An Open-Source Testbed to Visualise ICS Cybersecurity Weaknesses and Remediation Strategies – A Research Agenda Proposal

Conference Paper · June 2021

DOI: 10.1109/ISSC52156.2021.9467852

3 authors:

Conrad Ekisa
Institute of Technology, Carlow
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Diarmuid O'Briain
Technological University of the Shannon
12 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Yvonne Kavanagh
Institute of Technology, Carlow
32 PUBLICATIONS **141** CITATIONS
SEE PROFILE

An Open-Source Testbed to Visualise ICS Cybersecurity Weaknesses and Remediation Strategies – A Research Agenda Proposal

1st Conrad Ekisa, 2nd Diarmuid Ó Briain and 3rd Yvonne Kavanagh
engCORE Research Centre,
Department of Aerospace, Mechanical & Electronic Engineering,
Institute of Technology, Carlow, Ireland
Email: conrad.ekisa@itcarlow.ie

2021 32nd Irish Signals and Systems Conference (ISSC) | 978-1-6654-3429-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ISSC52156.2021.9467852

Abstract—**Industrial Control Systems (ICS) are responsible for the control of several processes in various critical infrastructure deployments ranging from energy, power and water utilities, to manufacturing sectors such as pharmaceutical precision engineering. They ensure the smooth, safe running and High Availability of these critical infrastructure and manufacturing processes. ICS cybersecurity is of increasing concern and this is evidenced by the mounting examples of cyber threats and attacks on ICS infrastructure that are referenced both within the technical community and the public media. The barriers of entry to ICS cybersecurity are still high given the limited skills base, expensive and proprietary hardware and software, as well as the inherent dangers of manipulating real physical processes. This greatly inhibits the practical application of cybersecurity tools in ICS environments and therefore the opportunity for practitioners to gain valuable experience. Furthermore, historical ICS testbeds have not delivered a practical application of accessing and improving ICS security posture as poisited in known ICS industry standards. This project seeks to build a comprehensive opensource virtualised ICS testbed to demonstrate typical cybersecurity weaknesses in an ICS environment as well as suitable remediation strategies. This testbed shall simulate real world industrial systems as closely as possible without replicating an entire plant. This research will identify a suitable ICS testbed to visualise the stages of an ICS cyber attack with reference to the ICS cyber kill chain proposed by the SysAdmin, Audit, Network and Security Institute. With the selected ICS testbed as a reference, this project shall also demonstrate an ICS cybersecurity evaluation based on the US National Institute of Standards and Technology cybersecurity framework, detailing how defenders can identify vulnerable components in the ICS, identify potential threat vectors within the environment and develop suitable mitigations to improve the organisations overall security posture. This project contributes to growing ICS cybersecurity skills to better protect industrial processes and critical infrastructure.**

Index Terms—**ICS, Cybersecurity, GRFICS, ICS Cyber Kill Chain**

I. Introduction

Historically, ICS were created to control and manage processes within manufacturing control zones. These functions greatly influenced the initial design criteria with a focus more on ensuring High Availability (HA) and Safety, and less on the first two aspects of the Confidentiality, Integrity and Availability (CIA) triad. This was also at a time when connection of the ICS to the Internet was not considered in the design equation. Today, ICS are at the heart of a number of critical infrastructure deployments such as water processing plants, power generation and distribution, nuclear plants, transportation, food and beverage industry, pharmaceutical, oil and natural gas and discrete manufacturing [1]. In an effort to improve the efficiency, reliability and oversight into ICS processes, technological shifts such as the integration of the Internet of Things (IoT) and Cloud computing are becoming commonplace. Early reports of damage to ICS installations due to electronic intrusions and malware attacks, include the Maroochy Shire Water Treatment Facility in Australia in 2000 [2], as well as the attack that raised awareness to the dangers of ICS cybersecurity, was the notable Stuxnet attack on an Iranian Nuclear Enrichment Plant in 2010 [3]. However, over time, the volume and extremity of ICS attacks has increased as evidenced by the May 2021 ransomware attack on Colonial Pipeline - one of the US' largest pipelines [4].

