International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2020): 6.733

A Comprehensive Analysis of Methodologies for Threat Assessment of Industrial Automation Systems in Cyber-Security

Karan Chawla

Abstract: ***Industrial automation systems come in a variety of forms, including fixed (hard) automation, programmable automation, flexible (soft) automation, Totally Integrated Automation (TIA). The majority of PLCs have historically been hijacked or compromised by outsiders with malicious intentions, but in extremely rare instances, hackers have altered the PLC's source code to gain additional access to the OT network and access to the workers' workstations and the data connected to them. One notable instance is the 2020 cyberattack on Israel's water system, which allowed hackers to overwhelm the system with chlorine. This review paper will analyze the attack vectors such as the deeper access to the OT network in PLCs, SCADA systems and DLCs (Distributed Control System). The vital infrastructures of the country, including industrial control systems (ICS) and supervisory control and data acquisition (SCADA), are becoming more exposed to internal and foreign threats. The timing is right for these systems to implement security best practices. Furthermore, the importance of these systems' risk assessment cannot simply be dismissed as unimportant. For DCS, cybersecurity is a developing worry and is seen as the most important issue. A security breach might have disastrous consequences, including financial loss, information loss, and bodily damages by disrupting system operations. DCS enters the domain of CPS once the internet is introduced in order to gain remote access, efficiency, and ubiquity. The DCS is susceptible to risks that are not being adequately addressed by current risk mitigation and cybersecurity measures, necessitating a novel approach to cybersecurity. This Review paper analyzes cybersecurity related threats to the three most important components of Industrial Automation namely, PLCs, SCADA and OT networks.***

Keywords: SCADA, OT Networks, Programmable Logic Controllers, Distributed Control System

1.Introduction

Industrial automation systems may be classified as Fixed (Hard), Programmable, Flexible (Soft), and Totally Integrated Automation (TIA) systems. With specialized equipment, this kind of automation is employed in high-volume manufacturing situations. The equipment comes with a pre-installed operating set that can help it function properly. This method's manufacturing machinery is designed to allow the operation sequence to be changed to accommodate various product designs. Because we may customize and make necessary modifications during the manufacturing process, it is mostly employed when creating items in batches.

In programmable automation, the production process is always under the direction of an instruction programme. In this instance, we only need to put the programme into the hardware system to start creating new items right away. All system components are managed or controlled by a central computer, and the material-handling system connects many machine tools in flexible automation. Some important terms to know would be the OT Network, SCADA systems, DLCs and PLCs. Operational technology (OT) is a mix of hardware and software that uses direct monitoring and/or control to identify and/or alter industrial resources, processes, and occurrences. The phrase was created to characterize the functional and technological distinctions between settings for normal IT systems and those for industrial control systems. SCADA stands for Supervision and Data Acquisition Systems. A control system architecture called supervisory control and data acquisition uses computers, networked data transfers, and graphical user interfaces to monitor machinery and industrial processes at a high level. This procedure may be facility-based, industrial, or based on infrastructure: Industrial processes can operate in continuous, batch, repetitive, or discrete modes in the manufacturing, power generating, manufacturing processes, and refining industries, for example. Examples of public or private infrastructure activities include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electricity transmission and distribution, and other infrastructure projects.

A distributed control system, or DCS for short, is a manufacturing plant control system having autonomous controllers spread throughout it. The dispersion of control system design throughout the facility has resulted in more efficient approaches to increase control stability, process quality, and plant productivity. Both software and hardware make up a DCS. The majority of controllers' local installation is straightforward, which lowers installation costs. Low-latency automated control that is implemented locally increases dependability while central control features and alternate remote controls enable for human supervision. Individual processes have their own controllers with distinct CPUs, unlike a central controller system, allowing other processes to continue in the case of a failure.

A Programmable Logic Controller (PLC), a type of industrial control system, continuously assesses the state of input devices and determines how to govern the state of output devices based on a specific programme. A PLC automates a process or piece of equipment by monitoring inputs, making choices based on its programme, and controlling outputs. The majority of PLCs have historically been hijacked or compromised by outsiders with malicious intentions, but in extremely rare instances, hackers have altered the PLC's source code to gain additional access to the OT network and access to the

workers' workstations and the data connected to them. Programmable Logic Controllers are part of the SCADA system.

