International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 6, 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Industrial Control Systems Cyber Security Resilience & importance of Remote Laboratory

Deshabhushan Chougule
(IAPCP, ABB Corporate Research Center, Bangalore, India
Email: deshabhushan.chougule@in.abb.com)

----------**********----------

Abstract:

Increase of Information & Operational Technology (IT/OT) applications into Industrial Control Systems (ICS) has improved the scalability & flexibility of the systems as well as it has enabled the possibility to access them from external nodes. However, in many cases, this evolution has exposed the Industrial Control Systems to a series of unprepared threats. These threats are currently found in most of critical infrastructures.

Although, it's not realistic to protect against every cyber threat but a resilience at certain level of threat can be achieved to safeguard Industrial Control Systems. Looking at larger potential consequences, the existing cyber resilience is not adequate. This situation can be improved through effective adoption of existing standards, processes & resources. Internal policies & procedures (like User Management & Role Based Access Control, Regular Maintenance, Backup & Recovery etc.) with appropriate architecture of redundant Control Systems can have a substantial impact as well as its ability to withstand or recover from a cyber incident. Further some Node & Network based Controls (like System Hardening & Application Control, Antivirus & Security Update Management, Network Segregation & IPSec, Firewall Rules etc.) can be used as recovery actions against corresponding Resilience categories.

In this case, we can prepare a Remote Laboratory based on the replication of a simple Industrial Control System that enables performing cybersecurity tests instead on real ones.

Keywords — **Cybersecurity, Resilience, Industrial Control Systems, Automation, Remote Laboratories, Vulnerability Scanner, Industrial Communication Protocols and Networks, Critical Infrastructures.**

----------**********----------

I. INTRODUCTION

The digital transformation of Industries is having a profound impact in Industrial Control Systems (ICS). Improvements in cost & performance have encouraged the evolution of the ICS by utilizing IT & OT capabilities in existing systems, resulting in many of todays "smart" systems such as the smart electric grid, smart transportation, smart buildings & smart industry (4.0). Technological advances have made possible that Industrial Control Systems have great flexibility, scalability & connectivity. Thanks to the intensive use of Information & Operational Technology (IT/OT) at all levels.

However, these systems were originally designed to be isolated systems instead of connected to a Corporate Network or Internet, so most of them lack security mechanisms to protect them against external attacks. Replacement of such systems by IT/OT increases the connectivity but at same time criticality of these systems, creates a greater need for their safety & security resilience.

This evolution has exposed them to a series of threats for which they have unprepared & made them vulnerable to malicious attacks which

 ©IJSRED: All Rights are Reserved

compromise ICS security properties (e.g. integrity, confidentiality, authentication or availability). On the other hand, this evolution has also allowed the ICS application to society not limited to the industry, such as Oil & Gas, Power Generation & Distribution, Transport, Health, Communications etc. Attacks on such facilities, especially those categorized as critical infrastructures, would involve extremely serious consequences. Therefore, cybersecurity should be a matter of priority to avoid incidents that interfere with its operation & cause serious economic losses, compromise the safety of people or cause environmental disasters.

Many cyber events go undetected or unreported. However, there are notable attacks on ICS, such as the German Steel Mill Attack in 2014, where hackers had manipulated the control systems in such a way that a blast furnace could not be properly shut down which resulted in massive damage. Another cyber-attack on the multinational Pharmaceutical giant, Merck reported $385 million in direct financial losses in the 2017 annual report. In this context, cybersecurity of Industrial Control Systems (ICS) is one of the most important aspects to be taken into consideration. It is necessary to provide robust cyber security mechanisms for Industrial Control Systems that are acquired in both IT & OT specific cyber security.

This paper presents some practical & effective steps that ICS provider can take to improve resilience & business continuity in the event of a cyber incident. Since it is not possible to perform the experiments on real control systems, hence need to rely on labs or testbeds. Most of the testbeds have research-oriented purpose to simulate of the actual process. In case of Remote Lab, the contents should be aligned with the standards & recommendations that are generally used in the field. The system manufacturers, users & integrators can have most relevant standards, which defines ICS security concepts & requirements.