Fuelled by the increasing relevance of cybersecurity to ICS, particularly in keeping critical infrastructure safe and available, there has been an increase of resources deployed to strengthen both knowledge and skillset around cybersecurity to protect Operations Technology (OT) in ICS environments. Industry standards and guidelines such as the IEC-62443 standard [5], and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 [1], are now available as guides to ICS cybersecurity practitioners on how to evaluate and improve the security posture of OT. ICS environments are unique in nature and each environment shall slightly differ in how and where each standards applies. What do these industry standards mean for ICS cybersecurity practitioners? How can these standards be applied to evaluate and improve their ICS security posture?

The barriers to entry, for cybersecurity practitioners, to ICS remain high, given the nature of the these networks and the actuator, sensor and control equipment they contain. These

Funded by the 2020 IT Carlow President's Research Fellowship

978-1-6654-3429-4/21/$31.00 ©2021 IEEE

differ significantly from the network and equipment found on enterprise Information Technology (IT) networks. There are few opportunities for practitioners to learn how to defend ICS as such OT equipment controls critical processes, sensitive to disruption of their normal operation. Nonetheless, there is requirement for testbed solutions that can emulate, as closely as possible, real-world industrial systems giving cybersecurity practitioners the opportunity to study these environments and apply frameworks to protect them.

This project considers a holistic approach to ICS cybersecurity and seeks to identify and develop an open source collection of tools that closely emulate the major components of an ICS environment. These components include a Programmable Logic Controller (PLC), a Human Machine Interface (HMI), a data historian, a workstation for configuring PLCs and the components under their control. This environment shall form a specific case study that the project will use to identify common ICS cybersecurity vulnerabilities giving learners an opportunity to attack a controlled ICS environment and gain valuable experience of common OT cybersecurity vulnerabilities. This in-depth attack platform shall also provide a learning aid to the consequences of successful cyber-physical attacks. An additional aim will focus on healthy approaches to the reduction and the mitigation of ICS cyber risk. From this research, an ICS cybersecurity framework, based on the NIST cybersecurity framework, will emerge, detailing how a ICS cybersecurity practitioner can identify vulnerabilities in the ICS, identify potentially exposed threat vectors and both select and deploy suitable mitigations to improve their organisation's security posture. This shall include Intrusion Detection and Prevention capabilities that detect attacks and facilitate analysis of the Tactics, Techniques and Procedures (TTPs) employed to deliver them.

An emphasis will be placed on the use of open source tools in an effort to reduce barriers of entry to ICS cybersecurity. Furthermore the project will deliver a toolkit of knowledge, tools and practical insight that can be deployed to evaluate and assist a practitioner to recommend improvements to an organisations OT security posture. While the ICS environment of individual organisations will differ from the case study environment, the attack, evaluation and risk mitigation approaches are still applicable and can be applied to many different ICS contexts.

II. Objectives

The main goal of this research is the development of an testbed that cybersecurity practitioners can use to visualise and appreciate Cyber attacks on OT, as well as provide approaches based on known Industry Standards to evaluate and improve the OT security posture of an ICS.

The specific objectives of the project are:

- Identify a suitable ICS testbed that can emulate the major OT components such as PLCs, HMIs, workstations and an process within an ICS.
- Examine common ICS cybersecurity vulnerabilities by performing various cyber attacks on the testbed with a goal of exposing cyber-physical weaknesses.
- Develop a comprehensive evaluation and risk mitigation strategy, informed by the IEC 62443 and NIST SP 800-82 Industry Standards.
- Develop a toolkit based on the technical outcomes of the evaluation and risk mitigation strategy.

III. Methodology

This research work shall take the form of an ICS testbed, a simulated ICS Cyber attack and the development of a comprehensive evaluation. The project shall be divided into four focus areas in line with the project objectives.

A. Identification of a suitable ICS Testbed

Part A of this research involves the identification and development of a suitable ICS testbed based on the following criteria:

- The testbed integrates major OT components such as PLCs, HMIs, engineering workstations, firewalls, and data historians.
- The testbed incorporates known ICS protocols such as Modbus/TCP, EtherNet/IP, or Distributed Network Protocol 3 (DNP3). Much as ICS environments tend to leverage both routable protocols such as Modbus/TCP, DNP3 as well as non-routable protocols such as DeviceNet, these non-routable protocols were designed to be open conduits for data flow and not for secure communications. It is unlikely that legacy protocols will be modified to include any security protection. This research will only focus on routable protocols and will specifically focus on the popular and widely deployed Modbus/TCP.
- The testbed follows or can be be constructed following the well known ICS Purdue model [6], a defense-in-depth model that has driven the development of the IEC 62443. strategies,.
- The testbed will be built using open source tools facilitating ease of deployment and offers potential for future enhancements.
- The testbed will integrate a 3D visualisation to simulate the ICS control process. This is to allow for visualisation of the physical consequences of a successful cyber attack on an ICS.
- The entire testbed should not be too resource intensive, otherwise it would be a form of constraint to learners and researchers attempting to recreate it for learning purposes. The resource constraints set for this project are 16GB RAM, 100GB HDD, 4 CPUs @ 2.4GHz, 4GB dedicated graphics card.

