Paper Submission

CIS 6357 – CONTROL SYSTEM SECURITY

Dhanaraj Chalil | dvchalil@uh.edu

TABLE OF CONTENT

ABSTRACT

This paper describes applying security principles to Industrial Control Systems (ICS). Primarily, this paper focuses on thoughts to apply security to process control systems and network, by referring to those major security strategies which have been deployed for enterprise security. While ICS security currently focuses on compliance with rules and regulations, there should also the proper implementation of defense and detection strategies to keep it secure. First few sections provide an idea on the industrial control systems and operational technology. It also draws attention to the importance of having security measures for ICS. This describes the impact of cyber attacks on ICS organization and economy, drafted after analyzing several threat incidents. Current trends in ICS security is also explained in the following section. Later sections compare OT and IT security, focusing on the difference these security measures have, and how it differs when trying to implement security strategies in ICS organizations. It was observed that a direct convergence of these security measures is not possible, as these organizational environments differ on how they operate. So, enterprise security standards must be tailored to fit for securing industrial control systems and network. In the end, all necessary security thoughts for ICS organizations, which involves defensive and preventive measures are presented detailing on its importance.

1. Introduction

Industrial control system (ICS) is a general term that incorporates several types of control systems or control components, used to operate or automate industrial processes. ICS allows operators to monitor and control industrial processes. The part of the system mainly concerned with producing the output is referred to as the process. A typical ICS may contain Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and remote diagnostics and maintenance tools built using an array of network protocols. ICS control industrial processes are mostly deployed in electrical, water, oil and natural gas, chemical, transportation, food and beverage, and discrete manufacturing industries.

The SCADA systems integrate data acquisition systems with data transmission systems and HMI software, to provide a centralized monitoring and control system for numerous processes. The SCADA systems are designed to collect field information, transfer it to the HMI system which represents data graphically or textually to the operator. This allows the operator to monitor or control

an entire system from a central location. Many of the ICS systems are connected to sensors and other devices over the internet, which increases the risk of cyber attacks on ICS.

To demonstrate the technological and functional differences between traditional IT systems and ICS environment, the word 'Operational Technology' (OT) is being used. OT illustrates the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices. OT is also the use of a computer to monitor or alter the physical state of the system. Use of internet for the functioning of ICS represents the link of OT systems to IT systems. This made OT be the victim of cyber attacks, a major security concern IT being stuck on. Irrespective of IT, the security of ICS has different priorities and a different infrastructure to protect. ICS security focuses on keeping these specific systems secure to keep it up and running.

It is important that organizations leverage lessons learned to secure enterprise IT but adapt those lessons to the unique characteristics of OT. This includes moving beyond perimeter-based security in a facility and adding security controls to the assets that matter most – the proprietary control systems, which have primary responsibility for process safety and reliability. The following sections discuss on ICS security, illustrating how to apply security knowledge from enterprise IT security to a process control network.

2. Importance of industrial control system security

It is a fact that ICS technology is being evolved slower compared to IT because of business constraints in the industrial space. For example, system lifecycles are measured in decades, there is a much lower staffing level, and have a heavy dependence on vendors or system integrators. These business constraints and the technology ecosystem tend to keep infrastructures in a vicious cycle of poor security decisions. Another critical reason for which ICS stays far away from security is the high availability requirements of ICS. With this, these systems cannot be updated in easily. However, these same systems often lack a backup or failover.

There is a common misconception that ICS attacks must exploit ICS specific vulnerabilities only. Cyber attacks on these systems will also target system software and network vulnerabilities too. The Stuxnet worm took advantage of both Windows zero days and a few software vulnerabilities in the Siemens control systems software. ICS also have characteristics that differ from traditional information processing systems. Cyber attacks on ICS systems have a direct effect on the physical world which includes significant risk to the health and safety of human lives, serious damage to the environment, as well as serious financial issues due to production losses, negative impact to a nation's economy, and compromise of proprietary information. ICS have unique performance and reliability requirements, and often use operating systems and applications that may be considered unconventional to typical IT system.

ICS cybersecurity programs should uphold security to ICS operations, reliability, and enterprise data and communication assets. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. Comparing with objectives of IT security, ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality.

Initially, ICS had very little resemblance to IT systems, because these were isolated systems running proprietary control protocols using specialized hardware and software. Many ICS components were in physically secured areas and the components were not connected to IT networks or systems. As ICS are adopting IT solutions to support corporate business systems connectivity, remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they started resembling IT systems. This enhanced ICS to support new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems. This generated a high necessity to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are personalized for the ICS environment.

