RICS-el: Building a National Testbed for Research and Training on SCADA Security (short paper)*

Magnus Almgren[1], Peter Andersson[2], Gunnar Björkman[3], Mathias Ekstedt[3], Jonas Hallberg[2], Simin Nadjm-Tehrani[4], and Erik Westring[2]

[1] Chalmers University of Technology, Sweden
[2] FOI, Swedish Defence Research Agency, Sweden
[3] KTH Royal Institute of Technology, Sweden
[4] Linköping University, Sweden
http://www.rics.se

Abstract. Trends show that cyber attacks targeting critical infrastructures are increasing, but security research for protecting such systems are challenging. There is a gap between the somewhat simplified models researchers at universities can sustain contra the complex systems at infrastructure owners that seldom can be used for direct research. There is also a lack of common datasets for research benchmarking. This paper presents a national experimental testbed for security research within supervisory control and data acquisition systems (SCADA), accessible for both research training and experiments. The virtualized testbed has been designed and implemented with both vendor experts and security researchers to balance the goals of realism with specific research needs. It includes a real SCADA product for energy management, a number of network zones, substation nodes, and a simulated power system. This environment enables creation of scenarios similar to real world utility scenarios, attack generation, development of defence mechanisms, and perhaps just as important: generating open datasets for comparative research evaluation.

Keywords: Cyber security in C(I)I systems, Modelling, Simulation, Analysis and Validation approaches to C(I)IP, Training for C(I)IP and effective intervention

1 Introduction

Since the appearance of Stuxnet, a malware specifically targeting industrial control systems (ICS) in 2010, research on identifying new attack vectors and new defence mechanisms on specific testbeds devoted to experimentation with ICS

* This work has been supported by the Swedish Civil Contingencies Agency (MSB) in the context of the RICS project. The authors are listed in alphabetical order, with Simin Nadjm-Tehrani being the corresponding author simin.nadjm-tehrani@liu.se.

cyber security has accelerated [1–5]. However, the lack of environments in which realistic scenarios can be created, devices emulated, protocols tested, methods evaluated, and data collected, has been known for a long time. Efforts have been spent to reduce this gap, notably through European projects (e.g. CRUTIAL [6]) or US national labs. Two recent surveys [7, 8] provide an excellent overview of the existing testbeds. However, to the best of our knowledge none of the reviewed testbeds openly share data for comparative research, a critical feature for research quality.

A review of discussions in a recent NSF-funded workshop focusing on remotely accessible testbeds for cyber-physical systems security points out a "significant gap" between the theoretical foundations, small scale experimentations, and real deployments with societal impact [9].

An ideal research environment for enhancing cybersecurity should facilitate comparison of different methods in relevant scenarios, using access to common testbeds and parameter settings. This in turn requires structures for sharing knowledge and datasets [10]. Adapting the scenarios and testbed configurations to various stakeholders needs should be possible and efficiently repeatable. This will need to accommodate obvious confidentiality barriers, but also practical realisations.

The Swedish research centre on Resilient Information and Control Systems (RICS) works towards reducing this research gap by realising such an environment as one of its cornerstones since its start in 2015. RICS research leads to methods for security assessment, prevention and detection of cyber threats in ICS, with a focus on electricity, water, heating, and transportation sectors. The stakeholders closely collaborating with RICS include a major SCADA vendor, and 13 other enterprises (utility companies, security product vendors, security consultants, and a national regulating body).