Programmable Logic Computers (PLCs)

An industrial control system called a Programmable Logic Controller (PLC) continually evaluates the condition of input devices and decides how to regulate the state of output devices based on a unique programme. A PLC automates a process or piece of equipment by monitoring inputs, making choices based on its programme, and controlling outputs. An Interesting aspect to PLCs is that most PLCs in the past have been redirected or hacked by external parties for malicious intents but in very rare circumstances have hackers caused the modification of code of the PLC to gain deeper access into the OT network and gain access of the workers' workstation and information related to it. One such example is the attack on Israel's water supply in 2020 which gave hackers the ability to flood the water supply with chlorine. A PLC has three parts, input, output and CPU.

PLCs can be used as a means for gaining a deeper access to the OT network. These desktop applications frequently serve as a link between corporate networks and operational technology networks. When an engineer's workstation is compromised and its vulnerabilities are used, the attacker has easy access to the internal network, which allows them to move across systems and further access other PLCs and critical systems. Engineers who configure and debug PLCs to guarantee the safety and dependability of operations across crucial industries such as utilities, power, water and wastewater, heavy industry, manufacturing, and automotive, among others, are the focus of the assault.

An attacker intending to physically interrupt a process would first need to do a thorough enumeration of those controllers in order to discover the appropriate one to target. OT networks may include hundreds of PLCs regulating industrial operations. The PLCs become the instrument rather than the target of the evil PLC attack. By turning one PLC into a weapon, a hacker may get access to all the other PLCs on the network and the engineer's workstation, which is the greatest source for process-related data. The attacker may simply change the logic of any PLC with this access and knowledge. The plan is to get an engineer to connect to a hacked PLC; the easiest method to do this is to cause a problem on the PLC. An engineer would typically reply to such a situation, connect, and use their engineering workstation programme as a troubleshooting tool. The hacker weaponized the PLC by identifying vulnerabilities in each of the seven engineering workstation platforms, causing the engineering workstation to execute our malicious code each time an upload procedure was carried out. Upload procedures involve the transfer of metadata, configurations, and text code from the PLC to the engineering workstation. With the use of data that isn't often included in static or offline project files, this strategy armours the PLC with the ability to execute code upon an engineering connection or upload. The PLC is not the target of this attack vector, unlike, for instance, the infamous Stuxnet virus, which secretly altered PLC logic to do physical harm. Instead, we aim to attack the engineers who programme and maintain the PLC in order to obtain deeper access to the OT network. It's crucial to emphasize that none of the vulnerabilities we discovered were in the PLC firmware; rather, they were all in the engineering workstation software. The majority of the time, the software didn't undertake thorough security checks since it completely trusted the PLC's data, which led to the existence of the flaws.

A Shodan and Censys search will show PLCs that are open to the internet and typically lack security features like authentication and permission. Through malicious download methods, an attacker who gains access to a PLC in this manner can change settings or the behavior and logic of the device. Opportunistic attackers locate PLCs with internet connections, connect to them using engineering workstation software from a commercial source, and upload the current project, which contains PLC code and parameters. The attackers will then alter the project's logic before performing a download method to update the PLC logic with their changes. One instance of such an occurrence was the 2020 attack on Israel's water system, in which assailants attempted to flood the water supply with chlorine by taking advantage of open PLCs. According to study, attackers may exploit the PLCs that are connected to the internet as a launching pad to access the whole OT network. Attackers might arm these PLCs and purposefully produce a malfunction to draw an engineer to them rather than just connecting to them and altering the logic. The engineer will upload a procedure that will compromise their equipment as a diagnostic technique. The OT network is currently under the control of the attackers.

Third-party engineers and contractors frequently deal with several networks and PLCs as part of modern OT management. The system integrator serves as a connecting point between the PLC and the engineering workstation, which is in charge of overseeing a number of OT networks, in this assault scenario. An attacker would find a PLC in a far-off, less secure building that is known to be run by a system integrator or contractor. This is how the attack would go. The attacker will then turn the PLC into a weapon and purposefully introduce a bug. Thus, the victim engineer will be persuaded to visit the PLC in order to do a diagnosis. The integrator will do an upload procedure throughout the diagnosis phase, compromising their equipment. Attackers might assault and potentially weaponize newly available PLCs inside other organizations after acquiring access to the integrator's system, which by design can access many more PLCs, further expanding their control. From a defensive standpoint, where it may be employed to trap attackers, this attack vector is beneficial. As engineers and attackers frequently use the same commercial tools, defenders can intentionally build up armed PLCs that are publicly accessible and make them accessible to attackers. As a honeypot, these PLCs will entice attackers to engage with them. The weaponized code will, however, run on the attacking computer if an attacker falls for the trap and

initiates an upload from the fake PLC during the enumeration procedure. By forcing attackers to defend themselves against the target they intended to attack, this strategy may prevent them from attacking internet-facing PLCs and can be used to identify assaults in the early stages of enumeration.

