International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

ANALYSIS OF SECURITY SOLUTIONS FOR INDUSTRIAL CONTROL SYSTEMS

Dayanand Kumar [#1], Goutham J [#2], Chaitra B R[#3]
[#1#2, #3] *Student, Department of Computer Science and Engineering,*
Vivekananda Institute of Technology, Bangalore-74, INDIA

Abstract*-- Industrial Control System (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Depending on the industry, each ICS functions differently and are built to electronically manage tasks efficiently. Today the devices and protocols used in an ICS are used in nearly every industrial sector and critical infrastructure such as the manufacturing, transportation, energy, and water treatment industries. There are several types of ICSs, the most common of which are Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS).ICS is increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. However, ICS generally have little protection from the escalating cyber threats. In order to understand the potential danger and to protect ICS, in this paper, we highlight their difference from standard IT systems based on architecture and present a set of security property goals. Furthermore, we focus on systematically identifying and classifying likely cyber-attacks, and analysis of solutions to secure the industrial control systems

***Keywords:* ICS, DCS, SCADA, PLC, Cyber Security, Security Controls.**

I. INTRODUCTION

Control system (ics) is a general term that encompasses several types of control systems. used in industrial production, including supervisory control and data acquisition (scada) systems, distributed control systems(dcs), and other smaller control system configurations such as programmable logic controllers(plc) often found in the industrial sectors and critical infrastructures. the term "ics," as used throughout includes supervisory control and data acquisition (scada) systems, process control systems, distributed control systems, and other control systems specific to any of the critical infrastructure industry sectors. Although differences in these systems exist, their similarities enable a common framework for discussing and defining security controls. Standard cyber security concepts apply to all computer hardware and software, and common issues in ics can be discussed in general terms. Industrial control systems have traditionally been protected due to the isolated environment. However, the introduction of information technologies such as ethernet, tcp/ip and wireless technologies within industrial control system has resulted in significantly less isolation from the outside world. Consequently, industrial control devices will face more vulnerabilities and attacks than ever before. it became intensely urgent that what approaches and tools can be used to test security of industrial control devices for the sake of security risk reduction.

II. OVERVIEW ON ICS

An industrial control system (ICS) is integrated hardware and software In Order To Perform Three Main Operations Acquisition, Control and Supervision. ICS Collects Sensors Measurements Results and Operational Data from the Process field, process, analyse, display them for system operators and execute control logic in local or remote control devices. Several standard architectures are defined by standardization organizations such as isa [1], nerc [2], aga [3] etc., these architectures describe the different levels of the system from two points of view, network and operations. In the following paragraph we discuss scada systems that are used for large and geographically dispersed facilities, typically for distribution. While ICS are in many ways becoming standard it; ICS do have some distinguishing features that, unfortunately, tend to impede the implementation of security controls: ICS are typically used to control critical processes. Key priorities are the 24 by 7 continuity and the ability for operations to view and control the processes. ICS triggered disruption of the production or critical functions, may affect the organisation's profit and reputation. This causes a strong reluctance to apply any system changes that could harm the continuity of the production and its

III. ICS ARCHITECTURE

A. SCADA ARCHITECTURE

SCADA is not a system that can provide full control. Instead its capabilities are focused on providing control at the supervisory level. SCADA systems are composed of devices (generally Programmable Logic Controllers (PLC) or other commercial hardware modules) that are distributed in various locations.

SCADA systems can acquire and transmit data, and are integrated with a Human Machine Interface (HMI) that provides centralized monitoring and control for numerous process inputs and outputs.

