SHORT-PAPER

WADI: a water distribution testbed for research in the design of secure cyber physical systems

CHUADHRY MUJEEB AHMED, Singapore University of Technology and Design, Singapore City, Singapore

VENKATA REDDY PALLETI, Singapore University of Technology and Design, Singapore City, Singapore

ADITYA P MATHUR, Singapore University of Technology and Design, Singapore City, Singapore

Published: 21 April 2017

CPS Week '17: Cyber Physical Systems Week 2017
April 21, 2017
Pennsylvania, Pittsburgh

CySWATER '17: Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (April 2017)
https://doi.org/10.1145/3055366.3055375
ISBN: 9781450349758

WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems*

Chuadhry Mujeeb Ahmed
Singapore University of Technology and Design
chuadhry@mymail.sutd.edu.sg

Venkata Reddy Palleti
Singapore University of Technology and Design
venkata_palleti@sutd.edu.sg

Aditya P. Mathur
Singapore University of Technology and Design
aditya_mathur@sutd.edu.sg

ABSTRACT

The architecture of a water distribution testbed (WADI), and ongoing research in the design of secure water distribution system is presented. WADI consists of three stages controlled by Programmable Logic Controllers (PLCs) and two stages controlled via Remote Terminal Units (RTUs). Each PLC and RTU uses sensors to estimate the system state and the actuators to effect control. WADI is currently used to (a) conduct security analysis for water distribution networks, (b) experimentally assess detection mechanisms for potential cyber and physical attacks, and (c) understand how the impact of an attack on one CPS could cascade to other connected CPSs. The cascading effects of attacks can be studied in WADI through its connection to two other testbeds, namely for water treatment and power generation and distribution.

CCS CONCEPTS

•Security and privacy →Intrusion/anomaly detection; •Computer systems organization →Sensors and actuators; Embedded systems; *Dependable and fault-tolerant systems and networks;*

KEYWORDS

Cyber Physical Systems, Industrial Control Systems, Cyber Security, Attack Detection, Water Distribution Testbed

ACM Reference format:
Chuadhry Mujeeb Ahmed, Venkata Reddy Palleti, and Aditya P. Mathur. 2017. WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems. In *Proceedings of The 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, Pittsburgh, PA USA, April 2017 (CySWATER 2017),* 4 pages.
DOI: 10.475/123_4

1 INTRODUCTION

A Cyber Physical System (CPS) consists of one or more physical processes controlled using computing systems [5] commonly referred to as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). Communications networks that connect PLCs, RTUs, and the Supervisory Control and Data Acquisition (SCADA) systems enable effective control and monitoring of the physical processes[4]. However, the same networks simultaneously expose the system to adversaries. Experimental and design-based approaches for detecting cyber attacks [2] use testbeds to demonstrate the effectiveness of attack detection methods. Such experimental studies point to the importance of testbeds for CPS security research. The notion of design enters these approaches through the derivation of invariants from the physical design of the critical infrastructure. The invariants are essentially rules based on the physics of the process and, when violated during operation, indicate process anomaly.

Water distribution networks are often geographically spread and require automatic control to operate. Automation makes the water distribution network vulnerable to cyber-physical attacks [7]. ICS-CERT has reported several attacks against water utilities [1]. There is an urgent need to build state of the art testbeds and make these available for researchers. This paper describes an effort to achieve this goal by introducing an operational water distribution testbed.

Contributions: (a) Description of an operational WAter DIstribution (WADI) testbed. (b) Two attack scenarios and a powerful attacker model is proposed. (c) Results from experiments conducted using WADI.

Organization: Architecture of the WADI testbed is described in Section 2. Experiments performed on the WADI testbed are in Section 3. Section 4 is a discussion on the lessons learned and how security by design approach can be applied to CPS. A summary and directions for future work are in in Section 5.

2 ARCHITECTURE OF WADI

In this section the design, process and communication architecture of WADI is described. Figure 1 is a pictorial view of the testbed. WADI is an operational testbed supplying 10 US gallons/min of filtered water. It represents a scaled-down version of a large water distribution network in a city. WADI contains three distinct control processes labeled P1 through P3 (Figure 2) each controlled by its own set of PLCs.

