http://dx.doi.org/10.14236/ewic/icscsr19.12

ICS Interaction Testbed: A Platform for Cyber-Physical Security Research

Henry Hui, Peter Maynard, Kieran McLaughlin
Centre for Secure Information Technologies (CSIT)
Queen's University Belfast
{hhui01,pmaynard01,kieran.mclaughin}@qub.ac.uk

To perform cyber security research on cyber-physical systems, the involvement of real physical systems and components is an obvious benefit. However, in the area of industrial control systems, limited accessibility to operational systems for experimentation motivates a growing trend for researchers to develop testbeds for security research. Comprehensive testbeds require a significant investment of resources to develop, which may not be the most efficient or feasible option for researchers. This work documents the physical and network architecture of a small but diverse testbed, comprising multiple PLC devices and physical processes. The contribution of this work is to facilitate research that requires capturing of the interactions between cyber systems and physical processes, and the effect of cyber-attacks on physical components and processes in real-time. A classification approach to better understand and communicate how testbeds are utilised in the research community is also proposed and provides context for this work.

Keywords: Cyber security, Cyber-Physical systems, ICS, PLC, SCADA, Testbed

1. INTRODUCTION

In Industrial Control System (ICS) research, to obtain data and observe the behaviour of a cyber-physical system, the involvement of the actual physical component in the research process serves a huge benefit, e.g. more realistic data can be generated and testing can be done directly on an actual component. However, ICS involves machinery or physical processes and it is generally difficult for the research community to gain access to a real world ICS in order to perform cyber security experiments, to test solutions and develop prototype systems. This is due to constraints like access to remote locations, hazardous environment, and the possibility of affecting the availability of the system. Testbeds are a traditional approach on resolving the problem. However, while complex testbeds like those presented by (Mathur & Tippenhauer 2016) and (Cruz et al. 2016) can provide excellent data to replicate a real industrial process, these testbeds require significant investment into resources and extensive domain knowledge, which is often a significant challenge. For research that has a specific purpose but not necessarily dependent on faithful representation of a specific ICS process these testbeds can be very cost inefficient. On the other hand, although benchtop and virtualised testbeds, (Koganti et al. 2017; Anon n.d.; Gao et al. 2013), provide an easier way to investigate novel attacks or to generate experimental data, the data can be monotonous and the scope offered by such a testbed can be limited. Such testbeds also lack interconnectivity of physical components. Moreover, researchers with an IT background can find it difficult to develop an ICS testbed without extensive knowledge of various ICS components and physical processes. This paper aims to address the above problems by documenting the design and construction of a testbed that involves a system with diverse, interconnected and interdependent physical processes, which are controlled by a number of programmable logic controllers (PLC). The aim is to limit the physical size of the testbed to an ordinary server cabinet. The paper will also describes the IT network supporting the operation of the physical processes, which is implemented based on recommended industrial best-practice standards. Overall, the presented testbed aims to be diverse, with reasonably complex data being generated, when compared to a typical benchtop testbed. This paper is structured as follows: Section 2 describes the physical and network architecture of the testbed. Section 3 analyses the related work, and consequently proposes a new way to classify ICS testbeds to better understand their aims and capabilities, particularly for cyber security research.

2. AN ICS INTERACTION TESTBED

2.1 Motivation

This testbed is designed to provide realistic network interaction and to facilitate network data collection with a specific research purpose of investigating the effect of cyber-attacks on physical processes. (Reed & Gonzalez 2012; Paul-Pena et al. 2017; Aubel et al. 2017) has demonstrated the possibility of exploiting physical properties like power consumption, EM emission and timing characteristics of a PLC. This testbed will facilitate research in similar areas on top of incorporating the interdependence of different processes and interference from the physical environment. In other words, the purpose for this testbed is to create a platform to explore methods to take advantage of these physical proprieties on the PLCs and processes to create cyber detection and defence mechanisms. However, this further work is considered out of scope for the purposes of the presented paper. The remainder of Section 2 consists of two parts, the physical architecture and the network architecture.

