Detecting Attacks in Power Plant Interfacing Substations through Probabilistic Validation of Attack-Effect Bindings

Julian L. Rrushi†* and Roy H. Campbell*

*Department of Computer Science
University of Illinois at Urbana-Champaign
201 N. Goodwin Avenue, Urbana, IL 61801, USA

†Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39/41, I-20135, Milano, Italy

E-mails: {jrrushi, rhc}@uiuc.edu

Abstract: *In this paper we provide a mathematical approach to detection of attacks on relays in electrical substations speaking IEC 61850, i.e. an abstract industrial protocol devised by the technical committee 57 of the International Electrotechnical Commission as a standard for substation communications. Our contribution regards those electrical transmission substations which interface with the generators of a power plant through step-up transformers. In this paper we take as an instance power plants which use nuclear reactors as a source of energy. The basis of the proposed approach is formed by structural equations which semantically model the relations between operational variables of substation and nuclear power plant components as monitored by the respective control systems. Causality relations investigated via structural equations are reflected on Bayesian Belief Networks to probabilistically characterize the legitimacy and abnormality of IEC 61850 traffic. We then employ the Stochastic Activity Network formalism to construct composed models of substation operation from which we derive intrusion detection rules.*

Keywords: *Anomaly Intrusion Detection, IEC 61850, Stochastic Activity Networks, Structural Equations, Bayesian Belief Networks.*

1. Introduction

In this paper we discuss an intrusion detection approach for IEC 61850 [5] which builds upon statistical and probabilistic methods, namely structural equations modeling (SEM) [17], Bayesian belief networks (BBN) [16], and stochastic activity networks (SAN) [10, 19]. The work discussed here is part of a larger intrusion detection framework that we have devised for operation in nuclear power plants. This framework is based on SAN modeling of a fusion of control protocols used in nuclear power plants, for example Modbus [13], protocols used in electrical substations, for example IEC 61850 [5], and the operation of physical components of a nuclear power plant and an electrical substation, respectively. The electrical substations considered in this research are those which interface with power plant generators and use step-up transformers to prepare for transmission the power generated by the plant.

The work discussed in this paper was initially based on finite state machines as a fundamental state transition and event recognition mechanism. SANs demonstrated to be more viable in this context responding to a considerable necessity of parallelism and nondeterministic decision making during the modeling process. The intrusion detection approach we propose in this paper is build upon investigation of causal relations between logical nodes (see Section 2 for an overview of IEC 61850). Such causal relations are in turn driven by the relations between the mechanical operation of substation physical components such as power transformers, switches, circuit breakers, busbars, etc., and protection and power regulating functions carried out by intelligent electronic devices (IEDs) communicating via the IEC 61850 standard.

We analyze IEC 61850 traffic to determine legitimate communication flows, and construct structural equations models of cyber-physical components of a simulated electrical substation using the R language and environment for statistical computing [18]. We then employ the BBN formalism through the MSBNx tool [12] to estimate probabilistic profiles of PICOMs in client-server and peer-to-peer associations. We do so by basing probability calculations on the causal relations between logical nodes as investigated through structural equations models.

We model the proposed intrusion detection approach via stochastic activity networks (SANs) using the Möbius tool [2]. Each IEC 61850 logical node is atomically modeled in relation to its interaction with other logical nodes. We use the *Join* operation to logically group atomic SAN models into composed SAN models of logical devices. Similarly, we join SAN models of logical devices into composed SAN models of physical devices, i.e. IEDs. We then

solve SAN models to study the proposed approach and derive intrusion detection rules.

The remaining of this paper is organized as follows. Section 2 provides an overview of the IEC 61850 standard. Section 3 proceeds with a threat model documenting the problem domain and explaining in what cases intrusion detection for IEC 61850 is employable and in what other cases it isn't. Section 3 then provides the proposed intrusion detection approach devised upon the application of statistical and probabilistic techniques. Section 4 summarizes our contribution, provides directions for future work, and concludes the paper.