SCADA Systems

You must create screens for SCADA where you must map the PLC's variables. The PLC and SCADA connect with one another through a communication protocol, and the control portion then functions in tandem. The primary role of SCADA is to monitor and record data and reports, display trends and alerts, and, in general, display all activities taking place inside a PLC on its displays.

This aids the operator in diagnosing and figuring out what's going on within the PLC.

It is important to remember that a PLC may function in a system without SCADA. There are certain simple programmes where the user simply has start and stop controls, therefore there is no need for visuals.

A control system architecture called supervisory control and data acquisition uses computers, networked data transfers, and graphical user interfaces to monitor machinery and industrial processes at a high level. This procedure may be facility-based, industrial, or based on infrastructure: Industrial processes can operate in continuous, batch, repetitive, or discrete modes in the manufacturing, power generating, manufacturing processes, and refining industries, for example. Examples of public or private infrastructure activities include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electricity transmission and distribution, and other infrastructure projects. Subsystems make up the SCADA System. They are: a) A human-machine interface, often known as an HMI, is a piece of equipment that displays process data to a human operator and enables the operator to monitor and manage the process. b) A computerized supervisory system that gathers (acquires) process data and communicates instructions (controls) to the process. c) Remote terminal units (RTUs) connect to processing sensors, convert sensor signals to digital data, and provide the digital data to the monitoring system. Some of the major manufacturers of SCADA are Honeywell, Schneider Electric and ABB, Siemens Energy and General Electric.

The CORAS framework consists of a model-based risk assessment technique, a specification language based on the Unified Modelling Language (UML), a collection of reusable packages, an integrated platform for a data repository, and a risk assessment reporting system. The CORAS project's goals are to establish a useful framework for risk analysis, evaluate the framework's applicability, usability, and effectiveness, and look into its potential for commercial success. A data-portable, open-source risk assessment tool is the CORAS platform. It was created in 2002 by a group of collaborators from four different European nations.

There are two main categories of CORAS technique processes. As well as documenting the assumptions and restrictions required for the next risk analysis, the first group creates a shared understanding of the goal for study. Focused on the actual risk analysis is the second category. Our choice to utilize this tool was mostly influenced by the fact that it is open source, system agnostic, and extremely user pleasant for developing risk models quickly. The CORAS framework uses a number of symbols, including an untrained technical staff member as an example of an accidental human threat, a hacker as an example of a deliberate human threat, a vulnerability as an example of an unpatched system, company information as an example of a direct asset, company reputation as an example of an indirect asset, a natural phenomenon as an example of an unwelcome incident, and threat scenario as an example of an example of a rogue access point connected to the company Initial danger diagrams are created by a brainstorming session in which stakeholders, security experts, and risk modelers engage. The ICS technician made the ICS system vulnerable in a number of ways. The hacker or eavesdropper will then use these weaknesses to their advantage in order to obtain access to the ICS system or jeopardize its secrecy. In this case, the lack of training for the ICS technician results in both a misconfiguration of the ICS system and the installation of an unauthorized access point into the ICS network. Giving the ICS technician full system access is another vulnerability related to the technician. In this situation, a hacker may use social engineering to deceive the ICS technician into disclosing information or they could find the rogue access point and use it to break into the network.

Another approach the hacker can use is to tamper with the commands sent to the ICS system, which also tampers with the data integrity of the ICS. Both the direct assets-safe operations, corporate data, and regulatory compliance-and the indirect assets-profitability and brand recognition-are impacted by this. The rogue access point set up by the ICS technician may likewise be used by the hacker to threaten the ICS system. Bypassing network authentication, the hacker gains access to the network, which has an impact on both the direct and indirect assets of the firm, including profitability and brand reputation. The rogue access point will be used by the spy to connect to the network. The ICS system is vulnerable to unencrypted transmissions, which allows an eavesdropper to violate its secrecy and steal business secrets.