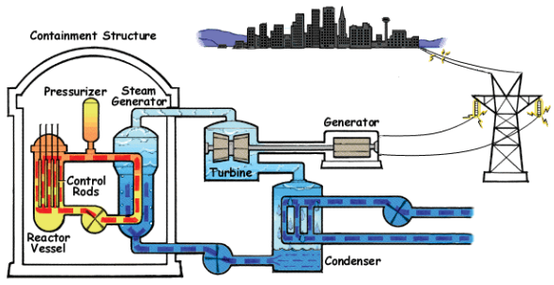

Figure 1. *Nuclear reactor (© Creative Commons)*

2.2 Physical system architecture

The testbed was built referencing a nuclear reactor. Figure 1 depicted the overall process of a reactor (United States Nuclear Regulatory Commission 2017). In summary, a reactor has fuel rods inside the reactor vessel which create heat that heats up water. The water turns into steam which is directed to the turbine. The turbine drives the generator which generates electricity. The unused steam is exhausted to the condenser and is turned into water and pumped back to the main vessel. For the

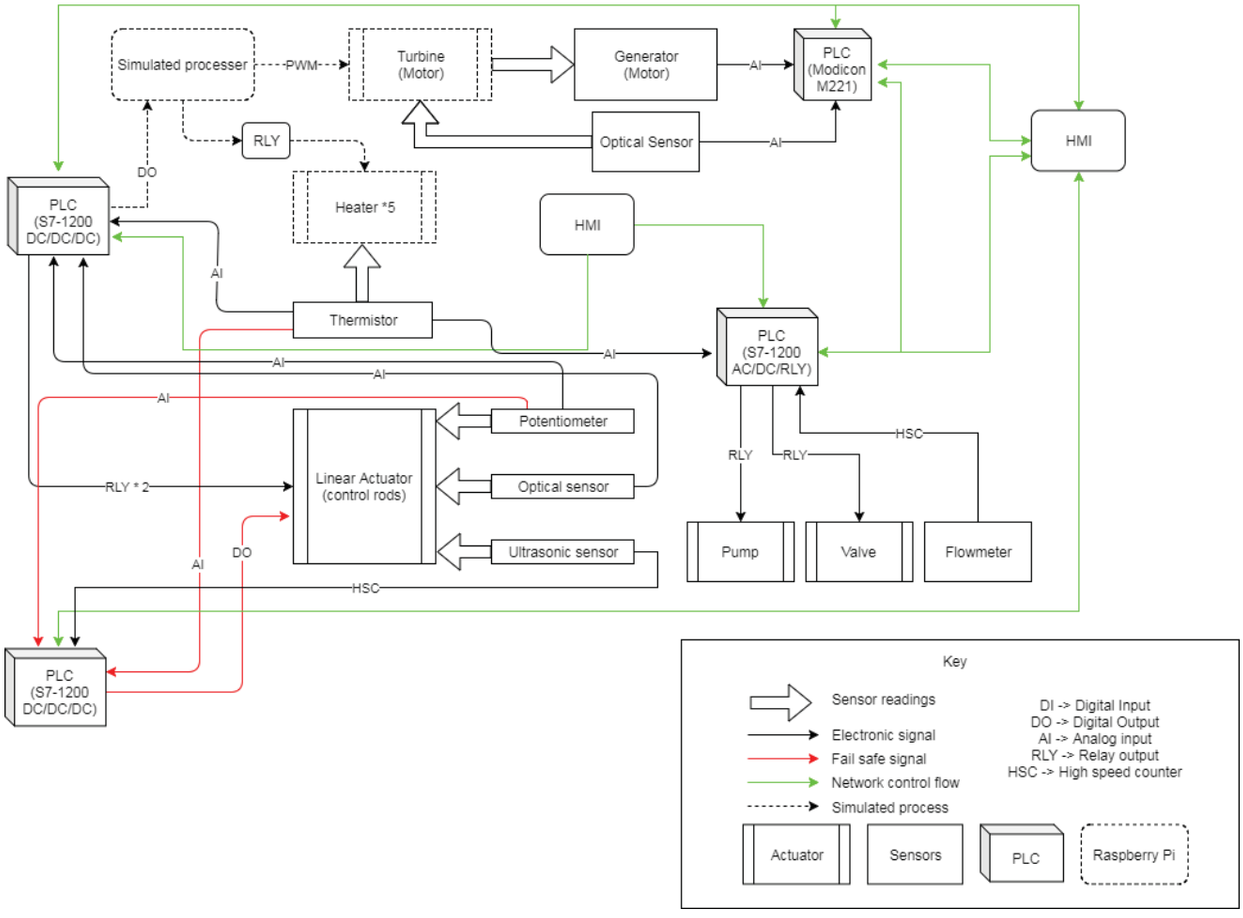

Figure 2. *High level process interaction diagram*

testbed, four main sub-processes are chosen to represent a reactor: the main tank processes (control rods), a heat exchanger, a fail-safe process and a generator process. Figure 2 shows the overall system architecture and components in the testbed. The four main sub-processes are controlled by four different PLCs, which take in various sensor data, e.g. distance, temperature, flowrate, etc. The PLCs used include three Siemens S7-1200 PLCs and a Schinder Modicon M221 PLC. The Siemens PLCs are programmed and managed in Structured Control Language (SCL) using TIA Portal while the Schinder PLC is in Ladder Logic using SoMachine Basic. The Siemens KTP-400 Human Machine Interface (HMI) is used to control the processes. A Raspberry Pi is used for additional simulated processes, in particular the heating process and the turbine, which represent the heat generating fuel rods and the steam-driven rotating turbine. For practical reasons, these two processes are not reproducible, but are implemented by alternative methods to emulate similar behaviours that can produce appropriate stimuli and measurements via sensors in the testbed. The interaction of these simulated processes will be described along with the four main physical sub-processes. The interactions between sub-processes are enabled by IP network communication or physical interactions, via direct electronic connections. The idea for process interactions in a testbed is so that when one data point changes in a process (either physical or virtual), some other data points in other processes will change accordingly. If testbed fidelity (i.e. how representative the data generated by the testbed is, compared to data generated by ICS processes in production environments) is not the prime concern of the testbed, implementing process interaction can be easily planned and implemented on top of existing processes. In this testbed, the four sub-processes interact with each other to form the overall process.