3. Trends in industrial control systems cybersecurity

With connectivity to the outside world, cyber attacks on ICS constitute an extremely dangerous threat, as these will create a devasting impact on organization, environment, and economy. Cybersecurity is, therefore, becoming more and more important. It is essential to understand the trends in ICS cybersecurity. An analysis of this is made from both businesses as well as threats perspective.

On a business perspective, the current trends point that organizations oftentimes don't carry out associated security measures. Almost, only 23% of companies are compliant with minimal cybersecurity guidance and regulations. Many companies do not even detect or track cyber attacks. It is astonishing that 10% of respondents still do not measure the number of incidents and breaches they've experienced in today's day and age. As the level of digitalization raises for ICS, the frequency of cyber attacks will increase respectively. A major challenge in adopting cybersecurity is to hire ICS cybersecurity professionals with the right skills. ICS organizations had frequently experienced malware attacks and ransomware infections over a decade. Intruder attacks were also reported for the industry sector. Moreover, it had experienced advanced persistent threats and several automated attacks. Only after several incidents, leadership and department managers became conscience about ICS security. In recent years, there were improvements in deploying recommended technology controls for protecting

ICS, but not enough people to manage them. With this scenario, organizations were able to identify vulnerabilities but don't have people to fix them.

With respect to threat perspective, current ICS cybersecurity trend projects that the ICS computers attacks reached to 41.2%, up from 36.6%, over a year timescale. The increase is due to an overall increase in malicious activity. The main sources of infection for computers in organizations' industrial network infrastructure are the internet, removable media and email. In 2018, it was discovered that the internet was the source of threats on 27.3% of ICS computers. Today, an interface between the industrial network and the corporate network is needed both to control industrial processes and to provide administration for industrial networks and systems. Removable media is one another source of infection, where the USB threat to ICS became a serious concern. The analysis of email-borne threats indicates that the information security level has virtually no effect on the number of phishing emails and malicious email attachments that get through protective measures at the network perimeter and reach ICS computers. Attackers commonly used spear phishing via PDF documents, software installers with Trojan installers and waterhole attacks through pre-compromised websites. Once a machine had been successfully exploited, the attack framework could install additional modules to expand the attackers' foothold.

4. Comparing ICS and IT Systems Security

ICS have many characteristics that differ from traditional IT systems, including different risks and priorities. ICS have different performance and reliability requirements, and also use operating systems and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyberattack. Initially, ICS had little resemblance to IT systems. As ICS are adopting IT solutions to promote corporate connectivity and remote access capabilities and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities.

The environments in which ICS and IT systems operate are constantly changing. The environments of operation include but are not limited to: the threat space; vulnerabilities; missions/business functions; mission/business processes; enterprise and information security architectures; information technologies; personnel; facilities; supply chain relationships; organizational governance/culture; procurement/acquisition processes; organizational policies/procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs).

ICS is generally time-critical, with the criterion for acceptable levels of delay and jitter dictated by the individual installation. Some systems require reliable, deterministic responses. High throughput is typically not essential to ICS. In contrast, IT systems typically require high throughput, and they can typically withstand some level of delay and jitter. Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Control systems often cannot be easily stopped and started without affecting production. The use of typical IT strategies such as rebooting a component is usually not acceptable solutions due to the adverse impact on the requirements for high availability, reliability, and maintainability of the ICS. In a typical IT system, data confidentiality and integrity are typically the primary concerns. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns. ICS operating systems (OS) and control networks are often quite different from IT counterparts, requiring different skill sets, experience, and levels of expertise. ICS and their real-time OSs are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have desired features including encryption capabilities, error logging, and password protection. Indiscriminate use of IT security practices in ICS may cause availability and timing disruptions. Communication protocols and media used by ICS environments for field device control and intra-processor communication are typically different from most IT environments and may be proprietary.

Change management is paramount to maintaining the integrity of both IT and control systems. Unpatched software represents one of the greatest vulnerabilities to a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policy and procedures. In addition, these procedures are often automated using server-based tools. Software updates on ICS cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor of the industrial control application and the end user of the application before being implemented. Additionally, the ICS owner must plan and schedule ICS outages days/weeks in advance. The ICS may also require revalidation as part of the update process. Another issue is that many ICS utilizes older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. The change management process, when applied to ICS, requires careful assessment by ICS experts working in conjunction with security and IT personnel. Typical IT systems allow for diversified support styles, perhaps supporting disparate but interconnected technology architectures. For ICS, service support is sometimes via a single vendor, which may not have a diversified and interoperable support solution from another vendor. Typical IT components have a lifetime on the order of 3 to 5 years, with brevity due to the quick evolution of technology. For ICS where technology has been developed in many cases for very specific use and implementation, the lifetime of the deployed technology is often in the order of 10 to 15 years and

sometimes longer. Most IT components and some ICS are located in the business and commercial facilities physically accessible by local transportation. Remote locations may be utilized for backup facilities. Distributed ICS components may be isolated, remote, and require extensive transportation effort to reach. The component location also needs to consider the necessary physical and environmental security measures.

