Digital Forensic Readiness in Critical Infrastructures: A Case of Substation Automation in the Power Sector

Asif Iqbal[1,2(✉)], Mathias Ekstedt[1], and Hanan Alobaidli[2]

[1] School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden
asif.iqbal@ee.kth.se, mekstedt@kth.se
[2] Athena Labs, Dubai, UAE

Abstract. The proliferation of intelligent devices has provisioned more functionality in Critical Infrastructures. But the same automation also brings challenges when it comes to malicious activity, either internally or externally. One such challenge is the attribution of an attack and to ascertain who did what, when and how? Answers to these questions can only be found if the overall underlying infrastructure supports answering such queries. This study sheds light on the power sector specifically on smart grids to learn whether current setups support digital forensic investigations or no. We also address several challenges that arise in the process and a detailed look at the literature on the subject. To facilitate such a study our scope of work revolves around substation automation and devices called intelligent electronic devices (IEDs) in smart grids.

Keywords: Digital forensics · Forensic readiness · Substation automation
Smart grid · Forensic investigation · Critical infrastructures

1 Introduction

A critical infrastructure comprises of systems and assets, whether physical or virtual, that are so essential to a nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination thereof [1–3]. Our modern societies depend on critical infrastructures (CIs) to a great extent and sixteen such sectors of different critical infrastructures are defined by Department of Homeland Security [4]. For instance, several days long failure of power delivery in a large geographical area would not only lead to most business activity ceasing; it would also cause long-term damage to a range of industrial processes (e.g., animals dying in farms) and disrupt basic logistics that support our very living [5]. In the recent years, attacks on critical infrastructures and industrial control systems have become more frequent and more sophisticated [6]. State and non-state actors in today's volatile cyber arena are giving rise to increased cyber-attacks including those that target specifically critical infrastructure, like the recent attack on Ukrainian power grid [7] and the well-known Stuxnet [8, 26]. At the same time, the proliferation of computer tools

P. Matoušek and M. Schmiedecker (Eds.): ICDF2C 2017, LNICST 216, pp. 117–129, 2018.
https://doi.org/10.1007/978-3-319-73697-6_9

and skills enabling individuals and teams to perform sophisticated cyber-attacks has been increasing, which leads to the attackers having to possess less skill and resources to launch a successful attack of a given sophistication compared to the past.

This paper zooms in onto investigative capabilities, through studying digital forensic readiness in critical infrastructures. Digital forensic readiness is the capability of an IT environment as a whole to determine whether or not an incriminating activity has taken place, using the remnants of different activities (e.g., state of systems, logs). While there have traditionally been many applications of digital forensics and forensic readiness within the domain of personal and enterprise IT, often used in law enforcement investigations; much less attention has been directed at applying digital forensics to critical infrastructures. As it is evident from the [9] that digital forensic readiness is of crucial importance but still it's quite at its infancy as far as critical information infrastructures are concerned. If we look through the published research as well as industry archives we see hints of other domains present in the literature but rarely anything to do with CIs. Here are a few examples that deal with network forensic readiness [10, 11].

2 SCADA System Architecture

There are different hardware components that create a (Supervisory Control And Data Acquisition) SCADA system. These components maybe considered as data sources in an investigation. Hence this section will mention some of the main components that might contain evidence in an investigation.

1. PLC (Programmable Logic Controller): A general control system that can function as a standalone system or participate in a network of PLCs. It has a flexible input and output facilities and it is programmed using techniques such as "Ladder logic". It is adapted to control manufacturing processes that require high reliability control and ease of programming such as assembly line and robotic devices.
2. RTU (Remote Terminal Unit): Typically used in SCADA systems as a communication hub where it collects data from sensors and actuators in substations and remote locations to a central system. It can also be used as a relay system for control commands.
3. IED (Intelligent Electronic Device): A term mostly used in power industry describing multifunction devices used for monitoring, protection and control. It is also used for upper level communication independently without the aid of other devices. It can receive data from sensors and power equipment's which can be used to issue control commands such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level.
4. HMI (Human Machine Interface): System engineers and operators utilize the HMI to interpret and visualize data received from the SCADA system through a graphical and/ or numerical presentation. It is also used to transfer algorithms, configure set points and adjust parameters of controllers. Depending on nature of the SCADA system controlled and monitored the HMI can be either a dedicated

hardware containing a control panel of switch and indicators to a software version either on a computer/ mobile application

