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).

![The Purdue Model](image_url)
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 automated; “Memory Manipulation” attacks require 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, Profinbus, 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-
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.
Table 1: ICS roles and associated system levels

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

(3.4.2 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 and maintenance and intervention 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 impact 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 modeling 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