The identified ICS testbed shall form a case study and the building block for the remaining parts of the project.

B. An ICS Cyber Attack

Part B of the project involves performing various ICS cyber attacks on the testbed that follow the ICS cyber kill chain, as proposed by the SysAdmin, Audit, Network and Security (SANS) Institute. This involves a *Cyber Intrusion Preparation and Execution stage* and a *ICS Attack Development and Execution stage*. Assumptions to be made at this stage include:

- The attacker has successfully penetrated through the organisation corporate zone to the ICS De-Militarised Zone (DMZ) to the control zone represented by the testbed.
- The only information the attacker has is the ability to access the DMZ and does not have any further information about the topology, components or protocols used within the control zone and must utilise common attacker TTPs to attempt access to the ICS.
- The ICS testbed shall employ default security configurations during simulated attacks. The purpose of this will demonstrate the depth to which an attacker can penetrate typical ICS systems.

The goal of the attacker is to study the ICS environment and develop attack plan options with various levels of potential impact. Roumani et al [7] assess the effectiveness of various solutions against cyber attacks ranking their effectiveness from low, medium to high, and this project derives its ranking approach from this work. The attacker must achieve this reconnaissance and subsequent execution of an attack without being detected. Impact analysis is defined as follows:

- *Low impact attacks* - to the industrial control zone that facilitate ex-filtration of sensitive information about the ICS but otherwise do not interfere with its operations.
- *Medium impact attacks* – to the ICS zone that manipulate results and the data returned from sensors and monitors in the industrial control zone and while such attacks can affect the ICS process over time they have no immediate impact. These attacks do not cause damage to equipment but may affect the ICS process outputs.
- *High impact attacks* – are those with the potential to inflict catastrophic damage within the industrial control zone and could potentially result in major property damage and even loss of life. These attacks may or may not have immediate effect but ultimately result in catastrophic damage.

The tools and steps taken to achieve each of these impact levels will be documented and inform the steps and procedures to be taken in Part C.

The MITRE Corporation, Attack Tactics, Techniques and Common Knowledge (ATT&CK) ICS framework, has gained traction within the ICS community in recent years as a tool for understanding attacker TTPs. The MITRE ATT&CK framework has come to provide a common industry language of threat actor tactics and techniques based on real-world observations. MITRE regularly conducts product evaluations to provide independent transparency on the capabilities of security products to defend against known cyber adversary attacks and the framework acts as a single repository that lists all publicly known threat behaviours. It is a curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target [8]. The attacks demonstrated in the testbed will leverage the TTPs detailed in the MITRE ATT&CK for ICS in an effort to contextualise realistic attacker threat behaviour patterns within the testbed.

C. Development of an ICS evaluation and risk mitigation strategy

Part C of this research shall focus on the development and documentation of an evaluation and risk mitigation strategy, informed by both the IEC-62443 and the NIST SP 800-82 standards, appropriate to the protection of the simulated ICS testbed. While the simulated nature of the testbed is a constraint, the evaluation of it will mirror a real-world ICS in as much as is possible. Learners will still obtain practical insight into the development of ICS cybersecurity evaluation plans. This knowledge will be valuable when applied to an organisation's industrial control zone and form part of the overall cybersecurity posture and plans of senior management. This project shall consider two specific tools at this stage.

Cyber Security Evaluation Tool (CSET) [9], provides a systematic, disciplined and repeatable approach for the evaluation of an organisation's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and IT network security practices. Practitioners can use this tool to evaluate the cybersecurity stance of their own organisations infrastructure. The tool permits users to select one or more government and industry recognised cybersecurity standards such as NIST SP 800-53, NIST SP 800-82 or IEC 62443, and then generates ICS evaluation questions that are specific to those requirements.