5. Historian: A term used for a database management system that acquires and stores data sent to the control center. It is also used to create audit logs for all activities across a SCADA network. Hence it is considered important in any incident investigation
6. MTU (Master Terminal Unit): Is a central server that is sometimes referred to as SCADA server which is used to collect and process RTU/field devices data as well as issuing commands. It can provide a communication channel with these devices and it may be used to pre-process data before sending it to a historian. It also can provide a graphical representation of the information to be transferred and displayed on the HMI [12].

3 Related Work

According to the CESG Good Practice Guide No. 18, Forensic Readiness is defined as "The achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyze digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law" [9]. Implementing a forensic readiness system either specifically for digital forensics in general can provide several benefits such as [11]: Preparing for the potential need for digital evidence such as email communication, minimizing the cost of investigations, blocking the opportunity for malicious insiders to cover their tracks, reducing cost of regulatory or legal requirements for disclosure of data, showing due diligence, good corporate governance, and regulatory compliance.

Hence in the context of CI, it would be of paramount importance that we determine all such parameters that assist in such attribution to malicious activity as also defined in [13]. At the same time, digital forensics in critical infrastructure can provide benefits beyond capturing attackers. It can be useful in the context of troubleshooting, monitoring, recovery and the protection of sensitive data [14]. For example, it can be used to define and verify system monitoring requirements. This is done through determining logging conditions identifying errors and problems that can occur under failures or security breaches. It also identifies if this is done using software or hardware security equipment. It can also assist in the learning phase of advanced intrusion detection methods like anomaly detection, whitelisting and deep protocol behavior inspection [15].

3.1 Challenges to SCADA Forensics

According to a white paper by Enisa [16] with the security risks facing SCADA environment it becomes crucial to respond to critical incidents and be able to analyze and learn from what happened. The paper identified an incident analysis process based on good practices and recommendations for digital forensics. This process is divided into five stages which are: Examination, Identification, Collection, Analysis of evidence as well as Documentation of the process and results. Through these phases

several challenges are faced by forensic investigators. This is divided into 3 categories of challenges: Data collection, Data Analysis and Operational.

Ahmed et al. [17] discussed some of the challenges faced while investigating a SCADA environment. The challenges mostly lay in the range of data acquisition. They stated that as per the sensitive nature of the SCADA environment that focuses on the availability of the services provided techniques such as live forensics would be needed. Nevertheless, this requires a prompt acquisition of the data as valuable information might be lost. At the same time, an important aspect of the forensic investigation process might be affected, this aspect is digital evidence integrity validity. As the data acquired from a live system that needs to be kept running methods such as creating hash value of the acquired image would be rendered apostolate. This is because data on the system will keep changing hence no two hash values will be the same.

Another challenge to the acquisition process may be resulted from the deterministic network traffic in SCADA environment, which might prevent forensic tools from operating properly. For example, a firewall might have strict rules that allow communication between specific SCADA components but disallow communication between the investigator's machine and SCADA components during data acquisition. Also, customized operating system kernels such as the one available in PatriotSCADA (firewall solution for SCADA networks) might affect the usability of acquisition tools. That is because tools such as DD might not run on customized kernels unless they are compatible with each other.

Other challenges include the unavailability of data to be acquired. For example, resource constrained devices such as RTU and PLC have limited resources hence data can have a limited life expectancy before being overwritten by other processes. Also logs in these devices might be considered inadequate for forensic investigation as they are geared toward process disturbances, not security breaches.

Ahmed et al. [17] also discussed some measures for forensic readiness in SCADA environment. They stated that forensic process can be improved in SCADA systems through preparedness and the selection of appropriate tools. The measure discussed was the creation of a data acquisition plan which consists of three steps. The first step is identifying the system environment; the second step is defining environment-specific requirements such as the impact of vendor solutions on OS. Finally, the third step is identification and collection of data such as activity and transaction logs.

