IDC TECHNOLOGIES

2nd Safety Control Systems & Hazardous Areas Conference
Auckland, New Zealand
Tuesday 22nd – Wednesday 23rd August 2017

Session Five

Practical Cyber Security for Safety Instrumented Systems

Peter Jackson
Senior Systems Engineer – ECL Engineering Control

Abstract

Cyber attacks on a DCS/PLC/SCADA systems can lead to serious consequences. The consequences on SIS can be even more significant. International best practice as defined by IEC/ISA standards requires that the cyber security level needs to provide more risk reduction than required safety integrity level for SIF to be effective. Proper management of ICS Cyber Security is key to mitigating the risks of a security breach of an SIS. This paper outlines 10 steps to help defend against targeted and non-targeted threats:

1. Cyber Security Management
2. Asset Inventory
3. Network Segmentation
4. Secure Access
5. Role-Based Access & Logging
6. Password Policy
7. Device Hardening
8. Personnel & Training
9. Involve Management
10. Detect & Response Plan

Disclaimer

It is acknowledged that even well-defended organisations may experience a cyber incident at some point. This paper cannot, and does not, offer any insurance against such incidents. Organisations are urged to seek professional advice in addressing the risks identified here.

Introduction

Included in the new revision of IEC 61511 are requirements to identify security threats and provide reliance against identified security risks. This paper will outline practical techniques in accordance with best practice to ensure that the safety instrumented system will function effectively despite increased risk in the 21st century. Air-gaps and firewalls only provide limited protection. An intentionally or unintentionally comprised SIS could result in reduced process safety protection, or worse still, initiate unsafe or unstable process conditions, as recent ICS security incidents have shown. Functional safety and cyber security can work together to improve plant safety only when security risks are considered and controls are implemented and managed effectively.

Body

Process Industry Standards

The following process industry standards relate to Cyber Security for Safety Instrumented Systems (SIS):

The IEC 61511 standard [1] defines the design, implementation and management of safety instrumented systems in the process industry as a part of functional safety and risk management required by IEC 61508. This standard was updated in 2016, with clause 8.2.4 specifically requiring *a security risk assessment [to] be carried out to identify the security vulnerabilities of the SIS*. Users of the IEC 61511 standard are directed to seek guidance related to SIS security from IEC 62443-2-1 and ISA TR84.00.09.

The IEC 62443 series of standards [2] defines procedures for implementing electronically secure Industrial Automation and Control Systems (IACS), also referred to as Industrial Control Systems (ICS) of which the SIS is a part. Developed by the ISA99 committee, there are thirteen documents currently planned or published for the IEC 62443 series. The standards outline (among other things) aspects of creating and managing an effective IACS security program as well as system design guidance and requirements for the secure integration of control systems.

ISA TR84.00.09 [3] follows on from the work by the ISA99 for IEC 62443. The technical report addresses countermeasures that can be used to reduce the likelihood of a security breach that degrades the ability of the SIS to perform its functions. It describes performance criteria to guard against internal and external security threats to the SIS and provides guidance on how to comply with IEC 61511.

Together these standards outline best practice design for Safety Instrumented Systems globally.

In addition, the New Zealand National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau (GCSB). Their role is to protect New Zealand’s most significant organisations from cyber borne threats. In partnership with the New Zealand Control Systems Security Information Exchange (CSSIE) group has developed the NCSC Voluntary Cyber Security Standards for Industrial Control Systems [4] to recognise and address cyber security risks associated with the operation of ICS technologies in New Zealand.

These standards set the framework by which Industrial Control Systems (ICS), including the more crucial Safety Instrumented Systems (SIS), can be managed effectivity. The aim is for all systems to function as designed without impact from malicious or inadvertent cyber security threats.

The Time for Cyber Security is Now

In the past, ICS components including SIS and Programmable Logic Controllers (PLC) were isolated from all network connections – effectively air gapped. At this time, there was no credible risk to these systems as they were isolated and running proprietary software. As various technologies have developed, the advent of networking has enabled remote access, monitoring and control to these systems. Furthermore, incidents such as Stuxnet [5], the German Steel Mill attack [6] and the Ukraine Black Energy [7] have highlighted that threats exist for ICS. This is not surprising as these types of systems have typically not been design with security in mind. Exasperating this effect is the high reliability of these systems and difficulty in patching, upgrading or replacing due to continuous operation of these systems in industry. Add in the increased availability of malware tools available and the perfect storm emerges, with ICS in the centre.

Practical SIS Cyber Security

The framework provided by the standards offers best practice protection for ICS and especially SIS. The following practical aspects should combine to reduce risk to the ICS and SIS, with the intention to stop or slow attackers as they attempt to impact operations. These steps will help defend against targeted as well as non-targeted threats.