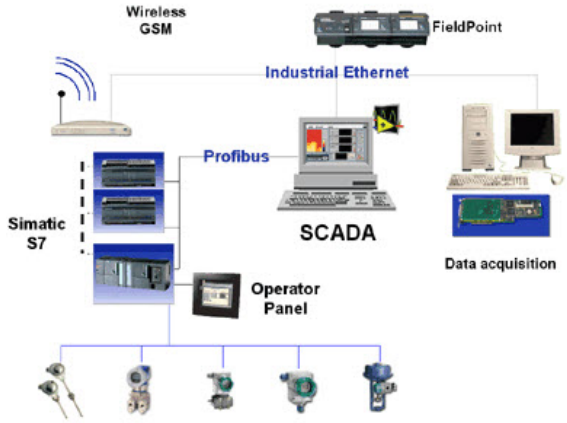

Fig 1. SCADA ARCHITECTURE

B. DCS ARCHITECTURE

This is a system that is used to control production systems that are found in one location. In a DCS, a set point is sent to the controller that is capable of instructing valves, or even an actuator, to operate in such a way that the desired set point is maintained. Data from the field can be stored for future reference, used for simple process control, or even used for advanced control strategies with data from another part of the plant. Each DCS uses a centralized supervisory control loop to manage multiple local controllers or devices that are part of the overall production process.

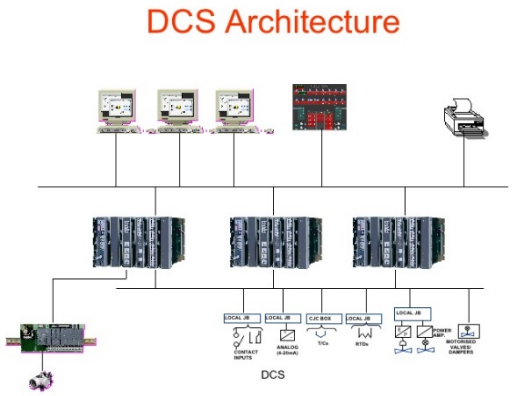

Fig 2. DCS ARCHITECTURE

IV. ICS COMPONENTS

A. IT AND OT

Operational Technology (OT) variables include the hardware and software systems that monitor and controls physical devices in the field. OT tasks vary with every industry. Devices that monitor temperature in industrial environments are examples of OT devices. The convergence of IT and OT provides enterprises greater integration and visibility of the supply chain– which include their critical assets, logistics, plans, and operation processes.

b. PROGRAMMABLE LOGIC CONTROLLER (PLC)

This is a type of hardware that is used in both DCS and SCADA systems as a control component of an overall system. It also provides local management of processes being run through feedback control devices such as sensors and actuators. In SCADA, a PLC provides the same functionality as Remote Terminal Units (RTU). In DCS, PLCs are used as local controllers within a supervisory control scheme. PLCs are also implemented as primary components in smaller control system configurations.

C. REMOTE TERMINAL UNIT (RTU)

An RTU is a microprocessor-controlled field device that receives commands and sends information back to the MTU.

D. CONTROL LOOP

Every control loop consists of hardware such as PLCs and actuators. The control loop interprets signals from sensors, control valves, breakers, switches, motors, and other similar devices. The variables measured by these sensors are then transmitted to the controller to carry out a task and/or complete a process.

F. Human Machine Interface :

A graphical user interface (GUI) application that allows interaction between the human operator and the controller hardware. It can also display status information and historical data gathered by the devices in the ICS environment.
It is also used to monitor and configure set points, control algorithms, and adjust and establish parameters in the controllers.

V. ICS PROTOCOLS

A. Process Field Bus (PROFIBUS)

PROFIBUS uses RTU to MTU, MTU to MTU, and RTU to RTU communications in the field. There are two available variants: Profibus DP (decentralized peripherals), which is used to operate sensors and actuators through a central controller, and Profibus PA (process automation), which is used to monitor measuring equipment through a process control system.

B. Distributed Network Protocol (DNP3)

This is a protocol with three layers operating at the data link, application, and transport layers. This protocol is widely used in electricity and/or water and wastewater treatment plants

C. Modbus

Modbus uses serial communications with the PLCs and has been the de facto communications protocol in an ICS environment. There are two types of Modbus implementations: Serial Modbus – which uses the high-level data link control (HDLC) standard for data transmission, and Modbus-TCP – which uses the TCP/IP protocol stack to transmit data.

D. Open Platform Communication (OPC)

The OPC is a series of standards and specifications for industrial communications. The OPC specification is based on technologies developed by Microsoft® for the Windows® operating system family (OLE, COM, and DCOM).

E. Building Automation and Control Networks (BACnet)

This is a communication protocol that is designed to control heating, ventilating, and air-conditioning control (HVAC).