They combined this with the need for data acquisition monitoring using tools such as EnCase CyberSecurity. This is needed in order to ensure that the acquisition process would not affect the availability of the SCADA system. They also recommended the use of lightweight data acquisition by using tools that have minimal impact so that adequate system resources are available for SCADA services to work properly.

Similar to the Enisa white paper [14] discusses investigation process of CI which starts with the identification of possible sources of evidence. They mention some of these sources which are engineering workstations, databases, historian, Human Management Interface (HMI), application server, Field devices like PLC, RTU, IED, firewall logs, web proxy cache and ARP tables. The second step is the preservation of the identified evidence, followed with data acquisition and data analysis.

Wu et al. [18] discussed a SCADA digital forensic process consisting of seven steps which are Identification and Preparation, Identifying data sources, Preservation,

Prioritizing and Collection of evidence, Examination Of the collected evidence, Analysis of the collected evidence, Reporting and Presentation, and finally Reviewing results. The paper also stated some challenges to the SCADA forensic investigation. These challenges are live forensics and integrity of data, lack of compatible forensic tools for field devices, lack of forensically sound storage, identifying data sources on SCADA systems, and finally increase of sophisticated attacks.

There were also other efforts by government organizations such as the Department of Homeland Security's the Control Systems Security Program to provide a guideline for the forensic investigation process [19].

Eden et al. [12] discussed a SCADA forensic incident response model consisting of four main stages: Prepare, Detect, Triage, and Respond. The model focuses on preparation before an incident occurs that would require a forensic investigation to happen. These stages are Prepare, Detect, Triage, and Respond. This paper also agreed with the SCADA forensic challenges mentioned in Ahmed et al. [17] work.

Figure 1 represents a mind map of the SCADA forensic challenges in relation to the discussed research.

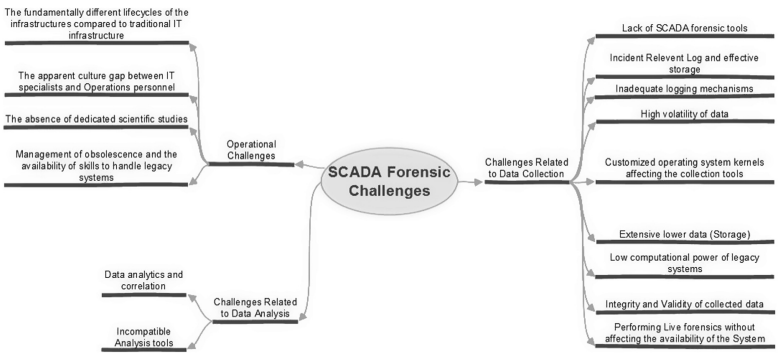

Fig. 1. Forensic challenges in SCADA environment [20]

3.2 SCADA Forensics Research

Some research such as the work done by Kilpatrick et al. [21] focused on network forensics in SCADA environment. The paper presented an architecture that is based on introducing forensic agents to the SCADA network. These agents are positioned on areas that will capture most of the network traffic in the SCADA network. The agents then forward the captured packets to a data warehouse using an isolated network in order to insure the integrity of the gathered information. The gathered information can also be used to incorporate mechanisms for monitoring process behavior, analyzing trends, and optimizing plant performance.

Valli [22] focused on exploit traceability during an investigation. The research presented a framework for producing verified signatures for Snort IDS using known and published vulnerabilities of SCADA and control systems. The research methodology consisted of five steps. The first step was the identification of vulnerabilities or

traces at Black Hat, hacker, vendor, CERT or relevant cites. After identifying the possible vulnerabilities, a replication of the attack is designed through a script or a code base in order to ease the testing phase. These vulnerabilities are then studied from the networking perspective by analyzing the communication using modbus or DNP3 network protocols. Afterwards based on the gathered information a rule-set for Snort IDS is created. Finally, this ruleset is tested in an experimental environment.