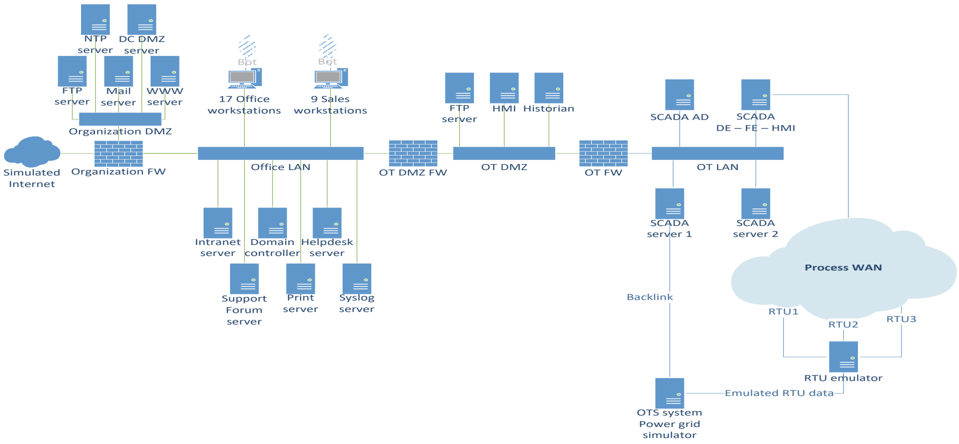

Fig. 1. Overview of the testbed zones, nodes, and connections

This paper presents an overview of RICS-el, a testbed for experimenting with supervisory control and data acquisition (SCADA) systems that has been realised in collaboration with RICS stakeholders and the Swedish defence research agency (FOI). Since the project is ongoing, the work is in an evolving state, but is already providing its first benefits to the collaborating universities in RICS.

In the following sections of the paper we first present an overview of the testbed, followed by a more detailed description of the architecture divided into the information technology (IT) and the operational technology (OT) subparts. The paper will also include a brief description of the utility of the testbed so far.

2 The RICS-el testbed

Our overall ambition with building the testbed is to make a simplified yet realistic copy of a utility's information and communication technology (ICT) infrastructure. In the first iteration, we have focused on an electric power operator, as this domain is opting higher digitalisation and where attacks are also prominent. At the core of RICS-el we find a modern SCADA product for power system control from one of the large vendors in that segment (the top right part of Fig. 1). To model a power system, we use the operator training simulator module from the SCADA product that provides us with an emulated grid (the bottom right part of the figure). The test environment also features an office IT segment (the left part of the figure).

The testbed is built on top of the Cyber Range And Training Environment (CRATE) infrastructure at FOI which is a virtualized environment. The details of how it is typically used to create environments for training and security awareness can be found elsewhere[5]. Here, we focus on enhancement of the platform to enable SCADA experiments. All the hosts in RICS-el are run on virtual machines (VMs) using VirtualBox, including the emulation of the wide area network (WAN) that connects the remote terminal units (RTUs) included in the testbed. CRATE contains an in-house configuration tool where all organisations, networks, hosts with parameters are defined and stored in a database.

2.1 The office IT segment

As shown in Fig. 1, the office IT part of the testbed consists of two subnets, the demiliterized zone (DMZ) for the Organization and the Office LAN zone. The Organization DMZ contains servers for file transfer protocol (FTP), web, domain controller for DMZ, mail, and network time protocol (NTP). The external firewall filters traffic between the Organization DMZ, the Office LAN, and the CRATE Internet (cyber range emulated Internet). The Office LAN contains 10 office workstations, 9 office sales department workstations, and 6 other support

[5] https://www.foi.se/en/our-knowledge/information-security-and-communication/information-security/labs-and-resources/crate—cyber-range-and-training-environment.html

servers. Interesting from a security perspective, and also realistic, some of the sales and office workstations have been given credentials and a VPN connection to the OT DMZ, described next.

2.2 The OT segment

The OT section of the RICS-el environment (the right segment in Fig. 1) is divided into four main parts: the demilitarized zone (OT DMZ), the OT LAN, the substation communication wide area network (Process WAN), and the power grid simulator, including the emulations of Remote Terminal Units (RTUs). This segment has been designed by vendor experts and researchers together.

The OT DMZ is included to isolate the OT LAN from the office LAN so that users in the office LAN will not be able to directly access the SCADA servers. Since certain SCADA data is of interest to the office users, a replicated Historian and an HMI are placed in the OT DMZ. By use of these replicated servers the office user can access SCADA data without having direct access to the SCADA server. It is possible for office users to view SCADA displays, e.g. real-time station diagrams, using the HMI in the OT DMZ.

In a similar way, certain data produced in the office environment is required in the SCADA zone. Examples are long-term generation schedules or load forecasts. Such data are sent as files to the FTP server in the OT DMZ where they can be picked up by the energy management system (EMS) or the distribution management system (DMS) applications in the SCADA system.