Common Industrial Protocol (CIP)

A CIP is a set of services and messages for control, security, synchronization, configuration, information, and so forth. The ICP can be integrated into Ethernet networks and the internet. CIP has a number of adaptations providing intercommunication and integration for different types of networks.

G. Ethernet for Control Automation Technology (EtherCAT)

An open-source communications protocol used to incorporate Ethernet into industrial environments. EtherCAT is used in automation applications with short updating cycles ($\leq 100\mu s$) and with jitter $\leq 1\mu s$.

VI.CYBER SECURITY REQUIREMENTS FOR ICS

Several standardization and governmental organizations, such as NERC, ISA and NIST came with a set of functional and Organizational requirements to protect industrial control systems from cyber-attacks. All those requirements have a goal; the insurance of the security objectives. As we are interested by the systems security functional requirements, we summarize in the following security requirements for ICS.

- Timeliness and Performance Requirements

ICS are 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.

- Availability Requirements

Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensure high availability (i.e., reliability) for the ICS .Some ICS employ redundant components, often running in parallel, to provide continuity when primary components are unavailable.

- Physical Effects

ICS field devices (e.g., PLC, operator station, DCS controller) are directly responsible for controlling physical processes. ICS can have very complex interactions with physical processes and consequences in the ICS domain that can manifest in physical events. Understanding these potential physical effects often requires communication between experts in control systems and in the particular physical domain.

- System Operation

ICS operating systems (OS) and control networks are often quite different from IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel.

- Resource Constraints

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.

- MANAGED SUPPORT

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.

- COMPONENT LOCATION

Most IT components and some ICS are located in 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. Component location also needs to consider necessary physical and environmental security measures.

VII. SECURITY THREATS ININDUSTRIAL CONTROL SYSTEMS

We classify attacks into three main categories: Attacks targeting availability, attacks targeting confidentiality, attacks targeting integrity.

- *Attacks targeting Availability: attacks targeting availability intend to deny access to system assets as well as operations. In ICS, this refers to deny of access to all the components of a systems like the ICS assets; Operator workstations, Engineering stations, communications system as well as control devices.*
- *Attacks targeting Integrity: by illegally modifying the content of a message or the content of system assets. In ICS that becomes to modify acquired messages or control commands transiting through the three system levels as well as modifying the content of databases or control programs in PLCs or RTUs.*
- *Attacks targeting Confidentiality: their aim is to acquire unauthorized data or resources in the Industrial control network. Acquired data such as passwords, PLCs configurations may be used unintentionally to replay.*

These threats can exploit the vulnerabilities if the ICS, in classification with the above .Here are the most relevant attacks on Industrial Control System

a. Dos Attack: This attack reduces the availability of the system for it's intend purpose
b. Eavesdropping: This attack violates the confidentiality of the communication for ex: sniffing packets in local area network
c. Man in the middle: the attack is carried out on both end points which results in confidentiality violations, this results in modification of the exchanged messages; man in the middle exploits weakness and gain control over the encrypted session.
d. Breaking into the system: this attack results in violation of authentication and access control objectives where the attacker gains the ability to control aspects of the behaviour of the communication system including the ability to overcome confidentiality and integrity objectives. A break-in usually involves the consecutive penetration of multiple subsystems and the step-wise elevation of the privileges of the attacker.

The followings are the most sophisticated attacks identified by security researchers and experts:

Stuxnet: Stuxnet is a Microsoft Windows computer worm discovered inJuly 2010 that specifically targets industrial software andequipment of the Iranian nuclear facility [4]. Stuxnet specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.

Slammer Worm : Slammer (also known as Sapphire, Helkern or SQLExp) was a worm that appeared in 2003 January and was the fastest-spreading worm of its time. The worm was an extremely simple piece of code and its payload was an unintended by-product of its spreading ability. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm, Slammer infected a private computer network at the nuclear power plant in Ohio, disabling a safety monitoring system formerly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly.

Shamoon Malware : Is a malware attack that targeted the Saudi Aramco refineries which are the 8th largest refinery in the world. The malware targeted system's Master Boot Records (MBR), partition tables and other random data files. This caused the systems to become unusable [4].