Sohl et al. [23] discussed a set of vulnerabilities that can affect industrial control systems (ICS) as well as the fundamentals of forensic investigation in ICS with relation to these vulnerabilities. These vulnerabilities can be of low level in the control system such as stack overflow or heap overflow memory errors. Other discussed vulnerabilities were hardcoded credentials in control systems as well as vulnerabilities in Active X and cross site scripting (CSS) which can be used to attack system operators when visiting a malicious web site. An example of a SCADA system affected by the Active X vulnerability is MICROSYS PROMOTIC SCADA/HMI system before version 8.1.5 the vulnerability allows remote attackers to cause a denial of service via a crafted web page [24]. Another vulnerability to the MICROSYS PROMOTIC published is related to heap-based buffer overflow in versions before 8.3.11 which allows remote authenticated users to cause a denial of service via a malformed HTML document [25]. Sohl et al. [23] also discussed some of the possible evidence that an investigator will sought after while investigating an industrial control system. These evidences can be injected shellcode, rogue OS processes, additional malware code, code injected into the address space of existing OS processes, modifications to various kinds of data on the industrial control system, new client or server sockets, file creation and file access data. The author also discussed some forensic tools that can be used in control systems when suitable such as Linux LiME forensics tool for capturing volatile data along with Volatility Framework tool. Other tools discussed were FTK Imager, Dshell for network packet analysis. The authors stated that most of the tools are designed to work with general computing environment hence tools need to be designed to cope with specific interfaces, networking, and operating systems of control systems.

Nevertheless, most of the research focuses on the network element or the HMI of the SCADA environment but there isn't much discussion of the PLC or RTU devices regarding forensic investigation.

4 Discussion of the Related Work

As seen in the related work section there is variety of challenges that can affect the digital forensic investigation in SCADA systems. Most of these challenges are related to the fact that SCADA systems were designed at first with limited networking and security in mind. Most of the SCADA systems were isolated from the outside network such as the internet, but with the advancement in technology and the need for larger and faster processing they had to be connected. As a result, they became vulnerable to different attacks.

Also, SCADA system environment differ from traditional computing system with regard to the emphasis of availability. This emphasis proves to be one of the main challenges regarding digital forensics. The investigation process and technique needs to

take this as a main consideration because if these systems went down the outcome maybe catastrophic to the country infrastructure. Hence traditional forensic techniques will not be suitable, but techniques such as live forensics will be of great value. Never the less more studies need to be done regarding live forensics techniques and tools that can be used in SCADA system.

Additionally, there are challenges related to the data created in the system, as it was mentioned above SCADA systems were not designed with security in mind. Hence data that can be gathered from sources such as logs may not cover all the needed aspects of the investigation. The logs mostly are designed to answer the system operator's needs not the security needs. Moreover, the issue of the limited logging capability in devices as well as limited storage makes a lot of the needed data to be highly volatile.

To overcome some of these challenges the research field discussed the possible investigation process. As per the author opinion the most comprehensive process were discussed in [12, 18]. The designed process paid a great attention toward the preparation phase as it covers a challenge related to the limited knowledge of forensic investigators about the SCADA environment. Also these two processes shed light on the challenge of volatility of data sources by prioritizing which data sources are providing the most valuable evidence in an investigation and acquiring the data accordingly. Never the less the process in [18] focused more in the investigation of the acquired evidence while the process in [12] introduced a detect phase that is related to identifying an attack and how it affected the system.

While in terms of other technical research in SCADA forensics filed the focus is on the network element or the HMI. There isn't much discussion of the PLC or RTU devices about the forensic investigation, some discussed that these devices don't have forensic capability or may not provide much data to the investigation. Having said that we consider these devices to be of value to the investigation and they should be studied and identify the possible evidence in these systems. Along with identifying the possible evidence the author believes that measures need to be implemented to make these devices provide more forensic evidence.

5 Case Studies

The aim of these case studies was to approach the problem of digital forensic readiness through an implementation point of view.

Substation automation refers to using data from intelligent electronic devices (IED), control and automation capabilities within the substation, and control commands from remote users to control power-system devices.

Figure 2 indicates our scope of work for this research as well as typical substation automation architecture.

