Spring 4-12-2016

CRITICAL INFRASTRUCTURE TESTBED FOR CYBER-SECURITY TRAINING AND RESEARCH (4)

William Hurst
Liverpool John Moores University, W.Hurst@ljmu.ac.uk

Nathan Shone
Liverpool John Moores University, N.Shone@ljmu.ac.uk

Shi Qi
Liverpool John Moores University, Q.Shi@ljmu.ac.uk

Critical Infrastructure Testbed for Cyber-security Training and Research

W. Hurst, N. Shone and S. Qi (Liverpool John Moores University)

Abstract

Critical infrastructures encompass various sectors such as energy resources, manufacturing and governmental services, which tend to be dispersed over large geographic areas. With recent technological advancements over the last decade, they have developed to be increasingly dependent on Information and Communication Technology (ICT); where control systems and the use of sensor equipment help facilitate operation. In order to sustain the ever-increasing demands, it is essential that these systems can adapt by integrating various new and existing digital technologies. However, this results in an increased vulnerability to cyber-threats. In addition, the persistently evolving global state of ICT has resulted in the emergence of sophisticated cyber-threats. As dependence upon critical infrastructure systems continues to increase, so too does the urgency with which these systems need to be adequately protected. Unfortunately, the consequences of a successful cyber-attack can be dire, potentially resulting in the loss of life or a devastating effect on the operation of government services and the economy. Despite the seriousness of this problem, the development of new and innovative cyber-security methods are being hampered by the lack of access to real-world data for training, research and testing new design methodologies. As such, the project presented in this paper highlights an in-progress project, funded by UKAIS, for the development of an easily-replicable and affordable critical infrastructure testbed for cyber-security training and research.

Keywords: Critical Infrastructure, Cyber-security, Testbed, Research, Data Analysis

1.0 Introduction

Protecting critical infrastructures from cyber-threats, in an increasingly digital age, is a concern for governments and private industries. The consequences of a successful cyber-attack could be life-threatening, compromise military defence, damage the economy or have a devastating effect on the operation of government services. Notably, at present, the level of cyber-attack awareness and the lack of threat-intelligence sharing between critical infrastructure providers, is a major point of discussion within the UK and the wider European Union (Walker *et al*.,) (McDonogh *et al*.,).

The increasing complexity of cyber-attacks and the open source availability of attack-toolkits means that security critical infrastructures in a difficult task. Unfortunately, devising suitable cyber-attack countermeasures requires real-world critical infrastructure data for both teaching and research purposes, which can be highly problematic. Real world data is sensitive and often classified, thus companies are unwilling to part with it, even to aid those investigating cyber-security methods that may help safeguard their systems in the future. Consequently, this lack of available

data hampers undergraduate studies, MSc projects, PhD and Post-Doctoral research in cyber-security, and crucially, in critical infrastructure protection.

The Micro-CI project addresses the lack of both access to experimental data and the hands-on experience needed to properly understand the challenges involved in an era of growing digital threats. As such, the intended output of this project is to support the construction of a bespoke bench-top testbed for data generation; consisting of a model critical infrastructure and control system. The testbed will be used for cyber-security research purposes and testing new experimental methods for enhancing the level of security in cyber-critical systems, specifically those under current exploration by the investigators (Hurst(a) *et al*.,). In result, the following objectives are defined for the completion of the project.

- Construct an affordable and easily-replicable bespoke bench-top testbed for obtaining realistic data sets for cyber-security research and education. The testbed will consist of a hackable Water Distribution plant with control system and realistic infrastructure data output. A full overview of the system is presented in Section 4. This will result in the creation of a safe and interactive environment, in which, theoretical cyber-security systems can be tested.
- To provide freely-available data that enables investigators to test security-related concepts, whilst retaining the environmental realism. Simulation data is often used to test theoretical cyber-security systems; however, data constructed through such emulators is inherently lacking in realism and a hands-on learning experience is missed.
- Use the equipment to share knowledge and expertise in the area of critical infrastructure protection; aiding students to become employable software and systems engineers (including manufacturing systems engineers) who are knowledgeable in cyber-security.

Society has a dependence on critical infrastructure service provision and, through this project, we endeavour to assess the inherent risks of a successful cyber-attack, and how this changes vital service provisions, through a small-scale focused case-study on a water distribution plant.