To the best of our knowledge this paper is among the first papers describing research on (cyber) intrusion detection capabilities for electrical substations whose communications are based on the IEC 61850 standard. As of this writing we haven't identified related work which we could have referenced in this paper.

2. An Overview of IEC 61850

Byte-oriented protocols such as DNP3 have long been used as a means of supervisory and control communications in the electrical power grid. The configuration of byte-oriented protocols in IEDs, i.e. computer-based devices monitoring and controlling electrical substation operation, requires power system engineers to manually map protocol data objects to substation operation variables. Further, the amount of time spent on configuration tasks and the level of complexity of such protocols are considerably high. The IEC 61850 protocol is a new standard devised by working group 10 of the IEC Technical Committee 57 which has significantly alleviated the high complexity, time consuming, and interoperability issues in substation automation.

IEC 61850 is a virtual protocol which consists of abstract models of data and services. One of the fundamental models of IEC 61850 is the logical node, i.e. a virtual representation of a real substation device or function. Logical nodes are grouped according to the substation function they carry out. For instance, logical nodes in the protection functions group include direction comparison (*PDIR*), distance protection (PDIS), directional overpower (*PDOP*), etc. Logical nodes in the switchgear group include virtual circuit breakers (*XCBR*) and virtual circuit switches (*XSWI*). And so on. A logical device model in IEC 61850 is a composition of logical nodes which have common features, while a physical device model represents the relay where logical devices reside.

Communication services in IEC 61850 are also abstract and model-driven. Such services are defined by the Abstract Communication Service Interface (ACSI) and are organized in two groups of communication services. Services in one group are used in a client-server model and generally control or get data values, while services in the other group are used in a peer-to-peer model where data is sent fast and reliably from one IED to a group of other IEDs. The substation information exchanged between IEDs is referred to as Pieces of Information for Communication (PICOM), while the path established for transmission of PICOMs is referred to as an association.

As IEC 61850 data and services are abstract and cannot themselves provide a concrete interaction between IEDs, they are mapped to concrete communication protocols. Such a mapping is carried out by the Specific Communication Service Mapping (SCSM). SCSM defines the syntax and encoding of messages and how they are passed over the network. IEC 61850 could be mapped to any communication protocol, although mapping to byte-oriented protocols may introduce subtleties. A common communication stack to which IEC-617850 is mapped comprises Manufacturing Messaging Specification (MMS), TCP/IP and Ethernet. Refer to [5] for a thorough specification of IEC 61850 protocol.

There is a growing concern in devising and deploying defensive capabilities for securing IEC 61850 implementations in electrical substations. Application vulnerabilities are continuously identified even in recently developed electric power automation software [23, 24, 25], and several attack scenarios have been identified, including those on electrical substations [6]. Further, NERC CIP reliability standards require deployment of security mechanisms for identification and characterization of attacks targeting critical infrastructures [14]. Consequently intrusion detection for IEC 61850 profiles is among the focal points of research on the security of electrical substations.

3. A Mathematical IDS Approach for IEC 61850 Communications

3.1 Threat Model

Admittedly the feasibility of possessing or acquiring the ability to send network packets to IEDs in a target electrical substation determines the level of exposure of that substation to network attacks. In common power grid deployments the Intranet or other private networks of a power grid operating company are usually connected to electrical substation networks.

Consequently such private networks represent potential links from where attacks on electrical substations could be mounted. Gaining access to these private networks could also allow for hitting electrical substations from an external point. The private networks in question may be connected to Internet, in which case bypassing the corresponding firewalls (if any) opens the way toward a target electrical substation network.

The deployment of wireless segments within such private networks provides additional attack opportunities. With the aid of antennas wireless network attacks could be mounted from outside the wireless network coverage range and eventually from outside the physical area of a target electrical utility company. Common IEDs deployed in electrical substations provide what is referred to as engineering access through dial-in modems. Engineering access represents an additional opportunity for attackers who may use war dialing to identify IED modems and subsequently attack through them.