5.1 Example 1: Digital Forensic Investigation of an IED Device

Transformer protection IED is a protection, control, and monitoring IED with extensive functional library, configuration possibilities and expandable hardware design to meet

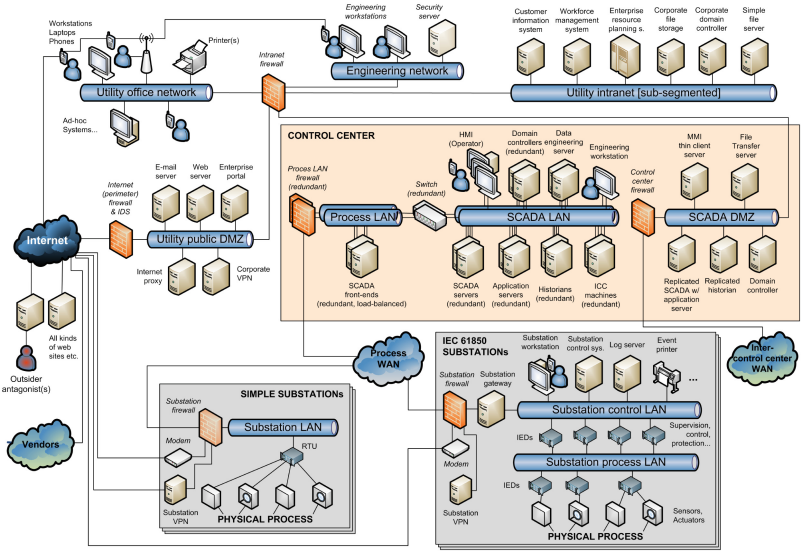

Fig. 2. A detailed SCADA network with a substation network

specific user requirements. It is usually used with a protection and Control IED manager. It helps manage protection and control equipment all the way from application and communication configuration to disturbance handling, including automatic disturbance reporting. The manager interacts with IEDs over fast and reliable TCP/IP protocols through LAN or WAN (rear communication port of the IED) or alternatively directly through the communication port at the front of the IED. It can read and write all configuration and setting parameters of an IED.

There are several elements of a substation automation and protection system. However, this use case will consider the interaction between only two of them. Measurements from a physical power system process are taken using Current Transformers (CTs) and Voltage Transformers (VTs). Those measurements are sampled using a device called Merging Unit (MU). MUs merge 4 voltage and 4 current samples per measurement point into a single IEC61850-9-2 Sampled Value (SV) packet which is then being distributed on an Ethernet based process bus using multicast.

The IED is implemented as a transformer differential function. Essentially, the function takes current measurements from both sides of a transformer and calculates the difference between the two. If this difference is greater than some predefined value, it disconnects the transformer from the grid by opening the corresponding breakers. The IED sends the IEC 61850-8-1 GOOSE messages to the I/O devices which oversee the opening of the transformer breakers.

Undesired opening of transformer breakers might have significant economical and societal consequences. Therefore, this use case attempts to demonstrate how operation of the power system can easily be disrupted by crafting GOOSE message packets. To simulate a power system process, operation of MUs and I/O devices, a real-time Opal-RT simulator is used. The simulator is connected to the IED via an Ethernet

switch. Both IEC61850-9-2 SV packets and IEC 61850-8-1 GOOSE packets are sent via this switch. During a normal operation, the IED would send cyclic multicast GOOSE packets to the simulator with a Boolean value equal to False which corresponds to the closed state of the breaker. Conversely, when there is a fault in the system, IED would initially send avalanche of packets with Boolean value equal to True. This change in value would cause I/O devices to open the breakers and clear the fault.

However, if an attacker gains access to the network, it can craft the GOOSE messages which will cause the breakers to open regardless of the current state of the system. It should however be noted that, to craft the message, the structure and the content of the GOOSE message would have to be known, see Fig. 3.

