A survey of the state-of-the-art in industrial control systems security

Prajjwal Dangal
Department of Computer Science
University of Colorado
Colorado Springs, USA
prajjwal.dangal@gmail.com

***Abstract*—An industrial control system (ICS) is a general term that denotes systems consisting of actuators, control stations, and network, that help manage processes and functions in an industrial setting. Also included within the scope of the term are systems like EPICS that are primarily deployed in research labs and critical national infrastructure around the world alongside others like DCS and SCADA. In this paper, I provide a thorough background of ICS in terms of its different variants, networking-related hardware, software infrastructure etc after which I dwell into security challenges from the perspective of system security. I have leveraged this to map the literature on ICS security along with using a comparison between ICS and IT system.**

I. Introduction

Industrial Control Systems is an umbrella term for large scale systems that help automate and make efficient the production of goods and services in an economy. Alternate terms include Process Control System (PCS), Automation Control System (ACS), Digital Control System (DCS) [17] etc. Sometimes, SCADA also serves the scope of these terms but for this paper, SCADA is a member of the set, not the universal set. These systems help automate lengthy physical/mechanical/electro-mechanical tasks such as transportation of goods in their intermediate stages within a plant during their manufacture, facilitate mineral extraction through flotation in mines etc. While their use in experimental physics arena is for high-precision data acquisition through the use of specialized detectors, high-resolution cameras as Ill as monitoring systems at fine grain time interval (on the order of nano seconds). Similarly, through their application to critical national infrastructures, they help control flow of electricity, water and establish resiliency in case of component failure. Before the widespread adoption of this paradigm, people/companies/organizations used manual effort or mechanical switches. A great example is Bell Labs where it was feared that all the electricity produced would get consumed after the lab installed automatic telephone switchboard, an electronic system known for heavy electricity draining. [9] Fast forward a few years and modern controls emerged, mostly in the form of ladder logic and the Programmable Logic Controller (PLS). An example is mentioned in Hayden et al.'s report about a car company that installed the then new technology PLC in their factory except its employees didn't know the sophisticated programming that one needed to know in order to be able to use those controllers. This necessity, the tale goes, was how ladder logic was born which sees widespread use even today. (Figure 1).

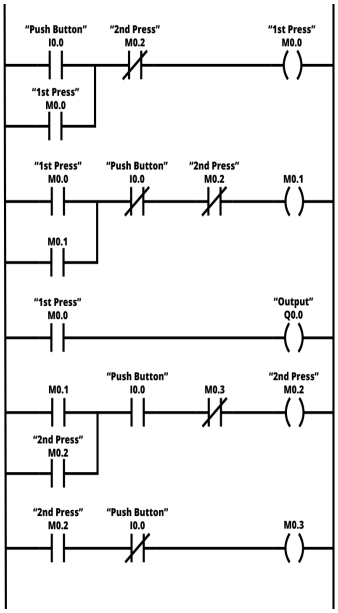

Fig. 1. Single push button on-off ladder logic [3]

II. Background

It is important to understand ICSs before we can understand how they might be exploited. This is comprised of understanding ICS type, architecture, networking protocols, and system devices in order to be able to come up with a holistic security strategy often called defense in depth [16].

ICSs vary in their make-up and function like already discussed. ICSs like Digital Control Systems (DCS) come with the graphical user interface integrated with the rest of the control system and feature more code reuse than Supervisory Control And Data Acquisition (SCADA) systems. Hence, from the outset, one can see that the latter warrants system integration testing as Ill as end-to-end testing as ways of security assurance after the graphical system is integrated to it. Also, these graphical system are special purpose system called Human Machine Interface (HMI).