2.1 Stages in WADI

WADI is designed to account for the likelihood of low (or no) demand occurring during weekends and allow user to input various flow rate (subjected to maximum of 10 US gallons/min) to simulate water consumption in accordance with time varying demand patterns. As shown in Figure 2, water distribution process in WADI is

*This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cyber Security R&D Programme (in part by Award No. NRF2014NCR-NCR001-40 and in part by NRF2015NCR-NCR003-001) and administered by the National Cybersecurity R&D Directorate.

CySWATER 2017, Pittsburgh, PA USA

DOI: http://dx.doi.org/10.1145/3055366.3055375

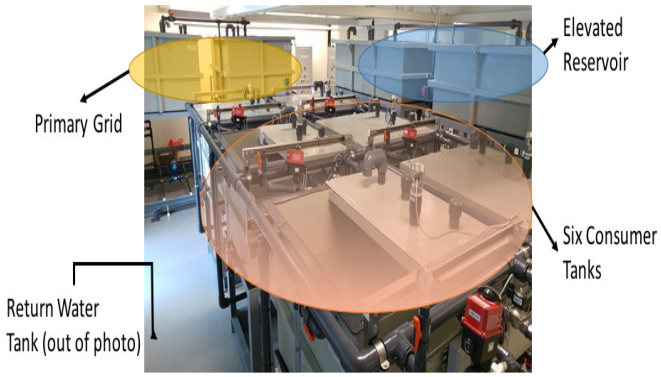

Figure 1: A pictorial view of WADI. Six consumer tanks are seen in the front, while elevated reservoir tanks and primary grid tanks can be seen in the background. Return water section is on left hand side (missing in the photo).

segmented into the following sub-processes: P1: Primary grid, P2: Secondary grid, P3: Return water grid.

Primary grid: The primary grid contains two raw water tanks of 2500 liters each, and a level sensor (1-LIT-001) to monitor the water level in the tanks. Water intake into these two tanks can be from the water treatment plant named SWaT, from Public Utility Board inlet, or from the return water grid in WADI. A chemical dosing system is installed to maintain adequate water quality. Sensors are installed to measure the water quality parameters of the water flowing into and out of the primary grid.

Secondary grid: This grid has two elevated reservoir tanks and six consumer tanks. Raw water tanks supply water to the elevated reservoir tanks and, in turn, these tanks supply water to the consumer tanks based on a pre-set demand pattern. Once consumer tanks meet their demands, water drains to the return water grid. Return water grid is equipped with a tank.

2.2 Communications Infrastructure of WADI

Figure 3 provides an overview of the communications infrastructure in WADI. Within each process stage, a PLC obtains data from local sensors and controls the actuators such as pumps and valves. In addition to the actuators, sensors such as level sensors in each tank, enable the PLCs to monitor the status of the system and to decide when to turn a pump ON or OFF. Several other sensors are available to check the physical and chemical properties of water flowing through the three stages.

The communication network contains layer-0 (L0), layer-1 (L1) and layer 2-(L2). L0 is at process level and connects actuators/sensors and I/O modules via RS485-Modbus protocol. L1 is the plant control network where all PLCs are connected to a central node in a star topology. Communication among PLCs and RTUs takes place over Ethernet switches using NIP/SP based on TCP and High Speed Packet Access (HSPA) cellular gateways using GPRS modem. L2 is a communication network between a touch panel Human-Machine Interface (HMI) and the plant control network. This network is implemented using star topology and consists of PLCs and RTUs. A firewall isolates the enterprise network from the plant control network. A SCADA workstation provides an interface between the plant operators and PLCs for remote monitoring and control.

2.3 Hardware and Software Components

Process PLCs constitute a significant hardware component for each of the three processes. Each PLC is housed in a chassis that contains input/output modules. Sensors and actuators are connected to the Input/output module through hard-wired connection or by serial Bus connection. Remote Terminal Units (RTUs) provide interface between SCADA and the remote instrument/equipment. The communications between instruments and equipment takes place via supervisory system messages by transmitting all telemetry data to the SCADA workstation.