II. Cyber Security Standards for Industrial Control Systems

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) has published the ISO/IEC 27000 standards on IT Security techniques for Information Security Management Systems & Requirements. In 2017 US Security Framework Adoption Study reported that 70% of the IT organizations have preferred NIST Cybersecurity Framework as the most popular/best practice for IT Security, but they have also reported that it needs significant investment.

There are a range of standards, regulations & guidelines available in the ICS field. For guidance on how to secure ICS there is “Guide to Industrial Control System (ICS) Security” by National Institute of Standards & Technology (NIST). Another useful document is “Cyber Resiliency Design Principles” produced by MITRE Corporation. It provides a set of cyber resiliency design principles. However, one of the most prominent is the ANSI/ISA99 standard by International Society of Automation (ISA). It is an international standard on “Industrial Automation & Control Systems Security” being further utilized by International Electrotechnical Commission (IEC) in producing the multi-standard ISA/IEC 62443 series.

ISA/IEC 62443 addresses the systems whose compromise can result in any following situations:

1. Endangerment of Public or employee safety
2. Loss of Public Confidence
3. Violation of Regulatory Requirements
4. Loss of Proprietary or Confidential Information
5. Economic Loss & Impact on National Security

Though it is possible to consider recommendations at the national & international level but on top of it there are few region or sector specific guidelines must be followed by security practitioners. In Europe, government authorities have increased their involvement in the ICS cybersecurity. In March 2013, the European Network & Information Security Agency (ENISA) has published a study about the ICS cybersecurity

 ©IJSRED: All Rights are Reserved

called "Protecting Industrial Control Systems - Recommendations for Europe", which details the current situation & gives recommendations for improvement. In the United States, government organizations are also significantly active, establishing a framework to assess the cybersecurity in critical sectors. In 2016, ICS-CERT (Cyber Emergency Response Team) published the report with total 245 incidents, out of which energy (32% of the incidents) & critical manufacturing processes (27% of the incidents) were the most affected sectors. Further NERC CIP (North American Electric Reliability Corporation - Critical Infrastructure Protection) has planned the set of standards designed to secure the assets required to operate the North America's bulk Electric Systems.

III. Cyber Security Resilience Plan for Industrial Control Systems

ICS cyber security defence across all the industry sectors is inadequate. Unfortunately, the likelihood of a cyber-attack is difficult to estimate. We need complete approach that includes the relevant aspects or factors that can be categorized as below:

1. Size of Control System – Complexity of Automation been achieved in ICS e.g. whether its simple Digital System or Distributed Control System.
2. Hardware & Software integration – Level of third-party Hardware integration been done at control floor or the number of ERP Software integration been done at plant floor
3. Connectivity – Dependency over legacy Fieldbus devices like Modbus TCP or Profinet. Usage of Internet (including cloud & mobile platforms)
4. Standardization – Companywide standard processes & technology used in systems replicate both strengths & weaknesses

In case of Software integration, ICS provider need some degree of trust with third party OEMs as its necessary to keep the infrastructure up to date with AV & Security Updates. However, sometimes AV & OS patch update can be highest target for malware (or unintentional errors). A real example of this is the consequences of McAfee AV false positive detection with 4715 DAT update that incorrectly deleted different file types in mass (including Excel). As OEMs cannot test their updates against every ICS application, so these risks can be managed by designing internal testing procedures & hosting cybersecurity services/support within organization.

Key Elements to be considered in ICS Cycler Security Resilience Program

The security resilience categories range from "very long downtime with high recovery cost" (due to ineffective backup & recovery strategies, unhardened system designs, lack of firewall) to "short or no downtime with very less recovery cost" (by doing regular maintenance, controlling the applications & implementing IPSec).

Standard Procedures & Policies are shown in Table 1.