The OT LAN features two redundant SCADA servers with a real-time database for the process state as well as the two servers for DMS and EMS, with functionality such as state estimation, optimal power flow, and energy scheduling. Additionally, one host contains software modules for Human Machine Interface (HMI), data engineering (DE), and a communication front-end (FE), where the latter is a communication gateway to the WAN connecting the RTUs in the substations. Finally, there is an Active Directory (AD) host performing authorization of and granting access to the users in the zone.

The process WAN is built from 15 nodes forming a meshed communication network where each site (substation, electricity generation, main office) has an entry. Three RTUs are emulated using the RTU emulator and data from the power grid simulator. The communication between the SCADA front-end and the three emulated RTUs is performed by means of the IEC 60870-5-104 protocol routed through the process WAN to the front end (FE). If one of the communication nodes goes down the traffic is automatically rerouted using another route.

The power grid simulator is a key piece of the architecture to add realistic responses to any attacks or actions in the testbed. It is also instrumental for generating realistic traffic and events in the whole RICS-el environment. The simulator is using the Operator Training Simulator module (OTS) of the SCADA product. The OTS contains an extended power flow model that is designed to train grid operators for different operational scenarios in a realistic yet fictitious power grid. During operator training the OTS resides on the SCADA server, communicates directly with the SCADA database and the trained operators are acting over the HMI.

Within RICS-el, the OTS is used to give a realistic pseudo-dynamic model of the electrical process. The back bone of the OTS is a high voltage 400 kV grid with some twenty substations. Also some medium voltage transmission is included, but no low voltage parts. Hence, this corresponds to the business Transmission System Operator (TSO). Functionally the OTS operators can do all normal grid operation manoeuvres, e.g. open breakers, and the OTS model will respond by updating equipment states, power flows, etc. Scenarios of varying loads and production over a period of few days are used to give "life" to the emulated power flows. Since the OTS is developed with the purpose of training SCADA operators, grid emulation is updated on a higher level. This is the resolution on which the SCADA is normally managing the grid, so transients and and other fast power system dynamics are not captured.

Using the operator training version of the product would be problematic in RICS-el, since the OTS in the original product operates directly on the SCADA database and does not generate any SCADA and substation traffic. For that reason we have made the OTS a stand-alone component by developing individual RTU emulation for three specific RTUs. The emulated power flows for these stations and corresponding power lines are then translated to IEC 60870-5-104 messages in the RTU emulator and sent to the SCADA front-end over the WAN as normal RTU traffic. These can therefore be potentially monitored by security components deployed in the testbed later. For the time being the other RTUs in the OTS use an internal backlink to update their status, but our intention is to completely remove this backlink in the future.

2.3 Emulated users, traffic and scenarios

So far the structure of RICS-el has been described, but without any events this is an empty and deserted universe. For that reason, ongoing work is focused on adding realistic traffic to each segment in Fig. 1. The Office IT segment features a number of office worker bots, that send and read emails, surf the web, or open, edit, and close documents. Ongoing work includes emulating data exchanges over the SCADA DMZ, with the major inbound flow being load forecasts to the SCADA and the major outbound flow being the grid operation data sent from the SCADA to the Historian for further analysis by office users.

At the power grid end there are event generators in the form of scenarios provided as part of the OTS module from the vendor. These scenarios are 24 hour power generation and consumption profiles. The OTS also offers an interface (for the operator trainer) for introducing arbitrary power grid events. This means that traffic that flows over the substation communication network to the SCADA database and on to the HMI can be generated and such power grid operator bots are under construction. In their first version these bots will feature simple and rational behaviour similar to real grid events.

Note that by building RICS-el in the CRATE environment we are also able to generate arbitrary attack scenarios initiated on (the emulated) Internet including denial of service attacks. The Office LAN is connected to the OT DMZ via the firewall (OT DMZ FW) and via the OT DMZ and another firewall (OT FW) to the OT LAN. The OT DMZ can be removed by configuration to simulate some situations in real-life where office zones are connected to the SCADA systems via one (or no) firewall, making security vulnerabilities concrete.