The remainder of this paper is structured as follows. Section 2 presents a background discussion on critical infrastructures, simulation, cyber-security and related testbed

projects. Section 3 presents the methodology that will be employed for the completion of this project. Section 4 details the planned application and implementation process. Finally, the paper is concluded in Section 5.

2.0 Background

As technology has rapidly changed over recent decades, modern society has become increasingly dependent upon a number of key infrastructures (Merabti *et al*.,). These key infrastructures, referred to as critical infrastructures, work together to provide a continuous flow of goods or services (Eusgeld *et al*.,). These services include food and water distribution, power supply, military defence, transport, healthcare and government services, to name but a few (Wang *et al*.,). Failure in one can have a direct impact on the others.

Beyond these conventional critical infrastructures, non-traditional ones have also emerged, in particular, telephone systems, banking, electrical energy distribution and manufacturing. Having a well-established critical infrastructure network is often considered a sign of civilised life, and nations are usually judged by the strength of their critical infrastructure network and the services they can provide to their citizens. However, dependence on these infrastructures is one of society's greatest weaknesses, due to the fact that a disruption to a single critical infrastructure can result general debilitating consequences on the population, economy and government (Yusufovna *et al*.,). As dependence on these critical infrastructures increases it is important that the ability to avoid disasters is enhanced (de Melo Leite *et al*.,).

2.2 Critical Infrastructures

Critical infrastructures are comprised of a network of interdependent man-made systems that function together to provide a continuous flow of goods or services, which are essential for economic development and social well-being. One of the key defining factors of a critical infrastructure is society's dependence on the services provided and the loss that would be encountered if successful physical or cyber-attack takes place.

All critical infrastructure areas are now becoming heavy Information and Communication Technology (ICT) users; with automation playing a key role in production (Parmar *et al*.,). ICT has also increased in areas such as agriculture, food

and water, where control systems and the use of sensor equipment is increasing the efficiency of production; making it more adaptive to the growing demands (Mafuta *et al*.,). For example, the use of robotics in farming to assist with labour-intensive work, is revolutionising the way in which crops are grown and maintained (Mafuta *et al*.,).

Infrastructure interdependencies have developed as ICT usage has increased. However, the risk that a disruption, or a critical failure, in one infrastructure, can directly lead to disruptions in others has exacerbated. This increase in digitisation and interconnectivity has also meant that such failures could be deliberately implemented from a remote location by means of a cyber-attack.

2.2 Cyber-Attack Types

Cyber-crime has a significant impact upon the economy and critical infrastructure service provision. The various current levels of different types of digital criminalities have the potential to cause extensive damage. Most cyber-attacks have the aim of making a profit from either offering the attack as a paid for service or through spear-phishing attacks to steal personal financial information.

Paid for cyber-attacks are usually in the form of Distributed Denial of Service Attacks (Hurst(b) *et al*.,) which operate as a Botnet, and can be used to incapacitate the host servers of a business. Spear-phishing attacks rely on human error and a lack of threat awareness to be successful. Their aim is to trick victims into thinking an email-based scam is legitimate by ensuring the information inside is specific to that person or organisation. As a result of successful spear-phishing attacks, numerous military and private industry systems have been breached in recent years (McAfee *et al*.,). Each penetration is the direct result of lack of understanding about the nature of the attack, which leads to sensitive information being disclosed. Unfortunately, once attackers have gained an initial point of entry to the system, they can often freely move throughout most of the network.

The control systems currently used in critical infrastructures systems are understandably closed source and not publically available. However, such systems continue to be at risk of cyber-attacks; and the facilitation of essential cyber-security research remains inherently a challenge.

2.3 Critical Infrastructure Testbeds

Ordinarily, the production of reliable and accurate research results would require the purchase of critical infrastructure hardware, which is extremely expensive and impractical.

This has led to the development of specific software-based simulators such as Technomatix, and the adaptation of existing software-based simulators such as OMNET++, Simulink and Matlab. These software simulators allow for affordable representations of critical infrastructure systems, by modelling their behaviour, interactions and the integration of their specific protocols (e.g. MODBUS).

However, the suitability of simulation has long been disputed; with the argument that simulations do not represent real world scenarios accurately, as they lack the ability to model the interactions of control system components. As such, this project aims to provide a platform that is rudimentary and low-cost to build, but can also be expanded to cover the various types of critical infrastructure systems. The practical nature of the testbed aims to provide users with a greater level of realism, and a more accurate representation of how different events and behaviours would manifest themselves in real-world scenarios.