1. Cyber Security Management

Develop a plan for implementing ICS Cyber Security in your organisation. Schedule regular meetings with stake holders to ensure that actions are assigned and completed and progress is made to strengthen existing barriers and add additional barriers. Develop methods, process and philosophies for securing ICS systems. Ensure that the boundary for the ICS Cyber Security personnel is clear so that they know what is within the scope of their control.

This management framework forms a foundation for the other steps in this paper.

2. Asset Inventory

Work through a systematic process to catalogue all configurable devices in the ICS. Include servers and workstations as well as SIS, PLCs, switches and firewalls. Record data on the make, model, firmware, anti-virus software, operating system including versions, networking information. This information will assist in disaster recovery, cyber risk assessment and incident response. Ensure critical assets are identified including SIS components (controllers, configuration workstations, etc.). Consider the appropriate place for your organisation to store this information as it contains valuable information that a hacker would want to know to penetrate your systems. Ensure that the access is restricted and the data is password protected.

3. Network Segmentation

Implement network segmentation between various aspects of the ICS. This can be via isolating systems or connecting them using a firewall appliance. Ensure that all firewalls are configured to a design, tested and kept up to date with the latest security patches. By separating resources into different network areas, a compromise of one system has less effect on other systems. Be mindful that air-gapped systems offer some protection, but investing in a ‘castle wall’ strategy only offers one layer of protection. Often, system connectivity is an advantage allowing remote visibility and/or control, but should be managed securely. Ensure that firewall logs are part of a log management system so that if/when a compromise occurs, the cyber security team can be aware of the breach and respond accordingly. For best results, a certified network security barrier should be utilised. For Windows machines, Windows firewall should be enabled if supported by relevant vendor software, adding an additional layer of protection.

Part of a network segmentation defence-in-depth strategy is use of the Purdue Model for Control Hierarchy. An example is show in Figure 1

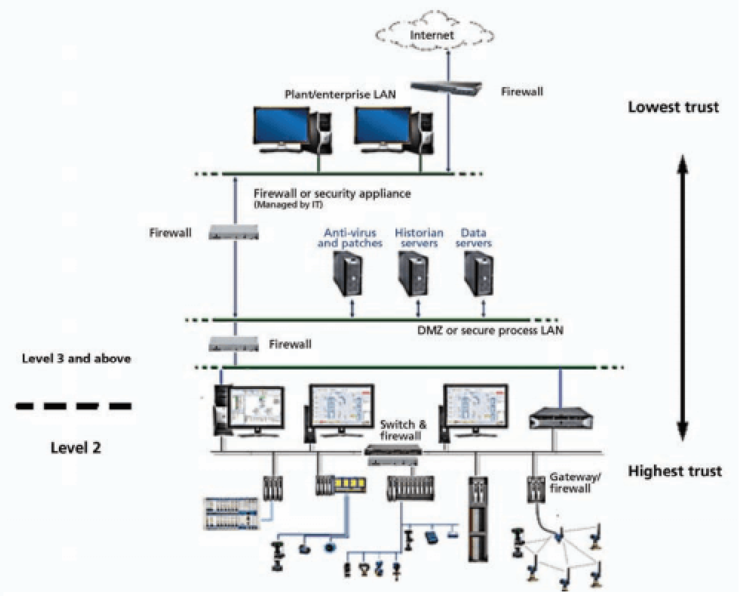

Figure 1 – Purdue Model example

Use of this type of structure allows multiple layers of protection, ensuring that if a breach occurs in the enterprise network, there is still protection in place for the lower levels including application network, control systems network and safety systems network. For more information on this architecture, see the SANS Institute: Secure Architecture for Industrial Control Systems paper [8].

In implementing appropriate network segregation, organisations will likely come across a meeting between information technology (IT) and operational technology (OT). IT personnel are typically responsible for operation and maintenance of infrastructure in the enterprise network (Purdue level 4+). OT personnel are typically responsible for operation and maintenance of infrastructure in the control systems network (Purdue level 3-). Some of the conflicts between IT and OT are shown in table 1:

Information Technology	**Operational Technology**
• Level 4+ • Servers/PCs • People focus • Lifetime 3-5 years • Server focus • Confidentiality and integrity focus	• Level 3- • All configurable devices • Device focus • Lifetime 15-20 years • End-point focus • Safety and availability focus

Table 1 – IT vs OT

This conflict between IT and OT should be managed by ensuring that IT and OT representatives form a part of the cyber security team. Policies and procedures should clearly outline roles and responsibilities so that effect cyber security management can take place. For more information on IT vs OT, see the Nex Defense: IT OT Convergence Whitepaper [9].