In summary, the operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals need to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on ICS may not operate correctly IT cybersecurity solutions because of specialized ICS environment architectures.

5. Converging IT security strategies to OT security

As attackers increasingly focus on manufacturers and other industrial targets, IT and OT must work together to protect the organization. Most of the CIOs and CISOs of industrial organizations don't have much visibility into their operational technology (OT) environments. Most of them have expertise in the IT domain and are primarily focused on IT security. Over a decade, malicious actors increasingly focus on ICS industries and critical infrastructures, IT and OT must work together to protect the business better. Applying traditional IT security approaches to the OT side will not fit properly for defending cyber attacks.

Collaborating IT and OT to create a personalized security plan is a way to adopt IT security strategies for OT. From inception, analyze the differences between the IT and OT environments and then embrace the reality that IT security cannot be translated directly to OT. Generate a plan that suits for operational system security with a reference on IT security strategies should be the focal point on converging IT security strategies to OT. Establish a common reference around cybersecurity of the organization, which means taking what IT security are passionate about and translating those into concerns in the operations domain to show how the right security investments can improve operational outcomes. Further, using the OT security plan which was jointly created, work in partnership to identify and implement a handful of security protections that aren't in place today and that will demonstrably improve the environment without negatively impacting operations. Let's consider an example to explain this security adoption strategy.

Confidentiality and integrity of data is a major focus in IT security strategies. In the OT sector, the business side should be able to consume production data, that flows from operation centers to the business side in a secured manner. Direct communication between business and operational centers potentially allow threats to move laterally across these sectors. This will be a burden for an organization to handle secure communication and data security. Establishing a robust demilitarized zone (DMZ) to isolate systems on each side can provide better protection and allow only authorized communication through. Clear ownership of the DMZ based on established security leading practices is a critical factor that will help facilitate this process.

Access control is another security measure widely adopted in the IT sector, which will be an effective measure in adopting security. Every industrial organization has employees, contractors, and vendors who need remote access to their OT environments. Clearly defined access controls, particularly for these people, can help protect against threats they may unwittingly introduce to the environment. However, restricting access to vendors can be more challenging because much of the OT equipment must be remotely maintained by a vendor under the terms of a support contract or warranty. If organizations can't support this capability, then warranties might be voided, the software might not be patched with certified updates, equipment might not be maintained, and the risk of failures could increase. An effective secure remote access implementation plan is a must. Restrict portable media use through corporate-issued devices. Some of the most destructive malware is very often carried into the OT environment by an employee with a USB drive or a vendor whose laptop may have become infected. These pose a risk to critical equipment and processes. Operational integrity can be enhanced through effective security procedures and policies that appropriately restrict portable media use.

Ultimately, the goal of IT/OT convergence is to make the OT side more resilient through effective cyber protections. This is done by adopting security strategies of IT and tailoring it to fit perfectly for OT. By demonstrating a proactive approach with measurable improvements to OT security while accommodating operational priorities, will help in establishing advanced protection using the security knowledge from IT. A detailed explanation of this is provided in later sections of this paper.

6. Focus on ICS security principles

Today, while the enterprise security measures focus on prevention, detection strategies, ICS security measures are emphasized mostly on prevention strategies by maintaining good compliance with security standards. Obtaining compliance is more about policy and procedure than technology. But, successful security measures should combine prevention, response, and compliance. There are numerous ICS security standards, including many that are industry-specific. The most notable and broadly applicable standards are IEC 62443 and NIST SP 800-82. However, we do find that the existing standards focus primarily on prevention rather than detection and response.

The management of organizational risk is a key element in the organization's cybersecurity program and provides an effective framework for selecting the appropriate security controls for systems. The risk management framework provides a process that integrates security and risk management activities into the system development life cycle. Following the approach to industrial cybersecurity organizes to help reduce complexity, prioritize risks and form a basis for adopting a risk-based framework.

Securing the Industrial Network is one of the major steps to be followed. For this, organizations should begin by focusing on designing a good network with well-secured boundaries, and then segmenting it based on recommended standards. The Perdue model of segmenting a network with respect to zones is a great approach. Later, monitoring the security status of a network is common practice for IT security teams which should be adopted in industrial network infrastructure. Validate the state of all network systems based on a secure baseline state.