The Handbook for Self-Assessing Security Vulnerabilities and Risks of ICS on Department of Defence (DoD) Installations [10], was intended primarily for use by Department of Defense (DoD) installation commanders, supported by staff members as a management tool to self-assess, prioritise, and manage mission-related vulnerabilities and risks that may be exposed or created by connectivity to ICS. The guide is intentionally generic, recognising that approaches to vulnerability assessment and risk management are similar regardless of the ICS category. This handbook outlines an eight step process to assessment process: (i) Analyse Missions, (ii) Identify Assets, (iii) Determine ICS Connectivity (iv) Determine ICS Dependencies, (v) Assess Risk to Mission, (vi) Prioritise Risk Management Approaches, (vii) Implement Actions, as well as (viii) Monitor and Reassess.

This research shall draw on the strengths from both this handbook and the CSET tool as a basis for the cybersecurity evaluation on the ICS testbed as they incorporate known industry standards and are designed by credible bodies in the ICS cybersecurity space. The technical results from the evaluation, for example, recommendations for Intrusion Detection and Presentation capabilities in the system, stronger password policies, network segmentation shall then be applied to the testbed. The cyber attack mentioned in Section III: Part B above will be repeated to gauge the effect of the established security recommendations, as part of the *Monitor and Reassess* phase.

D. ICS cybersecurity Toolkit

The focus of the research in Part D will switch to the open source tools a defender can leverage when performing the technical aspects of the ICS evaluation and risk mitigation strategy. A toolkit will be developed to allow practioners carry out activities such as the identication of assets, risk assessments to business, recommended actions, monitoring and reassessments. The toolkit will incorporate the tools involved in the various stages. This toolkit will be made available to the public via institute software repositories.

IV. Technology Description

A. Industrial Control Systems

ICS is a broad umbrella term that encompasses Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control devices such as PLCs that are interconnected either via serial connections or, as is becoming more popular, deterministic Ethernet networks, using the TCP / Internet Protocol (TCP/IP) protocols, to acquire data from sensors and control mechanical actuator devices. These systems are usually very complex and include heterogeneous hardware and software components and processes being controlled or monitored, computational nodes, communication protocols, SCADA systems and controllers. Control can be fully automated or may include a human in the loop who interacts via a Human Machine Interface (HMI). The historical nature of many connections and the rapid migration towards Ethernet and TCP/IP widens the scope for a new generation of attacks exploiting newly exposed vulnerability planes.

1) The ICS Architecture: is generally defined by the Perdue Model [6]. As depicted in Figure 1, the Purdue module divides a manufacturing company or utility network, including the manufacturing control zone into six levels:

a) The Enterprise Zone: consists of Levels 4 and 5. Level 5, the upper level, is the Enterprise Network where the office staff operate from and is usually connected to the Internet via the corporate firewall. Level 4 is the Business Logistics level and forms the traditional IT portion of the network. Devices found at this level include email exchange servers, printers, inventory or asset management systems, and capacity planning systems.

b) The Demilitarised Zone: separates the Enterprise (IT) zone from the OT devices in the control zone and ideally facilitates the secure exchange of data between both zones. All traffic exchange between the two zones must pass through the DMZ.

c) The Control Zone: forms the OT portion of the network and is comprised of 4 levels as illustrated in Figure 1. The ICS components that make up this zone are briefly explained in the next section.

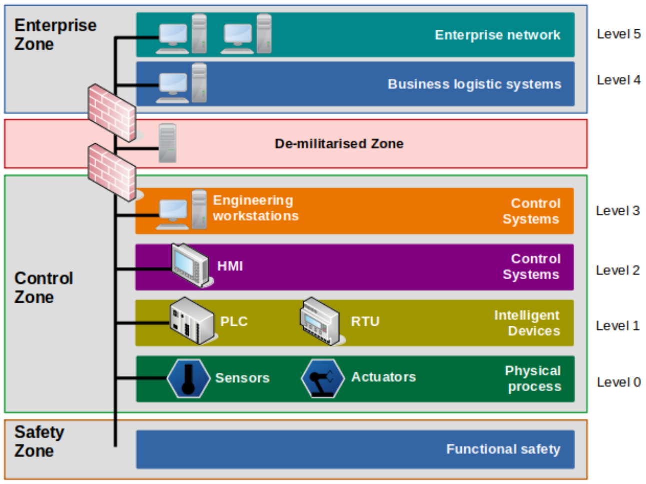

Fig. 1. ICS Purdue Model

d) The Safety Zone: includes the Safety Instrumentation Systems (SIS) that independently serve to ensure that the ICS is operating in a safe state by monitoring the status of the various control process in the plant. The SIS is designed to either, flag an unsafe operating state to the site operator, restore a process back to safe operating state, or shutdown an unsafe process until operators can to analyse it.

