Secure Cyber: Modelling Physical Impact of Cyber Attacks over Cyber Physical System Network

Mohammad Shahir, Suhaimi Ibrahim
Advanced Informatics School, UTM

Abstract

To increase reliability and remote operation capability, automated control based on SCADA systems were introduced in the electrical grid. This exposed the grid to cyber-attacks which, due to the cyber-physical nature of the combined system, can cause physical damage such as power outages. This dual nature makes it hard for grid operators to evaluate the physical impacts of cyber-attacks. To do so, we introduce a modification of the ICS sandbox architecture to perform impact assessment of cyber-attacks. This is done by interfacing the emulated SCADA network with the PyPower SCADA simulator which provides global information about the state of the electrical grid. Finally, to demonstrate the effectiveness of the system, a cyber-attack based on an optimal disruption experiment is run and its effects in terms of operation cost are graphed in real time.

1. Introduction

The electrical grid used to be a purely physical system governed by the physical principles of electricity. However, the drive for increased performance and resiliency of systems introduced a complexity that made the grid increasingly difficult to operate without some form of automation. Consequently, remote operation of electrical equipment, and eventually even automated control of the grid, was introduced, allowing faster response time to failures and increased ability to operate at peak efficiency. Unfortunately, with this increase in reliability and efficiency came increased risk. To enable automation and remote control, Industrial Control Systems (ICS) operators turned to Supervisory Control and Data Acquisition (SCADA) networks to collect telemetry and allow remote control. For a while, these systems were relatively safe, even though riddled by cyber vulnerabilities as Cardenas et al. [1] point out, because they were located on isolated networks. However, for cost saving purposes, SCADA systems eventually migrated to TCP/IP and interconnected networks where there is a wealth of cyber attacker knowledge and proficiency.

A number of cyber attacks have targeted SCADA systems. Because of the cyber-physical nature of SCADA networks, these attacks eventually caused physical damage. In 2000, sewage was dumped in drinking water at the Maroochy water plant [2]. Detected in 2010, the Stuxnet virus sabotaged uranium enrichment and the machinery used in that task [3]. In 2013 attackers modified the operating parameters of what they believed was city water systems [4]. Those same hackers are responsible for multiple attacks on targets in the energy sector [5], including a supplier of SCADA equipment and software [6]. There is little doubt that cyber attackers are targeting these systems not just for the sake of hacking them, but for the express purpose of causing physical damages. For defenders, it is hard to be able to gauge the physical risk associated with a cyber attack. We need a way to provide impact assessment in a metric that makes sense to utility operators such as quantity of energy delivered or cost of operations rather than number of machines rooted. This requires a modelling of the interaction between the physical portion of the electrical grid and the cyber component.

This paper presents an adaptation of the ICS sandbox [7] to perform impact assessments of cyber attacks. We start by presenting background information about SCADA systems and cyber impact assessment in SCADA network. We then present our adaptation of the ICS sandbox to perform impact assessments. Finally, we present and discuss the results obtained from this adaption and we offer a brief conclusion.

2. Background

To fully understand the complexity of modelling the physical impacts of cyber attacks, we must first grasp how the cyber physical nature of electrical grids manifests itself and see how other researchers have attempted to tackle the problem. This section offers a brief overview of the role of SCADA systems in the electrical grid and shows how their use transforms the grid in a cyber physical system. Then, a brief review of how researchers have tackled the problem of impact assessment in interdependent and SCADA systems is presented.

2.1. SCADA as a cyber-physical system

The electrical grid is quickly becoming too complex to be operated manually. The strong trends toward micro-generation, electric vehicles and adaptive pricing are expected to increase rather than reduce this complexity. It is no wonder that utilities are turning toward automated control of the electrical grid. The tool used to implement this automated control is Supervisory Control and Data acquisition (SCADA) networks. These networks are designed to provide remote telemetry (data acquisition) and allow for remote operation of active elements such as breakers, relays and set-point controllers (supervisory control). Using the SCADA system, an operator can estimate the state of the electrical grid and, based on that estimation evaluate the alterations required to that state for the grid to behave optimally. These alterations can be translated in a series of desired states for individual active elements. Commands can then be issued to those elements through the supervisory command element of SCADA. Figure 1 summarizes that control loop for the power grid.