2.2.1 Main reactor sub-process
The control of the main reactor (vessel) process is done by the Siemens S7-1211C PLC. The PLC takes in temperature data from the thermistor in the main tank and determines whether to adjust the position of the control rods, which is represented by a linear actuator. The control rods move up or down to control the rate of "reaction" from the fuel rod. The movement of the control rod is monitored by the PLC using an optical sensor and potentiometer. This control rod information will also be fed into the simulated heater process controlled by a Raspberry Pi via a digital signal from the PLC. The Pi will determine the signal received and a relay is in place to switch on or off a heater, effectively controlling the rate of heating. This physically emulates the real behaviour of control rod positioning in a real rector core.

2.2.2 Heat exchanger sub-process
The heat exchanger process is controlled by a S7 PLC. This process takes in the same temperature measurements as the main reactor process and engage the pump and open the valve for water to flow in water pipes that pass through the main tank process. The operator can also manually engage this process via the local HMI.

2.2.3 Fail-safe sub-process
The overall process is constantly monitored by a fail-safe process that is control by a S7 PLC. The fail-safe process can be triggered manually by the press of a physical button or from the HMI, or by the PLC automatically. The automatic process takes in sensor measurements from a thermistor and ultrasonic sensor, and data received from other process to determine whether the process is in a "safe" state, for example monitoring whether the main tank temperature is too high or water level is abnormal. Once certain readings pass a safe threshold, a digital signal is sent to an electric circuit which will drive the control rods down regardless of the state of the main tank process. The position of the control rods is monitored using a potentiometer. The simulated heating process, which takes in the position of the control rods, will be shut down correspondingly.