2) The ICS Components: consist of a wide range of devices that serve specific roles. Starting from Level 0 and working upwards, this section shall briefly list and describe the more common ICS components.

An ICS is comprised of field devices that include digital and/or analogue sensors and actuators that control physical processes. These field devices communicate with PLCs that read values from these sensors and process them via small programs. They can also issue instructions to field devices such as actuators. The PLCs are connected either directly or indirectly to HMIs that visualise the state of an industrial process and facilitate direct human interaction with the devices. The industrial control zone also comprises of engineering workstations, general-purpose computers, designated as interfaces with PLCs and field devices. Communication between the control zone and the enterprise zone is secured via firewalls in the DMZ. Nodes that need to communicate both with the enterprise and control zones also exist at this level. Such nodes include data historians that provide long-term memory for sensor reading and process states.

Other ICS components such as Master Terminal Units (MTU), Remote Terminal Units (RTU), Intelligent Electronic Devices (IED) exist. However, the above-mentioned components shall be the simulated in this project using open source tools, and their functionality shall be leveraged in the ICS testbed.

3) ICS Protocols: exist within the ICS space, many of which can be considered proprietary given the uniqueness of the ICS equipment that these protocols run on. The majority of these ICS protocols were designed to operate in an air-gapped environment. Less attention was given to the security aspects of these protocols and this design criterion is commonly referred to as *security by obscurity*. A great deal of ICS applications have relied completely on the network infrastructure for protection. This means that any valid, correctly formatted, protocol messages received by a device are trusted by default. “Trusted” in this case means that the message came from the anticipated source and the data was not altered in transit. A number of these protocols contain no security features such as authentication and encryption and this weakness can be exploited for a malicious purpose such as data ex-filtration, impersonation and service disrupting [11]. Examples of ICS protocols include Modbus/TCP, EtherNet/IP, EtherCAT, Message Queue Telemetry Transport (MMQT), DNP3, ControlNet, DeviceNet, Profibus, BBC 7200 and many others. In this project, the initial ICS protocol of focus is the Modbus protocol.

Modbus is a serial communication protocol initially published by Modicon (now Schneider Electric) in 1979 for use with its PLCs. It was later adapted for use over TCP/IP. Modbus is an application layer messaging protocol, positioned at the Process Layer of the TCP/IP model (Layer 7 of the Open Systems Interconnection (OSI) model), that provides client/server communication between devices connected on different types of buses or networks [12]. Today, Modbus is one of the most popular protocols in ICS. Numerous vendors have implemented their own versions of Modbus over TCP (Modbus/TCP). The Modbus protocol has passed through four major evolutions to date; (1) Modbus American Standard Code for Information Interchange (ASCII) which operates over serial RS-232 and RS-485 interfaces; (2) Modbus Remote Terminal Unit (RTU) which also operated over serial RS-232 and RS-485 interfaces; (2) Modbus Plus (Modbus+ or MB+) which is proprietary to Modicon and operates over twisted pair with speeds of up to 1Mb/s using token rotation and; (4) Modbus/TCP that operates over TCP/IP on port 502. Modbus messages are passed in clear text, easy to decode and require no authentication or authorisation. Communications over Modbus consist of three main stages; (1) the formulation of a request from the server to the client; (2) the execution of the actions necessary to satisfy that request and; (3) the response from the client to the server [13]. The main difference between Modbus and Modbus/TCP is that each Modbus Protocol Data Unit (PDU) contains a function code and data block. The Modbus/TCP specification also defines an Application Data Unit (ADU) that introduces a Modbus Application Protocol (MBAP) header at the front of the Modbus applicaiton PDU.

V. Results

While this project is in its early stages, research has been carried out to identify suitable ICS testbeds that will formulate into a model for an attack plane. The requirement for an open source design presents a specific challenge as there are only a handful of projects currently existing in the field. As part of the selection process, ICS Testbed models from Thiago et al [14], Genge et al [15], Maynard et al [16], Giani et al [17], David et al [18] and Bertrand et al [19] were considered. While the ICS testbed models mentioned are by no means exhaustive, they do represent some of the projects considered as part of the implementation of Part A.

