Testbed Diversity as a Fundamental Principle for Effective ICS Security Research

Benjamin Green, Sylvain Frey, Awais Rashid, David Hutchison
Security Lancaster Research Centre
Lancaster University
United Kingdom
{b.green2, s.frey, a.rashid, d.hutchison}@lancaster.ac.uk

ABSTRACT

The implementation of diversity in testbeds is essential to understanding and improving the security and resilience of Industrial Control Systems (ICS). Employing a wide spectrum of equipment, diverse networks, and business processes, as deployed in real-life infrastructures, is particularly difficult in experimental conditions. However, this level of diversity is key from a security perspective, as attackers can exploit system particularities and process intricacies to their advantage. This paper presents an ICS testbed with specific focus on infrastructure diversity, and end-to-end business process replication. These qualities are illustrated through a case study mapping data flow/processing, user interactions, and two example attack scenarios.

Categories and Subject Descriptors

C.3 [**Special Purpose and Application-Based Systems**]: industrial control systems

General Terms

Security, Human Factors, Experimentation, Design

Keywords

Industrial Control System; ICS; Supervisory Control and Data Acquisition; SCADA; Testbed; Security; Resilience

1. INTRODUCTION

The use of testbeds is essential to understanding and improving the security and resilience of Industrial Control Systems (ICS). The wide spectrum of equipment, diverse networks, and business processes, deployed in real-world infrastructures is particularly difficult to replicate in experimental conditions. ICS broadly spans across three fundamentally different *zones*, with a variety of equipment, skill-sets, and role groups, each summarised here.

- The *manufacturing zone* is where physical process operations take place, prominently built around devices and systems broadly categorised as operational technology (OT), used for monitoring, controlling, and automating process decisions through the implementation of sensors, actuators, and controllers. Observation and manual control of physical processes though human machine interfaces (HMI), engineering workstations, remote terminal units (RTU), data historians, and control servers, is also possible within this zone.

- The *demilitarised zone* forms a boundary between manufacturing zones and enterprise zones, presenting an interface by which data can be captured and stored for further processing. Performing critical functions, devices residing in this zone lean towards conventional information technology (IT), yet have the ability to interact with OT, facilitating remote alarm management, historical data collection, remote desktop access, etc.

- The *enterprise zone* hosts conventional IT devices and systems, further utilising data collected through the demilitarised zone to perform global supervision and long-term strategic planning for the entire infrastructure.

For a more granular view of end-to-end ICS environments, see the Purdue model (figure 1).

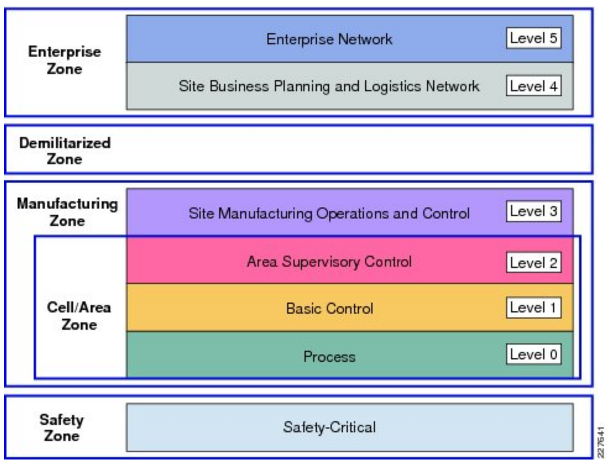

Figure 1: The Purdue Model [2]

The level of diversity in ICS environments is important from a security perspective, as attackers are able to focus their attacks to disrupt operational objects derived from varying ICS zones. First, consider a “Fuzzing” attack exploiting a controller vulnerability; secondly, a controller “Memory Manipulation”. The two attacks vary in their outcome. The first could be considered a disruption attack, designed to cause an undesired impact on physical process operations. The second manipulates data used for a variety of objectives, opening several possible end results (reduced efficiency, confusion, disruption, etc.), impacting local and/or remote level (demilitarised zone and enterprise zone) visibility and control of operational processes, and data.