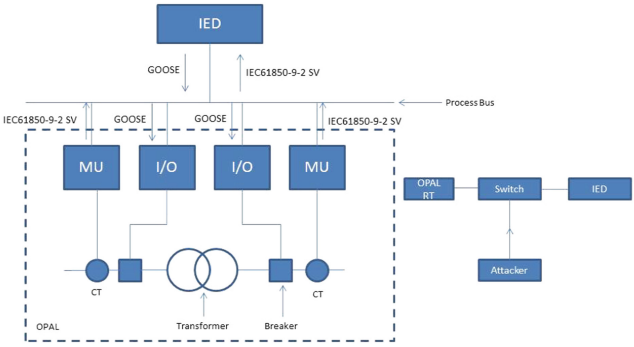

Fig. 3. IED attack example

5.2 Example 2: Digital Forensic Investigation of a Phasor Measurement Unit (PMU) Device

5.2.1 Introduction to PMU Device

Phasor Measurement Unit (PMU) is a device which measures the amplitude and phase of a power-grid voltage and/or current, relative to a known reference [27]. Synchrophasor technology uses PMUs to measure voltage and current waveforms and calculate phasors. Each measurement is time-stamped and thus synchronized against Coordinated Universal Time (UTC) using a time source such as the GPS [28]. PMU data is sampled between 30 to 120 samples per second which is fairly high enough, such that dynamics of the power-grid can be measured accurately.

Due to having high resolution data with accurate time-stamped information, Synchrophasors technology is being used for Wide-Area Monitoring System (WAMS), forensic event analysis and verification of grid model etc. [28].

5.2.2 Synchrophasor Network

As shown in Fig. 4, GPS receiver takes the timing signal from satellite. A substation clock interprets the GPS signal and converts into a protocol which is readable by PMUs. PMUs compute Synchrophasors using IEEE C37.118.2 standard [29] and

streams data over Ethernet to Phasor Data Concentrator (PDC). PDC streams are sent via Wide Area Network (WAN) to a power system control center, where different monitoring, control and protection application utilize the PMU/PDC data.

5.2.3 Vulnerability of a PMU Device to Spoofing/Jamming Attacks

PMUs are vulnerable to cyber-attack because it uses TCP/IP and UDP/IP protocol which make it more susceptible to various attacks [30]. For example, modification attacks like malicious code injection, data fabrication attack in the form of data spoofing and jamming the input signals to the PMUs etc. [30–32]. A GPS signal which provides a time synchronization input to the PMUs, is one of the most vulnerable signals to a cyber-attack as shown in Fig. 4. An attack on GPS signal infects PMU data, which could adversely impact the performance of the power system applications which utilize the infected PMU data.

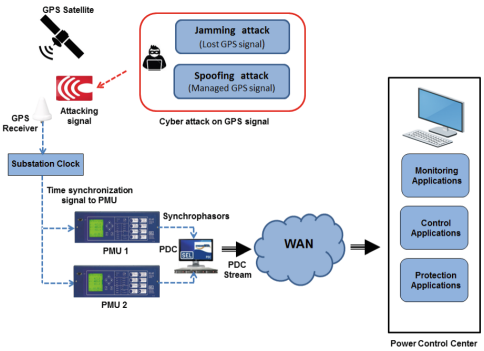

Fig. 4. Synchrophasor network

The impact of loss of time synchronization signal (in case of jamming attack) on synchrophasor based applications is investigated in [31]. As mentioned in [31], if PMU loses its GPS signal, this results in erroneous time-stamp calculations which lead to the wrong synchrophasors computations. This ultimately results in corrupted power system monitoring & control results.

In [32], the impact of time synchronization spoofing attacks on synchrophasor-based monitoring, protection and control applications has been extensively discussed. It was identified in [32] that the current PMUs lacks the functionalities to identify between authentic and spoofed time signals. This makes current PMU device to be highly vulnerable to cyber-attacks.

5.2.4 Digital Investigation of SEL-421 PMU

From [32], it can be concluded that, currently, PMU device is not smart enough to detect any cyber attacks on GPS signal (signal loss & data spoofing). In this paper, SEL-421 PMU device [33] is selected for a analysis in order to investigate the current shortcomings and limitations of this device for forensic analysis in case of any cyber attack. The data logs in a device are very important for its forensic analysis.

Figure 5(left) shows a snapshot of SEL-421 configuration software called SEL acSELerator QuickSet [34]. SEL-421 device is equipped with some nice data logging features. There are different triggers to capture data in the SEL-421 which are Relay Word bit TRIP assertions, SELOGIC® control equation ER (Event Report Trigger) and TRI command. The two main log sources we can consider as the connection log created using Terminal logging as well as the Sequential event Recorder (SER).

