Mission Impact Modeling in Power Grids

Mona Lange[1], Marina Krotofil[2], Ralf Möeller[1]
Universität zu Lüebeck[1]
Germany

European Network for Cyber Security[2]
Netherlands

ABSTRACT

A high number of low-level alerts are reported by information security systems . This justifies the interest in gathering and aggregating data from various sources. Subsequently, we propose an approach that correlates security events to detect upcoming cyber threats and determining the impact of these cyber threats. The proposed mission impact assessment (MIA) approach allow event correlation, the recognition of mission threatening events and computing the impact of this event. An offline component that develops a network dependency model by learning a state machine from network traffic captures. Additionally, a dependency model of the power grid is modeled to allow the analysis of cyber-physical impacts. This allows the analysis of how cyber events might impact the ongoing mission on an operational level.

1.0 INTRODUCTION

SCADA systems can be found in critical infrastructures such as electrical, gas and water distribution system, building monitoring in railway stations and airports, production systems for food, cars, ships and other products. Yet, Dell's annual threat report states a 100% increase in SCADA attacks [22]. This report is based on analysis of data gathered by Dell's global response intelligence defense network that consists of millions of security sensors in more than 200 countries. Hence we conclude that current critical infrastructures are not sufficiently protected against cyber threats. Critical infrastructures are cyber-physical systems that connect supporting IT infrastructure with systems interacting with the real world. To underpin this statement we refer to the director Sean McGurk of the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security [23]:

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

On an operational level an electrical grid is a network of power providers and consumers that are connected by transmission and distribution lines. Hence, the mission of an electrical power grid is to deliver electricity from suppliers to consumers. For monitoring purposes, they are additionally connected to IT infrastructures. In the past power system IT infrastructures used to be isolated, stand-alone systems. However, they are increasingly integrated with other IT infrastructures at power utilities, including public infrastructures in order

to increase business efficiency and effectiveness and reduced operational costs. Especially, the development of trustworthy smart grid requires a deeper understanding of potential impacts resulting from successful cyber attacks. Estimating feasible attack impact requires an evaluation of the grid's dependency on its cyber infrastructure and its ability to tolerate potential failures. In the following, we define physical tasks in the context of power grids as all tasks that strictly rely on physical power grid components and their local power applications. In the context of this work the understanding of what constitutes a mission is analog to Barreto [24]. In order to understand the significance of a cyber event for a mission requires mapping physical tasks to their supporting infrastructure. This allows an integrated view of cyber and physical behavior.

The rest of this paper is organized as follows: Section 2.0 describes related research of Mission Impact Models and critical infrastructure analysis. Section 3.0 explains how the underlying network model that is based on the internet layer of the internet protocol suite. The power grid model is provided in section 4.0. The overall integration of all these models is specified in section 6.0 and lastly experimental results are reported in section 7.0.

2.0 RELATED RESEARCH

Related research can be divided into research of Mission Impact Assessment (MIA) and critical infrastructure analysis.

2.1 Mission Impact Model

The concept of MIAs was developed in military research and is sometimes also referred to as mission-centricity in cyber security. [25], [26], [27] and [28] all propose distinct mission-centric approaches to cyber security. [29] proposed a framework for cyber attack modeling and impact assessment in order to allow risk analysis by generating attack graphs and calculating security metrics. Another approach was proposed by [30], who conceptualized mission-centric cyber-security as a convex optimization problem.

2.2 Critical Infrastructure Analysis

Before considering protective measures for critical infrastructures, it is necessary to understand the functioning of an infrastructure and identify critical processes. This is why infrastructure analysis is crucial in the context of this work. [31] analyzed dependency aware integration of Cyber-Physical Systems in smart homes. [32] researched how risk and system theory apply to critical infrastructure vulnerabilities and how can to quantify them applied to water systems.

[33] proposed CANDID, which is a framework for the classification of assets in networks by determining their importance and dependencies. Prior work includes [34], who proposed a methodology for modeling complex infrastructures, [35], [36] and [37], who all analyzed and modeled interdependence in critical network infrastructures.

