National Security Agency/
Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Securely Managing Industrial Control System (ICS) Networks

This publication is the fourth in a series intended to help Industrial Control System (ICS) owners and operators in need of improving the security posture of their systems. This document will focus the reader on aspects of implementing a secure ICS network management program through comprehensive network management policies and procedures. An effective network management program is an essential element of maintaining the security posture of critical ICS network segments. This publication covers important recommendations that should be included in secure and effective ICS network management programs.

Control Systems Division

Contents

1. Introduction 1

2. The Importance of Defining Security Management Policies and Procedures 1

3. Manage Network Changes 2

4. Manage the Risk of Malware Introduction 4

   4.1. Controlling Removable Media 5
   4.2. Controlling Electronic File Transfers 5

5. Monitor the Current State of the ICS Network 6

   5.1. Enforce a Log/Event Monitoring Policy 7
   5.2. Perform Non-Periodic Network Audits to Verify Security Policy Compliance 8

6. Manage User Accounts and Authentication Credentials 8

   6.1. Cryptographic Key Management 9
   6.2. Password Management 10

7. Software and Firmware Patch Management 12

8. Conclusions 13

1. Introduction

The process of securing critical ICS network infrastructures begins with installing proven technologies to eliminate or isolate potentially vulnerable services and block electronic intrusions. Security improvements such as employing secure network architectures, isolating network segments with routers and firewalls, choosing more secure ICS components, or augmenting vulnerable services with cryptographic protections are initially realized at the design and implementation/modification phase. Once a network installation or modification is complete, the system will ideally exhibit an acceptable resistance to electronic attack or intrusion. Unfortunately, all networks exist and operate in a dynamic environment in which requirements, threats, and even known vulnerabilities change on a regular basis. Failing to acknowledge and manage these dynamics will almost certainly result in the gradual degradation of the effective security posture of any network: over time, the network will no longer exhibit the intended resistance to electronic attack. Maintaining the intended security posture of installed/operational networks is an ongoing process that must be carefully managed to ensure the reliable operation of critical ICS network components.

2. The Importance of Defining Security Management Policies and Procedures

There are many dynamic factors that can reduce the security posture of an operational ICS network. Many of these security reducing factors originate from within the organization. For example, insecure practices by authorized users can severely jeopardize the security and reliability of the network. A user may inadvertently introduce a worm or virus onto critical ICS networks by opening infected files from a personal CD, USB stick or other external data source. Once activated, a virus or worm can quickly disrupt critical ICS services and leave the entire controlled process open to critical failure. Such security breaches can often be avoided by ensuring that authorized users on the system are educated about the potential danger of such risky actions, and are responsible for following formalized rules that impose consequences for such behavior.

Dynamic factors that impact the security of ICS networks can also originate from outside the organization. For example, vulnerabilities are very often identified that jeopardize the security of popular software/hardware products. The details of these vulnerabilities are often published upon discovery, making them available to malicious individuals that may use them to attack effected systems on exposed ICS networks. Naturally, the security of a given asset will decline as more vulnerabilities are discovered that effect it. The best way to prevent such degradation of security is to formalize the process of monitoring vulnerability releases and periodically applying security-related software/firmware patches to effected assets to remove discovered vulnerabilities.

Securing a network is not a “fire and forget” activity: formalized network management processes are required to ensure that the security posture of the network remains at or above the intended level. Formalized security policies and procedures must be defined, documented, and taught to inform users and network design/administration personnel of their responsibilities. These policies and procedures should be carefully crafted by personnel with an appropriate mix of information technology (IT) and ICS network design, operation, and security expertise. Many aspects of a formal network management program can serve to improve the reliability and availability of critical ICS systems and services.

Unauthorized network or ICS device configuration changes, risky behavior by system users, or security breaches caused by undiscovered electronic vulnerabilities can all lead to unpredictable network and/or ICS systems behavior that can jeopardize the safe, reliable operation of critical ICS components. Managing and mitigating these risks is essential to maintaining the reliability of the system. Implementing comprehensive network management policies and procedures will require a company-wide commitment, and an appropriate allocation of resources: qualified personnel must be made available to maintain security procedures and to audit and enforce policy compliance. An effective network management program is an essential element of maintaining the security posture of critical ICS network segments.