VIII. SECURITY SOLUTIONS FOR ICS

Multiple security counter measures have been designed for ICS standards for securing ICS dependable systems as a requirement definition steps, security solutions for network protection as well key management systems for the design of authentication, authorization and integrity management.

a. NIST Guidelines

National institute of standards and technology (NIST) started a project on security of industrial control systems with applying NIST SP8053 [5] in Industrial control system.

The aim of this project was the appliance of Federal Information Processing Standards (FIPS) [6] [7] to industrial control systems as part of the federal systems. FIPS 199 and FIPS 200require the following security controls for Federal systems: Access control, Awareness and training, audit and accountability, security assessment, configuration management, Identification and Authentication as well as Incident response.

These requirements were introduces in Specific publication for security in industrial control systems NIST 800-82 [8]. NIST guide to industrial control systems security provides typical ICS architectures and topologies, then discuss main threats and vulnerabilities of these systems. The document provides also security countermeasures to mitigate the risk associated to the ICS vulnerabilities and threats.

b. IEC 62433

IEC 62443 formally called ISA99 Industrial Automation and Control Systems (IACS) Security; its aim is to create guidance documents on how to apply IT security in Industrial control systems including Hardware and software systems such as SCADA, DCS, PLC, HMI, networked sensors and devices.IEC 62443 is categorized into four main requirement categories; General requirements, Policies and procedures requirements, System requirements and Component requirements. IEC62443 is the first standard that details requirements from system point of view by introducing inIEC62443.3.x [9] Security Assurance Levels (SALs) for industrial control systems and for specific security controls to implement for each SAL. Security assurance levels are assessed for each functional zone using seven functional requirements; Identification and authentication control, Use control, Data integrity, Data confidentiality, Restricted dataflow, Timely response to event, Resource vailability.IEC62443.3.x series are adopted by most of ICS vendors.

IX.CONCLUSION

This paper presents a deep overview on industrial control systems architectures, components and main protocols for a better understanding of the security issues in the ics. We discussed the main security objectives and requirements for industrial control systems and the differences between security in it and security in ics. Cyber-attacks already discovered in the ics raises the high requirement of deep investigation of security solution tailored for the industrial world. The challenge for us and for all researchers in the ics cyber security filed is to propose tailored security solution taking into account all the functional constraints of ics. This challenge conducts us to review all the design of industrial control system components and communication protocols then redesign security mechanisms. The presented shadow security unit concept is a low-cost solution for securing scada systems, being complementary to existing siem architectures and, to the best of the authors' knowledge, constituting a new approach to the problem of security monitoring in ics.

REFERENCES

[1]. Stewart A.Boyer " SCADA: Supervisory Control and Data Acquisition" International Society of Automation 2009. International Society of Automation: www.ISA.org
[2]. North American Electric Reliability Corporation: http://www.nerc.com
[3]. American Gas Association : www.AGA.org
[4]. Fraser,Roy E., Process Measurement and Control: Introduction to Sensors, Communication, Adjustment, and Control, Upper Saddle River, New Jersey: Prentice-Hall, Inc., 2001.
[5]. Knapp, Eric, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Waltham, Massachusetts: Syngress, 2011.
[6]. U.S. Government Accountability Office (GAO), GAO-15-6, Federal Facility Cyber security; DHS and GSA Should Address Cyber Risk to Building and Access Control Systems, December 12, 2014
[7]. Swanson, Marianne, et al., NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems,February 2006.
[8]. Stouffer, J. Falco, K. Scarfone, "Guide to Industrial Control Systems (ICS) Security Special Publication 800-82," Second public draft, National Institute of Standards and Technology, September 2007.
[9]. M.J. Karam, F.A. Tobagi, Analysis of the delay and jitter of voice traffic over the Internet, in: Proc. of IEEE INFOCOM '01, 2001.
[10]. P. Neumann, "Communication in industrial automation - what is going on?" in Control Engineering Practice. Elsevier Ltd, 2006, vol. 15,pp.1332–1347.
[11]. Erickson, Kelvin, and Hedrick, John, Plant Wide Process Control, Wiley & Sons, 1999.
[12]. Paul Didier, Reference Architectures for Industrial Automation and Control Systems, ODVA Industry Conference & 15th Annual Meeting October 2012.