Distributed Control Systems

Distributed control systems (DCS) are digitized, automated industrial control systems that employ geographically dispersed control loops and distributed, autonomous controllers. In the most recent industrial revolution, DCS emerged as the mainstay of the modern industrial period and is now used in a variety of sectors, including smart grids, nuclear power plants, petrochemical and refineries, cars, and agriculture. By allowing each machine in its network to have its own dedicated controller, DCS maintains qualities like precision, sensitivity, stability, dependability, speed, noise reduction, and communication bandwidth while still operating the

machine. A cyber physical system (CPS) is made up of sensors, actuators, and specialized processes that are used in DCS. The use of DCS in critical infrastructure and its connection to the cyber realm make it a target for cyber espionage.

Process-oriented systems with a restricted size and geographic spread, distributed control systems are made up of subsystems. The DCS's fundamental design is made up of four main parts; the controller manages how various devices are configured and carries out control algorithms among them. The distributed controller receives commands from the main controller and directs control of field devices, primarily newly installed field devices. The human machine interface (HMI) uses graphics to represent plant data like alerting indications. Conversely, a channel for communication between field equipment and controllers. These come in both wired and wireless varieties.

These systems cooperate with one another to carry out predetermined tasks in order to attain common goals. Different parts, levels, and requirements make up distributed control systems. Operational layer consists of the central computer and control room that oversees activities. A master controller receives reports from several connected servers including data management and activity action logs. PLCs and supervisory control and data acquisition (SCADA) systems are utilized to govern the movements of the relevant equipment. Through sensors and actuators, these systems exchange data. Critical infrastructure like power and energy as well as extensive industry applications including healthcare, defense, and finance all use DCS. While balancing other services, communication, control, computing, and security are seen as DCS's primary problems.

The main goals of cybersecurity, which is a growing concern for DCS, are to protect the organization's and/or the nation's assets from known and unknown vulnerabilities, threats, and advisories. These goals include confidentiality, integrity, availability, authenticity, and validation.

The continuity of DCS's service delivery is essential. Any prolonged lack of service has the potential to be devastating. An attacker can take advantage of this vulnerability by using up system resources and demanding pointless tasks to stall essential system functions. It is crucial for DCS to provide whole system security, achieve a feeling of availability, validity, and validation for data and transactions, and uphold the reputation of the various DCS infrastructure components.

Knowing the many forms of cyberattacks is the first step in identifying the risks, resources, and security flaws on DCS. The cyber-attack against DCS may be threatened from both the inside and the outside. Dealing with both kinds of risks is crucial. External risks include rival companies, hackers, etc. Inadequate actions, irate workers, and the usage of technology can all be considered internal dangers.

Due to the use of commercial off-the-shelf (COTS) technology, which allows companies to purchase ready-built control systems made available to the general public, control systems are defenseless against external attacks. Internal threats can happen as a result of careless actions, such as when a worker in the industry accidentally runs a set of programmes in the live control system, resulting in a half-day production loss owing to improper communication with the designer who created that system.

The main weaknesses of control systems include poor input validation, insufficient data authenticity checks, inadequate arrangements and methods, a lack of defense in depth during design, poor programming, insufficient remote access, the inability to observe improper movement within the control system, and the use of plain-text network communication protocols that are not encrypted. Threats can access control systems in a variety of ways. Recent studies have shown that demand for DCS has risen in recent years; but that demand has been restrained by security issues such recent cyberattacks and malware targeting.

The communication route is secured using a digital signature authentication approach. The approach exchanges information or allows for communication via the Distributed Network Protocol 3 (DNP3) channel. Each communication using this technique has an authentication fragment (AF). The AF is made up of an encrypted hash digest of the message together with a time-stamp that the receiver uses to ensure that the time of receipt does not change from the predetermined time. To speed up processing, this approach encrypts only the sender's private key rather than the message itself. If the transmission is not delayed, there is no changed data and the recipient can securely decrypt the message.

The communication route for control systems is likewise secured using this method. In this method, one party poses a question as a challenge, and the other side must provide an appropriate response as an answer in order to be verified. The most fundamental and straightforward example of a challenge-response system is password authentication, in which you are asked for your password as a challenge and must enter the right password as your legitimate response in order to be authorized. The four stages of this method's mechanism are as follows: one party sends a random challenge to the other, the other party responds, the challenger party verifies the validity of the response before moving on, otherwise it ends the session or process, and the authenticator sends new challenges and repeats the process.