I have included a simplified form of an ICS architecture in Figure 2. It is derived from an experimental physics setting, in

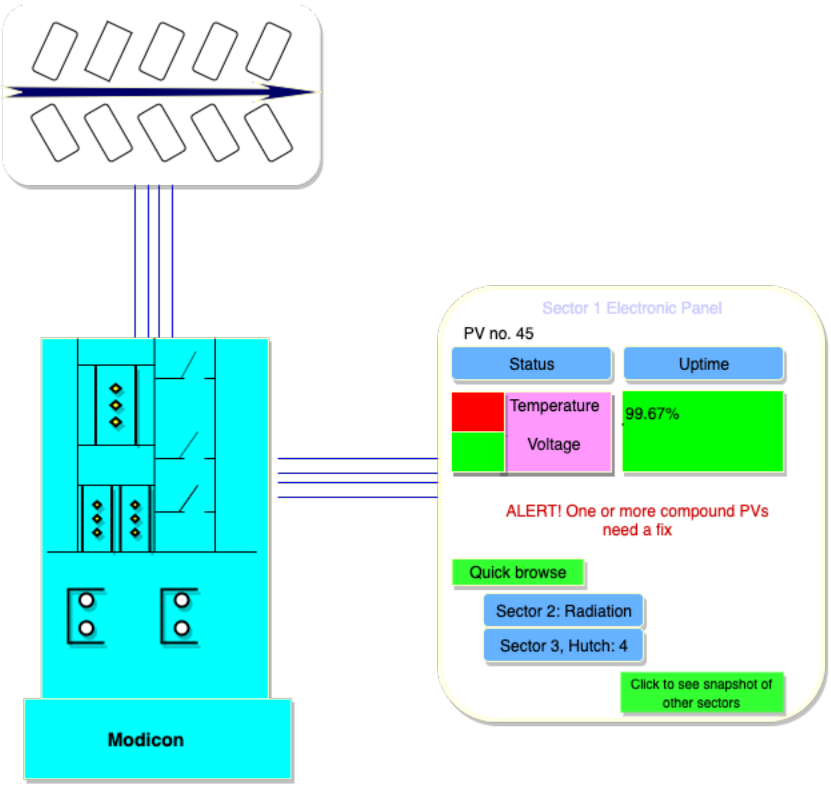
Sector 1 Electronic Panel
PV no. 45
Status
Uptime
Temperature
Voltage
99.67%
ALERT! One or more compound PVs need a fix
Quick browse
Sector 2: Radiation
Sector 3, Hutch: 4
Click to see snapshot of other sectors
Modicon

Fig. 2. ICS Architecture

that, the topmost box is an undulator. An undulator is an array of magnets arranged so as to help produce laser by utilizing the motion of electrons. [15] That box is called a process-connected device in an ICS architecture [11]. Typically, process-connected devices are sensors, servos, motors and other actuator devices that serve as the first point for telemetry data. They are connected to control devices like Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). The PLC in Figure 1 is the edifice below the process-connected device that reads 'Modicon'. It contains switches and relays. These types of devices can be programmed using a stack consisting of assembly-type language, electrical circuit diagram, and graphical programming language [1], [14]. From PLCs/RTUs the data is transmitted to supervisory systems. This latter is nothing but an end-point consisting of human operators who use HMI to interact and control the rest of the control system. Some of these control systems In our figure, this corresponds to the panelled display on the right. This is a good point to transition into dIlling more upon the different types of ICSs.

A. System Heterogeneity

In addition to the more popular ICSs that I have mentioned before, FactoryTalk View SE (FTV-SE), PVSS, TANGO are some of the other ICSs and ICS peripherals that are in use in current market. HoIver, not all ICS are comparable in their scope. For example, FactoryTalk View SE only provides the HMI capability for Allen-Bradley PLCs. Only after the two are combined do they compare with the larger ICSs like EPICS and SCADA. An important thing to note while we are discussing comparison is that these system denote physical world quantities by terms such as Process Variable (PV), Tag, Field etc. Hence, those terms are equivalent to one another in more ways than not. Figure 3 displays the comparison between common ICS system which helps elucidate interesting properties of these systems like pure polling. Pure polling is different from simulated polling in that the former is finer than the former in terms of timing interval.

B. ICS Network

ICS network and communication is a crucial part of the any ICS architecture. This is true in terms of functionality as Ill as security assurance. But given that the current ICS networks no longer operate in isolation like they used to before, but are connected to the external networks, new avenues of attacks have been added. Along with that, time sensitive networking (in a real-time sense) is often of importance given that ICS are often a combination of soft and hard real-time sub-systems.