Laptops of power system engineers are also a potential mechanism of gaining access to electrical substation networks. In addition to electrical substation networks, such laptops may occasionally get connected to various networks potentially including Internet. Such connectivity allows for attacking these laptops and possibly using them as a bridge into electrical substation networks. Physical intrusions into locations of equipment with connectivity to electrical substation networks could also facilitate the implementation of network attacks on those substations. As an instance, an attacker could physically intrude into an unmanned electrical substation, connect an attacking machine to the substation LAN, and from there attack remote guarded substations.

In most cases physical intrusions come with their own complexities due to deployment of infrared motion sensors and/or physical barriers, but these issues are out of the scope of this paper. A circumstance, in which an attacker is able to send messages over the network to IEDs in substations whose communications were based on byte-oriented protocols such as DNP3, meant that the attacker had gained complete control over the physical components of the compromised substation. Under these assumptions there was no need to carry out an attack for being able to destroy the compromised substation. It would have been sufficient to specify in a protocol data unit the correct function code along with the correct indices and data denoting a command such as open or close a circuit breaker or switch, and send it to a process interface IED for damaging the substation to a considerable degree.

In substations whose communications are based on the IEC 61850 protocol the condition described above does not always hold. The IEC TS 62351 standard

[4] defines data and communications security also for IEC 61850, providing for authentication, integrity and confidentiality. The secure operation of IEC 61850 builds upon the cryptographic protection provided by IEC TS 62351 and defines an access control model. IEC 61850 access control object definitions provide the capability to enforce the accesses to specific class instances, class instance attributes, and ACSI services in a server for all possible communication clients [5].

IEC 61850 enforces what is referred to as virtual access view. According to this concept a client gets preliminarily identified and subsequently acquires visibility only on those instances or attributes along with the supported services that it is allowed to access. All accesses to IEC 61850 resources are monitored and any violations are recorded. As a matter of fact IEC 61850 comes with a logical node referred to as generic security application (*GSAL*) entirely dedicated to monitoring of violations regarding authorization (handled via the *AuthFail* attribute), access control (handled via the *AcsCtlFail* attribute), service privileges (handled via the *SvcViol* attribute) and inactive associations (handled via the *Ina* attribute).

Referring to the problem domain covered by the work described in this paper, whether adversaries need to carry out an attack or not in order to damage a target electrical substation depends on up to what degree attackers have advanced in the power system network via exploitation of vulnerabilities not related to IEC 61850, and what privileges or cryptographic material have fallen in their hands. As an instance, most of the IEDs commonly found in electrical substations support an ASCII based interactive protocol for allowing power system engineers to log into an IED from a remote location and issue configuration or diagnostic commands. If attackers exploit a vulnerability in an implementation of this protocol running in an IED that serves as a process interface device, and consequently acquire access over the network to this IED at an access level which allows for, say, opening or closing a circuit breaker, then no attack traffic will be ever generated via the IEC 61850 protocol.

On the other hand, a large set of attack scenarios includes attackers injecting malicious IEC 61850 traffic into an electrical substation network. Such scenarios also include attackers possessing a limited virtual access view, which does not allow for damaging the electrical substation, and acting from within the electrical substation network against target IEDs to maliciously modify data in highly critical logical nodes residing in such IEDs. In large electrical substations such as those distribution substations interfacing with the generators of a power plant, the attackers' goal may be to cause a massive damage, probably extending to the whole target substation.

