires taking cyber security training as per the design of the OPSEC plan
- Must not be unique to the employee, but be available to peer users, contractors, and other personnel that have access to the control system information resources to do their job function
- Be enhanced and perpetuated through the development of internal security working groups, with outreach supported by newsletters, e-mail broadcasting, and memos

- Include, but not be limited to, content associated with the cyber OPSEC plan:
    - Cyber security policy (including both business and control system specific content)
    - A review of physical security
    - Access controls, administration, and operating safeguards
    - Security and system acquisition (to allow for procurement and feedback into Design phase)
    - Incident reporting, handling, and continuity of operations planning
    - Data protection, data storage, and safe handling of data.

It is understood that in many cases, organizations have limited security staff and limited resources to create, manage, and deploy cyber security training programs. With that, it is commonplace for organizations operating in the control systems realm to provide specific systems training and outsource the cyber security training to a third party. If that is to occur, an organization may wish to ensure that the training content is applicable and aligned with both the operation's specifics and, where applicable, system-specific security content. It is paramount that the correct level of content is delivered in the right way (i.e., content for an operator is different from content for managers), so organizations are encouraged to seek references prior to outsourcing cyber security training for their operators.

Required content in the training should include:

- Background primer on computers, communications, and networking in control systems environments
- An introduction to cyber security risks in control systems (inclusive of relevant examples)
- A concise discussion addressing threats, common vulnerabilities, and architecture shortcomings that may reduce the overall level of cyber security in the operations enclave
- Training on contemporary IT security technologies and practices that can be used in controls systems (as well as methodologies used for proper deployment)
- Training on sector specific cyber security guidelines and organizational specific guidelines
- Training on any vendor-specific security guidelines
- Hands-on training to provide in-depth experience in working with control systems cyber security technologies, mitigation activities, and best practices.

# 4. Conclusion

Cyber security is frequently defined as a process. Most importantly, corporate and control system managers must begin the process of building this culture, and the development of an OPSEC program is an excellent start to promoting the vigilance required to establish and maintain this culture.

Organizations that have a fundamental business involving control systems have historically been very well prepared from a physical security perspective. Recent issues in convergence, where isolated systems are becoming more interconnected to business networks and each other, now require new capabilities to protect their systems from a cyber attack or attacks on their related information resources. A robust operational security plan, or OPSEC, can play a vital role in creating a robust cyber security program. This program can be used to combat and mitigate the threat of cyber attacks, reduce the overall risk to an organization, and increase the cyber security posture. By creating a cyber OPSEC plan and selectively populating it with the relevant content and information unique to an organization, operational procedures, systems life cycle, and overall user knowledge can be enhanced. Implementation of this plan can drive new understating of the importance of cyber security in the control systems domain, and create a cyber security culture that can perpetuate the protection of information and operational resources.

# 5. References


DHS Control Systems Security Program http://www.us-cert.gov/control_systems/, October 2006

Instrumentation, Systems, and Automation Society http://www.isa.org/community/SP99, November 2006

National Association of Regulatory Utility Commissioners http://www.naruc.org/, November 2006

North American Electric Reliability Council (NERC) http://www.nerc.com/, November 2006

Electric Power Research Institute http://www.epri.com/, November 2006

AGA-12: Cryptographic Protection of SCADA Communications General Recommendations“ http://www.gtiservices.org/security/AGA12Draft3r6.pdf, November 2006

Sandia National Labs Center for SCADA Security http://www.sandia.gov/scada/home.htm, November 2006

21 Steps to Improve Cyber Security of SCADA Networks http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf, January 2007

Common Vulnerabilities in Critical Infrastructure Control Systems http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf, January 2007

Process Control Systems Forum (PCSF) http://www.pcsforum.org/, November 2006

TSWG SCADA Security Website http://www.tswg.gov/tswg/ip/scada.htm, November 2006
NIST PCSF http://www.isd.mel.nist.gov/projects/processcontrol/, November 2006

Infragard http://www.infragard.net/, November 2006

Information System Security Association http://www.issa.org/, November 2006

Partnership for Critical Infrastructure Security http://www.pcis.org/, November 2006

Information Systems Audit and Control Association http://www.isaca.org/, November 2006

Presidential Directive on Critical Infrastructure: Identification, Prioritization, and Protection - HSPD-7 http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html, November 2006

Executive Order 13231: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/eo/eo-13231.htm, November 2006

Presidential Decision Directive 63: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/pdd-63.htm, November 2006

The National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/, November 2006

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets http://www.whitehouse.gov/pcipb/physical.html, November 2006