Once formalized security policies and procedures are created, all effected personnel must be trained to understand their responsibilities and the consequences of non-compliance. User compliance must be monitored and enforced by dedicated network security administration personnel to ensure that the ICS system maintains the required levels of security and reliability. The sections that follow include important recommendations that should be included in an effective ICS network management program.

3. Manage Network Changes

An effective network management program ensures that qualified security personnel take necessary steps to maintain an acceptable system security posture. It is essential that network security personnel maintain "situational awareness" by knowing the current security posture of the network. This awareness is dramatically reduced if users add new PCs and ICS equipment to the network, or make network architecture changes without involving network security administrators. Enforcing an effective network change management program sets up a formal framework that allows potential security and reliability impacts of proposed network changes to be assessed by a single, consistent group of qualified personnel who have an up-to-date, accurate view of the current state of the network (e.g. network layout, networked device types and firmware/software revisions, enabled communications services, assigned network addresses, etc.)

In this section, we discuss the benefits of a change management policy for specific types of network changes. Of particular concern are physical architecture, or software configuration changes that alter the availability of services and capabilities at various points on the ICS network.

Unauthorized network changes can lead to the introduction of significant vulnerabilities into critical ICS networks. A user requiring additional services or functionality may simply take the necessary steps to solve the problem without considering the implications of their actions. Users often lack the training to make critical security-related network decisions and usually lack the resources to support the changes that were made (e.g. monitor or patch newly installed devices).

Seemingly minor changes to the physical network infrastructure can dramatically reduce the security and reliability of critical ICS networks. Some examples include:

- Adding new devices to a network can result in address conflicts (e.g. repeated supervisory control and data acquisition (SCADA) protocol or Internet protocol (IP) addresses) and unpredictable behavior that can jeopardize the reliability of critical ICS communications.

- Adding a new PC with an out-of-date, unpatched operating system to an exposed network segment can provide exploitable vulnerabilities that attackers can use to get a foothold on the network.
- Connecting a device to two TCP/IP network segments via independent network interfaces can result in unauthorized bridging of the two networks. Connections can bypass carefully-managed security mechanisms like firewalls, router access control lists, and VPNs.
- Connecting a laptop with an enabled wireless network interface card to a critical ICS network segment can expose the connected laptop to remote, wireless attack and jeopardize the security of other networks to which it is connected.
- Installing an unprotected wireless network modem (e.g. 802.11x directional radio) to collect telemetry data from equipment in the plant or substation yard can expose critical ICS networks to wireless attack.
- Connecting a modem for engineering or direct vendor support can provide a back door into the critical ICS network for unintended uses.

A formal review process ensures that network changes can only be authorized by a qualified review committee after a thorough assessment of the potential security and reliability impacts of proposed changes. Significant security vulnerabilities like those listed above are unlikely to survive the assessment process without significant modification and security improvements.

Changes to the configurations of existing networked assets can also dramatically impact the security of the network. Devices that are directly responsible for maintaining network security are of particular importance. For example, minor changes or errors in firewall/router configurations can reduce or eliminate network isolation and expose critical ICS network segments to electronic attack. Changes to the configurations of security-critical assets including routers, firewalls, cryptographic security devices (e.g. inline modules or VPNs), intrusion detection systems, domain controllers, etc. should also be subject to the rules of the change management policy to prevent intentional or accidental reduction of their effectiveness.

Changes to other existing networked ICS assets can also impact the security of the network…

Written, formalized security policies and procedures should be created to prevent unauthorized network and asset changes that can jeopardize the security and reliability of critical ICS systems. The security policies should define the following:

- The networks, systems, assets, etc. that are to be governed by the network change management procedures.
- A change authorization process that ensures that proposed changes are thoroughly reviewed by a consistent group of personnel with a high level of network security and ICS networking expertise.
- Procedures for documenting all changes such that networks maps, asset management records, etc. remain up to date and accurate.
- Consequences for not complying with security policies and procedures.