The PLCs are programmed by using National Instruments (NI) LabVIEW software. Process logic is developed mainly by using two types of programming methodologies: (a) SubVI: composed of block diagrams representing smaller sections of codes and (b) Clusters: to group data elements logically. RTUs are programmed using Schneider Electric SCADAPack workbench. The workbench allows both ladder logic and structure text programming.

Sensor values or actuator settings are mapped to tags. Each tag can be addressed either via a string descriptor defined by the system designer, e.g., 1-MV-001 for motorized valve 1 in process 1, or a more direct mapping to bank number and pin number or similar (directly referring to digital/analog pins of an IO panel). Communications among sensors, actuators, and the PLCs can be via either wired Ethernet or the GPRS links. Manual switches allow changing the configuration between the wired and wireless communication.

3 EXPERIMENTS PERFORMED ON WADI

The communications infrastructure of a CPS is often connected to an external network. Such connections render a CPS susceptible to cyber attacks. In its current design, WADI is not connected to an external network. However, it does have a wireless network that connects PLCs to sensors, actuators, and to the SCADA workstation and another engineering workstation. The *control network* composed of the three stages of WADI can be connected to the SCADA workstation either through the wired or wireless network thus resulting in infiltration. Having compromised one or more links, an attacker could use one of several strategies to send fake state data to one or more PLCs, or simply do reconnaissance for a possibly subsequent attack. WADI, though designed to function efficiently, does not have any security mechanisms in its original design.

3.1 Attacker Model and Attacks

The attacker model used here [3] contains the attacker intentions and the components of the CPS that are targeted. In general, which components of CPS are targeted by an attacker depends on the objective of the attack. In this work, the attacker intent is "cut off water supply to the consumer tanks." We assume that the attacker has remote access to the SCADA system. In the following we explain two attacks launched on WADI.

Example 1: Here the attacker spoofs the level sensor readings in the primary grid. Figure 4 shows the launch of this attack where the attacker alters the sensor reading from 76% to 10% of the tank