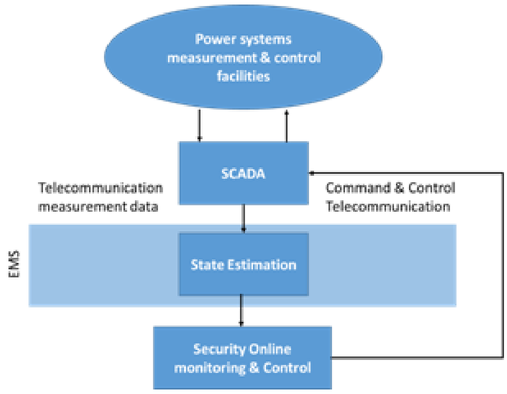
Power systems measurement & control facilities
SCADA
Telecommunication measurement data
Command & Control Telecommunication
EMS
State Estimation
Security Online monitoring & Control

Figure 1. Power grid control loop (adapted from [8])

Naturally, the grid is a complex system. As such, the description of its state is also relatively complex. To do so, measurement devices are installed all over the electrical grid. These devices collect the telemetry for the SCADA network and are named measurement points. Similarly, in order to achieve the granularity of control required to alter the state of the grid, a number of devices are installed on the active elements of the grid to allow for remote control. These are called control points. The basic control loop used to control the electrical grid can then be illustrated as shown in Figure 2.

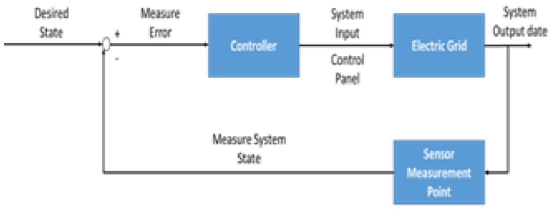

Figure 2. Power grid control loop

Although the SCADA network is a cyber system, it acts as the control loop for the electrical grid, and its state has direct impact on the state of the physical system. On the other hand, because the content of the network traffic depends on the state of the electrical grid, the physical component also has a direct influence on the cyber system. This creates a cyber-physical system whose behaviour is very hard to study by considering each component in isolation.

2.2. Studying the impact of cyber attacks

The fact that the electrical grid and its SCADA system form a cyber-physical system implies that the cyber and the physical component are interdependent infrastructures. An alteration in one system will affect the other. The modeling of impacts of large-scale events such as natural disasters in interdependent infrastructure is an ongoing field of study in the discipline of critical infrastructure protection. A major cyber attack on the SCADA network, where malicious individuals could alter the state of the electrical grid on a massive scale, would fall in the same event category as a natural disaster. A number of techniques are used to estimate impact in such scenarios. For example, the modeling of input/outputs introduced by Haimes et al. [9] and Aung and Watanabe [10] or the modeling of exchanged resources described by Robert and Morabito [11]. However, when considering SCADA systems where hundreds or thousands of measurements and commands are exchanged every second, these models soon become too unwieldy for simulation.

A number of researchers in computer security have attempted to evaluate the impact of cyber attacks on SCADA systems. For example, Fovino and al. [12] have attempted to study the impact of malware designed to cause damage in SCADA systems. To do so, they modeled a power plant based on observations made at a real-world site and created a testbed. Unfortunately, they did not model their attacks with the same level of fidelity, opting to emulate the attacks with a mobile agent simulator that replicates the behaviour of malware. While this level of fidelity may be adequate to draw some conclusions about network data, the observed metrics focus on system-level (with the exception of the minimal DDoS case study) with no evaluation of the impact of the implementation of their malware model or the middleware required to run their mobile agent. For example, they noticed that none of the worms they attempted to reproduce caused a system failure. It is impossible to tell if this is the result of resiliency in the SCADA network or the result of their malware simulator not interacting with the systems in the same way real malware would, perhaps locking up a thread, consuming all of the memory, modifying network paths and so on.