3.0 NETWORK MODEL

To model the connectivity of the network on the internet layer, we parse router configuration files. The data model that the router configuration is parsed into is exemplified in table 1. In this data schema, we list all possible next-hops of a subnet and specificy what subnet devices are eligble to connect through a specific next-hop. This allows us to derive the underlying connectivity of the network and automatically update this network

Table 1: Router configs are parsed into this data schema before deriving the network model.

via	dev		
ip-address	subnet	device name	ip-address
	subnet	device name	ip-address
	subnet	device name	ip-address

model. Router configuration files are text files, containing device names, subnetworks and next hops of these devices. The network model N represents this information as follows:

$$N = (Q, \Sigma, \delta, q_0, M, F), where \tag{1}$$

- Q is a set of states,
- Σ is a finite set of input symbols,
- $\delta \subseteq Q \times \Sigma \times Q$ is a state transition function,
- $q_0 \in Q$ is a start state,
- $M \subset Q$ is a set of mission-critical states and
- $F \subset Q$ is a set of acceptance states.

In this model, network devices correspond to states and consist of an subnet that the device belongs to, an ip-address and a device name. Communication devices ("Next-hops") that other network devices are able to connect to are contained in the set Σ. The transition function δ models a connection from one network device to another.

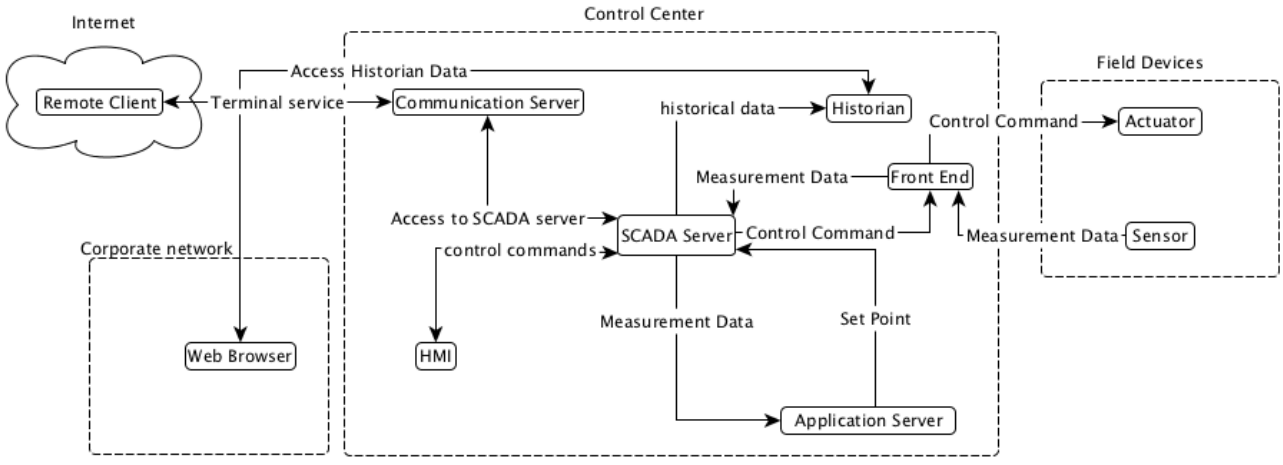

Figure 1: Routine operations within an electrical communication network

4.0 NETWORK DEPENDENCY MODEL

The network is represented as a Probabilistic Mealy Automata (PMA) where a network device corresponds to a state. Communication between network devices (or states) eventually through a specific port, corresponds to an edge This is a simple concept that is well-established in the theory of computation.

A probabilistic Mealy automaton M is a tuple

$$M = (Q, \Sigma, \Delta, \delta, p, h, \lambda, q_o), \tag{2}$$

where

- Q is a set of states,
- Σ is a finite set of input symbols,
- Δ is a finite set of output symbols,
- $\delta \subseteq Q \times \Sigma \times Q$ is a state transition function,
- $p : Q \times \Sigma \times Q \to [0, 1]$ asigns a occurance probability to state transitions,
- $h : Q \times \Sigma \to [0, 1]$ asigns a probability of halting in the same state,
- $\lambda : Q \times \Sigma \times Q \to \Sigma \times \mathbb{N}$,
- $q_0 \in Q$ is a start state.