4. Manage the Risk of Malware Introduction

Malware, like viruses and worms, can pose a significant threat to critical ICS networks. Infected workstations, servers, or embedded ICS devices can cease to function properly, potentially effecting critical ICS functions. In addition, self-propagating malware variants can cause a dramatic rise in network traffic as infected systems probe the network looking for additional targets. The resulting reduction in network performance can negatively affect critical ICS functions that require low-latency, reliable communications to perform correctly.

In addition to the reliability concerns discussed above, malware can pose a significant threat to the electronic security of infected assets. Some worms, viruses, and Trojan horse applications are designed to install backdoor communications services on infected assets, allowing attackers to partially bypass user access controls in the operating system. A remotely-accessible backdoor service can give an attacker elevated access to the infected asset, often including the ability to execute commands or upload and run malicious code (e.g. attack programs) on the compromised device.

There are two main classes of malware transfer avenues:

1. **Vulnerable Communications Services:** self-propagating malware takes advantage of flaws in specific communications services to automatically spread from an infected computer to a target computer.
2. **File-borne Infection:** a user opening an infected data file or program activates the malicious payload and causes infection of the computer on which the file was opened.

Threats from the first malware transfer avenue, vulnerable communications services, can be mitigated by isolating critical ICS network segments with secure network architectures protected by firewalls/routers with strict traffic filtering rules; if vulnerable communications services are not allowed to flow between less secure networks and protected, critical ICS network segments, they cannot be used to propagate malware. Applying security-related software patches is also critical for fixing communications vulnerabilities before a worm can exploit it to get a foothold on critical ICS network segments and/or spread between assets on a critical ICS network segment. We discussed network isolation and traffic filtering in previous documents in this series and we discuss patch management in a latter section of this document.

Because a properly-designed ICS network should be largely isolated from less secure network segments (e.g. the Internet or corporate network), the second malware transfer avenue, file-borne infection, is a more likely means to affect most critical ICS networks. The most effective way to mitigate the threat of file-borne malware is to implement strict policies and procedures to control the transfer of external files (e.g. data files that originate from outside the controlled network infrastructure) onto critical ICS network segments.

There are two primary sources of file-borne malware that must be controlled: the introduction of infected files via portable/removable media and the electronic transfer of infected files via file transfer communications protocols.

4.1. Controlling Removable Media

Policies and procedures must be in place to strictly control the use of portable sources of external data on critical ICS network segments. Removable media such as CDs, DVDs, flash memory sticks/cards, and removable hard drives can contain infected files which can be imported onto critical ICS network assets by users. Any data source containing files that originate from outside protected ICS network segments should be considered a potential risk. This definition includes less obvious data sources like digital cameras or media players (when connected to a networked ICS computer), and portable laptop computers that are allowed to leave ICS facilities and occasionally connect to outside networks.

Strict policies should be put in place to restrict the use of portable external data sources and to define the procedures required to transfer files from portable data sources onto critical ICS network. Policies should include the following recommendations:

- The use of portable sources of external data must be reviewed and approved by qualified personnel on a per instance basis. The source and purpose of the files on the media should be assessed to eliminate risky items.
- Upon approval, the contents of the media must be scanned by virus/malware detection software prior to allowing the contents of the media onto the protected network.
- A process should be defined to ensure that the virus definitions on the media-scanning PC are sufficiently up to date (e.g. updated at least once per week).
- Computers that have connected to external, untrusted networks should not be allowed to connect to critical ICS network segments; it is simply too difficult to ensure that the entire file system is malware-free.
- All software installed on ICS network assets should be supplied by trusted vendors

It is often convenient to set up a dedicated workstation isolated from critical ICS network segments from which portable media can be scanned by the review team. This setup ensures that virus definitions can automatically be kept up to date by connecting to the vendor's virus definition update servers via the Internet. It also prevents potentially infected files from accidently being transferred onto ICS network segments before the scanning process has successfully completed.