Another attempt by Sridhar [13] was made to assess impact of integrity attacks on SCADA systems. This study creates an analytical model of the attacks and integrates those attacks in a generic power flow balancing methodology. The assumption is that an operator would follow the methodology, come to an erroneous conclusion about the state of the system and perform an action that is contrary to his interests. A simulation is then constructed based on the analytical model to show that the analytical model performs as expected. Unfortunately, there is no validation of the model and the model seems to present serious limitations at first glance. Notably, there is no feedback loop that creates an electrical network effect based on the reaction of the operator. For example, if an operator is tricked into activating a breaker, the power flow will be diverted on other lines and this will trigger new measurements that are based on the ground truth and not on the falsified report. This would require the attackers to recompute the expected values for their falsification software faster than the actual system converges. At the same time, the power of the attacker is underestimated. In their model, an attacker can only set a sensor to the minimum or maximum value of the sensor for a limited amount of time where in reality an attacker can send arbitrary values (even impossible ones) for an unlimited amount of time if he obtains administrative access to a machine.

The team of Bobbio and al. [14] have also attempted to study the impact of DDoS attacks on the SCADA network. Unlike Sridhar [13], the attack model is very detailed and is based on an actual failure scenario. The network model is also very detailed because it is based on the actual systems. However, the study focuses only on the network effects of the DDoS attack on the telco network. While the delay between the different SCADA nodes is calculated, we have no indication of how this delay affects SCADA traffic, if any critical packets are dropped or if operations are impaired in any way. In that sense, while the data might be useful for someone with a SCADA test bed to calibrate the network traffic generated by an attack, it provides little insight on its own.

3. Modelling

Because there is no approach that allows us to inject a cyber attack and directly observe its physical impact in the literature, a new experimental approach must be devised. This section presents how the ICS sandbox was adapted to enable impact assessment of cyber attacks. It starts by presenting the attack scenario that will serve as the proof of concept. Then, it details the modifications that were required to the ICS sandbox. Finally it presents the chosen control scheme for the IEEE reliability test system (IEEE-rts) and justifies the use of an Optimal Power Flow (OPF) solver as a proxy for automated energy management.

3.1. Attack scenario

The first step is to establish a scenario for the attacker's goals in terms of physical impact for the cyber attack. Salmeron et al. [15] analyzed the resiliency of the electrical grid to terrorist attacks. The goal of their paper was to identify critical components of the electrical grid by evaluating how terrorists could maximize their damage with a given set of resources. In their words, they strive to identify critical sets of a power grid's components [...] by identifying maximally disruptive, coordinated (nearly simultaneous) attacks [...] which a terrorist group might undertake. Because they are uncertain of what kind of resources a terrorist group might possess, they consider a range of capabilities. However, they only consider physical destruction and assume that it is impossible for the group to perform cyber attacks on the SCADA system.

However, the same effects can be achieved with a cyber attack. Gaining remote access on a server and then leveraging that access to shut down a breaker will have the same physical effect as disabling a line through explosive, i.e. the line is unavailable to transmit energy. Therefore, we can use the findings for optimal attacks as a template for the attacker's goals.

Among their findings, Salmeron et al. identify two interdiction plans for the single IEEE reliability test system. The two "near-best" plans, are illustrated in Figure 3. In the first plan, the main substation, interconnecting buses 9, 10, 11 and 12 is destroyed and a number of lines (both lines of branch 15-21, branch 16-17 and both lines of branch 20-23) are cut. In the second plan, only lines are cut (branch 7-8, branch 11-13, branch 12-13, branch 12-23, both lines of branch 15-21, branch 16-17 and both lines of branch 20-23). Of these two plans, plan 2 sheds slightly more load (1373 MW compared to 1258 MW), but plan 1 is identified as being the most severe. This analysis is based on the destruction of the substation in plan 1 which is dubbed more difficult to repair than the line cuts in plan 2. The reasoning is that the cost in the entirety of the outage, measured in MWh, will be much higher if the impact in power is similar, but the time to repair is orders of magnitude larger.