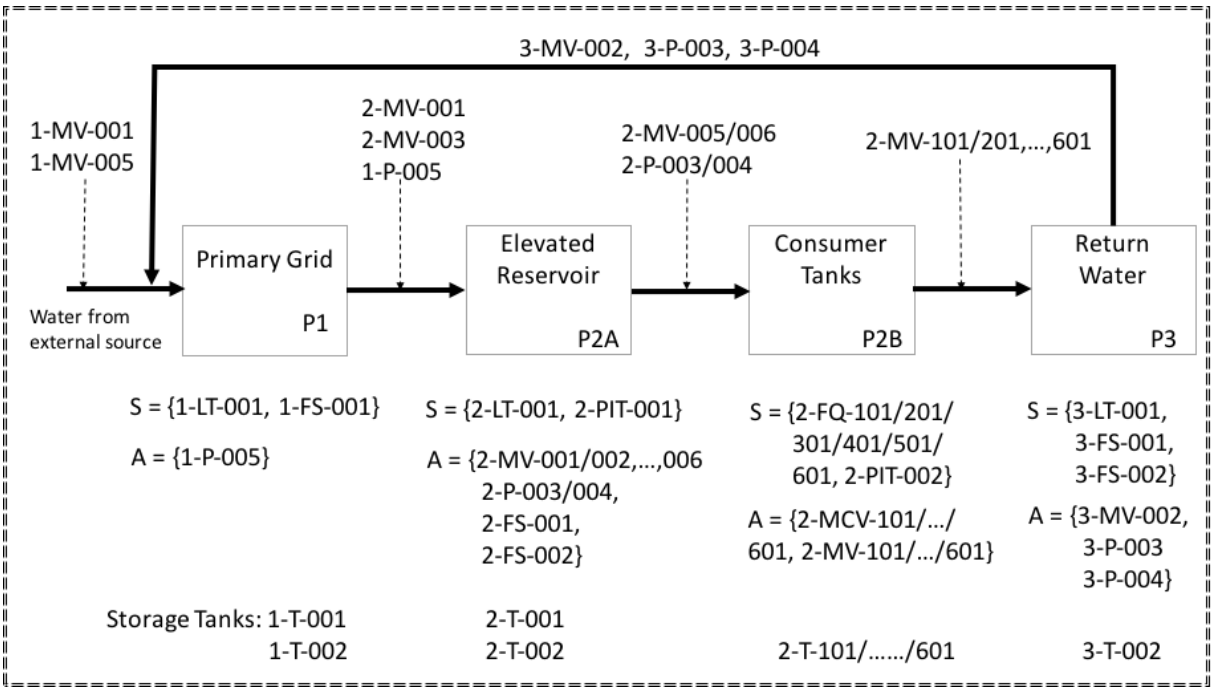

Figure 2: Three stages in WADI are shown. Solid arrows indicate flow of water and sequence of processes. S and A represent, respectively, sets of sensors and actuators. 1-LT-001: level sensor in stage 1 and tank 1; 1-FS-001: flow meter 1 in stage 1; 1-T-001: Tank 1 in stage 1; 2-MV-001: motorized valve 1 in stage 2; 2-MCV-101: motorized consumer valve 1 in stage 2; and 3-P-004: water pump 4 at stage 3.

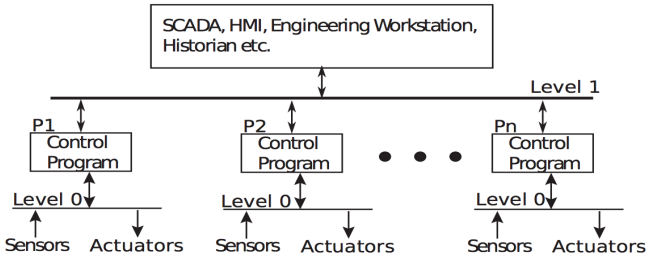

Figure 3: Architecture of the control portion of a CPS. P1, P2,. . . ,Pn denote PLCs. Each PLC communicates with its sensors and actuators through a local network at Level 0. PLCs communicate among themselves via another network at Level 1. Communication with SCADA and other computers is via a Level 3 network not shown here.

capacity which corresponds to a "low' state." Consequently the controller sends a command to turn on the return water pump or the PUB inlet valve to fill the raw water tank. At the same time, owing to the false data indicating low water level in the raw water tank, there will not be any water supply from primary grid tanks to the secondary grid tanks.

Note that at the time of attack launch, the secondary grid tanks contain water and thus the supply of water to the consumer tanks continues. Consequently, water levels in the secondary grid tanks decrease (Figure 4). Once the water level in the secondary grid tanks reaches to low level, the supply to consumer tanks is suspended. Now the level readings of both the primary grid tanks (spoofed) and the secondary grid tanks (actual) are "low". Consequently, there is no flow of water from the primary to the secondary grid and to the consumers. Despite this situation, the return water tank pump or the public water supply continues to fill the primary grid tanks and because of no outflow from these tanks there is an overflow. ■

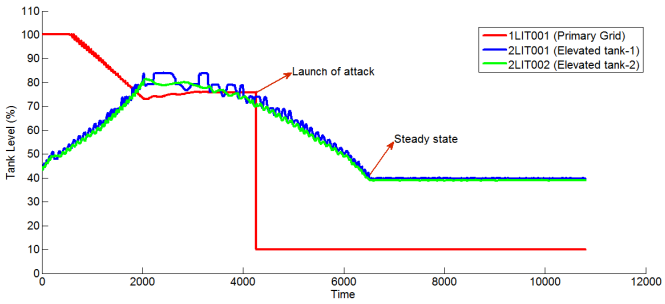

Figure 4: The impact of an attack on the primary grid level sensor

Example 2: - It is observed from the above examples that an attacker can successfully achieve the goal of stopping water supply to consumers by altering the readings of the primary grid level sensor and the water conductivity meter. There may also exist other ways