For a state q the probabilities of halting h and moving on p sum up to 1. This can be written as

$$h(q) + \sum_{a \in \Sigma, q' \in Q} p_m(a, q'|q) = 1, \forall q \in Q. \tag{3}$$

4.1 Learning of the network dependency model

This network dependency model is learned from previously collected network flow data. An elemetary connection pattern is

$$\Phi^i = \phi_0 : \text{ip-address[:port]} \to \phi_1 : \text{ip-address[:port]}, \tag{4}$$

which represents the communication from source ϕ_0 to destination ϕ_1. To derive the network dependency model, we are interested to learn the response of ϕ_1. The response of ϕ_1 consists of an elemetary communication pattern that follows shortly after receving the first one and where the source address is ϕ_1. If this truely is a response to the previously observed elementary communication pattern than this sequence of events will frequently occur within the data set. We will denote the frequency of a pattern i as c_i. Let us assume that there are n distinct patterns that contain the same destination address. This allow us to compute the overall frequency of occurance $c = \sum_{i=0}^{n-1} c_c$. Then, we are able to compute the probability of a state transition occuring p and the probability of halting in the same state h with the entropy

$$H(c_i) = -\sum_{i=0}^{n-1} \frac{c_i}{c} log(\frac{c_i}{c}). \tag{5}$$

5.0 POWER GRID MODEL

5.1 Power Grid

The system state of the physical power grid may be written as

$$x = [V, \theta, P, Q], \tag{6}$$

with a vector of voltages V, a vector of voltage angles θ, a vector of active power P and a vector of reactive power Q. The vector of active power loads is denoted as P^l and the vector of reactive power loads Q^l. The vector of active power generators is denoted as P^g and the vector of reactive power generators Q^g. The difference between active and reactive power can be explained greatly simplified as reactive power being the power that continuously bounces back and forth between source and load. Active power is simply the product of Voltage across the load and Current flowing through. Active and reactive power are equally important for maintaining a continuous power supply. Active power is the energy required to deliver energy to the end user and allow the user to for example heat a home or run a motor. Reactive power allows the regulation of voltage. The role of voltage is that if voltage on the system is too low, active power cannot be supplied. Reactive power is essential to move active power through the transmission and distribution system to the customer.

As the components of the physical power grid are only operational within a particular value window, a separate vector inv collects operational constraints. These operational constraints define acceptable operational conditions that, if they are violated during a maximum period of time, lead to the corresponding power line being tripped. All constraints inv for the current system state x of all n states (as seen in Eq. 6) can be written as

- $\{x \in \mathbb{R}^n \quad | \quad Q_{min} > x \quad \vee Q_{max} < x \wedge \Delta t^Q\}$,
- $\{x \in \mathbb{R}^n \quad | \quad P_{min} > x \quad \vee P_{max} < x \wedge \Delta t^P\}$.

Among the controls collected within the vector is the maximum and minimal reactive power capabilities as Q_{max} and Q_{min}. If these constraints are violated for a period of time $\wedge\Delta t^Q$, the corresponding power line is tripped. Similarly, we denote maximum and minimum real power capabilities as P_{max} and P_{min} and the acceptable violation time span is defined as $\wedge\Delta t^P$. It follows from this that the power flow can be written as

$$f(x, inv) = 0 \tag{7}$$

representing the power injection at each node in the system. Equation 7 represents the physical power grid and can be broken into active f_i^p and reactive parts f_i^q for a particular bus i. This definition of the power grid closely follow the definition of the electrical power grid given in [38]. The active power injection P_i at bus i, which has N outgoing power lines, is described by

$$f_i^p = -P_i^g + P_i^l + \sum_{j=1}^{N} |V_i||V_j|(G_{ij}cos\theta_{ij} + B_{ij}sin\theta_{ij}) \tag{8}$$

and the reactive power injection Q_i at bus i is denoted as

$$f_i^q = -Q_i^g + Q_i^l + \sum_{j=1}^{N} |V_i||V_j|(G_{ij}sin\theta_{ij} - B_{ij}cos\theta_{ij}). \tag{9}$$

Whereas the variables B_{ij} denotes the imaginary part of the element of the bus admittance matrix defining the admittance between buses i and j. Likewise, G_{ij} denotes the real part of the element of the bus admittance matrix.