2.2.4 Generator sub-process
The generator process is monitored by a Schneider M221 PLC which is attached to the turbine-

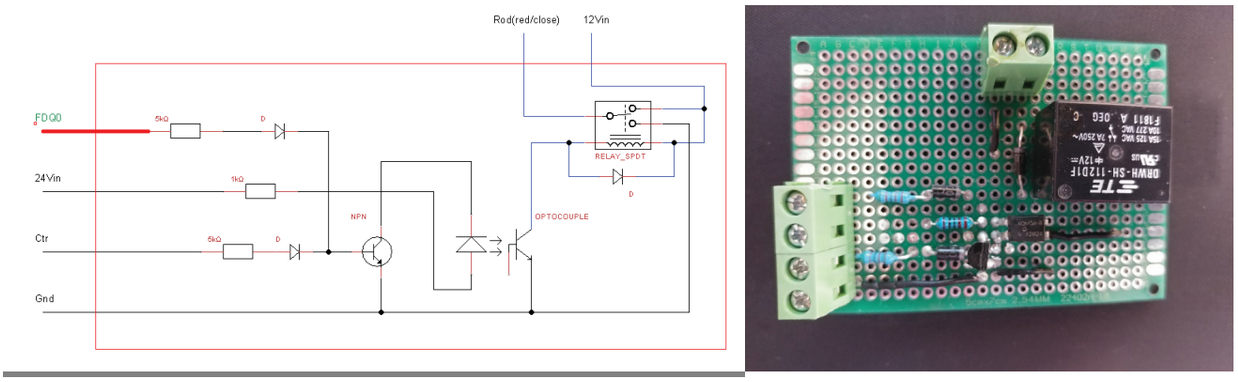

Figure 3. *Example circuit design and PCB*

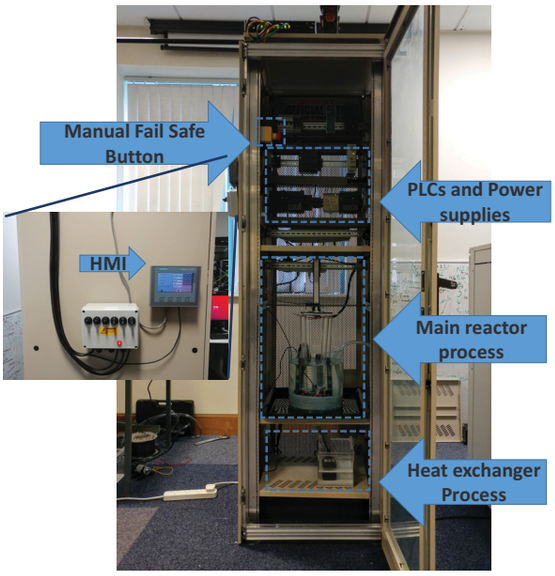

Figure 4. *Physical construction of the testbed*

simulated process. The turbine-simulated process takes in the temperature of the main tank and adjusts the rotational speed of the motor that is attached to the turbine. The turbine is attached to a generator which takes in the rotational work done by the simulated process and transforms it into a measurable voltage output. The PLC monitors the voltage output and adjust the "rate of reaction" in the main reactor as appropriate to maintain a stable output.

The construction of the testbed also involves the design of electronic circuits that sit between a PLC and an actuator. Figure 3 is an example of this circuit and the components being soldered on the PCB. This circuit turns the digital signal sent by a PLC to a suitable voltage that will turn on or off a relay, which control the linear actuator that act as the control rods. Figure 4 shows the physical construction of the testbed.

At present, PLCs from two different vendors are installed in the testbed and the industrial protocols used include S7 protocol, Profinet, and a custom protocol based on TCP. Future developments will include two additional processes to represent power transmission and an expansion of the failsafe process. The aim will be to provide further functional complexity and diversity of devices.

2.3 Network architecture

The overall power plant process is supported by an IT communications infrastructure, providing