3 Related works

To our knowledge, all the testbeds mentioned earlier are either only accessible to those that created the testbed whereby the data generated therein is not available to other researchers, or include only IT related datasets. The closest testbed we are aware of is SWAT, a testbed within the iTrust initiative in Singapore [11] where a water treatment plant including elements from the SCADA and IT infrastructure is intended for performing security exercises and sharing data with other researchers. Other major testbeds for studying power generation problems, e.g. one at University of Strathclyde[6] of course exist, but do not extensively emulate the SCADA, WANs, and office environments, and not tailored for security related data generation (including attacks).

4 Summary: current work using the testbed

In this paper, we have described RICS-el, a virtualized testbed for SCADA security research and training. Key design goals were to make the environment realistic by including both IT and OT elements and involving vendor experts. The current version of the testbed has already proven itself useful by: 1) generating synthetic but realistic data to form a basis of understanding the traffic flows and testing anomaly detection mechanisms, and 2) creating a "realistic" environment as a backdrop to exercises that the FOI team organises in order to train various participants in national security training and awareness raising exercises.

Data generation for anomaly detection The emulated testbed has already been used to generate ten days of data flow with IEC 60870-5-104 packets captured as pcap files. This has helped us understand the distinction between the traffic patterns that are regular (request response patterns) and those that are generated by spontaneous events (some flows that use the spontaneous category in the above protocol setting). Preliminary work on anomaly detection for these types of flows has been reported elsewhere [12, 13]. Our current work includes generating scenarios (using the OT and IT bots mentioned above) in which the pattern of spontaneous events in the SCADA elements can be systematically and repeatedly created for further studies.

[6] https://www.strath.ac.uk/research/subjects/electronicelectricalengineering/instituteforenergyenvironment/industryengagementresearchcentres/thepowernetworksdemonstrationcentre/

Deployed in exercises A replica of RICS-el has been used for the iPilot exercise in October 2017. iPilot trained Swedish nuclear IT/OT operators to detect and defend against IT/OT attacks. The exercise was overseen and observed by IAEA with delegates from 30 countries present. The event was sponsored by the Swedish Radiation Safety Authority and the EU. There are plans to use RICS-el in future exercises during the rest of 2018 and also in coming years.

References

1. B. Reaves and T. Morris. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11(4):215–229, August 2012.
2. B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera. A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers and Electrical Engineering*, 38(5):1146 – 1161, 2012.
3. C. Siaterlis, B. Genge, and M. Hohenadel. EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. *IEEE Transactions on Emerging Topics in Computing*, 1(2):319–330, December 2013.
4. O. Redwood, J. Reynolds, and M. Burmester. Integrating simulated physics and device virtualization in control system testbeds. In M. Rice and S. Shenoi, editors, *Critical Infrastructure Protection X*, pages 185–202. Springer, 2016.
5. U. Adhikari, T. Morris, and S. Pan. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining. *IEEE Transactions on Smart Grid*, 8(6):2744–2753, November 2017.
6. G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi. ICT resilience of power control systems: experimental results from the crutial testbeds. In *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pages 554–559, June 2009.
7. H. Holm, M. Karresand, A. Vidström, and E. Westring. A survey of industrial control system testbeds. In S. Buchegger and M. Dam, editors, *Proceedings of Nordic Conference on Secure IT Systems (NordSec), LNCS 9417*, pages 11–26. Springer, 2015.
8. S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, and R. Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5):1039–1057, May 2016.
9. M. Egerstedt and M. Govindarasu. Accessible remote testbeds: Opportunities, challenges, and lessons learned, workshop report. 2016.
10. E. Vasilomanolakis, C. G. Cordero, N. Milanov, and M. Mühlhäuser. Towards the creation of synthetic, yet realistic, intrusion detection datasets. In *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pages 1209–1214, April 2016.
11. A. P. Mathur and N. O. Tippenhauer. SWaT: a water treatment testbed for research and training on ics security. In *International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36. IEEE, April 2016.
12. C.-Y. Lin, S. Nadjm-Tehrani, and M. Asplund. Timing-based anomaly detection in SCADA networks. In *Proceedings of the 12th International Conference on Critical Information Infrastructures Security (CRITIS)*. Springer, October 2017.
13. C.-Y. Lin and S. Nadjm-Tehrani. Understanding IEC-60870-5-104 traffic patterns in SCADA networks. In *Proceedings of the 4th Cyber-Physical System Security Workshop (CPSS), AsiaCCS*. ACM, June 2018.