5.2 Hybrid Automaton

The previously introduced power grid is a switched continous system, hence it is modeled by a hybrid automaton. A hybrid automaton H is a collection

$$H = (Q, X, f, inv, E, R), \tag{10}$$

where

- Q is a set of discrete states,
- X is a set of continous variables,
- $f(x, inv) \rightarrow \mathbb{R}^n$ is a vector field,
- inv: $E \rightarrow P(X)$ are the guard conditions,
- E $\subseteq Q \times Q$ is a set of edges,
- R$(\cdot, \cdot) \rightarrow P(X)$ is a reset map.

The set of discrete states Q represents the number of buses multipled by the number outgoing power lines. State transitions between discrete states are due to violations of guard conditions inv, due to power line failure or a manual "trip line" request. The continous variables in set X are those mentioned in eq. 6. $P(X)$ denotes the set of all subsets (power set) of X. The vector field $f(x, inv) \rightarrow \mathbb{R}^N$ was already intruced in eq. 7, analog to the guard conditions inv. The reset map models a power line being reset after having been tripped before.

6.0 MISSION IMPACT MODEL

The overall infrastructure model I is the product

$$I = N \times M \times H \tag{11}$$

of all three network models:

- Network Model $N = (Q, \Sigma, \delta, q_0, M, F)$,
- Network Dependency Model
  $M = (Q, \Sigma, \Delta, \delta, p, h, \sigma, q_0)$ and
- Power Grid Model $H = (Q, X, f, inv, E, R)$.

This combined network model allows us to assess the impact of a reported network incident on the overall infrastructure. Let us assume that a network incident was reported on network device q_i. Evaluating the overall impact of this incident is now computing the probability of a Mission-critical device $m_j \in M$ depending on the network device n_i. Additionally, we can compute the impact on the power grid, if a cyber attacker where to reach a mission-critical device directly connected to it.

To compute the threat level that a network incident on device q_i posed to a mission critical device m_j, we assume q_i as a starting point in the product automaton in Eq.3. After assuming $q_i \in Q$ as start state, we are

interested to know whether any mission critical device $m_j \in M$ can be reached. Thus, we see computing the threat level as a reachability problem.

$$q_i \in Q \xrightarrow{*} \neg m_j \in M \tag{12}$$

In order to compute the likelihood of a cyber attacker reaching a mission-critical device, we than compute the shortest path between two network devices via Dijkstra's algorithm. As there can be more than one shortest path between two network devices in a large network, N_{ij} denotes the number of shortest paths. And for every possible shortest path,this computation gives us a set of network devices $D \subseteq Q$ and their corresponding probabilities p and h (if available).

If $N_{ij} = 0$ then the threat level t_{ij} of a mission critical device $m_i \in Q$ from a network incident that occurred on $q_i \in Q$ can be computed by

$$\tau_{ij} = \frac{\sum_0^{n-1} p}{D_{ij}}. \tag{13}$$

If $N_{ij} > 0$ then we compute τ_{ij} for all shortest maths and then average these values by computing

$$\tau_{ij}^{N_{ij}} = \frac{\sum_0^{N_{ij}-1} \tau_{ij}}{N_{ij}}. \tag{14}$$

7.0 EXPERIMENTAL RESULTS

The proposed mission impact model is tested within a cyber-physical testbed, based on the framework for power system and communication networks co-simulation FNCS [39]. The experiment is conducted using the IEEE 13-bus test system and the communication network is built based on topologies proposed in National Institute of Standards and Technologies - Guide to Industrial Control Systems (ICS) Security [40]. Using FNCS a communication network is built, based on the network simulator ns-3 [41]. The built communication network assumes that in every substation and within every control center a network based intrusion detection system is installed. The network based intrusion detection system relied on in the context of this work is snort [42].

An example for a cyber-physical attack that can be implemented and tested within this testbed is:

1) Due to a successful cyber-attack, the historian in the primary control center is infected with malware.

2) An ARP-scan causes an alert within the intrusion detection system installed in the primary control center.

3) Stealth NMAP scans with spoofed ip-addresses and mac-addresses raise multiple snort alerts.

4) Relay 2 reports an unsolicited request alert.

5) Due to a successful cyber attack, an attacker has control of relay 2.

6) Relay 2 enters a failure state and is unable to sends a message to the RAS controller.