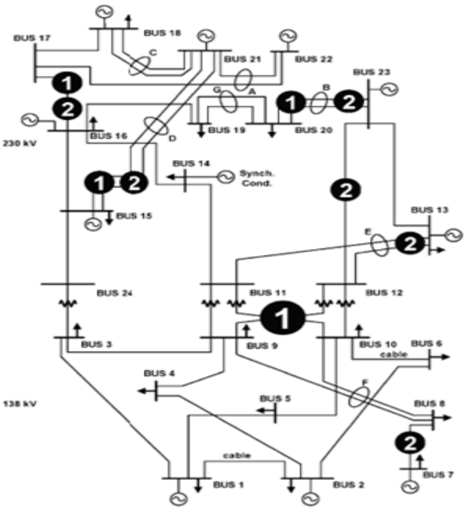

Figure 3. Interdiction (reproduced from [15] © 2004 IEEE)

3.2. Adapting the ICS sandbox

In order to observe the impacts shown in [15] in the context of a cyber attack, we need to compute the operation costs of the IEEE reliability test system under cyber perturbations. Using the black box approach of the ICS sandbox [7], it is possible to substitute the simulation system presented in the paper for a simulation system that can calculate the operation cost in addition to calculating the various electrical values. The resulting experimental system can now be operated in real time with actual SCADA components providing the cyber portion of the cyber-physical system and an electrical simulator replicating the state of the physical portion. PyPower [16], a python implementation of MATPOWER, provides built-in functionality to calculate power flows and operation costs using optimal power flow algorithms. In addition, PyPower includes an IEEE reliability test system class which provides us with an easy access to the various electrical components.

More importantly, because it is written in Python, it can easily integrate with other Python code, facilitating the construction of the interface between the cyber component emulated in the ICS sandbox and the physical component provided by the electrical simulation. So, for each SCADA field unit (RTU), we built a python communication program that enabled the RTU to update the value of its control points in the simulator. Because of this, the simulator can know the intended state of all controlled equipment such as breakers and set point interfaces. The simulator can then recalculate the electrical state of the system each time an RTU submits an update to its state. The results of this calculation are then passed back to enable the RTU to update the values of its measurement points such as voltmeters. Figure 4 shows the resulting architecture.

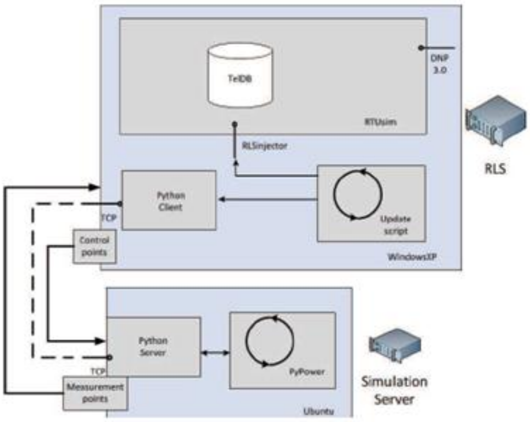

Figure 4. ICS Sandbox adapted with PyPower

While this architecture allows the mechanical integration of the ICS Sandbox with the PyPower simulator, we are still required to provide the integration between the SCADA components and the electrical components.

3.3. Control scheme for the IEEE-rts

The description of the IEEE reliability test system focuses on the electrical components and makes no mention of the control components. Therefore, we must extrapolate how a real world grid looking like the IEEE-rts would be instrumentalized and controlled.

To create a SCADA control scheme for the IEEE-rts, it was posited that the SCADA elements would reside in substations, with one RTU field unit per substation. Also, it was considered that each bus node represented a substation with the exception of the buses linked together by transformers, i.e. groups {bus 3,bus 24} and {bus 9, bus 10, bus 11, bus 12}. Each of those groups are considered to be a single substation.