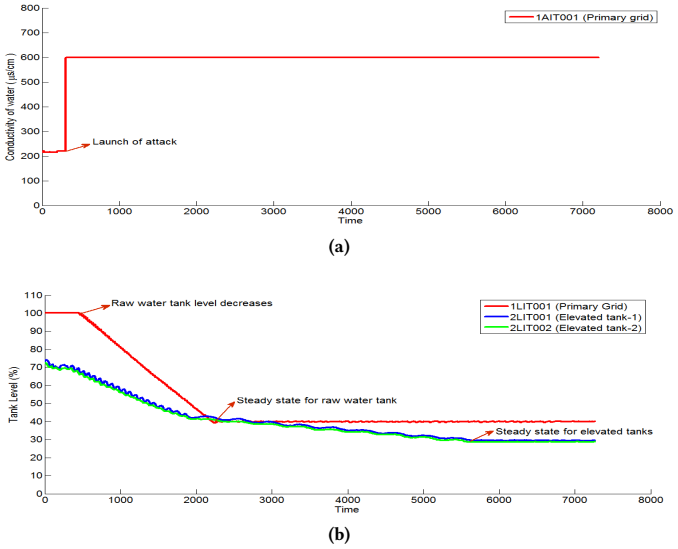

Figure 5: (a) Water conductivity sensor compromised, (b) The impact of attack when water conductivity sensor compromised.

of achieving this goal by compromising other sensor readings such as elevated tank sensors, closure of consumer tank valves etc.

4 DISCUSSION

One innate property of the design of WADI is its connectivity to the SWaT testbed [6]. This feature is added by design to help researchers model, execute and analyze cascading effects of cyber attacks.

Industrial Protocols: Modbus/TCP is chosen as a communication protocol in WADI. There is significant tool support available for such protocols from the research and commercial communities. Also, it diversifies the protocol stack to experiment with, as in another connected testbed SWaT, Ethernet/IP and common industrial protocol (CIP) are implemented.

Sensors: Sensors are an important system component to realize the automation in WADI. Tanks are equipped with level sensors and since water distribution network is mostly about flows, flow meters are abundant in design. Adequate sensor placement also allows collect ion of data and apply system identification techniques to get mathematical models for such networks thus aiding in security and fault analysis of the system.

Database and Historian: Historian is used to collect sensor and actuator data over time. Each tag is accessed separately to retrieve data from the historian. We can consider this as limitation of the design as this process is not fully automated and requires manual intervention. It turned out to be a time consuming and tedious task to retrieve data in a comma separated file for further analysis. It is recommended to make back-end databases more simple to query in future design.

5 SUMMARY AND FUTURE WORK

WADI has recently become available for experimentation. This paper offers an insight into the architecture of WADI to reach out to researchers to achieve the objective of designing secure critical infrastructure. Sample attack models are presented to show how realistic the threats are. WADI is physically connected to SWaT which supplies filtered water. A 75KW electric power generation and distribution testbed is also available to drive both WADI and SWaT. Such connectivity is intended for understanding how attacks on one critical infrastructure affects the behavior of another.

REFERENCES

[1] ICS CERT 2014. 2014. *ICS-MM201408: May-August 2014.* Technical Report. U.S. Department of Homeland Security-Industrial Control Systems-Cyber Emergency Response Team. https://ics-cert.us-cert.gov

[2] Sridhar Adepu and Aditya Mathur. 2016. Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plant. In *11th ACM on Asia Conference on Computer and Communications Security*. ACM, China, 449–460.

[3] S. Adepu and A. Mathur. 2016. Generalized Attacker and Attack Models for Cyber Physical Systems. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. IEEE Computer Society, Washington, DC, 283–292.

[4] Alaeddin Bobat, Tolga Gezgin, and Haeseyin Aslan. 2015. The SCADA system applications in management of Yuvacik Dam and Reservoir. *Desalination and Water Treatment* 54, 8 (2015), 2108–2119. DOI: http://dx.doi.org/10.1080/19443994.2014.933615 arXiv:http://dx.doi.org/10.1080/19443994.2014.933615

[5] Edward A. Lee. 2008. *Cyber Physical Systems: Design Challenges.* Technical Report UCB/EECS-2008-8. EECS Department, University of California, Berkeley. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html

[6] A.P. Mathur and N.O. Tippenhauer. April, 2016. SWaT: A water treatment testbed for research and training on ICS security. In *International Workshop on Cyber-physical Systems for Smart Water Networks*. IEEE, Vienna, Austria.

[7] Jill Slay and Michael Miller. 2008. Lessons Learned from the Maroochy Water Breach. In *Critical Infrastructure Protection*, Eric Goetz and Sujeet Shenoi (Eds.). Springer US, Boston, MA, 73–82. DOI: http://dx.doi.org/10.1007/978-0-387-75462-8_6