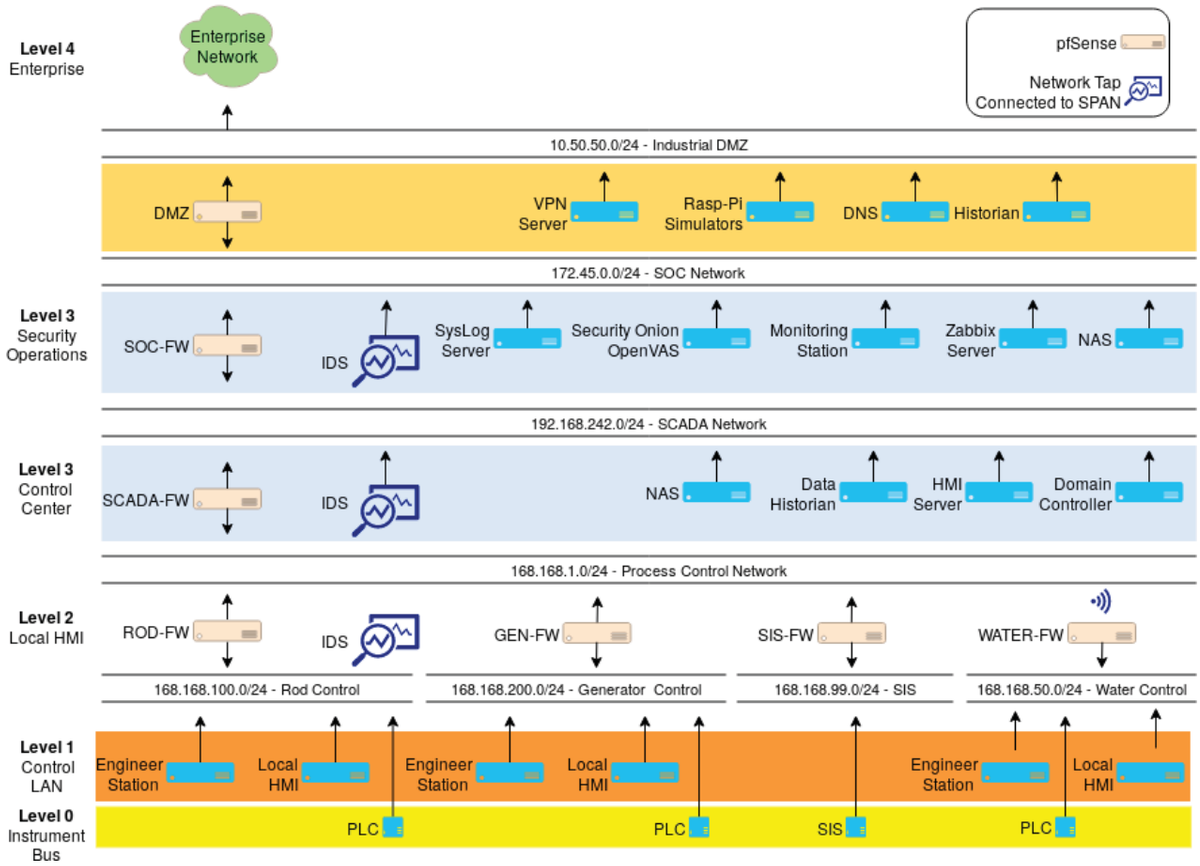

Figure 5. *Network architecture*

communication across interconnected devices and sub-systems. The network architecture is designed following industry standards such as (Ross 2013; Byres et al. 2005; ISA 2018). First the network is assigned a number of levels that align with the Purdue Model (ISA 2018), the levels are: Level 4, Business Logistics systems; Level 3, Manufacturing operation systems; Level 2, Control Systems; Level 1, Intelligent devices; Level 0, the physical process. The architecture is segmented with the use of dedicated firewalls to prevent unauthorised movement within the network, as proposed in (Stouffer et al. 2011). The actual testbed is built using a combination of physical and virtual switches, routers, and firewalls.

2.3.1 Network Architecture
Figure 5. describes the testbed networking architecture. Open vSwitch is used to virtualise the separate network switches at OSI Layer 2. While, pfSense is used for OSI Layer 3 routing and acting as a router and firewall. These are freely available and can work within any virtualisation hypervisor. The testbed uses two CISCO WS-C3750X-24 switches and a Linksys SRW2008 switch, to physically connect the hardware. The testbed does not rely on proprietary protocols or tools that are not freely available, this allows the basic architecture to be replicated. Following guidelines set out by NIST, segmented networks are implemented based on the devices and functions they provide. The lower down the Purdue levels you go, there are an increased number of firewalls with stringent polices in place to enforce the correct flow of data between devices and network segments in order to prevent lateral movement within the enclaves.

2.3.2 DMZ and Enterprise network
The network architecture employs a paired firewall with DMZ for shared enterprise and OT systems. In this specific instance, the DMZ is used to locate the simulated processes running on the Raspberry Pi, since the communications between the RPI and other devices should not interfere with the testbed. The DMZ houses other typical systems, such as an aggregated data historian, DNS, and VPN server. These services provided access for the enterprise network to allow data from within the OT network, while restricting access to the OT network.