4.2. Controlling Electronic File Transfers

It is often necessary to allow electronic file transfers to flow between less trusted network segments and protected ICS network segments. Examples include access to shared folders on external file servers, access to external file transfer protocol (FTP) or secure shell (SSH) servers, or file downloads via web services (e.g. direct download via a website or Microsoft SharePoint portal). Preventing the transfer of malware-infected files has been a common challenge in the IT world since the advent of modern networking. One very effective solution is to use communications proxy servers to transparently scan requested files for the presence of malware signatures prior to forwarding them to the requesting user/device on the protected ICS network. Proxy servers can be placed on a demilitarized zone (DMZ) subnet to allow safer access to external files while maintaining acceptable ICS network isolation. Proxy products are widely available that are designed primarily for securing web services and e-mail, but some

support dedicated file transfer protocols like FTP. Single purpose file transfer protocols like FTP or the secure copy command in SSH are a safer alternative than multi-purpose protocols like web services (e.g. http and https). Allowing web services to flow from less trusted network segments to critical ICS network segments can be dangerous (even if a proxy is used) because it is extremely hard to control and secure the diverse content and capabilities that can be transferred/accessed via http and https.

It is also possible to create a file sharing proxy on a DMZ by utilizing file replication services to synchronize files on shared folders on a file server on the less trusted network, with those available on the file server proxy on the DMZ. This approach allows file sharing protocols to flow between the ICS network and the less trusted network segment without bypassing the network isolation benefits of the DMZ subnet. If access to shared folders on less trusted networks is allowed, it is important to ensure that host-based virus scanning software is installed on the file servers and is set up to scan all files in the shared folders.

The contents of any accessible file stores should be carefully controlled by qualified personnel. The source of any file that may eventually be transferred to the protected ICS network must be carefully considered. All files available for transfer from less trusted network segments to critical ICS network segments (e.g. through the secured proxy via the DMZ) should originate from known, preferably trusted, sources. Examples include internal documents produced by coworkers and documentation or software from trusted vendors. Files from untrusted sources should not be placed on file stores accessible from protected ICS networks. Examples include external e-mail or software from unknown vendors.

Policies and procedures should be put in place to manage the security of the file transfer services. Policies should include the following recommendations:

- Processes must be defined to ensure that files available for transfer to critical ICS network segments originate from trusted sources.
- Transfers allowing file sharing protocols to flow between the ICS network and less trusted network segments must utilize the network isolation benefits of a DMZ subnet.
- File servers and/or file transfer proxy servers must be set up to ensure that all files are scanned by virus/malware detection software prior to transfer to critical ICS network segments.
- A process should be defined to ensure that the virus definitions on file servers or file transfer proxy servers are sufficiently up to date (e.g. updated at least once per week).

Because most critical ICS network segments should be significantly, or totally isolated from the Internet, automated virus update procedures may not be possible. On closed networks, it may be necessary to periodically download new virus definitions via a separate, Internet-connected computer that is not part of the critical ICS network. The downloaded virus definition updates will then have to be manually transferred to servers on the ICS network for distribution to virus/malware scanning client software.

5. Monitor the Current State of the ICS Network

Modern communications networks are dynamic and require constant consistent monitoring to verify that the system is operating in a secure and reliable state. Adhering to effective security policies and procedures will reduce occurrences of irresponsible user behavior and mitigate the presence of

significant electronic vulnerabilities on ICS networks. However, it is not sufficient to put such policies in place and simply assume that they are having the desired effect. The best tool to help prevent security policy/procedural breaches is periodic, frequent user education; users must understand their responsibilities and know the consequences of non-compliance. Network monitoring is required to ensure policy compliance and to increase the chance of detecting events that jeopardize the security of the system.