The RTUs would have one measurement point recording the line voltage for each branch connected to that substation. Additionally, each branch would have a control point, representing a breaker that allows operators to isolate the line from that substation. This control point was linked to the status value of the branch object in PyPower. So, if an operator wanted to send the breaker into an "Open" value, the status value of the associated branch would be turned to 0 in PyPower and the line would be considered inoperable by the simulator. This integration of the simulator with the SCADA system effectively allows us to control the state of the electrical grid though the SCADA console and receive measurements based on that state from the simulator. This feedback creates a real cyber physical system where we can see the physical impacts, in terms of alterations in the state of the electrical grid, of cyber attacks and create experiments to assess these impacts without impacting the lives of customers.

3.4. Using OPF as a substitute for EMS

The test system’s electrical network description only lists the parameters of each piece of equipment. If we want to determine how power flows through the network, and what values the current and voltages phasors take on each element, we have to calculate the values based on those parameters and on the electrical network topology.

In real-world electrical grids, most of the operations are performed by automated systems. For example, Energy Management Systems (EMS) and Distribution Management Systems (DMS) might use the state estimation derived from SCADA measurements to balance the flow of power for the optimal operation of the grid. Unfortunately, these systems are very expensive and are not publicly available. A substitute to determine how energy would be distributed across the grid, given a particular state, must be found.

The power flow problem is defined as a numerical analysis tool aimed at determining the values in steady state of the various power metrics, for example voltage, voltage angle, current, current angle, real power and reactive power. This analysis is typically done on line diagrams such as the diagram of the IEEE reliability test system in Figure 3. In other words, starting from the one-line diagram, the power flow analysis attempts to find the power, voltage and current for all pieces of equipment. Additional information, such as the power distribution in buses and the voltage and current for branches is also available. This is considered the base case for power flow analysis.

To solve this base case, the numerical solution must follow a certain number of constraints. In his book section [17], Bacher presents a summary of the constraints needed to build a mathematical model for the simulation. Essentially, the following physical constraints must be met:

- Energy is conserved in all passive power elements
- Kirchoff's law of current (the sum of all currents in a node must be equal to zero) is met at all circuit nodes.
- Ohm's law (power-voltage-current relationship) is met for all elements

Additional constraints based on real-world operating tolerances for the equipment may also be enforced. For example, a line may not exceed its base operating voltage by more than 5%.

For the majority of systems, there is more than one solution that meets all the constraints. For example, in the updated IEEE reliability test system, there is about 20% excess generation capacity compared to the total load. This means that there is a number of generation configurations that can meet demand. In order to satisfy conservation of energy constraints, some sources must be turned off. The base case power flow analysis does not discriminate between the solutions and returns a numerical solution that fits the constraints. The optimal power flow (OPF) analysis finds the solution which meets the constraints at the lowest cost. The costs are calculated based on parameters provided by the operator. For example, in the case of the IEEE reliability test system, the costs are calculated from generation parameters attributing to each source a cost per unit of power produced based on the type of power plant it emulates.

In a sense, this mimics the behaviour of a system under the control of an automated EMS and DMS that manage the grid to ensure reliability and minimize costs. So, even in the absence of these systems, the numerical values provided by an OPF calculation can be assumed to be similar to those of a grid with automated control based on a cost minimization discipline.

However, there is a significant exception. Because EMS and DMS rely on state estimation derived from SCADA measurements, it would be possible for an attacker to provide false measurements and confuse the automated state estimator. In that case, the behaviour of an OPF calculation would greatly differ from the automated control calculations. This kind of attack is out of scope for this particular experiment.

4. Results

With the ICS sandbox configured to match the IEEE reliability test system, only the operation of the SCADA controls is required to affect the state of the test system. The effects of the scenario from Salmeron et al. [15] can now be reproduced with cyber attacks. Unfortunately, while the effects can be reproduced, it is not possible with the current implementation to fully reproduce the results. Salmeron et al. report the results of their maximally disruptive attacks in terms of amount of load shed. The PyPower simulator description of the IEEE reliability test system does not natively support load shedding. This immediately causes a problem for the evaluation of the highly disruptive attacks offered by Salmeron et al. The paths between sources and loads are cut and the system does not possess sufficient transport capacity to service all the loads.