As critical infrastructure security research is a relatively infantile subject area, the existing research is currently limited. However, there are several similar existing research projects, as outlined below. However, each has a fundamental difference to the proposed project.

SCADA LAB (Aragó *et al*.,) is an EU funded project to build a critical infrastructure testbed with a conjoined security lab, to facilitate security experiments. However, the primary limitation of this system is that it is a remote access system, with both the configuration and experimentation carried out by a third party. We are aiming to produce a localised testbed, where researchers/students are able to oversee and manage all aspects of their experiments directly.

As the implementation of a working critical infrastructure testbed can be time-consuming, Farooqui *et al*., propose a hybrid approach, by combining physical commercial hardware and simulation software (Farooqui *et al*.,). However, our project aims to be as realistic as possible, so we will be fully implementing working control

devices, rather than relying on simulation software. Additionally, we will be utilising small-scale, and therefore portable, hardware; rather than rigid commercial hardware.

There are several existing proposals for critical infrastructure testbed architectures, which focus on specific systems, such as electricity substations (Wei *et al*.,). However, our long-term goal is not to constrain our testbed to a single role, but to adopt a modular approach; whereby new critical infrastructure roles can be integrated at a later stage. This would make it suitable and useful to a wider audience. Specifically, the proposed system focuses on a water distribution plant; however, the design is extendable and can be extended to incorporate other infrastructure types, such as an ecologically-aware power plant.

A framework has also been proposed to address the problem of simulating large-scale critical infrastructure systems on a localised testbed. This framework acts as a glue layer between distributed and hybrid simulation of components and targets (Ficco *et al*.,). However, at this early stage of the project, we are primarily concerned with the practical realism and reliability of the generated results.

The testbed proposed in by Morris *et al*., is the most similar existing research in terms of its design, and pedagogical and research purposes (Morris *et al*.,) . The research put forwards proposes a testbed that focuses on cyber-security and utilises miniature hardware for a realistic representation of critical infrastructures. However, both projects are only available locally at the authors' institution and are not easily replicable. A defining factor of this project is to develop a testbed, which is cheap and easily replicable for other institutions. The design and implementation will both be detailed in publications and make accessible during the dissemination process.

3. Methodology

Dependence on the critical infrastructure is one of society's greatest weaknesses. Disruption to a single critical infrastructure can have a far-reaching impact on various critical aspects of modern life. As dependence on these critical infrastructures increases, it is important that society's ability to avoid disasters is enhanced.

Traditionally, protecting against environmental threats was the main focus of critical infrastructure preservation. Now, with the emergence of sophisticated cyber-attacks, the focus has changed to critical infrastructure protection as they are facing a different danger, with potentially debilitating consequences. Current security techniques are

struggling to keep up to date with the sheer volume of innovative and emerging attacks; therefore, considering fresh and adaptive solutions to existing computer security approaches is crucial. Consequently, critical infrastructure data is a necessity in a research environment, which relies on realistic information to design and develop advanced cyber-protection systems.

3.1 Approach and Contribution

This research project supports the current lack of access to infrastructure data. In that respect, the key novelty of this project is the development of a platform that can be expanded to cover the various types of critical infrastructure systems. However, this project will also make the following specific methodological contributions to academic knowledge:

- The facilitation of cyber-security systems testing in a realistic environment outside of a simulation situation.
- The construction of realistic datasets that will be used for enhancing cyber-security development; proof of concept; testing of theoretic systems and evaluating innovative systems with high levels of accuracy.
- Academic knowledge will be furthered through the publication of the testbed construction and the freely-available datasets to enable other researchers to test theoretical models. The design will be for a replicable testbed to allow other institutions to implement the model.
- The testbed data will enable an assessment of potential critical infrastructure failures on society, through the evaluation of the cascading effects on the system and an assessment of existing system weaknesses, in terms of cyber-security.
- The testing of the technological phenomena of critical infrastructure cascading failure in a realistic environment will provide an academic assessment of how cascading effects spread through an infrastructure.