In this case attackers will need to attack other IEDs, even though from the actual position they could cause confined damage. Further, even causing a confined damage may not be feasible in those large electrical substations which contain one or more replicas of IEDs monitoring and controlling substation operation and actually not under the control of attackers. As anomalous conditions are created by attackers, the replicas sense the anomaly and eventually respond turning the attacked electrical substation into stable conditions. Attackers, again, have to carry out one or more attacks on replicas in order to prevent them from regulating the substation operation. In IEC 61850 the behavior of each logical node is specified via a state machine.
It may be possible to construct logical nodes, such as for instance state protection trip conditioning (*PTRC*), in such a way as to make these nodes aware of certain conditions which if created could harm the electrical substation. The state machine of the logical nodes in question then could transition from one state to another and hence operate on the electrical substation only if the corresponding effect, for example transmitting a trip message to an *XCBR* logical node, does not cause any damage. Consequently attackers may have to attack logical nodes in a target IED in order to evade possible state machine checks.
Thus, there is a considerably large set of circumstances and conditions under which potential attackers have to generate malicious IEC 61850 traffic for being able to attack IEDs and corrupt data in their logical nodes.

3.2 The Proposed IDS Approach

The main objective behind our employment of SANs, SEM, and BBNs is to probabilistically and statistically build a profile of legitimate data flows along with the main characteristics of the PICOMs exchanged and ACSI services invoked in an electrical substation interfacing with a power plant. Confirmatory experimentation in laboratory settings has shown that IEC 61850 communications are driven by protection and monitoring functions carried out by IEDs. For instance, the aim of protection functions is to monitor substation operation values such as voltages, currents, temperatures, phases, frequencies, amplitudes, etc., from switchgear. If values measured via instrument transformers such as current transformers or voltage transformers, phasor measurement units, etc., exceed predefined thresholds, the logical nodes carrying out the corresponding protection function transition into an alert state.

If some other predefined thresholds are exceeded clearly indicating the occurrence of a fault, then an interaction between logical nodes takes place resulting in the issuance of a trip which switches off the substation component affected by the fault. The underlying thesis which forms the basis of our contribution is that for each substation function there is an associated set of IEC 61850 communications with characteristics that may be estimated. In this section we provide the capabilities to estimate such characteristics and demonstrate that such estimated characteristics are employable as a mechanism to probabilistically determine whether IEC 61850 traffic received by a given IED is legitimate or offensive.

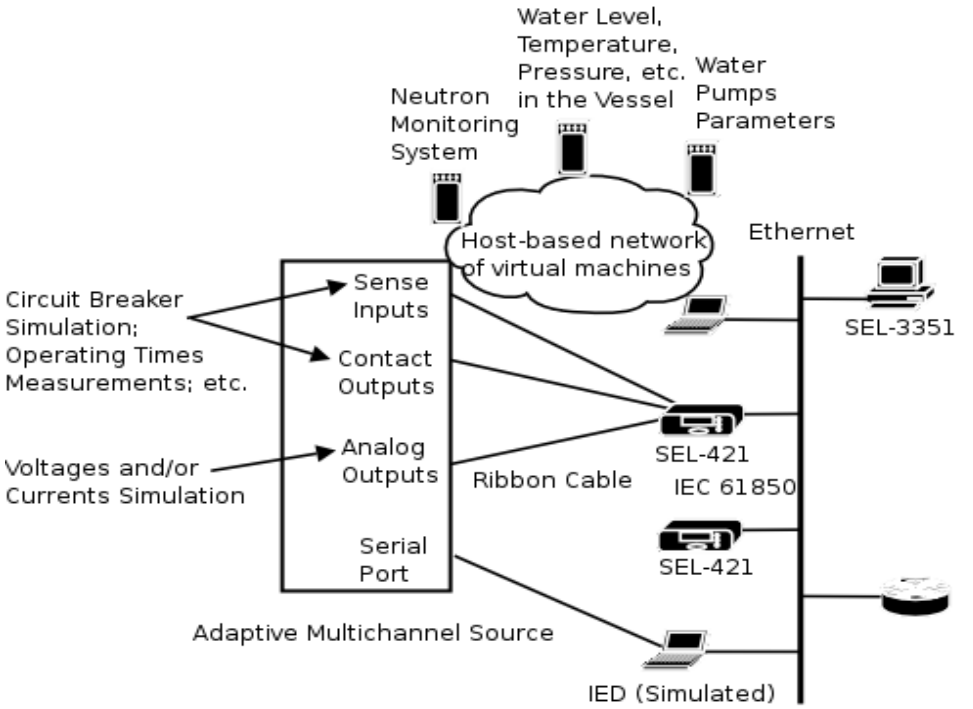


Figure 1. A high level description of the testbed where experimentation was carried out