2.3.3 OT Security Operation Centre
The testbed uses a dedicated OT security operation centre (SOC). While there is a debate (Viorel 2019) whether there should be a dedicated OT SOC and an IT SOC, or if they should be a single centre, there are a number of differences between the two which requires the need of a separate OT SOC. It should be made clear that the two level 3 network segments are not hierarchical, and they both have direct access to the DMZ. The OT SOC consists of a number of security monitoring tools, log storage and asset management. Not included in the diagram, but advisable, is a restricted network for analysing malware samples.

2.3.4 Control Centre
The second network at level 3 is the control centre, which contains the primary data historians, HMI and OT domain controller. This would be located at a central location, and could be duplicated at another location to provide additional resilience to natural disasters. All user accounts are managed in this network, and access is logged to the OT SOC.

2.3.5 Local process control enclave
The process control enclave, is further segmented into four networks: Rod Control; Generator Control; Water Control; and SIS. The process control network may communicate with the smaller control networks over various mediums, from local Ethernet/fibre, to wireless and even public switched VPN links. In the testbed case, the water control network is connected using wireless (WiFi) to represent a remote destination. Although this would not be the case for a real nuclear plant, it adds a further experimentally interesting dimension to the testbed.

2.3.6 Firewalls, IDS and Logging
Each network segment consists of a number of different inbound and outbound firewall rules tailored to the relevant network involved. Each network also contains a network IDS to monitor traffic at the router connection points. The logs and additional packet captures are stored locally for a limited period, and are also transmitted to the OT SOC. All devices that support the use of syslog or other logging services are enabled to do so, and forward their logs to the syslog server (†GrayLog), where failed logins and operation actions may be analysed and alerted upon.

2.4. Overall Capability

The four sub-processes in the simulated plant are constantly interacting with each other based on monitoring and acting upon the status of the main water tank, whereby a key data point in the overall process is the temperature of the main tank. Any action performed by a single sub-process will lead to disturbances and physical changes to another process. The generation and collection of related physical measurements and associated digital data, via custom electronic circuits, is a key beneficial attribute of the testbed for enabling research at a cyber-physical systems level. The comprehensive and realistic supporting network infrastructure, described above, facilitates this physical information to be captured alongside cyber-related data, such as alerts, logs, and so on, and provides a platform that will be used in future

† GrayLog: https://www.graylog.org/

research to investigate improved correlation of cyber-physical data under cyber-attack scenarios.

3. RELATED WORK

With the purpose and functionality of the testbed having been presented, the following section will analyse and discuss how this work fits alongside related research where ICS testbeds have been described in the literature. Developing meaningful ICS testbeds has been an important focus for cyber security research in recent years.

A virtualised framework, (Reaves & Morris 2012), that utilises virtualised devices and processes that allows the use of physical devices has been proposed. A similar idea (Gao et al. 2013) instead focuses on the use of physical PLCs and demonstrates how the PLCs can be interfaced with an emulated network and a Matlab simulated process. (Xie et al. 2018) has presented a testbed that utilised virtual devices and a well-known virtual chemical process, the Tennessee-Eastman process in the testbed. (Alves et al. 2018) has presented a few virtualised processes for different applications, one of which includes the use of virtualised PLCs. These PLCs control different virtualised processes that interacts with each other. A high proportion of the testbeds that use a virtualisation approach either implemented custom virtualised processes and devices, or utilised open source components. Although no doubt virtualisation has huge benefits to the construction of a testbed, implementation on either virtualised processes or devices requires a significant developmental overhead. However, even if such implementations are feasible, data fidelity needs to be carefully considered, especially the potential to generate monotonous data that may lack the diversity and complexity required for meaningful research experiments. Moreover, if the planned research is going to be component or process dependent, e.g. vulnerability analysis of devices and data fidelity of physical properties, a testbed such as that proposed by the current work has an advantage.

Of the publications that documented some of the comprehensive testbed, (Mathur & Tippenhauer 2016) provides a replica of a 6-stages water treatment processes; (Cruz et al. 2016) has presented a testbed that was designed by an Electric Company for research development and validation; and (Green et al. 2017) is built around a set of industrial components and supported by an extensive network. These publications provided some information that research community can consider while creating an extensive ICS testbed. However, although the testbeds presented provide a high level of fidelity, the complexity and the requirement of extensive domain knowledge and resources sets a very high bar to recreate such a testbed.