This prevents the finding of a solution that fits all of the model's constraints. We could engineer a load shedding discipline, but, in the absence of data of how this would be accomplished on the IEEE-rts, we preferred to present the partial results which violate constraints instead. To do so, it is possible to track the generation costs in real time and estimate the damage of the attacks in terms of increased generation cost. Because the generation cost is tracked in real time, the effect of each interdiction can also be seen as it happens, allowing the evaluation of the impact of each interdiction separately. In a normal cyber context, it would also be easy for the attacker to perform all the interdictions at the same time, but it was deemed preferable to allow for a delay between each interdiction to see the individual effects. This delay, however long in the scale of cyber attacks, is negligible compared to the ability of even the best terrorists to coordinate physical attacks.

In theory, the order of the interdiction influences the individual effect of an interdiction. For example, a break in a line might have little effect if the grid is in a relatively stable state. However, that same break might have disastrous consequences if the grid is already overloaded from previous failures. In practice, because the impact of individual interdictions in this experiment is only provided in a proof-of concept framework, the choice of order has little bearing on the validity of the results. So, we adopt the following arbitrary ordering of interdictions:

1. Interdiction of the transformer in substation 9 to 12
2. Interdiction of both lines from branch 15-21
3. Interdiction of the line from branch 16-17
4. Interdiction of both lines from branch 20-23

The generation cost of the optimal power flow in the face of these interdictions is presented in Figure 5.

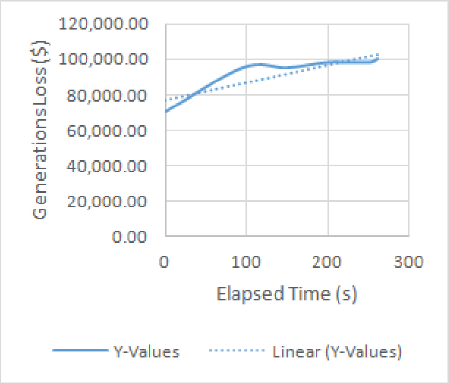

Figure 5. Financial impact of the interdiction plan

The effects of the loss of the transformer at around 75s can be clearly seen, imposing a $30,000 burden on generation costs. The significance of the loss is easily grasped because the loss of the transformer substation severely limits the transport capacity between the 138 kV and 230 kV portion of the IEEErts grid. This, in turn, reduces the ability of the high production generators in the 230 kV section to deliver power to the majority of the loads in the 138 kV section. The loss of the 15-21 branches around the 150 second mark has a smaller impact of around $3,000 and further losses of branch 16-17 and branches 20-23 also produce impacts of similar magnitudes. Effectively, the sum of these attacks splits the grid in three smaller networks, isolating the majority of the production capacity in a small portion of the grid with little load. These attacks have a smaller impact because the loss of the transformer substation already significantly reduced the ability to move power to the majority of loads.

Apart from the transients around the times of the interdictions due to the multi-threaded nature of the server, which may cause race conditions in the state of the system, the generation cost graph follows a strictly increasing cost curve as we would expect from mounting damages in the wake of the subsequent interdictions of an increasing amount of transport capacity. In that sense, we can assess that we can successfully track the impact of the cyber attack in terms of increased production costs.

5. Conclusion

By adapting the ICS sandbox with PyPower for the calculation of the optimal power flow, it was possible to estimate in near-real time the state of the power grid and the generation cost associated with that state. By creating a control scheme and instrumenting the simulated grid with SCADA equipment, it was possible to replicate the optimal disruption attacks proposed by Salmeron et al. [15] using cyber commands. Using this, the cost increase in generation cost, which represents the physical impact of the damage, can now be tracked. This leads to the conclusion that this approach presents a valid method to perform impact assessment of cyber attacks on the electrical grid's SCADA system.