Fig. 1 resembles the testbed where we carried out the experiments. In this work we used SEL-421 IEDs [21] which acted as fault locators, protection, and circuit breaker control relays. Each one of the SEL-421 IEDs was running a real world implementation of IEC 61850. We used a SEL-4000 relay test

system (RTS) [22] as an adaptive multichannel source. The analog outputs shown in Fig.1 simulate voltages and currents according to customizable test files, while the sense inputs and contact outputs are used to measure operating times and to simulate a circuit breaker [22]. The machine at the bottom of the Fig.1 was used to send packets with abnormal payloads, including machine code along with memory addresses and characters commonly used in command injection attacks.

The machine at the top of Fig.1 was running a host-based network of virtual machines simulating the replica of a distributed control system getting simulated sensor data from a simulated nuclear power plant. Each one of the virtual machines in such host-based network was running a free implementation of Modbus protocol, namely FreeModbus [26], on an uClinux operating system [1]. We used the *modpoll* Modbus master simulator to gather simulated Modbus PDUs denoting typical status data of various components of a nuclear power plant. The principal plant components that were simulated via generation of Modbus PDUs include the neutron monitoring system, the reactor feedwater system, and the main steam system. The machine in question served also as an analysis station where both simulated electrical substation data and simulated nuclear power plant data were merged and analyzed as a unified set of data.

By analyzing both physical and logical traffic generated by the SEL-421 IEDs in response to simulation of various faults via the corresponding test files in the SEL-4000 RTS, it is possible to observe regularities in the communication flow triggered by each fault. Fig. 2 depicts the communication flow observed during a simulated fault neutralized by the SEL-421 IEDs acting according to an example application of the generic substation event model (GSE)[1]. If we focus the analysis on both physical and logical IEC 61850 traffic seen during an interval of time $[t_0, t_0+\delta]$, where t_0 is the moment of time in which a fault is simulated and $t_0+\delta$ is the moment of time in which a process interface IED neutralizes the simulated fault, we can record what logical node accessed what other node via what ACSI services at what point in time within the interval under consideration. The time factor in this analysis serves as a mechanism to order the sequence of interactions between logical nodes in the communication flow corresponding to a fault.

[1]Intended exclusively as a GSE example.