4. Application

The main specific practical applications include the construction of a Critical Infrastructure Testbed and development of a Data Warehouse. The development of

the testbed will involve bespoke lab equipment in order to construct a Water-based critical infrastructure model, which will be bench-top size. The components will include a Human Machine Interface (control system) with an Ethernet port; pipe work for water flow and controller devices.

4.1 Construction Equipment

Specifically, the equipment used for construction will initially include: three control devices (one for the overall system control software, one for water control and one for hacking); a power source (solar panels); water pumps; water and light sensors; display screens; liquid flow sensors; weight sensors and an electronic platform to act as an end user for the water distribution.

The design displayed below, in Figure 1, presents a water-production plant. The specification is modest, meaning there is scope for future expansion; yet is sufficient in size to produce realistic infrastructure behaviour datasets for research purposes. The design is extendable to other applications in that it can be connected to other critical infrastructure models (such as power plants, telecommunications etc.), if additional equipment is to be included.

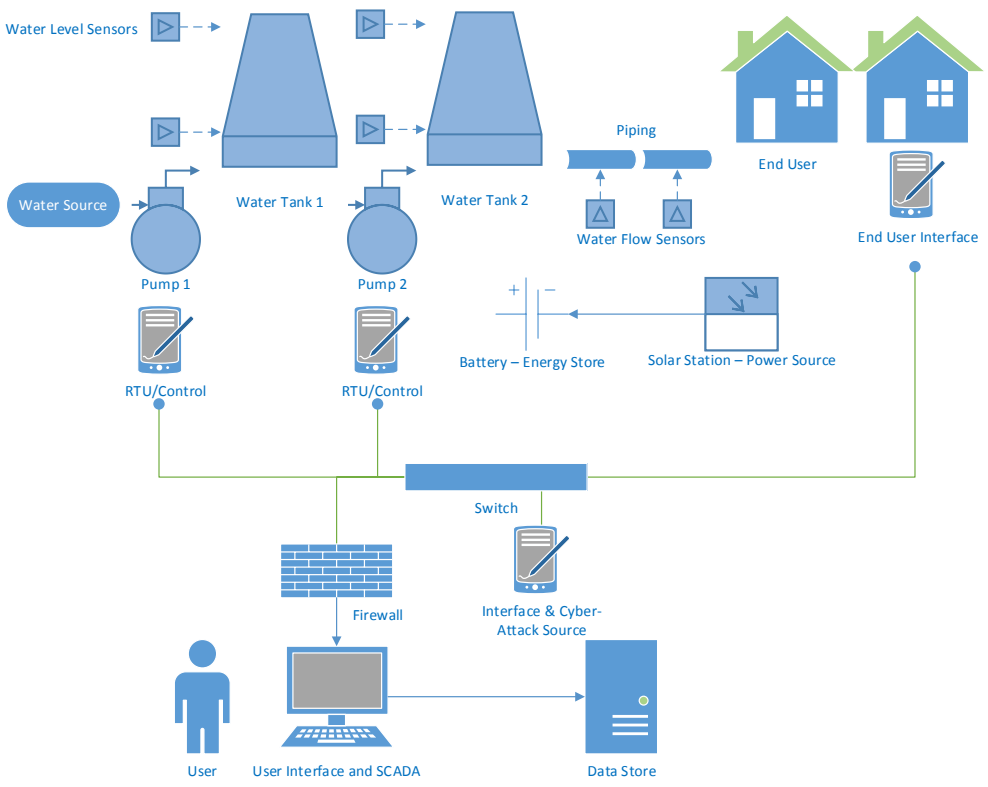

Figure 1. System Framework (Conceptual)

This would enable future research projects investigating the effect of cascading failures throughout a network of critical infrastructures, and its repercussive effects upon society.

4.2 Practical Output

The aim of the research is to have a threefold practical output; a fully working critical infrastructure testbed, a data store for research purposes and a prototype cyber-security system based on the investigators' theoretical research. The data server consists of a NAS (Network Attached Storage) device used to host the data repository. Both the data format and accessibility will ensure that it is usable for other academic researchers. Specifically, the data store will be constructed using a Synology DiskStation DS215j 2 Bay Desktop Network Attached Storage, which is able to store 4TB of research data, but this can be expanded at a later date if necessary. By using this approach, other researchers will be able to upload their own data generated to the server. This will not only enhance the utility of the system progressively over time, but also provide a repository of data to support experimental repeatability.