The *modus operandi* of the aforementioned attacks is also significantly different: a “Fuzzing” attack is relatively simple to carry out, and the process (target identification followed by target disruption) can be automatised; “Memory Manipulation” attacks requires an advanced understanding of the target network (data sources and destinations, critical data processing points, redundancy, etc.), and dedicated expertise to intercept and alter a specific data flow.

This paper presents an ICS testbed [5], with a focus on infrastructure diversity, including end-to-end business process replication (section 3). The testbed replicates not only infrastructure found within each zone (field sites, data-centres, and corporate sites), but for each zone proposes alternative forms of equipment, vendors, and protocols. These qualities are illustrated through the introduction of a case study, and two example attack scenarios (section 4). Section 5 investigates potential future work, notably related to the incoming Internet of Things (IoT) evolution.

2. RELATED WORK

Several testbeds have been proposed in the literature for power plants [7], and micro and macro grids [6, 3], based on combinations of real, emulated, and simulated components. Testbeds focusing on water treatment and distribution are less common than power grid oriented testbeds: [1] relies on simulation and virtualisation to reproduce large water infrastructures, favouring the scale and breadth of the testbed over the realism of deploying actual physical components. Some testbeds cover different sectors (power grid, water, gas): [8] is a simulation tool for building various SCADA infrastructures at scale; [9] proposes a combination of physical and simulated components.

The testbeds referenced here are spanning all zones of the Purdue reference model, although they do not always refer to this model explicitly. A variety of attacks has been studied in these environments, including Denial of Service (DoS, either by flooding or specific malicious packets), DNS and routing tables poisoning, traffic sniffing and Man In The Middle (MITM), and malware injections. However, the socio-technical particularities of each zone, and the propagation of attack effects across different environments, represent blind spots in these studies, as they generally focus on specific attacks and/or scenarios.

3. TESTBED ARCHITECTURE

As detailed in [5] the testbed was originally designed with three core factors in mind, flexibility, credibility, and reliability. Since its original conception in 2013, major works have been undertaken to further levels of diversity, and therefore credibility when compared with real-world scenarios. Figure 2 presents the diversity of each zone. Below we describe each zone in relation to the available devices and protocols.

Manufacturing zone: The physical process is built around a set of operational assets (tanks, pipes, pumps, valves, etc.), sensors, and actuators, supporting hard wired electrical signalling, such as 4-20mA, and wireless protocol technologies, such as WirelessHART. The monitoring, control, and automation of physical processes are achieved through a set of sensors, controllers, human machine interfaces (HMI), and network devices. These support the following protocols: S7 over MPI, S7 over Ethernet, DNP3, ModbusTCP, Profibus, Profinet, WirelessHART, OPC, RDP, HTTP, HTTPS, FTP, SFTP, TFTP, SSH, and Telnet.

Demilitarised zone: This zone contains a set of communication devices and servers supporting the handling of all IP based protocols discussed within the manufacturing zone.

Enterprise zone: This zone contains a number of workstations and servers supporting the handling of all IP based protocols discussed within the manufacturing zone.

4. ATTACK SCENARIOS

Figure 3 and table 1 are the output of a case study with a European utility company. Figure 3 provides a greater level of granularity on real-world data flow and processing, and has been replicated within the testbed environment. Table 1 provides a view of some critical role groups, spread across each ICS level [2].

Colour coded to provide basic guidance on the level in which each device resides, figure 3 can be mapped against role groups from table 1. As a risk assessment tool, the creation of data flow/process models, with accompanying role groups, provides a clear end-to-end view of the system.

Figure 3, highlights the complexity of data flow/processing. Operating at an abstracted level, we see the delegation of devices to meet the requirements of specific role groups. However, perhaps of greater interest is the lower-level view presented by the programmable logic controller (PLC). Here we see areas of PLC resources separated and shared based on their functionality. Take ”DB2.DBD1” as an example, this is a datablock address, an area of memory allocated for a specific function, in this case storing an input value. It is shared between three system levels (1,2, and 3), used as an input for Historian and RTU data collection.