5.1. Enforce a Log/Event Monitoring Policy

A secure network design incorporates technologies that allow system administrators to monitor network and user activity at key locations on the system. Exposed electronic attack entry points like a DMZ network segment separating a critical ICS network from a less secure network segment are great examples of key locations that should be routinely monitored. Many critical ICS assets including security products like intrusion detection systems, routers, firewalls, and VPNs, or critical PC-based assets like SCADA database servers or operator workstations can, and should be configured to generate activity logs that can be consolidated at a specified location (e.g. in a log server via the syslog protocol). These log entries are essential tools for detecting suspicious activity such as electronic attack traffic or suspicious user login attempts, but are only valuable if qualified personnel routinely analyze and respond to the collected logs. There are products available that can dramatically speed the analysis process, but the process of filtering, interpreting, and reacting to the collected log entries is still largely a manual process that must be conducted by qualified personnel. Especially important log entries, like those generated by intrusion detection systems must be extracted and analyzed quite frequently (ideally, in real-time). Most log analysis tools, like Security Information and Event Manager (SIEM) platforms, allow administrators to automate the filtering and extraction of suspicious log entries and support almost real-time notification (e.g. via e-mail).

It may also be prudent to periodically monitor activity on critical ICS assets that do not support generation of automated, centralized collection of event log messages. Most embedded ICS devices like programmable logic controllers (PLCs) or protective relays support some form of logging that can be used to detect suspicious behavior (e.g. login failures or unauthorized device configuration changes). Unfortunately, these activity logs often have to be analyzed manually by viewing them via the device's engineering access interface. This process can be quite time consuming, but may be worth the effort to monitor especially critical ICS systems for which automated monitoring techniques cannot be employed.

Policies and procedures should be put in place to monitor critical ICS systems for suspicious activity. Event log analysis policies should define and document the following items:

- Which ICS assets are to be monitored via log collection.
- Which events are to be collected and analyzed from each monitored asset.
- How logs are to be collected from each monitored asset.
- Who is responsible for collecting and analyzing event logs.
- The frequency with which each device's log entries are to be analyzed.
- Procedures for reacting to various classes of detected suspicious events.

It is extremely important to maintain critical ICS functionality when reacting to detected suspicious events (e.g. signs of an active electronic attack). Qualified individuals need to define and document procedures for reacting to potential attack scenarios while ensuring that critical ICS functions continue to operate safely, or are shut down in a predictable, safe manner. Log analysis personnel should know how to react to a wide variety of potential events in a way that ensures that the suspicious activity is successfully isolated while maintaining the safety of critical ICS functions.

5.2. Perform Non-Periodic Network Audits to Verify Security Policy Compliance

As stated earlier, effective security policies and procedures should contain components that eliminate unauthorized network changes. Unfortunately, user compliance with even the most formalized and established rules and procedures is not guaranteed. The best tool to help prevent unauthorized network changes and other security policy/procedural breaches is periodic, frequent, user education. Users must understand their responsibilities, know the consequences of non-compliance, and sign user agreements before access to critical assets is allowed. It is also recommended that qualified personnel conduct non-periodic network audits to verify policy compliance. It is not realistic that an audit team will discover all security policy violations during even the most rigorous network inspection. A thorough audit conducted by a qualified team should, however, detect many of the most dangerous violations including the presence of unauthorized devices, network bridges, electronic access points (e.g. dialup or wireless), or unauthorized/unused user accounts. Conducting these audits at unpredictable times increases the likelihood of finding violations/violators attempting to avoid detection.

A thorough visual network inspection should be conducted non-periodically by qualified security management personnel (e.g. approximately annually) to verify that the current network state matches documentation reflecting the presence and architecture of all authorized networked assets. The configurations of important security-related devices like firewalls, routers, VPNs, IDSs, and critical servers should also be compared against security policy and asset management documentation to verify that the security posture of the network has not been degraded. Device configuration audits can reveal unauthorized user accounts, changes to firewall/router access control lists, or other undocumented changes that can jeopardize the security of critical ICS network assets.

Policies and procedures should be put in place to audit critical ICS networks and assets to verify security compliance. Network and asset audit policies should define and document the following items:

- Which networks should be audited and which asset configurations should be verified
- Procedures for unauthorized asset and unauthorized user discovery
- Verification of existing network and user documentation and procedures to make revisions
- Procedures for verifying the correct scope of training and coverage of user agreements

6. Manage User Accounts and Authentication Credentials

Access control technologies are often implemented in critical ICS assets to protect against unauthorized electronic access. The effectiveness of most access control techniques rely on the secrecy of some form of authentication credential such as a binary cryptographic key or username and password string values.