The connection log records all communications between the relay and the PC. On the other hand SER captures and time-tags state changes of Relay Word bit elements and relay conditions. These conditions include power-up, relay enable and disable, group changes, settings changes, memory overflow, diagnostic restarts, and SER auto-removal/ reinsertion. Figure 5(right) shows a snapshot about how to use data logging functionality in SEL-421 using its configuration software.

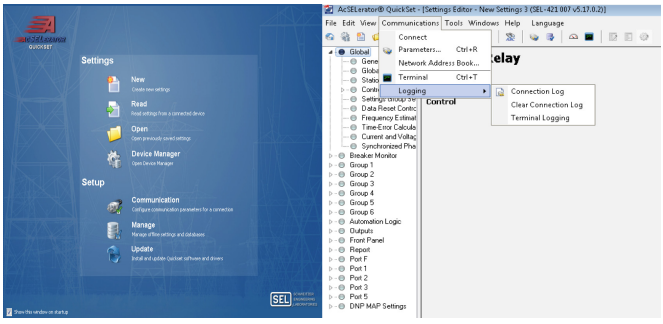

Fig. 5. Left: a snapshot from SEL-421 configuration software and Right: data logging functionality using SEL-421 configuration software [30]

The size of the event report length in SER affects the number of records available. With SEL-42 recorded events can range from 4 to 239 events before they get over-written again. Hence valuable information for an attack might be lost if it is not backed up. Moreover, the data logs available in SEL-421 device do not help in providing any notification or indication of any cyber attack. This leads us to a conclusion that current PMU technology is not forensically ready for digital investigation in case of any attacks.

6 Conclusions and Future Work

Having studied these devices for forensic purpose, it is evident that these devices are not forensic ready and there are no established methods that could be utilized to help in their forensic investigation.

As a future work, we intend to create a series of experiments in increasing complexity to measure the forensic readiness of SCADA controls. Following are the main points for the future work that we intend to perform:

- Development of a small suite of tools to extract and analyze the evidence from individual components of the SCADA network
- Creating a set of experiments with a base configuration to measure the forensic readiness of SCADA controls
- Using different configurations to measure the variance in results
- We'll document the experiments and their results, and based on the outcomes propose a set of recommendations to create a benchmark for SCADA forensic readiness.

Acknowledgment. This work has received funding from the Swedish Civil Contingencies Agency (MSB) through the research center Resilient Information and Control Systems (RICS).

References

1. U.S. General Accounting Office: Cyber security guidance is available, but more can be done to promote its use (2011). http://www.gao.gov/assets/590/587529.pdf
2. Alcaraz, C., Zeadally, S.: Critical infrastructure protection: requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. **8**, 53–66 (2015)
3. U.S. Department of Homeland Security: What is critical infrastructure? (2016). https://www.dhs.gov/what-criticalinfrastructure
4. Critical infrastructure sectors (2016). https://www.dhs.gov/critical-infrastructure-sectors
5. KTH Royal Institute of Technology (2013). Viking: https://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/proj/v/viking-1.407871
6. Trend Micro Incorporated: Report on cybersecurity and critical infrastructure in the americas (2015). http://www.trendmicro.com/cloudcontent/us/pdfs/securityintelligence/reports/critical-infrastructures-west-hemisphere.pdf
7. SANS ICS: Analysis of the cyber attack on the Ukrainian power grid (2016). https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
8. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**(3), 49–51 (2011)
9. CESG National Technical Authority for Information Assurance: Good practice guide: Forensic readiness (2015). https://www.cesg.gov.uk/content/files/guidancefiles/Forensic%20Readiness%20(Good%20Practice%20Guide%2018)1.2.pdf
10. Ammann, R.: Network forensic readiness: a bottom-up approach for IPv6 networks. Ph.D. dissertation, Auckland University of Technology (2012)
11. Sule, D.: Importance of forensic readiness (2014). http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx
12. Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., Stoddart, K.: A cyber forensic taxonomy for SCADA systems in critical infrastructure. In: Rome, E., Theocharidou, M., Wolthusen, S. (eds.) CRITIS 2015. LNCS, vol. 9578, pp. 27–39. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-33331-1_3
13. Cook, A., Nicholson, A., Janicke, H., Maglaras, L.A., Smith, R.: Attribution of cyber attacks on industrial control systems. EAI Endorsed Trans. Indust. Netw. Intellig. Syst. **3**(7), e3 (2016). https://doi.org/10.4108/eai.21-4-2016.151158
14. van der Knijff, R.M.: Control systems/SCADA forensics, what's the difference? Digit. Invest. **11**(3), 160–174 (2014). https://doi.org/10.1016/j.diin.2014.06.007. ISSN 1742-2876
15. Etalle, S., Gregory, C., Bolzoni, D., Zambon, E.: Self-configuring deep protocol network whitelisting. Security Matters (2013). http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_ics_EU.Pdf