Where the following sub sections introduce two attack scenarios, developed and applied within the testbed environment, identification of data processing points and user interaction, plays a critical part in the holistic understanding of potential impact.

4.1 Fuzzing

”Fuzzing”, is considered to be a blackbox security evaluation technique. Applied to discover software vulnerabilities, Fuzzing randomly mutates well-formed inputs, testing a pro-

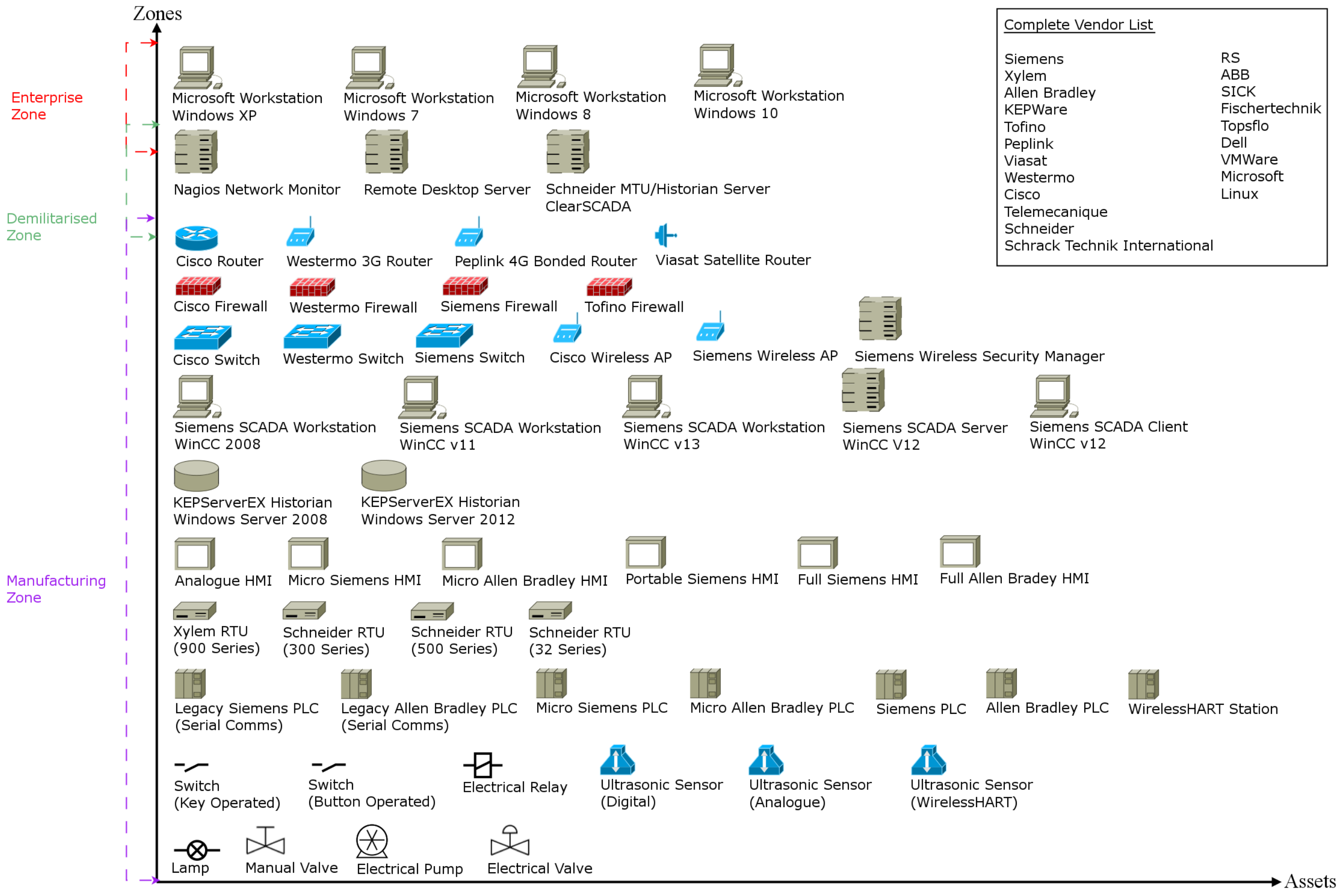

Figure 2: High-level architecture of the testbed

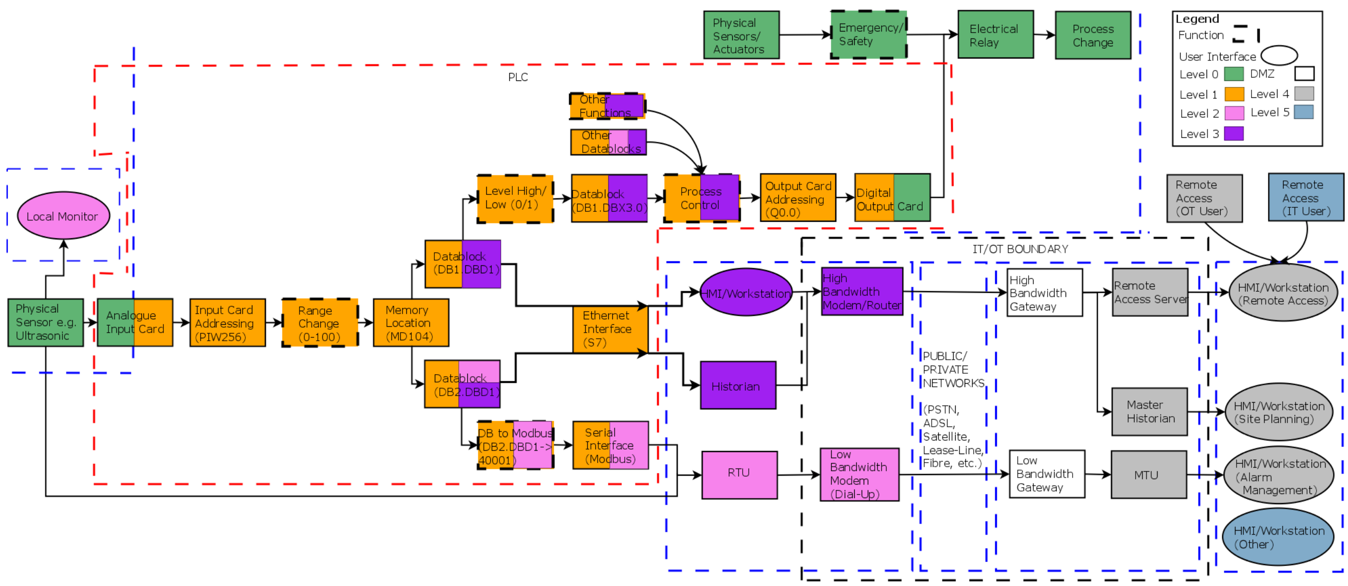

Figure 3: Data flow and processing

grams resilience upon their receipt [4]. Existing works discuss the application of fuzzing to ICS environments [10].

It is possible to conceive a vast array of opportunities where such testing/attacks could be conducted within the testbed

User Roles	ICS Level
Process Control Operators	2,3,4,5
Local Process Managers	2,3,4,5
Regional Process Managers	3,4,5
Regulatory Monitors/Testers	2,3,4,5
Performance Analysts	4,5
3rd Party Contractors	0,1,2,3,DMZ,4,5
Alarm Management Cetre Operator	4,5
Health and Safety Officers	4,5
Home Workers	3,4,5
Support/Maintenance Roles	ICS Level
Electrical Engineers	0,1,2,5
Mechanical Engineers	0,5
Control System Engineers	0,1,2,3,4
Instrumentation Engineers	0,1,2,5
Telemetry Engineers	0,1,2,3,DMZ,4,5
Communications Engineers	3,DMZ,4,5
Information Technology Engineers	DMZ,4,5
3rd Party Contractors	0,1,2,3,DMZ,4,5
Home Workers	3,4,5

Table 1: ICS roles and associated system levels

(section 3). Using figure 3, critical data processing points can be identified as described above. A number of which, where disrupted, could create a cascading effect up the data flow. For example, we applied a standard Fuzzing technique to the PLC, this caused the PLC to fail, requiring a manual reset (power down and up). This is where such attacks can prove devastating to process operations, and remote monitoring. While no level of resilience is configure to provide a replication of the PLC functionality, duplication of sensor data into a local monitor and RTU, directly from the ultrasonic sensor, still provided certain role groups access to critical data, highlighting an undesired change has occurred.