Active management of access control credentials and user accounts is necessary to ensure that only authorized users are allowed access to protected assets.

6.1. Cryptographic Key Management

Cryptographic technologies are a very effective mechanism for authenticating the identities of communicating devices or users, and/or protecting sensitive data from interception by unauthorized individuals. Large binary key values serve as authentication or encryption credentials that prevent unauthorized individuals from bypassing the cryptographic protections. Maintaining the secrecy of these binary key values is essential for preserving the integrity of the cryptographic security protections.

Cryptographic security mechanisms are usually configured by network security personnel. Once configured, the cryptographic protections often take place "behind the scenes" with no interaction from the user accessing the secured communications services. The average system user does not usually have to present cryptographic key values to access a protected asset or use a protected communications link. Because of this, only personnel responsible for configuring the cryptographic protections have to know the binary key values. From a network management standpoint, this is a good thing: it is easier to keep cryptographic key values secret, or periodically change key values when few people need to know them to perform their duties.

Sensitive cryptographic key values, or the passwords from which they are generated[1], should be physically stored in a location that is only accessible to personnel authorized to view/know them (e.g. a small team of network security personnel responsible for maintaining cryptographic security protections). Storing them in a stationary, fire resistant safe located in a physically-secured location is acceptable provided only authorized individuals can access the contents of the safe. Storing key values in an isolated, physical form (e.g. in encrypted form on a CD or flash drive) rather than electronically on a networked storage site ensures that they will be accessible even in the event of a severe degradation of network security or reliability.

Cryptographic key values should be changed when authorized security administration personnel no longer require knowledge of their values (e.g. when they leave or change roles within the organization). Any authentication credentials used to access the new stored keys (e.g. the safe combination and encryption password) should also be changed at this time.

Ideally, cryptographic keys should be changed periodically even when there are no significant changes to network security staffing that may otherwise necessitate a key change. Cryptographic key values are much less susceptible to targeted guessing attacks than password string values, but changing key values every year or two is still an effective way to limit the effects of an undetected compromise of cryptographic protections (e.g. theft or disclosure of key values by an insider). Most cryptographic devices support mechanisms that allow security administration personnel to minimize the impact on

[1] It is quite common for cryptographic service configuration utilities to allow system administrators to specify cryptographic key values by entering a password string or phrase; words or phrases are much easier to remember than large binary key values. Mathematical transformations, usually involving cryptographic hash algorithms, then form the binary key value from the specified string.

protected communications during key change operations (e.g. coordinated key switchover mechanisms to prevent unacceptable link downtime).

Policies and procedures should be put in place to implement access control protections ensuring that only authorized assets have access to critical ICS networks. Access control policies should define and document the following items:

- Which networks and assets should be access controlled, by which mechanisms, and to what level
- Procedures for keeping cryptographic keys and passwords secret and safely stored in an isolated physical form
- Procedures for safely changing key values and passwords both periodically and when personnel change

6.2. Password Management

Password-based user authentication schemes are extremely common in ICS networks. Password entry requirements prevent unauthorized access to PC workstations and servers as well as critical ICS devices like PLCs and protective relays. Preventing unauthorized individuals from knowing password values protecting critical ICS assets and functions is essential to maintaining the security of the ICS network.

Effective password management policies and procedures reduce the chance of password compromise. In an ICS environment, it is especially important to balance security improvements with system availability. Some password management techniques have the potential to prevent authorized users from accessing critical ICS systems and services. Unintended loss of user access can jeopardize the reliable operation of critical ICS components. For example, an automatic password expiration policy on a critical ICS operator workstation may detect that the operator's password was not changed in the required time period and prevent the user from logging into the workstation. An automated account lockout may prevent the operator from logging into the workstation to respond to an emergency situation and prevent system damage or human injury. The potential for unintended reduction of ICS system availability/reliability must always be considered when crafting network management policies and procedures.