4. *Secure Access*

Ensure that access to all ICS assets is restricted as much as practicable. This includes physical security to server rooms, control rooms, configuration workstations and plant areas. After-hours access should only be provided to those with a genuine need. Workstations should have a screen saver requiring a password to unlock to prevent unauthorised access (a continuously manned control room being the exception). Only authorised workstations (including laptops) should have access to the ICS network – these should have up to date anti-virus and operating system security patches. Utilise managed network switches for the ICS network, turning off unused ports and triggering an alert when port status changes. Where remote access is required, ensure a thorough risk assessment is completed and risks managed out as part of the design and implementation, including the use of VPN encryption. Use secure protocols where possible for configuration, access and management.

5. *Role-Based Access & Logging*

Where ICS systems have user management capabilities, implement role-based access control, ensuring that end users only have access to the applications and services they need to carry out their role. Named logins (Joe Bloggs not User1 or Administrator) ensure that user accounts can be enabled/disabled as team members come and go without changing a shared password every time or accepting residual risk. Furthermore, Joe may think twice about making unauthorised changes if he knows his actions have been logged. Ensure that all activities are logged in a separate log management location (to make it harder for threat actors to remove traces of their attack) and reported to support personnel to take appropriate action.

6. *Password Policy*

Consider your password policy. Short/simple passwords allow easy cracking via a brute force attack whereas longer passwords are harder to remember. Unique passwords can be difficult to manage unless a password manager is utilised. If a password manager is used, ensure that the passwords are stored securely and only on the client-side. Ensure that any new devices added to the ICS have default accounts/passwords changed or removed as part of commissioning to a unique password which is held securely and then used to set up role-based access if possible. Log password failure attempts to detect attempts at unauthorised access and implement account lock-out if this is feasible and report to support personnel to take appropriate action.

7. *Device Hardening*

Ensure that devices are made as secure as possible. For servers and workstations, implement anti-virus and operation system patching. Consider the benefits and risks of automated vs manual scheduled patching for these systems. Ensure that the anti-virus solution includes some form of proactive threat detection so that malware that doesn't match an identified virus signature can still be blocked. Register with vendors to get the latest firmware for all devices – many firmware updates are released because of security vulnerabilities that have been identified and published. This could be a 'low hanging fruit' for an attacker. Firewalls especially should be kept up to date to ensure they operate as designed for the lifetime of the device. Where a device cannot be updated or updates are no longer supported, consider replacing the device or providing an additional firewall or network security barrier to reduce the risk if required.

8. *Personnel & Training*

Identify and train key personnel that are responsible for ICS Cyber Security in your organisation. Other users should also receive awareness training to ensure that risks are understood so that user become an asset to the cyber security program – not a liability. Many attacks could have been prevented if users were able to identify the risks being exposed to the organisation at the time the breach occurred. Ensure that internal and external personnel having access to the ICS are verified and validated before accessing the network – in extreme cases, background and/or police checks can be sought. In general, a basic personnel risk assessment should be sufficient to ensure that the risk is managed appropriately.

9. *Involve Management*

Success in ICS Cyber Security relies on support from the whole organisation. Ensure executive leaders are engaged to ensure consideration and mitigation can be commensurate with the risk posed. Utilise resources such as the NCSC paper on Cyber Security Risk and Management – An Executive Level Responsibility [10] can assist engineers and team leaders obtain support from executives. The key is to 'Put cyber security on the agenda before it becomes the agenda'. Ensure that cyber risks are considered and incorporated into existing risk management and governance.

10. *Detect & Response Plan*

Even with barriers in place, organisations still experience breaches. Many cybersecurity experts have noted that experiencing a compromise is not really a question of 'if' but more of a question of 'when', especially in the case of a targeted attack. When a compromise occurs, the organisations that recover best are those that quickly detect the issue and have a plan in place to respond. Ensure that anti-virus, firewall and intrusion detection logs are monitored and alerts are configured if a risk is identified. Have a team and plan in place, ensuring that roles and responsibilities are defined. Practice cyber security drills. More information on setting up a team can be found in the New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs) [11]

References

1. IEC 61511 series: Functional safety – safety instrumented systems for the process industry sector
2. IEC 62443 series: Industrial communication networks – Network and system security
3. ISA-TR84.00.09-2017: Cybersecurity Related to the Functional Safety Lifecycle
4. [New Zealand] National Cyber Security Centre: Voluntary Cyber Security Standards for Industrial Control Systems

5. David Kushner: The Real Story of Stuxnet
6. SANS Institute: German Steel Mill ICS CP/PE Case Study Paper
7. E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid
8. SANS Institute: Secure Architecture for Industrial Control Systems
9. Nex Defense: IT OT Convergence
10. [New Zealand] National Cyber Security Centre: Cyber Security and Risk Management – An Executive Level Responsibility
11. [New Zealand] National Cyber Security Centre: New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)
12. Water Information Sharing and Analysis Centre: 10 Basic Cybersecurity Measures – Best Practices to Reduce Exploitable Weaknesses and Attacks