TABLE I
STANDARD PROCEDURES AND POLICIES

Standard Procedures & Policies	Node based Policies	Network based Policies
• User Management • Role based Acess Control • Regular Maintenance • Backup & (Disaster / Incident) Recovery	• System Hardeninig • Application Control • Antivirus & Security Update Management • Vulnerability Scanning & Analysis	• Network Segragation • Internet Protocol Security • Firewall Rules • Intrusion Detection & Prevention

Below are the four key areas/actions which are practical, effective for resilient systems.

1. System Architecture – Design the system architecture with inbuilt resilience which will be easy to safeguard.
2. System Version/Update Management – Keep the System up to date with latest Version & remove the obsolescence.

 ©IJSRED: All Rights are Reserved

3. Regular Maintenance & Backup – Maintain the System regularly & improve its ability to recover from any disaster.

4. Dedicated Support & Resource – Retain standards against pressures of cost, constrained resourcing & workflow.

A. System Architecture

There are few things to be considered while designing the control system architecture to safeguard it from cyber security attacks.

1. Make it Redundant – Minimize the downtime due to data loss or performance characteristics. In case of critical plants, redundancy can be achieved in many forms over independent standalone systems e.g. hot or cold standby control systems, automatic failover.

Though the design for redundancy can provide a significant level of resilience against many non cyber security related risks but using identical systems for redundancy can compromise the benefits due to the like hood of same malware.

2. Make it more Diverse – Minimize the potential damage from a dominant malware attack over usage of common third-party software e.g. operating systems, browsers, ERP solutions etc. This applies to all the levels of application but especially operating system hence suggestion is to use a range of different third-party software or its versions to host critical control systems (e.g. OS – Server 2019, 2016 or Browser – IE Edge, 11 or Office 2019, 2016 etc.).

Though greater usage of the common software creates greater vulnerabilities but differences in software presents different vulnerabilities & have different patch cycles. Moreover, many attacks are not simultaneously launched across different platforms.

There are some similarities in nature of threats but not all OS are vulnerable to a common viral threat. This can be challenging for few critical applications (like SCADA) which often supports a single OS, but this recommendation is based on the concept of diversity that will increase the overall resilience.

B. System Version/Update Management

A certain degree of change is required in order to keep the system up to date (e.g. AV dat files & software security patches or system upgrades & obsolescence). These changes need to be managed in a such way that it should not weak the system functioning.

Sometime the ‘fix’ is the virus (e.g. McAfee - Excel false positives). ‘Bad’ dat files may cause mess with such false positive observations or unqualified security patches may cause to stop the control system functioning.

Recommendations to minimize the risks:

1. Do internal analysis / testing of dat files & security updates before deployment.

2. Do not use automatic update tools as few may accidentally break the control systems.

3. Keep software & hardware within its support age as obsolete systems may contain vulnerabilities (few cannot be rectified).

4. On other side, use of most recent software or hardware is also not advisable as it may not be sufficiently tested against control systems.

C. Regular Maintenance & Backup

Ability to successfully recover from an attack is a one of the important aspects of resilience. Sometimes if a situation is so terrible, then certain level of downtime is obvious. However, an effective backup system can make the difference between downtime & not being able to recover. Virtual environments have brought many advantages including failover replication.

The purpose of a backup is to provide a copy of software that is enough to rebuild the system or function. In addition to regular, automated online / offline backups, it’s good to periodically backup the critical information to low cost disposable / removable media that can be write protected & can be physically relocated (e.g. Blu-ray).

Some issues may go unnoticed for long periods of time, so it is important to maintain a deep history of backup data.

 ©IJSRED: All Rights are Reserved

D. Dedicated Support & Resource

Maximum achievable resilience requires the effective / relevant standards, processes & resources. In many companies its battle to retain standards against pressures of cost, constrained resourcing & workflow. Getting right & immediate support is critical in cyber resilience as the cost of inadequately addressed cyber security will be extremely high.