Passwords should be changed every six months to one year to reduce the chance of compromise. In addition, when authorized users leave or change roles within the organization they should be denied access to ICS assets that they are no longer authorized to use. The process of denying user access often involves changing system passwords or deleting/disabling login accounts on ICS assets to which the user previously had authorization to access. There are two classes of password schemes common in ICS networks each of which requires a slightly different approach to managing password changes:

- **User Level Password Schemes:** each user on the system has a unique username and password combination and no two users share knowledge of a password value.
- **Role-Based Password Schemes:** login parameters are defined for a finite number of unique roles and potentially many users share the password value assigned to each role.

User level authentication is almost universally supported by modern PC operating systems: users log into a PC with a unique username and a unique, user-defined password value. For such systems, executing

periodic password changes is fairly straightforward because users themselves can change their own passwords with little or no coordination with other users or security administrators. Most PC operating systems support security policy options that will cause the system to automatically notify users when they need to change their password. If the user does not change the password in time, the system will lock the account. Automatic password expiration options are extremely effective and should be employed on systems for which the risk of forced user lockout is acceptable. For critical ICS systems for which unintended user lockouts are unacceptable, automated password expiration options should remain disabled. If automatic password expiration options are disabled, the security administration personnel should "manually" enforce password change policies by notifying users when their password must be changed, and verifying that they comply with the request. Finally, selectively denying a given user access (e.g. due to termination or job change) to an asset employing a user level password authentication scheme simply requires a security administrator to delete or disable the user's login account on the asset. Because the password is not shared by other users on the system, the account can be safely removed without affecting other users.

Role-based password schemes are very common in embedded ICS devices. For example, a device may only support two fixed login "identities" with a unique password for read-only access and another for read/write access. It is also common in ICS networks to set up shared PC workstations to use role-based authentication. For example, a plant monitoring and operations workstation may be set up with an account with the username, "operator", and a single password that is shared amongst all operations personnel that use the workstation. Executing password changes on a system with roll-based authentication requires coordination by security administration personnel. Because passwords are shared amongst potentially many users, the security administrator must choose the new password value and notify all effected users prior to executing the password change. Improper planning and execution of the password change can cause unintended user lockouts if all authorized personnel are not properly notified of the new password value. Security policies and procedures should be enforced to ensure that up-to-date documentation exists listing all password-protected assets on the ICS system and all personnel authorized to access each device. An accurate user access privileges document is essential for identifying which system passwords must be changed in the event of personnel changes (e.g. termination or job change) and for identifying which authorized personnel must be notified when executing a password change. Security administrators must take great care to ensure that all critical ICS components are available to authorized users that need them to ensure the safe, reliable operation of the system.

Password management policies should ensure that secure password values are chosen during all password changes. Default password values should never be used and, if possible, chosen password values should be resistant to automated password guessing attacks: password values should contain a mix of letters, numbers, and non-alphanumeric characters, and should not form a recognizable word. Critical ICS devices that do not support sufficiently strong passwords may need to be secured with additional access control technologies (e.g. inline cryptographic modules).

Password values for role-based access controls should be managed by security administration personnel to ensure that secure values are chosen and that system password values are properly documented and stored in a secure location. Password values for user level access controls are typically chosen by the user, so user education and active password management policies are required to ensure that secure

values are chosen. Most modern PC operating systems include options that security administrators can set to automatically enforce secure password policies: insufficiently complex password values will be automatically rejected by the operating system. Automatic password complexity enforcement policies should be activated whenever possible.

Policies and procedures should be put in place to implement user authentication ensuring that only authorized users have access to critical ICS networks and assets. User authentication policies should define and document the following items:

- Which networks and assets should have user access control, by which mechanisms, and to what level
- Define password complexity policies and how to protect critical ICS assets that don't support sufficiently strong passwords
- Define the circumstances where automatic password complexity, automatic password expiration, and automatic lockout policies can be safely implemented and not impact operational availability
- Procedures for changing default password and keeping all passwords secret to reduce the chance of compromise
- Procedures for safely changing passwords both periodically and when personnel change

7. Software and Firmware Patch Management

Software/firmware design flaws are the root cause of many of the electronic vulnerabilities that attackers exploit to gain a foothold on targeted networks and to propagate attacks to other networked systems. Such flaws often allow attackers to exploit vulnerabilities in exposed communications services to disable targeted assets, or to execute malicious code on targeted assets. Vendors routinely issue software/firmware patches to fix discovered vulnerabilities in specific applications or communications services. Failure to install issued patches can leave exposed communications services vulnerable to electronic attack and jeopardize the reliable operation of critical ICS components.