There are two types of ICS network protocols, viz. **fieldbus** protocols and **backend** protocols. Some of the fieldbus protocols include Modbus, Dnp3, Profibus, Profinet, Ethernet/IP, Ethercat, PoIrlink, Sercos, CC-link IE, GPRS, GSM, HART, WirelessHart, Zigbee, LoRal etc. [11], [13]. The RS-family protocols such as RS-232 are used underneath some of these application layer protocols.

EPICS	**SCADA**	**PVSS**
Mostly in use in labs that conduct natural science related research	Mostly in use in critical national infrastructures like water, electricity supplying authorities	Mostly used in labs like EPICS
Located in a periphery of few square miles	Typically, span over large geographical regions	Slightly smaller in geographic scope than EPICS
Open-sourced development and support	Could be open-sourced or proprietary	Proprietary (by Siemens)
Need/ability to define your own process variable	Need/ability to define your own process variable	Some ability to define variables according to one's need [4] as Ill as built-in tags [13]
Data acquisition method = simulated polling	Data acquisition method = pure polling	Data acquisition method = pure polling

Fig. 3. Comparison of different types of ICSs

1) MODBUS

MODBUS is one of the earliest ICS network protocols, developed in 1979 for Modicon PLC from which it also derives its name. It operates at layer 7 and is compatible with layer 1 protocols like RS-232C (point-to-point) or RS-485 (multidrop). Its communication mechanism is request/reply in that a master client requests a slave server to perform a particular function by supplying a Function Code and a Data Request. If all goes Ill in performing that request, the slave server will respond back with a Function code and a Data response. If there arise errors in processing the request, the server returns a Exception Function Code and Exception Code. Modbus is lightlight with very little processing overhead, because of which it is used in a real-time setting like ICS [11]. HoIver, there does exist a TCP infused version of Modbus that is widely used and its future looks uncertain among declining support and neIr protocol technologies. [8]

2) EtherCAT

EtherCAT is, as can be observed, the best solution for ICS networking for most scenarios unless there is a threat with regards to hacking physical world data. EtherCAT features a unique stack comprised of special ethernet controller and separate fields for real-time and non real-time data. [2]

3) Profinet

Profinet is a master-slave protocol that allows multiple masters through the use of token.

III. Interrelationship between ICS and IT system security

When we consider an ICS, security problems persist in three major areas: standalone ICS, standalone IT system that manages the data/business of the ICS site and the interaction between these two systems. A defense-in-depth system is often not possible without the true co-ordination between these areas and personnel awareness. This is because, despite segmentation of these two areas into separate networks, the human factor plays a crucial role in either augmenting or deteriorating overall ICS security.

A solid comparison is provided by Stouffer et al. [16] between IT systems (ITSs) and ICSs. I have included a peek from it in Figure 4. I would also highly encourage you to dive through the aforementioned document.

In terms of the general security and safety interplay, the following is one succinct example of how these aspects might diverge. For e.g., a system may be safe but not secure – such as a medical information system that enables a doctor to directly access patient records without entering a password. Alternatively, a secure system may not be safe – for instance, if it takes the clinician so long to enter a password that the patient dies before they can access their records. Similarly, intrusion detection cannot be too heavy or the attacker will have infiltrated the system before successful detection. [10]

This dynamics should definitely be kept in mind while designing security solutions in any kind of system including ICS.

IV. ICS Security

In their legacy form, ICS network protocols lack security features like authentication, integrity, and confidentiality [7]. However, through the use of TCP/UDP/IP, security features have been installed in these protocols. A whitepaper by Encoder [2] showcases a nice framework for different levels of safety and security in an ICS domain. I highly encourage you to go through it and see for yourself, especially page four. Trade-off between security and safety manifests itself in places where data security might be more imporatant than real-time satisfiability. For example, one is better off using EtherCAT in motion control where as using Powerlink or Ethernet \IP might be fine for non hard real-time tasks like basic automation. [2] Both, EtherCAT and Powerlink are standard ICS protocols like already mentioned in the background section. So, we can imagine how real-time protocols like EtherCAT, Sercos III, Profinet IO and CC-Link IE might be appropriate for the communication that takes place between nodes in a process-connected device network alongside the communication between the same slave nodes and master