Excessive use of third-party software or acceptance of irrelevant resilience workflow can collectively & unnecessarily lower the cyber security defence however provision of diverse hardware, software and applications will make it easier for customers to retain the system.

Recommendations to minimize the risks:

1. Learn from nature of security and integrate the relevant aspects into company standards.

2. Build cybersecurity collaboration with relevant third-party specialist & supply chain to maximize defence.

3. Do not trust in OEMs to the maximum extent, rather internally exercise managing, testing and rolling out security related updates.

4. May prefer virtual environments for offline redundancy option. Ensure that low cost high capacity removable storage is available.

IV. IMPORTANCE OF REMOTE LAB IN ICS CYBER SECURITY RESILIENCE PROGRAM

This section presents a laboratory to perform cybersecurity tests remotely, for the detection and analysis of vulnerabilities in ICS. Moreover, in the United States, there is a large-scale testbed program (National SCADA Test Bed-NSTB) dedicated to control system cybersecurity assessment, standards improvement and training. The proposed internal testbed includes software, controllers, field devices and communication technologies commonly used in real industrial control system. Automation can work with both real industrial equipment and simulations so let's see a detailed description of both the physical equipment/simulations used to build testbed and the setup/tools used for vulnerability tests, AV or security update validation. We must have effective backup & recovery strategies, system hardening with firewall exceptions & IPSec implementation. If required, we can have user management & application control policies in place.

Below testbed shown in Fig. 1 provides the possibility to perform remote cybersecurity tests using:

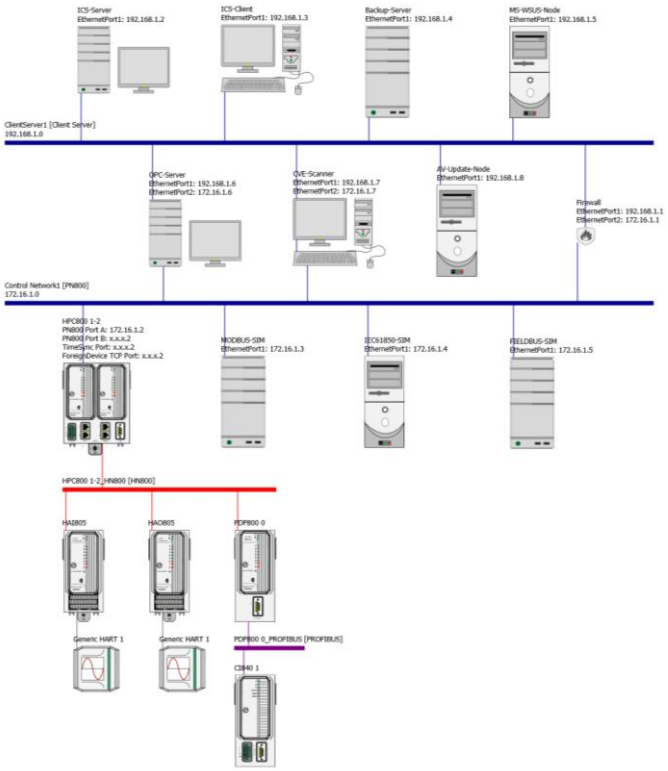

Fig. 1 Example of a Remote Test Lab for ICS Cybersecurity

1. ICS Server and Client – It contains the necessary software for the configuration of the SCADA, HMI and PLC. The HMI designed to control and monitor the physical systems is wired to the industrial PLC whereas SCADA system designed for monitoring and storage of the process variables. E.g. ABB SPlus Engineering can be used to configure the SPlus PLC and to design the HMI, and SPlus Operations cum History can be used to design the SCADA for the process variable monitoring.

 ©IJSRED: All Rights are Reserved

2. OPC Server – It's an additional communication server through which the OPC protocol can be implemented using a free tool developed by the Metricon group. It acts as a master, requesting data to & from the device or OPC Clients every second.