Securing the Industrial Endpoints should be protected against digital attacks by perimeter firewalls, proprietary software, specialized protocols, and air gaps. Also, PC-based endpoints need to be protected, and organizations need to defend their IT endpoints against attacks that traverse over to the OT environment. Organizations should begin by gathering and maintaining an accurate inventory of all endpoints' hardware and software, tracking the vulnerabilities in OT assets, assuring secure and hardened configurations are in place at each endpoint, and monitoring and alerting on unauthorized changes.

Securing the Industrial Controllers should focus on defending digital attacks by enhancing the detection capabilities and visibility into industrial control systems changes and threats, implementing security measures for vulnerable controllers, monitoring for suspicious access and change control, and detecting/containing threats in a timely manner.

Based on these, the following section describes the major focus points that an ICS facility should consider in implementing cybersecurity. Most of these are based on security knowledge and framework which is being used in enterprise security.

7. Security strategies for industrial control systems

Let's discuss the importance of compliance with ICS-specific Security Policies and Procedures as they are the root of every successful security program. These help to ensure that security protection is both consistent and current to protect against evolving threats. After an information security risk analysis has been performed, the information security manager should examine existing security policies to see if they adequately address the risks to the ICS. If needed, existing policies should be revised, or new policies created. The development of the security policies should be based on a risk

assessment that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently. Procedures that support the policies need to be developed so that the policies are implemented fully and properly for the ICS. Security procedures should be documented, tested, and updated periodically in response to policy, technology, and threat changes.

The management of ICS risks is another hazard confronting an organization. The RMF process includes a set of well-defined risk-related tasks that are to be carried out by selected individuals or groups within well-defined organizational roles. RMF tasks are executed concurrently with or as part of system development life cycle processes, considering appropriate dependencies. NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, introduces the risk management framework which addresses the process of implementing the framework.

The information security team should define, inventory, and categorize the applications and computer systems within the ICS, as well as the networks within and interfacing to the ICS. The team should review and update the ICS asset list annually and after each asset addition or removal. The security controls selected based on the security categorization of the ICS are documented in the security plan to provide an overview of the security requirements for the ICS information security program and describes the security controls in place or planned for meeting those requirements. Security control addresses the security concerns for a system and the plans for countering these concerns.

Organizations should assess the impacts to organizational operations which include mission, functions, image, and reputation, organizational assets, individuals, other organizations, and the Nation. The organization may perform a detailed risk assessment for the highest impact systems and assessments for lower impact systems as deemed prudent and as resources allow. The risk assessment will help identify any weaknesses that contribute to information security risks and mitigation approaches to reduce the risks. Risk assessments are conducted multiple times during a system's life cycle. The focus and level of detail vary according to the system's maturity. Based on this, organizations should prioritize the selection of mitigation controls. Security control implementation is consistent with the organization's enterprise architecture and information security architecture. The controls to mitigate a specific risk may vary among types of systems. Organizations should identify, evaluate, and implement suitable quick fix solutions as soon as possible to reduce security risks and achieve rapid benefits.

We have already discussed the importance of separating the ICS network from the corporate network because the nature of network traffic on these two networks is different. Network segmentation can be implemented by partitioning the ICS into security domains and separating the ICS from other networks, such as the corporate network, and presents illustrative security architecture. Operational risk analysis should be performed to determine critical parts of each ICS network and operation and help

define what parts of the ICS need to be segmented. Network segmentation involves partitioning the network into smaller networks. Network segmentation and segregation are one of the most effective architectural concepts that an organization can implement to protect its ICS. Segmentation establishes security domains, or enclaves, that are typically defined as being managed by the same authority, enforcing the same policy, and having a uniform level of trust. Segmentation can minimize the method and level of access to sensitive information, ICS communication and equipment configuration, and can make it significantly more difficult for a malicious cyber adversary and can contain the effects of non-malicious errors and accidents. Depending on the architecture and configuration of your network, some of the common technologies and methods used include Logical network separation enforced by encryption or network device-enforced partitioning, physical network separation to completely prevent any interconnectivity of traffic between domains, and network traffic filtering which can utilize a variety of technologies at various network layers to enforce security requirements and domains.

A single security product, technology or solution cannot adequately protect an ICS by itself. A multiple layer strategy involving two or more different overlapping security mechanisms, a technique also known as defense-in-depth, is desired so that the impact of a failure in any one mechanism is minimized. A defense-in-depth architecture strategy includes the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities along with effective security policies, training programs, incident response mechanisms and physical security.