Model critical infrastructure testbeds are sparse in the UK. Completing this project would provide research and teaching opportunities for the testing and development of security enhancements in a real-life scenario. It is also clear that the practical approach of the equipment will provide significant benefits in terms increasing the employability of students, through applicable knowledge and the scope for R&D collaboration.

4.3 Project Completion Stages

The proposed research project will be done through 4 stages, each with their own techniques and methods for completion. The research approach is detailed as follows:

- Stage 1 - Design and Construction of Testbed: This will be a practical process with the aim of bringing field research into the lab environment for Information Systems data analysis and collection. The procedure will involve a hands-on assembly of the critical infrastructure model, presented in Section 4. The specific HMI is provided through a Windows tablet; the control devices/RTUs are Arduino boards with Ethernet shields; Arduino compatible pumps are used to move the water round the system, which is constructed

from plastic piping. Bespoke components, such as the end-user houses, will be 3D printed. The sensors consist of Arduino compatible water and pressure sensors. The power is supplied by a battery charged by solar panels. The overall construction process will involve simple wiring processes to connect the Arduino to the components through the use of a breadboard. An Ethernet switch will connect all the control devices to the User Interface. The control system software will be Arduino compatible.

- Stage 2 - Generation of Data: Realistic critical infrastructure datasets will be created, containing varied information, based on the run-time conditions. During system operation, data can be collected from any of the system components. This is comparable with the collection of data from mechanisms (such as a pump or sensors) in a real critical infrastructure environment. The aim will be to support data collection through sensors, which provide the RTU components with information to feed back to the User Interface. The research methodology will involve a case-study process to identify the most realistic approach for data generation, based on the existing research presented in the background section. The subsequent process of qualitative data generation, involves interacting with the data source to produce high-quality research data.
- Stage 3 - Cyber-Attack, Data Research & Security Systems: The output of stage 1 and 2 will lead to state-of-the-art cyber-security and data analysis investigations. Specifically, first-hand experience of security systems will enable the investigators to assess the effectiveness of existing anti-malware systems, which use techniques such as signature-based detection, anomaly detection and protocol analysis. This will, effectively, enable field-work to take place in a research lab environment. Critical infrastructure security is referred to as having a hard outer shell with a soft gooey centre (Knapp *et al*.,). The subsequent results will be used to devise and test theoretical cyber-security devices for enhancing the weaker internal state of critical infrastructure security. Devised security systems will incorporate the use of advanced machine learning techniques to analyse data. The approach will involve specific data classification techniques including: Uncorrelated Normal Density based Classifier (UDC), Quadratic Discriminant Classifier (QDC), Linear Discriminant Classifier (LDC), Polynomial Classifier (PLOYC), k-

Nearest Neighbour (KNNC), Decision Tree (TREEC), Parzen Classifier (PARZENC), Support Vector Classifier (SVC) and Naïve Bayes Classifier (NAIVEBC). To date, the investigators have conducted research into the use of data classification for behavioural analysis in a critical infrastructure system (Hurst(a) *et al*.,). However, the results are based on simulation data and not put into practice in a real-life environment. This project will provide an opportunity to build on existing research and test out theoretical results in a realistic environment.

- Stage 4 – Societal Impact: Networks of interconnected critical infrastructures are the supporting mechanisms and pillars of every industrialised nation. Heavily interconnected and mutually reliant on each other, their service provisions often cross borders, and multiple countries can consider the same infrastructure as critical. However, this reliance is also a great weakness. Infrastructure interdependence means that failures are able to cascade and impact vital service provision. Understanding the implications of a cascading failure, remains a key challenge. Consequently, this testbed will allow for experimentation into finding an approach to identify the effects of cascading failures and how their effects can be mitigated. This will be achieved through a behavioural analysis of the system under cyber-attack using the datasets constructed.

5. Conclusion and Future Work

One of the main challenges for governments around the globe is the need to improve the level of awareness for citizens and businesses about the threats that exist in cyberspace. The arrival of new information technologies has resulted in different types of criminal activities, which previously did not exist, with the potential to cause extensive damage to internal markets.