This ability to model the physical damage of cyber attacks will allow defenders to accurately evaluate the actual risk involved with cyber attacks using easy to understand metrics such as delivered power or generation costs. Using this method, a number of new research problems can be tackled. In particular, investigations of other kinds of cyber attacks or investigation on networks other than the IEEE reliability test systems are identified as interesting avenues of research. Alternatively, improvements in the granularity of the simulation model by using a more complex electrical model or by introducing elements of automated control would also present interesting questions for future work.

6. Acknowledgement

This research is funded by the Research University grant of Universiti Teknologi Malaysia (UTM) under the Tier1-Vot no. 12H66. The authors would like to thank the Research Management Centre of UTM and the Malaysian ministry of education for their support and cooperation including students and other individuals who are either directly or indirectly involved in this project.

7. References

[1] A. A. Cardenas, S. Amin and S. Sastry, "Research Challenges for the Security of Control Systems," in 3rd USENIX Workshop on Hot Topics in Security (Hotsec 2008), San Jose, 2008.

[2] S. Jay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in Critical Infrastructure Protection, vol. 253, Boston, Springer, 2007, pp. 73-82.

[3] N. Falliere, L. O. Murchu and E. Chien, "W32.Stuxnet Dossier Version 1.4," Symantec Security Response, 2011.

[4] T. Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," 2 August 2013. [Online].Available: http://www.technologyreview.com /news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/ .[Accessed 10 October 2013].

[5] Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units," February 2013. [Online]. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [Accessed 8 August 2013].

[6] B. Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," Krebs on Security, 26 September 2012. [Online]. Available: http://krebson security.com/2012/09/chinese-hackersblamed-for-intrusion-at-energy-industry-giant-telvent/ [Accessed 8 August 2013].

[7] A. Lemay, J. Fernandez and S. Knight, "An isolated virtual cluster for SCADA network security research," in 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013), Leicester, 2013.

[8] M. Shahidehpour and Y. Wang, "Communication and Control in Electric Power Systems:Applications of Parallel and Distributed Processing," Wiley-IEEE Press , 2003, pp. 26,307-348,.

[9] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian and K. G. Crowther, "Inoperability Input-Output Model forInterdependent Infrastructure Sectors. I: Theory and Methodology," ASCE Journal of Infrastructure Systems, vol. 11, no. 2, pp. 67-79, 2005.

[10] Z. Z. Aung and K. Watanabe, "A Framework for Modeling Interdependencies in Japan's Critical Infrastrucure," in Critical Infrastructure Protection III, Boston, Springer, 2009, pp. 243-257.

[11] B. Robert and L. Morabito, "The operational tools for managing physical interdependencies among critical infrastructures," International Journal of Critical Infrastructures, vol. 4, no. 4, pp. 353-367, 2008.

[12] I. N. Fovino, A. Carcano, M. Masera and A. Trombetta, "An experimental investigation of malware attacks on SCADA systems," Infrastructure Protection, vol. 2, no. 4, pp. 139-145, 2009.

[13] S. Sridhar and G. Manimaran, "Data Integrity Attacks and their Impacts on SCADA Control System," in 2010 IEEE Power and Energy Society General Meeting, Minneapolis, 2010.

[14] A. Bobbio, G. Bonanni, E. Ciancamerla, R. Clemente, A. Iacomini, M. Minichino, A. Scarlatti, R. Terruggia and E. Zendri, "Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network," Reliability Engineering & System Safety, vol. 95, no. 12, p. 1345–1357, 2010.

[15] J. Salmeron, K. Wood and R. Baldick, "Analysis of Electric GridSecurity Under Terrorist Threat," IEEE Transactions on power systems, vol. 19, no. 2, pp. 905-912, 2004.

[16] R. Lincoln, "GitHub repository for rwl/PYPOWER," GitHub, November 2012. [Online]. Available: https:// github.com/rwl/PYPOWER [Accessed 01October 2013].

[17] R. Bacher, "Optimization in Planning and Operation of Electric Power Systems," Physica-Verlag (Springer), pp. 217-264, May 1993.