The authentication of a user or system is the process of verifying the claimed identity. Authorization, the process of granting the user access privileges, is determined by applying policy rules to the authenticated identity and other relevant information. Authorization is enforced by some access control mechanism. The authentication process can be used to control access to both systems (e.g. HMIs, field devices, SCADA servers) and networks (e.g., remote substations LANs).

The security architecture of an ICS must also incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks. Monitoring, logging, and auditing activities are imperative to understanding the current state of the ICS, validating that the system is operating as intended and that no policy violations or cyber incidents have hindered the operation of the system. Network security monitoring is valuable to characterize the normal state of the ICS and can provide indications of compromised systems when signature-based technologies fail. Additionally, strong system monitoring, logging, and auditing are necessary to troubleshoot and perform any necessary forensic analysis of the system.

Incidents are inevitable and incident detection, response, and system recovery plans are essential. Major characteristics of a good security program are how soon after an incident has occurred that the incident can be detected and how quickly a system can be recovered after an incident has been

detected. Incident response in ICS is closely aligned to disaster recovery, specifically to address the stringent uptime requirements of ICS.

Every enterprise has awareness programs for the most part and is more effective. However, when it comes to ICS, the focus is more on the existence of a policy that outline quarterly awareness training that discusses cybersecurity practices. Such training could include physical security practices as well. However, what these programs consist of is left to the facility itself to determine.

ICS-CERT and other organizations are starting to release indicators of compromise to asset owners. But many asset owners lack the capability to consume and apply that intelligence to their ICS environments. Better information sharing would lead to better ICS security and we're supportive of organizations like ICS-CERT and the ISACs that advance this mission. Organizations can start finding evil on their ICS networks and sharing the indicators of compromise or other lessons learned with their peers instantly.

8. Conclusion

Many of the security ideas and practices that are adopted from enterprise security, won't directly fit for securing ICS. While technologies are often the focus of ICS vulnerabilities, cultural differences related to how OT and IT teams have evolved are often the greatest challenge to resolving them. It's important to remember that successful ICS security programs are about people. Establish a team of interested individuals from across the stakeholder groups and establish regular meetings to develop the ICS security strategy, mission, and goals together. The group will become an important source of data, a sounding board, and a de-facto stamp of approval for new security policies and initiatives. To limit complexity, focus on finding common ground and establishing high-level wording that can be applied to both IT and ICS. Also, consider bringing in non-technical team members. Organizations that identify an executive-level security leader who is responsible for security across both IT and OT will move faster than organizations that rely on grass-roots efforts. One caveat is that the leader must be respected by both the IT and OT teams. Often the Legal or Risk Management departments are very interested in this topic and can be powerful allies and champions of the ICS security effort.

Focusing on the security measures, primarily make ICS access difficult for an attacker who has compromised a user's Enterprise IT credentials. To this end, ICS credentials should be managed separately from Enterprise IT credentials. Where possible, require two-factor authentication for remote access to the ICS. Similarly, separate the two-factor authentication token from the token used for enterprise VPN or other systems. Things can get tricky within the ICS environment itself. Some ICS software or devices may not have an authentication capability or may have hardcoded default credentials. Short of replacing these devices, the most effective strategy is reducing their exposure and

monitoring them closely for unusual events. Ensure that they are not placed at the perimeter of the ICS network. Next, implement a network security monitoring strategy that generates alerts for logins, changes, or other behavior that are relevant to monitor.

9. References

1. *Securing industrial control systems/SCADA – https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview*
2. *Homeland Security National Cybersecurity and Communications Integration Center – Steps to effectively control Industrial Control System attacks – https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf*
3. *A holistic defense in depth approach – https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/*
4. *Securing Industrial Control Systems Against Vulnerabilities and Malware – https://www.tenable.com/blog/securing-industrial-control-systems-against-vulnerabilities-and-malware*
5. *Securing industrial control systems – https://www2.deloitte.com/na/en/pages/risk/articles/securing-industrial-control-systems.html*
6. *NIST Special Publication 800-82: Guide to Industrial Control Systems Security – http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf*
7. *Challenges for Securing Cyber-Physical Systems – Alvaro A. Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry – https://pdfs.semanticscholar.org/d514/97e5827cc00d9d00c26e27a769d42284cfba.pdf*
8. *Challenges for securing cyber-physical systems – https://pdfs.semanticscholar.org/d514/97e5827cc00d9d00c26e27a769d42284cfba.pdf*
9. *NIST Information Technology Laboratory Computer security resource center: Risk management framework overview – https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview*
10. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security – https://sm.asisonline.org/ASIS%20SM%20Documents/nist_scada0107.pdf*