David et al [18] propose the Graphical Realism Framework for Industrial Control Systems (GRFICS). Developed by researchers from Fortiphyd Logic and Georgia Institute of Technology, GRFICS [20] is a open source ICS simulation tool based on the Tennessee Eastman process [21] with a goal of bringing practical ICS security skills to a wider audience. The testbed, built using Python on GNU/Linux, is currently designed for educational purposes and offers only a single ICS process, that is to say, the Tennessee Eastman process. Fortiphyd Logic have built similar simulations, available commercially, on their training portal. The GRFICS platform is comprised of a total of five VMs, built on the Oracle VirtualBox hypervisor that perform the functions of; a PLC, a HMI, a firewall, an engineering workstation and a novel 3D visualisation of the physical process [20]. The testbed also includes a network setup to be implemented within the Oracle VirtualBox hypervisor. The PLC is implemented using OpenPLC [14], the HMI is implemented using AdvancedHMI, the firewall is implemented with pfSense [22], an engineering workstation is a standard workstation with a GNU/Linux operating system and the software to make changes to the PLC, and lastly, the 3D physical process simulation is implemented with Unity Game Engine [23]. The testbed supports the running of a number of ICS related attacks such as Man in the Middle (MitM) attacks, Command Injections, False Data Injection, PLC Reprogramming, Loading Malicious Binary Payloads, and common IT attacks such as password cracking. While the GRFICS testbed is prebuilt, the source-code is available and can be customised or modified to meet the user’s requirements.

Based upon the different testbed frameworks that were evaluated, the GRFICS framework was chosen for the following reasons; it is open source with its code available for online download, it is built upon GNU/Linux using Python making it modular and scalable, the project visualises the major components of an ICS based on a well-known and understood plant model used in control system research, and the framework contains a novel lightweight 3D visualisation of the physical process providing for a richer cyber attack experience for learners. Furthermore, the framework is still relatively new and has not been extensively utilised in ICS cybersecurity research as well as being available for customisation and modification for a richer learning experience.

This research intends to build upon the GRFICS framework in the following ways: (i) make the overall testbed lighter through the use of LinuX Containers (LXC) in lieu of virtual machines, (ii) modify the testbed during the development of stronger security controls as defined in 3: Part D above.

VI. Research and Business Benefits

ICS greatly impact our lives today, controlling almost all critical infrastructure, from electricity and water supply to transport services, and various manufacturing plants. ICS components are becoming increasingly networked and without appropriate security measures in place, malfunctions or failures caused by cyber attack or by a lack of awareness to the threats by employees can spread extremely fast. In an effort to avoid costly damage or disruption to the HA charateristics of ICS, there is a requirement for competent capacity and awareness around ICS cybersecurity. Risks to ICS typically originate from the enterprise zone and spread to the industrial control zone and can potentially enable attackers to gain remote control of ICS systems enabling them make alterations to the control logic in the plants. However, risks can also originate from the ICS and these include; the use of weak passwords, infected hardware such as USB sticks and laptops in the control zone as well as infected or unauthorised devices such as smart phones or tablets connected to the ICS Wireless LAN (WLAN). The goal is to reduce the likelyhood of cyber security incidents because successful attacks can become very expensive financially due to equipment failure, extended production losses, staff injuries up to and including loss of life. Business recovery for an incident that is preventable with sensible upfront investment in cybersecurity causes further financial cost in terms of hiring external specialists, unplanned downtimes due to system restoration after system failure, turnover losses and enivitable can inevitable damage the company's reputation.

VII. Conclusion

Recent high-profile ICS cyber attacks reinforce the requirement to build ICS cybersecurity knowledge and skills and this project recognises the challenges associated with practical hands-on ICS cybersecurity training. Through a holistic approach to the development of ICS cybersecurity, this research will involve detailing the potential steps an attacker can take when targetting OT in an ICS and propose recommendations, actions and tools that a defending organisation can employ to better protect their systems and strengthen their security posture. This research is in its initial phases and expects to produce four deliverables at its conclusion; a portable and flexible ICS testbed, a detailed cyber attack in line with the objectives set out in 4: Part B, the production of a comprehensive guide outlining the steps a defender can take to improve the security in reference to the ICS testbed, and a toolkit based on the technical steps of the evaluation and risk mitigation strategy. The tests, findings and tools employed and developed as part of this research will be made publicly available through the institute repositories allowing researchers and learners to replicate the testbed and possibly further build upon it.