7) As the generation in substation 2 is not reduced due to the cyber-attack, relay 3 reaches it maximum time period for withstanding thermal overload and trips.

8.0 CONCLUSION

Understanding the impact of events on cyber-physical systems, such as the smart grid, requires understanding the complex relationship between cyber-based control mechanisms and the physical system. This paper introduced a mission impact model to represent the connectivity of the network, network device dependencies and the power grid. The introduced approach requires little human input as the derivation of the network model and the network dependency model is based on learning based approach. Additionally, an attack template was provided, however more research effort will be required to evaluate the introduced mission impact model.

REFERENCES

[1] DELL, "Dell Security Annual Threat Report," https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf, 2015.

[2] Subcommittee on National Security, Homeland Defense, and Foreign Operations, "Cybersecurity: Assessing the Immediate Threat to the United States," 2011.

[3] de Barros Barreto, A., Costa, P. C. G., and Yano, E. T., "A Semantic Approach to Evaluate the Impact of Cyber Actions on the Physical Domain," *STIDS 2012 Committees*.

[4] Goodall, J. R., D'Amico, A., and Kopylec, J. K., "CAMUS: automatically mapping cyber assets to missions and users," *Military Communications Conference, 2009. MILCOM 2009. IEEE*, IEEE, 2009, pp. 1–7.

[5] Musman, S., Tanner, M., Temin, A., Elsaesser, E., and Loren, L., "Computing the impact of cyber attacks on complex missions," *Systems Conference (SysCon), 2011 IEEE International*, April 2011, pp. 46–51.

[6] Jakobson, G., "Mission cyber security situation assessment using impact dependency graphs," *FUSION*, 2011, pp. 1–8.

[7] Sawilla, R. E. and Ou, X., "Identifying Critical Attack Assets in Dependency Attack Graphs," *Proceedings of the 13th European Symposium on Research in Computer Security*, 2008, pp. 18–34.

[8] Kotenko, I. and Chechulin, A., "A Cyber Attack Modeling and Impact Assessment framework," *Cyber Conflict (CyCon), 2013 5th International Conference on*, June 2013, pp. 1–24.

[9] Vamvoudakis, K. G., Hespanha, J. P., Kemmerer, R. A., and Vigna, G., "Formulating Cyber-Security as Convex Optimization Problems," *Control of Cyber-Physical Systems*, Springer, 2013, pp. 85–100.

[10] Munir, S. and Stankovic, J. A., "DepSys: Dependency Aware Integration of Cyber-Physical Systems for Smart Homes," 2014.

[11] Ezell, B. C., "Infrastructure Vulnerability Assessment Model (I-VAM)," *Risk Analysis*, Vol. 27, No. 3, 2007, pp. 571–583.

[12] Marshall, S., *CANDID: Classifying Assets in Networks by Determining Importance and Dependencies*, Master's thesis, University of California at Berkeley, 2013.

[13] Ghijsen, M., Ham, J. V. D., Grosso, P., Zhu, H., Zhao, Z., and Laat, C. D., "A Semantic-Web Approach for Modeling Computing Infrastructures," 2013.

[14] Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M., "Critical infrastructure interdependency modeling: a survey of US and international research," *Idaho National Laboratory*, 2006, pp. 1–20.

[15] Delamare, S., Diallo, A. A., and Chaudet, C., "High-level modelling of critical infrastructures' interdependencies." *IJCIS*, Vol. 5, 2009, pp. 100–119.

[16] Bloomfield, R., Popov, P., Salako, K., and Wright, D., "Deliverable D2.2.4 Report On Service Oriented Interdependency Analysis," Public deliverable, Information Society Technologies Project N ° 027568, 2007.

[17] Srivastava, A., Morris, T. H., Ernster, T., Vellaithurai, C., Pan, S., and Adhikari, U., "Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information." *IEEE Trans. Smart Grid*, Vol. 4, No. 1, 2013, pp. 235–244.

[18] Ciraci, S., Daily, J. A., Fuller, J. C., Fisher, A., Marinovici, L., and Agarwal, K., "FNCS: a framework for power system and communication networks co-simulation," *2014 Spring Simulation Multiconference, SpringSim '14*, 2014, p. 36.