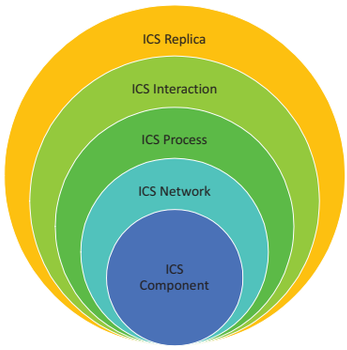

Figure 6. *Testbed by layer*

A good overview of existing testbeds is provided in a number of papers (Mclaughlin et al. 2018; Qassim et al. 2017; Holm et al. 2015) . However, during the process of studying various testbeds, the authors noted a lack of a common set of terms or framework to classify a given testbed, or to communicate its role and the research work that it facilitates. A new way of communicating an ICS testbed is therefore proposed in next section, after a brief discussion of current testbed classifications.

3.1 Current classification of testbeds

Currently testbeds are generally classified as a Physical, Virtual or Hybrid testbed. However, even the most comprehensive physical testbeds (Cruz et al. 2016; Green et al. 2017), involve the use of virtualised elements. On the other hand, there are obvious benefits to include a PLC between a simulated process and the networks. In other words, there is a tendency for ICS testbeds to adopt a hybrid approach in the research community. Therefore, this is no longer a sufficient classification approach. Alternatively, it is proposed that testbeds may be described via different layers that identify how a testbed can be utilised, and its purpose or experimental scope. The aim of this classification approach is to communicate the research more efficiently and provide researchers and the audiences of the presented research an indication of the scope and limit of a testbed

Central to this classification is to identify and describe the functional elements involved. Figure 6 shows how each layer of elements contributes to extending the complexity and fidelity of a testbed:

- **ICS Component**: Individual ICS components
- **ICS Network**: Network of components;
- **ICS Process**: Process or processes control by component(s) that are connected by a network

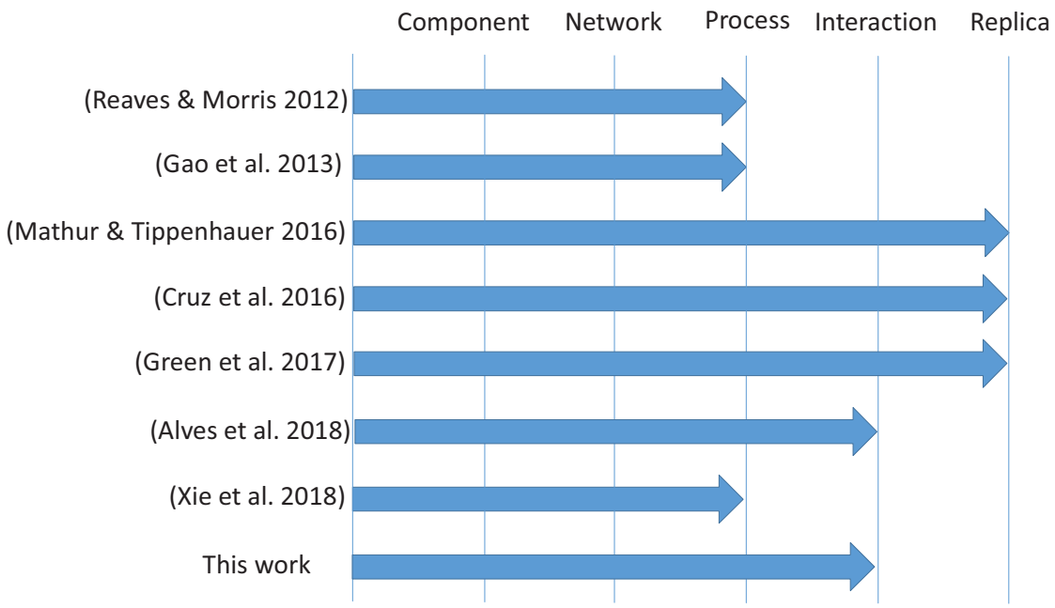

Figure 7: *Classification of current testbeds*

- **ICS Interaction**: Processes that interact with each other
- **ICS Replica**: Processes that interact as a real system, or a faithful replica.