References

[1] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., may 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

[2] N. Sayfayn and S. Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," 2017. [Online]. Available: http://web.mit.edu/smadnick/www/wp/2017-09.pdf

[3] R. Langner, "To Kill a Centrifuge - A Technical Analysis of what Stuxnet's Creators Tried to Achieve," The Langner Group, Arlington — Hamburg — Munich, Tech. Rep. November, 2013. [Online]. Available: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[4] D. E. Sanger, C. Krauss, and N. Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline - The New York Times," 2021. [Online]. Available: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

[5] ISA, "Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems," ISA - Global Security Alliance, Tech. Rep., jun 2020. [Online]. Available: www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

[6] L. Obregon and B. Filkins, "SANS Institute Information Security Reading Room Secure Architecture for Industrial Control Systems," Tech. Rep., 2021.

[7] M. A. Roumani, C. C. Fung, S. Rai, and H. Xie, "Value Analysis of Cyber Security Based on Attack Types," *ITMSOC Transactions on Innovation Business Engineering*, vol. 01, no. September, pp. 34–39, 2016.

[8] MITRE, "Overview - ATT&CK for ICS," mar 2020. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Overview

[9] CISA, "Assessments — CISA." [Online]. Available: https://us-cert.cisa.gov/ics/Assessments

[10] DoD, "Handbook for Self-Assessing Security Vulnerabilities and Risks for ICS on DoD Installations," no. December, 2012.

[11] G. Barbieri, M. Conti, N. O. Tippenhauer, and F. Turrin, "Sorry, Shodan is not Enough! Assessing ICS Security via IXP Network Traffic Analysis," pp. 1 – 20, 2020.

[12] Modbusorg, "MODBUS Application Protocol 1 1 b," Modbus.org, Tech. Rep., dec 2006. [Online]. Available: http://www.modbus-ida.org

[13] J. Gonzalez and M. Papa, "Passive scanning in modbus networks," in *IFIP International Federation for Information Processing*, vol. 253, 2007, pp. 175–187.

[14] T. Alves and T. Morris, "OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research," *Computers and Security*, vol. 78, pp. 364–379, sep 2018.

[15] B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera, "A cyber-physical experimentation environment for the security analysis of networked industrial control systems," *Computers and Electrical Engineering*, vol. 38, no. 5, pp. 1146–1161, 2012.

[16] K. Mclaughlin and S. Sezer, "An Open Framework for Deploying Experimental SCADA Testbed Networks," *SCADA Cyber Security Research*, pp. 92–101, 2018. [Online]. Available: https://doi.org/10.14236/ewic/ICS2018.11

[17] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley, "A testbed for secure and robust SCADA systems," *ACM SIGBED Review*, vol. 5, no. 2, pp. 1–4, jul 2008.

[18] D. Formby, M. Rad, and R. Beyah, "Lowering the Barriers to Industrial Control System Security with GRFICS," Georgia Institute of Technology and Fortiphyd Logic, Baltimore, MD, Tech. Rep., 2018. [Online]. Available: https://www.usenix.org/conference/ase18/presentation/formby

[19] M. Bertrand and T. Olivier, "Dissertation - Simulating Industrial Control Systems Using Mininet," 2017. [Online]. Available: https://dial.uclouvain.be/memoire/ucl/en/object/thesis%3A14706/datastream/PDF_01/view

[20] D. Formby, "GitHub - djformby/GRFICS: Graphical Realism Framework for Industrial Control Simulations," 2018. [Online]. Available: https://github.com/djformby/GRFICS

[21] T. J. McAvov, "BASE CONTROL FOR THE TENNESSEE EASTMAN PROBLEM," *Computers Chem Engng*, vol. 18, no. 5, pp. 383–413, 1994.

[22] P. Kamal, "Intrusion Detection using pfSense - Open Source FREEBSD Firewall," Tech. Rep., 2014. [Online]. Available: https://www.academia.edu/17560234/INTRUSION_DETECTION_USING_PFSENSE_OPEN_SOURCE_FREEBSD_FIREWALL

[23] U. Technologies, "Unity Real-Time Development Platform — 3D, 2D VR AR Engine." [Online]. Available: https://unity.com/