Given the fact that the Internet is boundary-less, it makes it difficult to identify where attacks originate from and how to counter them. Improving the level of support for security systems helps with the evolution of defences against cyber-attacks. This project supports the development of critical infrastructure security research, in the fight against a growing threat from the digital domain. The research project will further knowledge and understanding of Information Systems; specifically acting as a

facilitator for cyber-security research. In our future work, we will publish the constructed testbed and make the datasets available for cyber-security and critical infrastructure research.

Acknowledgements

The authors would like to thank the UK Academy for Information Systems (UKAIS) as the funding body for this research project (http://www.ukais.org.uk/).

References

J. Walker, B. J. Williams, and G. W. Skelton, "Cyber security for emergency management," in 2010 IEEE International Conference on Technologies for Homeland Security (HST), 2010, pp. 476–480.

McDonogh, "Opinion of the European Economic and Socail Committee on the 'Communication from the Commission to the European Parliament, the Counil, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Prot," Off. J. Eur. Union, vol. COM(2009), no. 149 final, 2010.

W. Hurst(a), M. Merabti, and P. Fergus, "Big Data Analysis Techniques for Cyber-Threat Detection in Critical Infrastructures," in Proceedings of the Eight International Workshop on Telecommunication Networking Applications and Systems, 2014.

M. Merabti, M. Kennedy, and W. Hurst, "Critical infrastructure protection: A 21st century challenge," in 2011 International Conference on Communications and Information Technology (ICCIT), 2011, pp. 1–6.

I. Eusgeld and C. Nan, "Creating a simulation environment for critical infrastructure interdependencies study," Ind. Eng. Eng. Manag. 2009. IEEM 2009. IEEE Int. Conf., pp. 2104–2108, 2009.

C. Wang, L. Fang, and Y. Dai, A Simulation Environment for SCADA Security Analysis and Assessment. IEEE, 2010.

F. S. Yusufovna, F. A. Alisherovich, M. Choi, E. Cho, F. T. Abdurashidovich, and T. Kim, Research on Critical Infrastructures and Critical Information Infrastructures. IEEE, 2009.

L. H. de Melo Leite, L. de Errico, and W. do Couto Boaventura, "Criteria for the selection of communication infrastructure applied to power distribution automation," in 2013 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), 2013, pp. 1–8.

A. Parmar, J. Gnanadhas, T. T. Mini, G. Abhilash, and A. C. Biswal, "Multi-agent approach for anomaly detection in automation networks," in International Conference on Circuits, Communication, Control and Computing, 2014, pp. 225–230.

M. Mafuta, M. Zennaro, A. Bagula, and G. Ault, "Successful deployment of a Wireless Sensor Network for precision agriculture in Malawi," in Networked Embedded Systems for Every Application (NESEA), 2012 IEEE 3rd International Conference on, 2012, pp. 1–7.

W. Hurst(b), N. Shone, and Q. Monnet, "Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures," in In the Proceedings of the 12th IEEE

International Conference on Dependable, Autonomic and Secure Computing, 2015.

McAfee Foundstone Professional Services and McAfee Labs, “Global Energy Cyberattacks:”Night Dragon”,” 2011.

C. Queiroz, A. Mahmood, J. Hu, Z. Tari, and X. Yu, “Building a SCADA Security Testbed,” in Third International Conference on Network and System Security, 2009, pp. 357–364.

M. Ficco, G. Avolio, L. Battaglia, and V. Manetti, “Hybrid Simulation of Distributed Large-Scale Critical Infrastructures,” Intell. Netw. Collab. Syst., pp. 616–621, 2014.

A. S. Aragó, E. R. Martínez, and S. S. Clares, “SCADA Laboratory and Test-bed as a Service for Critical Infrastructure Protection,” in Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research, 2014, p. pp 25–29.

A. A. Farooqui, S. . H. . Zaid, A. Y. Memon, and S. Qazi, “Cyber Security Backdrop: A SCADA Testbed,” in Computing, Communications and IT Applications Conference (ComComAp), 2014, pp. pp. 98 – 103.

Z. L. H. Wei, G. Yajuan, and C. Hao, “Research on information security testing technology for smart Substations,” in in International Conference on Power System Technology (POWERCON), 2014, pp. 2492–2497.

T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, “A control system testbed to validate critical infrastructure protection concepts,” Int. J. Crit. Infrastruct. Prot., vol. 4, no. 2, pp. 88–103, Aug. 2011.

E. Knapp and J. Broad, “Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems,” Syngress, Elsevier, 2011.