Network management policies must be put in place to ensure that qualified personnel actively monitor patch releases for products employed within the ICS network in order to maintain an accurate assessment of the current state of security of critical ICS functions. Whenever possible, applicable patches should be installed when published vulnerabilities jeopardize the security of critical ICS functions. Patches fixing published vulnerabilities in PC operating systems, popular PC-based software packages, and popular brands of embedded firewalls, managed switches, routers, VPNs, etc. are particularly important because such vulnerabilities are closely monitored by the hacking community and are routinely targeted by published exploits (e.g. worms and attack scripts/programs). Vulnerabilities in ICS-specific software packages and hardware products are less likely to be openly published, but may still be discovered by dedicated attackers interested in effecting critical ICS infrastructure targets.

Installing patches in an ICS environment is complicated by the need to maintain an acceptable level of availability of critical ICS services and function. Installing patches can reduce system availability in the following ways:

- Vendor issued PC software patches can be incompatible with other, interrelated software packages installed on the PC. For example, patching the operating system can break critical ICS packages like SCADA data servers or system operator human-machine interface (HMI) packages.
- Upgraded software packages or firmware upgrades may be incompatible with projects/configurations developed for older versions of the software/firmware. For example, upgrading an HMI package my cause the designed operator screens to stop working, or upgrading ICS device firmware may render the current device settings invalid.
- Installing software patches will cause system downtime while the software installs and, if necessary, the system reboots. This process can leave critical ICS functions unavailable for several minutes during the install.
- Installation errors during software patching or firmware upgrades can cause extended or permanent device failure. For example, a communications error during an ICS device firmware upgrade can leave the device in an indeterminate state and unable to successfully boot up.

An effective patch management program should minimize system downtime during security-related software/firmware upgrades. Qualified personnel must test vendor software patches for compatibility and stability on representative, offline test systems (e.g. not connected to the ICS network) prior to dispatching them on active ICS network assets. In addition, installing tested patches on active ICS network assets should be conducted in a manner that minimizes or eliminates the chance of negatively effecting the safe, reliable operation of critical ICS systems. Upgrades must only be applied to devices that can safely go offline for a potentially extended period of time while the process control system is online, or at times when the process control system can be brought offline or put in an otherwise safe state.

Policies and procedures should be put in place for effective patch management to fix vulnerabilities in critical ICS assets and limit exposure to exploitation. Patch management policies should define and document the following items:

- Which assets should have patches applied, by which mechanisms, and to what level
- Protections for critical ICS assets that have not been patched or can’t be patched
- Procedures for monitoring critical patch releases and assessing impacts to ICS security posture
- Procedures for safely acquiring patches from trusted sources and verifying them on off-line test systems before deployment in active ICS network assets
- When verified patches can be safely implemented and not impact operational availability

8. Conclusions

All networks exist and operate in a dynamic environment in which requirements, threats, and even known vulnerabilities change on a regular basis. Failing to acknowledge and manage these dynamics will almost certainly result in the gradual degradation of the effective security posture of any network: over time, the network will no longer exhibit the intended resistance to electronic attack. Maintaining the intended security posture of installed/operational networks is an ongoing process that must be carefully managed

to ensure the reliable operation of critical ICS network components. An effective network management program is an essential element of maintaining the intended security posture of critical ICS systems and includes written, formalized security policies and procedures to:

- prevent unauthorized changes
- manage the risk of malware introduction
- monitor critical ICS networks and assets for suspicious activity
- implement the correct scope of user training and coverage of user agreements
- perform non-periodic network audits and asset configuration change audits
- implement access control protections
- implement user authentication
- implement effective patch management