4.2 Memory Modification

"Memory Modification" modifies data stored in memory. Tools such as Snap7 [11] facilitate such modifications, providing an interface with Siemens PLCs over the S7 protocol. Consider the memory location discussed above (DB2.DBD1); once data flows and processing points are understood, selection and modification of memory locations such as this provide an excellent opportunity to cause physical process disruption, and/or inaccurate reporting/alarm management data.

We applied the Snap7 tool to DB2.DBD1, modifying the value beyond its normal operating boundaries. While this had no impact on the physical process, as the data processed through the RTU and historian (monitoring only), it moved up the data flow and into systems residing within the DMZ and Enterprise zones; this created warnings to system users that discrepancies between RTU and PLC derived data points have arisen. However, as the level of complexity found in historian calculations can be high, with reliance on the PLC alone for accurate data, it is possible that if left unchanged for some time, performance based analysis and investment decision could be made based on inaccurate data. This brings us back to the requirement for end-to-end testbed environments, and clear mapping of critical data processing points, with criticality not only identified based on the impact to operational processes, but holistic role group interaction/requirements.

5. FUTURE WORK AND CONCLUSION

In the near future, Internet of Things (IoT) devices are expected to invade a number of industries, including ICS. The extreme dynamism and diversity of the IoT contrast strongly with the slow, monolithic evolution rate of ICS. Our testbed will investigate ICS-IoT interactions through extensions to the existing infrastructure, in particular in terms of wireless technologies and wireless sensors. The diversity showcased in the testbed is also a motivation for automation to replace tedious manual adaptations to all particular devices and environments. Furthermore, formal modelling of system-user interaction and identification of critical data processing points as demonstrated earlier in this paper will be explored as promising and vital parts of our future research.

6. REFERENCES

[1] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad. Scadavt-a framework for scada security testbed based on virtualization technology. In *Local Computer Networks (LCN), IEEE 38th Conference on*, 2013.

[2] P. Didier, F. Macias, J. Harstad, R. Antholine, A. Johnston, S, S. Piyecsky, M. Schillace, G. Wilcox, D. Zaniewski, and S. Zuponcic. Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. *CISCO Systems and Rockwell Automation*, 2011.

[3] G. Dondossola, F. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi. ICT resilience of power control systems: experimental results from the CRUTIAL testbeds. In *Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2009*.

[4] P. Godefroid. In *2nd international workshop on Random testing (22nd IEEE/ACM Int. Conf. on Automated Software Engineering (ASE 2007))*.

[5] B. Green, B. Paske, D. Hutchison, and D. Prince. Design and construction of an industrial control system testbed. In *PG Net - 15th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, 2014.

[6] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *Smart Grid, IEEE Transactions on*, 4(2):847–855, June 2013.

[7] J. Hong, S.-S. Wu, A. Stefanov, A. Fshosha, C.-C. Liu, P. Gladyshev, and M. Govindarasu. An intrusion and defense testbed in a cyber-power system environment. In *Power and Energy Society General Meeting, 2011 IEEE*, pages 1–5, July 2011.

[8] C. Queiroz, A. Mahmood, and Z. Tari. Scadasim 2014;a framework for building scada simulations. *Smart Grid, IEEE Transactions on*, 2(4), 2011.

[9] B. Reaves and T. Morris. An open virtual testbed for industrial control system security research. *Int. Jour. of Information Security*, 11(4), 2012.

[10] R. Shapiro, S. Bratus, E. Rogers, and S. Smith. Identifying vulnerabilities in SCADA systems via fuzz-testing. In *Critical Infrastructure Protection V*, pages 57–72. Springer, 2011.

[11] Snap7. Snap7 - Overview. `http://snap7.sourceforge.net/`, 2016.