[19] Stouffer, K., Falco, K., and Scarfone, K., "National Institute of Standards and Technologies - Guide to Industrial Control Systems (ICS) Security," http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, 2011.

[20] Afanasyev, A., Moiseenko, I., and Zhang, L., "ndnSIM: NDN simulator for NS-3," Technical Report NDN-0005, NDN, October 2012.

[21] Roesch, M., "Snort: Lightweight Intrusion Detection for Networks." USENIX, 1999, pp. 229–238.

REFERENCES

[22] DELL, "Dell Security Annual Threat Report," https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf, 2015.

[23] Subcommittee on National Security, Homeland Defense, and Foreign Operations, "Cybersecurity: Assessing the Immediate Threat to the United States," 2011.

[24] de Barros Barreto, A., Costa, P. C. G., and Yano, E. T., "A Semantic Approach to Evaluate the Impact of Cyber Actions on the Physical Domain," *STIDS 2012 Committees*.

[25] Goodall, J. R., D'Amico, A., and Kopylec, J. K., "CAMUS: automatically mapping cyber assets to missions and users," *Military Communications Conference, 2009. MILCOM 2009. IEEE*, IEEE, 2009, pp. 1–7.

[26] Musman, S., Tanner, M., Temin, A., Elsaesser, E., and Loren, L., "Computing the impact of cyber attacks on complex missions," *Systems Conference (SysCon), 2011 IEEE International*, April 2011, pp. 46–51.

[27] Jakobson, G., "Mission cyber security situation assessment using impact dependency graphs," *FUSION*, 2011, pp. 1–8.

[28] Sawilla, R. E. and Ou, X., "Identifying Critical Attack Assets in Dependency Attack Graphs," *Proceedings of the 13th European Symposium on Research in Computer Security*, 2008, pp. 18–34.

[29] Kotenko, I. and Chechulin, A., "A Cyber Attack Modeling and Impact Assessment framework," *Cyber Conflict (CyCon), 2013 5th International Conference on*, June 2013, pp. 1–24.

[30] Vamvoudakis, K. G., Hespanha, J. P., Kemmerer, R. A., and Vigna, G., "Formulating Cyber-Security as Convex Optimization Problems," *Control of Cyber-Physical Systems*, Springer, 2013, pp. 85–100.

[31] Munir, S. and Stankovic, J. A., "DepSys: Dependency Aware Integration of Cyber-Physical Systems for Smart Homes," 2014.

[32] Ezell, B. C., "Infrastructure Vulnerability Assessment Model (I-VAM)," *Risk Analysis*, Vol. 27, No. 3, 2007, pp. 571–583.

[33] Marshall, S., *CANDID: Classifying Assets in Networks by Determining Importance and Dependencies*, Master's thesis, University of California at Berkeley, 2013.

[34] Ghijsen, M., Ham, J. V. D., Grosso, P., Zhu, H., Zhao, Z., and Laat, C. D., "A Semantic-Web Approach for Modeling Computing Infrastructures," 2013.

[35] Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M., "Critical infrastructure interdependency modeling: a survey of US and international research," *Idaho National Laboratory*, 2006, pp. 1–20.

[36] Delamare, S., Diallo, A. A., and Chaudet, C., "High-level modelling of critical infrastructures' interdependencies." *IJCIS*, Vol. 5, 2009, pp. 100–119.

[37] Bloomfield, R., Popov, P., Salako, K., and Wright, D., "Deliverable D2.2.4 Report On Service Oriented Interdependency Analysis," Public deliverable, Information Society Technologies Project N ° 027568, 2007.

[38] Srivastava, A., Morris, T. H., Ernster, T., Vellaithurai, C., Pan, S., and Adhikari, U., "Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information." *IEEE Trans. Smart Grid*, Vol. 4, No. 1, 2013, pp. 235–244.

[39] Ciraci, S., Daily, J. A., Fuller, J. C., Fisher, A., Marinovici, L., and Agarwal, K., "FNCS: a framework for power system and communication networks co-simulation," *2014 Spring Simulation Multiconference, SpringSim '14*, 2014, p. 36.

[40] Stouffer, K., Falco, K., and Scarfone, K., "National Institute of Standards and Technologies - Guide to Industrial Control Systems (ICS) Security," http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, 2011.