3. SPlus HPC800 Controller with HART and Profibus Devices – Its Industrial PLC (Programmable Logic Controller) connected to analog and digital module to simulate the real system. Devices communicates with PLC designed for this purpose using HART and Profibus protocol.

4. Simulators for Modbus TCP, DNP3, IEC104, IEC61850 & other Fieldbuses e.g. Profinet – It's a simulation tools through which the Modbus TCP, DNP3, IEC104, IEC61850 & other Fieldbuses e.g. Profinet protocol can be implemented using a free tool developed by the Axon, Triangle Microworks & Anybus groups respectively.

5. System Hardening with Firewall Enabled at Plant & Control Network – It helps to limit incoming traffic to the PLC, HMI & SCADA guaranteeing that they cannot be reprogrammed, modified from unauthorized users or devices. Furthermore, it also blocks all outgoing traffic, to isolate the testing environment.

6. Microsoft & Antivirus Security Update Node – It helps to overcome on security vulnerabilities & fully manage the distribution of updates that are released over Microsoft, McAfee or Symantec Update Server to computers in production environment. Microsoft update will be automatically synchronized with WSUS (Windows Server Update Services) whereas Antivirus update will be auto synchronized with McAfee ePO (ePolicy Orchestrator) or Symantec EPM (Endpoint Protection Manager) respectively.

7. Vulnerability Scanner – To reduce or mitigate the attack surface in order to increase the cyber security of ICS, it is advisable to perform vulnerability assessments periodically. This type of analysis identifies the vulnerabilities in system to be able to understand and patch them for which the vulnerability scanners (such as OpenVAS or Nessus) are useful tools.

8. Backup & Recovery Server – Its fileserver used to store server images and backups of Microsoft-based operating systems. Acronis Cyber Backup delivers the data protection too & helps for fast and reliable recovery of apps, systems and data on any device, from any incident.

V. CONCLUSIONS

Increasing use of information and communication technologies in Industrial Control Systems has exposed them to multiple threats for which they were unprepared, it makes them vulnerable to malicious attacks. By exploring ever-changing field of cybersecurity, companies need to manage risks from an expanded attack surface.

This paper presents few practical and effective measures that companies can take together with existing standards and frameworks, which will further increase the cybersecurity resilience. We also propose an approach for experimentation in cybersecurity of Industrial Control Systems, based on the replication of a simple ICS. The aim is to provide resilience for an easy definition of ICS cybersecurity. In order to achieve this purpose, the remote laboratories can provide excellent support that companies can consolidate their experimentation with real equipment used in the industry.

ACKNOWLEDGMENT

I would like to thank the management of ABB Corporate Research Center for permission to publish this work.

REFERENCES

[1] Article by Carlos J. Del Canto, Miguel A. Prada, Juan J. Fuertes (2015) – "Remote Laboratory for Cybersecurity of Industrial Control Systems" – Hosted by Elsevier Ltd. IFAC (International Federation of Automatic Control).

[2] Article by Michael J. Lees, Melissa Crawford, Christoph Jansen (2018) – "Towards Industrial Cybersecurity Resilience of Multinational Corporations" – Hosted by Elsevier Ltd. IFAC (International Federation of Automatic Control).

[3] Article by Manuel Dominguez, Antonio Moran, Serafin Alonso, Daniel Perez (2019) – "Experimentation environment for Industrial Control

 ©IJSRED: All Rights are Reserved

Systems Cybersecurity" – Hosted by Elsevier Ltd. IFAC (International Federation of Automatic Control).
[4] Technical report on "Cyber resiliency design principles" – Published by MITRE Corporation.
[5] "ICS Cybersecurity Programs for Multinational Corporations Summit" – Hosted by Kaspersky International Industrial Security.
[6] The 62443 Series Standards for "Industrial Automation and Control System Security" – Designed by ISA.
[7] Article on "McAfee antivirus update wreaks havoc" – Published by Computer World.
[8] ICS-CERT Monitor – Designed by National Cybersecurity and Communications Integration Center (NCCIC).

 ©IJSRED: All Rights are Reserved