In contrast to communication channels, RTU is vulnerable to both internal and external attacks. RTU's architecture is composed on five layers: the protocol layer, software application layer, middleware layer, kernel of the operating system, and hardware. Every layer is vulnerable to risks, for example, if it uses an insecure protocol it may be readily attacked, and COTS components at the software layer might have an impact on the entire system. Therefore, RTU authorisation must be planned in order to maintain the security of the control system. To address

this, a security-hardened RTU design is provided. It only allows one input output (IO) controller access to input output ports, and it uses an access control enforcement and security functions module to grant access to RTU status and command points, making it more difficult to compromise.

In a distributed system, people are the major source of internal dangers. The system may have been targeted intentionally or accidentally. Unintentional assaults might come from devoted workers who unintentionally introduce viruses or risks into the system's internal environment. This may be accomplished using USB storage devices, personal laptops, malicious discs, and unsecured internet connections. By letting friends within the security perimeter or leaving the guarded area accessible for visitors, the staff risk setting themselves up for failure.

The second type of internal danger is a systemic human attack that is planned. These attacks typically result from factors including workplace unhappiness, retaliation, selfish financial interests, and political pressure. It is generally advised to run a background check on any staff hired for the vital system to address such problems. Promotions and privileges must only be awarded following a thorough assessment and confirmation of the employee's dependability and aptitude. Employee compensation and benefits must be at levels that are deemed satisfactory. Employee loyalty to employers will increase as a result of this. Any indication of displeasure, irritation, suspicious behavior, aberrant attitude, or psychological issues has to be reported and handled right away.

Additionally, effort should be made to ensure that personnel are not influenced by rivals in order to learn more about or exert control over them. Disconnecting the systems, organizations, and personnel from any outside influences and disturbances is necessary. The system's hardware, software, and operating systems may also be a factor in the internal threats. A gadget or piece of software created by a third party supplier may have additional parts installed to allow the information to be disclosed to the unauthorized party. To prevent fraud, it is advised to buy the sort of hardware and software from several suppliers. Additionally, a remote attestation and verification mechanism is required to confirm that the hardware and software are operating as intended.

Analysis

One can see that Stuxnet, a malware created for taking down a nuclear facility in Iran, has 4 zero day exploits and is open-sourced. This creates a danger as adding more zero day exploits is not a problem for most seasoned hackers. One can see that PLCs may not necessarily be targeted directly but can be used for gaining a deeper access to the OT network as well as getting workstation related information by tricking the workers. Instead of being the target of the malicious PLC assault, the PLCs turn into its instrument. A hacker might get access to every other PLC on the network and the engineer's workstation, which is the main repository for process-related data, by using one PLC as a weapon. With this access and expertise, the attacker may easily alter the logic of any PLC. For Distributed Control Systems, Both internal and external threats may exist for the cyber-attack on DCS. It's important to handle both types of hazards. External hazards might come from adversarial businesses, hackers, etc. Internal hazards might include poor performance, disgruntled employees, and technological use.

2.Conclusion

PLC network and physical access should be kept as limited as feasible. There is no doubt that such gadgets shouldn't be visible online or accessible from the outside world. However, only authorized engineers and operators should have access within. We advise doing the following since securing the connection to your PLCs is a time-consuming, laborious, and, when done poorly, even ineffective, process: Network Segmentation and Hygiene: Strict network segmentation is the first step in safeguarding the connection to your PLCs. By restricting access to your PLCs to a select group of engineering workstations, you may significantly decrease the attack surface on your network. Use Client Authentication: In order to confirm the identity of the client, the engineering station, it is essential to set up the PLC to use a client authentication method. Currently, some vendors use such communication protocols whereby, rather than allowing any engineering workstation to communicate with the PLC, only a particular and predefined set of engineering workstations are able to interact with the PLC. This is done by requiring the engineering workstation to present the PLC with a certificate.

In DCS, A digital signature authentication method is used to safeguard the communication path. The method uses the Distributed Network Protocol 3 (DNP3) channel to exchange data or enable communication. Critical infrastructure applications including agriculture, smart grid, healthcare, defense, and finance use distributed control systems. Control systems and computer security intersecting identified several issues with its infrastructure, including cyber and physical threats. This issue prompted the need for a method to safeguard the environment of distributed control systems, specifically strategies for systematic risk assessment to guarantee the secure availability of the vital infrastructure.