[41] Afanasyev, A., Moiseenko, I., and Zhang, L., "ndnSIM: NDN simulator for NS-3," Technical Report NDN-0005, NDN, October 2012.

[42] Roesch, M., "Snort: Lightweight Intrusion Detection for Networks." USENIX, 1999, pp. 229–238.

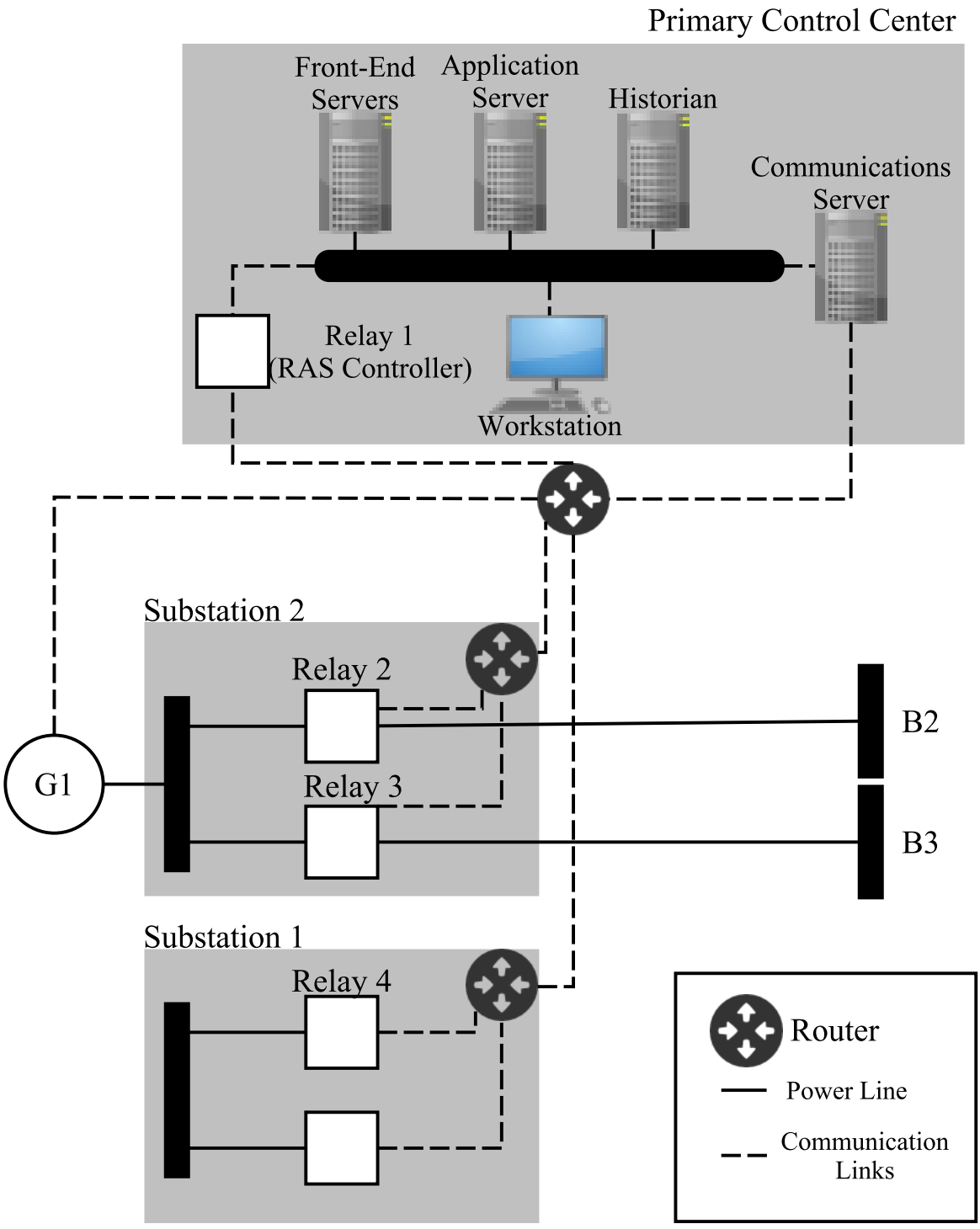

Figure 2: Example for the interaction between communcation network and electrical power grid.