16. Pauna, A., May, J., Tryfonas, T.: Can we learn from SCADA security incidents? – ENISA, 09 October 2013. https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents
17. Ahmed, I., Obermeier, S., Naedele, M., Richard III, G.G.: SCADA systems: challenges for forensic investigators. Computer **45**(12), 44–51 (2012). https://doi.org/10.1109/mc.2012.325
18. Wu, T., Pagna Disso, J.F., Jones, K., Campos, A.: Towards a SCADA forensics architecture. In: Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, pp. 12–21 (2013)
19. Fabro, M., Cornelius, E.: Recommended practice: creating cyber forensics plans for control systems. DHS Control Systems Security Program (2008). https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf. Accessed 15 May 2017
20. Iqbal, A.: [Extended Abstract] Digital Forensic Readiness in Critical Infrastructures: Exploring substation automation in the power sector. Stockholm (2017). http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-209689
21. Kilpatrick, T., Gonzalez, J., Chandia, R., Papa, M., Shenoi, S.: An architecture for SCADA network forensics. In: Olivier, M.S., Shenoi, S. (eds.) DigitalForensics 2006. IAIC, vol. 222, pp. 273–285. Springer, Boston, MA (2006). https://doi.org/10.1007/0-387-36891-4_22
22. Valli, C.: SCADA forensics with Snort IDS. In: Proceedings of the 2009 International Conference Security and Management (SAM 2009), pp. 618–621. CSREA Press (2009)
23. Sohl, E., Fielding, C., Hanlon, T., Rrushi, J., Farhangi, H., Howey, C., Carmichael, K., Dabell, J.: A field study of digital forensics of intrusions in the electrical power grid. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC 2015), pp. 113–122. ACM, New York (2015)
24. CVE Details, Security Vulnerabilities, Promotic. https://www.cvedetails.com/vulnerability-list/vendor_id-649/product_id-22225/Microsys-Promotic.html
25. Hunt, R., Slay, J.: Achieving critical infrastructure protection through the interaction of computer security and network forensics. In: 2010 Eighth Annual International Conference on Privacy Security and Trust (PST), pp. 23–30. IEEE (2010)
26. Langner, R.: Robust Control System Networks: How to Achieve Reliable Control after Stuxnet. Momentum Press, New York (2011)
27. IEEE C37.118.1-2011: IEEE Standard for Synchrophasor Measurement for Power Systems
28. NASPI Technical Report: Time Synchronization in the Electric Power System, USA, March 2017. https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf
29. IEEE Standard for Synchrophasor Data Transfer for Power Systems. In: IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005), pp. 1–53, 28 December 2011
30. Beasley, C., Zhong, X., Deng, J., Brooks, R., Venayagamoorthy, G.K.: A survey of electric power synchrophasor network cyber security. In: IEEE PES Innovative Smart Grid Technologies, Europe, Istanbul, pp. 1–5 (2014)
31. Almas, M.S., Vanfretti, L.: Impact of time-synchronization signal loss on PMU-based WAMPAC applications. In: 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, pp. 1–5 (2016)
32. Almas, M.S., Vanfretti, L., Singh, R.S., Jonsdottir, G.M.: Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing. IEEE Trans. Smart Grid **8**(99), 1 (2017)
33. SEL: Protection Relays by Schweitzer Engineering Laboratories. https://selinc.com/products/421/
34. SEL-5030 acSELerator QuickSet Software. https://selinc.com/products/5030/