Category	**IT system**	**ICS system**
Performance requirements	Non-real-time, response must be consistent, high throughput is demanded, high delay and jitter may be acceptable, less critical emergency interaction, tightly restricted access control can be implemented to the degree necessary for security	Real-time, response is time-critical, modest throughput is acceptable, high delay and/or jitter is not acceptable, response to human and other emergency interaction is critical, access to ICS should be strictly controlled but should not hamper or interfere with human-machine interaction
Availability Requirement	Responses such as rebooting are acceptable	Responses such as rebooting may not be acceptable because of process availability requirements
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years

Fig. 4. Differences between ICS and ITS [16]

PLCs. Similarly, Ethernet \IP, Modbus, Profinet, etc. are examples of some secure protocols that might be appropriate to use between master HMI and slave PLCs.

Moving into the discussion about backend protocols, they serve the primary purpose of facilitating cross-protocol communication at the control device as well as supervisory control area. A popular choice is Open Process Communications (OPC). OPC is based on the a set of Microsoft technologies like Object Linking and Embedded (OLE), Component Object Model (COM) and since, there wasn't much of a cybersecurity risk back in 1996 when these technologies were developed, the future of systems that use OPC is said to be shaky as far as security is concerned. [11]

V. ICS System Security

ICSs are often built out of a number of sub-systems which in turn consist of embedded devices like embedded processors, ad-hoc controllers, and peripherals. It would be good idea to have a simulation tool that would help conduct analysis of time sensitive networking within these sub-systems or a combination of the members of these sub-systems. In particular, real-time schedulability analysis of these protocols seem like a promising field to conduct further research. For instance, one previous work has developed a way to spin-off an spin-off i.e. a copy of a simulated object [5] which should not fail to hit home the value of simulation testbeds and simulation software in this area. Coupled with promising frameworks that the research community is putting forth such as Hydra that makes the management of dynamic program components like command line arguments, logging and configuration easier, it should make for a highly adaptive software solution to ICS security.

VI. Conclusion

Fast forward few decades since the advent of PLCs and ICSs have become quite ubiquitous in our day-to-day life. So has been the attacks on ICS which were observed to have increased by a factor of five in recent years [12]. But, recently, the trend has slightly contracted [6] which is how it should be kept with diligent effort. This warrants learning at a consistent basis along with learning fast.

References

[1] 2010.

[2] 2019.

[3] Academy, P. *Single push button ON/OFF ladder logic example. Also known as "push to on, push to off" logic function.* 2019.

[4] Briss, B., Schagginger, M., and Knipp, L. *PVSS II Getting Started - Basics*. ETM.

[5] Eckhart, M., and Ekelhart, A. A specification-based state replication approach for digital twins. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy* (New York, NY, USA, 2018), CPS-SPC '18, ACM, pp. 36–47.

[6] Filkins, B., Advisor, D., and Dely, J. *SANS 2019 State of OT/ICS Cybersecurity Survey A SANS Survey*. 2019.

[7] Fovino, I. N., Carcano, A., Masera, M., and Trombetta, A. Design and implementation of a secure modbus protocol. In *International conference on critical infrastructure protection* (2009), Springer, pp. 83–96.

[8] Group, E. T. *Industrial Ethernet Technologies: Overview*. 2019.

[9] Hayden, E., Assante, M., and Conway, T. *An Abbreviated History of Automation Industrial Controls Systems and Cybersecurity*. SANS Institute, 2019.

[10] Johnson, C. Security of safety-critical systems.

[11] Knapp, E. D., and Langill, J. T. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[12] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., and Jones, K. A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9* (2015), 52–80.

[13] RealPars. *What are the Differences between DCS and SCADA?* 2019.

[14] sbaresearch. sbaresearch/cps-twinning, Jun 2019.

[15] slacims. Youtube, 2019.

[16] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. Nist special publication 800-82 revision 2 guide to industrial control systems (ics) security supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc).

[17] Warwick, K., and Rees, D. *Industrial digital control systems.* No. 37. IET, 1988.