It should be noted that each layer could be virtualised individually. When describing how a testbed is being utilised, the purpose can also be narrowed to focus on a specific layer, or spread across multiple layers. For example, "Network centric" testbed is used for testing network intrusion detection systems, regardless of the ICS components in place, while a "Network" testbed facilitates the testing of a vulnerability on an industrial device via the network. Similarly, a "Component-Process" testbed may be used to investigate the vulnerabilities of an ICS device and how this discovery can be exploited to affect a physical/virtualised processes in the testbed, regardless of the network architecture. Figure 7. provides a classification of the testbed proposed in this work and the aforementioned testbeds in the related work.

4. CONCLUSION

Data for physical properties of devices and processes are always being generated in the background of ICS processes but are usually not being utilised for cyber security. This paper presented a testbed that is designed with specific emphasis on capturing the interactions between physical processes and the physical properties of ICS components and processes. The data captured from the testbed will be utilised to design a detection system that pick up anomaly that might be caused by a cyber attack. The physical and network architecture of the testbed is presented and serves as an example of how such a testbed can be created. A simple classification of the ICS testbed is also proposed to enable the efficient communication of how various testbeds in the research community can be utilised, and the functionality that they offer for cyber security researches. The presented testbed fits within this classification model as an ICS "Interaction" testbed which is intended to support future planned research on investigating how the cyber-physical data, which is generated from the interacting and interdependent cyber and physical processes, can be utilised to improve cyber security detection and mitigation approaches for ICS.

5. REFERENCES

Anon, SIMATIC Controllers System Overview - PLCs - Siemens. Available at: http://w3.siemens.com/mcms/programmable-logic-controller/en/system-overview/Pages/Default.aspx [Accessed April 25, 2017].

Aubel, P. Van et al., 2017. Side-channel based intrusion detection for industrial control systems.

Byres, E., Karsch, J. & Carter, J., 2005. Firewall deployment for scada and process control networks. *Centre for Protection of National Infrastructure, Government Digital Service*.

Cruz, T. et al., 2016. A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems. *Ieee Transactions on Industrial Informatics*, 12(6), pp.2236–2246.

Gao, H. et al., 2013. The design of ics testbed based on emulation, physical, and simulation (eps-ics testbed). In *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. pp. 420–423.

Green, B. et al., 2017. Pains, gains and PLCs: ten lessons from building an industrial control systems testbed for security research. In *10th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET}17)*.

Holm, H. et al., 2015. A survey of industrial control system testbeds. In *Nordic Conference on Secure IT Systems*. pp. 11–26.

ISA, I., 2018. Industrial automation and control systems security.

Koganti, V.S. et al., 2017. A virtual testbed for security management of industrial control systems. In *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*. pp. 85–90.

Mathur, A.P. & Tippenhauer, N.O., 2016. SWaT: a water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. pp. 31–36.

Mclaughlin, B.S. et al., 2018. The Cybersecurity Landscape in Industrial Control Systems. , 104(5), pp.1039–1057.

Paul-Pena, D. et al., 2017. Process-aware side channel monitoring for embedded control system security. In *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. pp. 1–6.

Qassim, Q. et al., 2017. A survey of scada testbed implementation approaches. *Indian Journal of Science and Technology*, 10(26).

Reaves, B. & Morris, T., 2012. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11(4), pp.215–229.

Reed, J.H. & Gonzalez, C.R.A., 2012. Enhancing Smart Grid cyber security using power fingerprinting: Integrity assessment and intrusion detection. In *2012 Future of Instrumentation International Workshop (FIIW) Proceedings*. pp. 1–3.

Ross, R.S., 2013. Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800(53), pp.8–13.

Stouffer, K., Falco, J. & Scarfone, K., 2011. Guide to industrial control systems (ICS) security. *NIST special publication*, 800(82), p.16.

United States Nuclear Regulatory Commission, 2017. The Pressurized Water Reactor. Available at: https://www.nrc.gov/reading-rm/basic-ref/students/animated-pwr.html.

Viorel, P., 2019. Two sides of IT vs. OT Security and ICS Security Operations. *TechaPeek*. Available at: https://www.techapeek.com/2019/05/08/two-sides-of-it-vs-ot-security-and-ics-security-operations/.

Xie, Y. et al., 2018. VTET: A Virtual Industrial Control System Testbed for Cyber Security Research. In *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*. pp. 1–7.