References

[1] Amin, S., Litrico, X., Sastry, S. S., and Bayen, A. M. Stealthy Deception Attacks on Water SCADA Systems. In Proceedings of the 13th ACM international conference on Hybrid systems: computation and control (2010).
[2] Beresford, D. Exploiting Siemens Simatic S7 PLCs. In Black Hat USA (2011).
[3] Byres, E., and Lowe, J. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In ISA Process Control Conference (2003).

[4] Cárdenas, A. A., Amin, S., and Sastry, S. Research Challenges for the Security of Control Systems. In Proceedings of the 3rd conference on Hot topics in security (2008).
[5] Cimatti, A., Clarke, E., Giunchiglia, F., and Roveri, M. NuSMV: A New Symbolic Model Verifier. In Computer Aided Verification. Springer Berlin / Heidelberg, 1999.
[6] Constantin, L. Researchers Expose Flaws in Popular Industrial Control Systems. http://www. pcworld. com, January 2012.
[7] Éireann P. Levertt. Quantitatively Assessing and Visualising Industrial System Attack Surfaces. Master's thesis, University of Cambridge, 2011.
[8] Evans, R. P. Control Systems Cyber Security Standards Support Activities, January 2009.
[9] Falcione, A., and Krogh, B. Design Recovery for Relay Ladder Logic. In First IEEE Conference on Control Applications (1992).
[10] McQueen, M., Boyer, W., Flynn, M., Alessi, S. Quantitative Risk Reduction Estimation Tool for Control Systems, Suggested Approach and Research Needs. Idaho National Laboratory. International Workshop On Complex Network and Infrastructure Protection (2006A).
[11] McQueen, M., Boyer, W., Flynn, M., Beitek, G. Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System, In Proceedings of the 39th Hawaii International Conference on System Science, Kauai, Hawaii. (2006B).
[12] National Institute of Standards and Technology (NIST), SP 800-82, "Guide to Industrial Control Systems (ICS) Security," Website: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, September 2008.
[13] Ralston, P., Graham, J., and Hieb, J.2007. Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46 (4), 583-594.
[14] Schneier, Bruce.1999. Attack trees: Modeling security threats. Dr. Dobb's Journal of Software Tools, 24 (12), 21-29.
[15] Stølen, Ketin.2001. CORAS-A Framework for Risk Analysis of Security Critical Systems. In supplement of the 2001 International Conference on Dependable Systems and Networks, pages D4-D11, July 2-4, 2001, Gothenburg, Sweden
[16] Cardenas, A., Amin, S., Lin, Z., Huang, Y., Huang, C., and Sastry, S. Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. In Proceeding of the ASIACCS'11 Conference, (March, 2011). ACM, DOI 978-1-4503-0564-8-8/11/03.
[17] Beitel, G. A., Gertman, D. I., and Plum, M. M.2004. Balanced Scorecard Method for Predicting the Probability of a Terrorist Attack. Risk Analysis IV: 581-592, WIT Press, Brebbia, C. A., ed. .
[18] V. Costan, L. Sarmenta, M. Van Dijk, and S. Devadas, "The trusted execution module: Commodity general-purpose trusted computing," Smart Card Research and Advanced Applications, pp.133-148, 2008.
[19] J. Docherty and A. Koelmans, "Hardware Implementation of SHA-1 and SHA-2 Hash Functions," 2011.
[20] A. Wright, J. Kinast, and J. McCarty, "Low-latency cryptographic protection for SCADA communications," in Applied Cryptography and Network Security, 2004, pp.263-277.
[21] A. T. Group and others, "Cryptographic protection of scada communications general recommendations," Draft3, AGA Report, no.12.
[22] H. Berger, Automating with SIMATIC: integrated automation with SIMATIC S7-300/400: controllers, software, programming, data communication, operator control and process monitoring. Wiley-VCH, 2003.
[23] A. S. Alkalbani, T. Mantoro, and A. O. M. Tap, "Comparison between RSA hardware and software implementation for WSNs security schemes," in 2010 International Conference on Information and Communication Technology for the Muslim World (ICT4M), 2010, pp. E84-E89.
[24] A. Böttcher, B. Kauer, and H. Härtig, "Trusted computing serving an anonymity service," Trusted Computing-Challenges and Applications, pp.143-154, 2008.
[25] E. B. Fernandez and M. M. Larrondo-Petrie, "Designing Secure SCADA Systems Using Security Patterns," in System Sciences (HICSS), 2010 43rd Hawaii International Conference on, 2010, pp.1-8