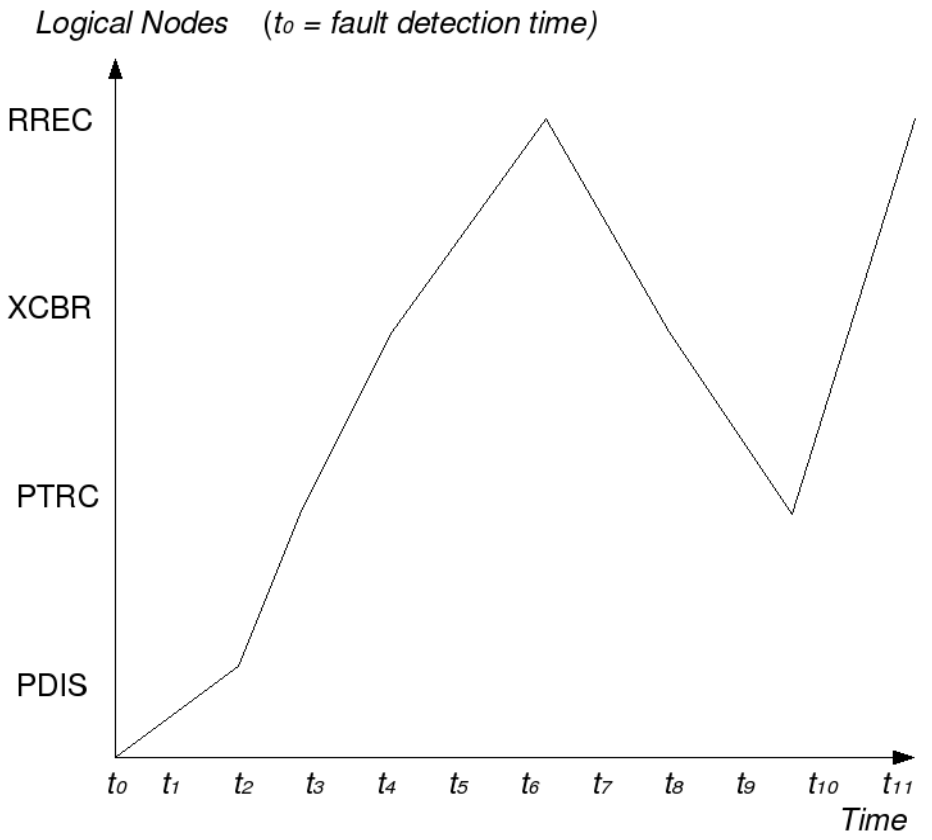


Figure 2. A graph representation of a communication flow in an example application of the generic substation event model.

Depending on the position used to potentially launch attacks on an electrical substation, the effects of a subset of such attacks consist of deviations from the legitimate communication flows. Nevertheless, we deem that, while autonomous attack agents are more susceptible to detection via communication flow deviations, communication flow profiles alone are not sufficient to detect mimicry attacks if the latter are applicable. During a reconnaissance phase preceding an attack, attackers could analyze IEC 61850

traffic flowing over the substation network, learn legitimate communication flow profiles, and follow one of them if it allows for reaching the attack goals. Thus, an attacker could mimic a legitimate communication flow while injecting PICOMs whose mapping to a concrete protocol PDUs would consist of offensive payloads onto a target application. We now submit and develop our other thesis that PICOMs exchanged in each legitimate communication flow have characteristics that may be estimated. We augment the construction of substation operation profiles by using structural equations to investigate causal relations in IEC 61850 communication flows. Moving along the line of the *Divide and Conquer* paradigm, we devise a structural equations model for each logical node at a time. As an example, Fig. 3 depicts the structural equations model of the PTRC logical node as involved in the GSE application example previously discussed.

Note that such structural equations model is intended exclusively as an example and is provided for illustration purposes only. The original version of this model is quite quantitative and involves tens of other endogenous and exogenous variables from both the nuclear power plant and substation and IEC 61850 sides. We represent the data in the logical node under consideration as endogenous variables. Further, we represent as exogenous variables the data in those other logical nodes which interact with the logical node under consideration, the data regarding the operation of physical components within an electrical substation, and the data regarding the operation of a nuclear power plant.

The structural equations model of each logical node is composed of two submodels, namely a structural submodel and a measurement submodel. An excerpt of the structural submodel for the PTRC logical node is depicted in Table 1. The indication of the existence of regression coefficients in the model is generally guided by a preliminary analysis of the IEC 61850 configuration in an IED to be protected. Nevertheless, a modeler could take an exploratory approach rather than a confirmatory approach and declare all possible regression coefficients and covariances, letting those which do not hold be zero after estimating the model in question with the *sem* package in R.

After simulating a fault with the SEL-4000 RTS and collecting the IEC 61850 traffic consequently generated, we used the *sem* package of R to fit the structural equations model for a logical node under consideration. The formulation used to estimate the model in question is the reticular action model (RAM). Estimation of the model for each logical node analyzed generally consists of model specification via the *specify.model* function,

computation of the covariance matrix via the *cov* function, and model fitting via the *sem* function.

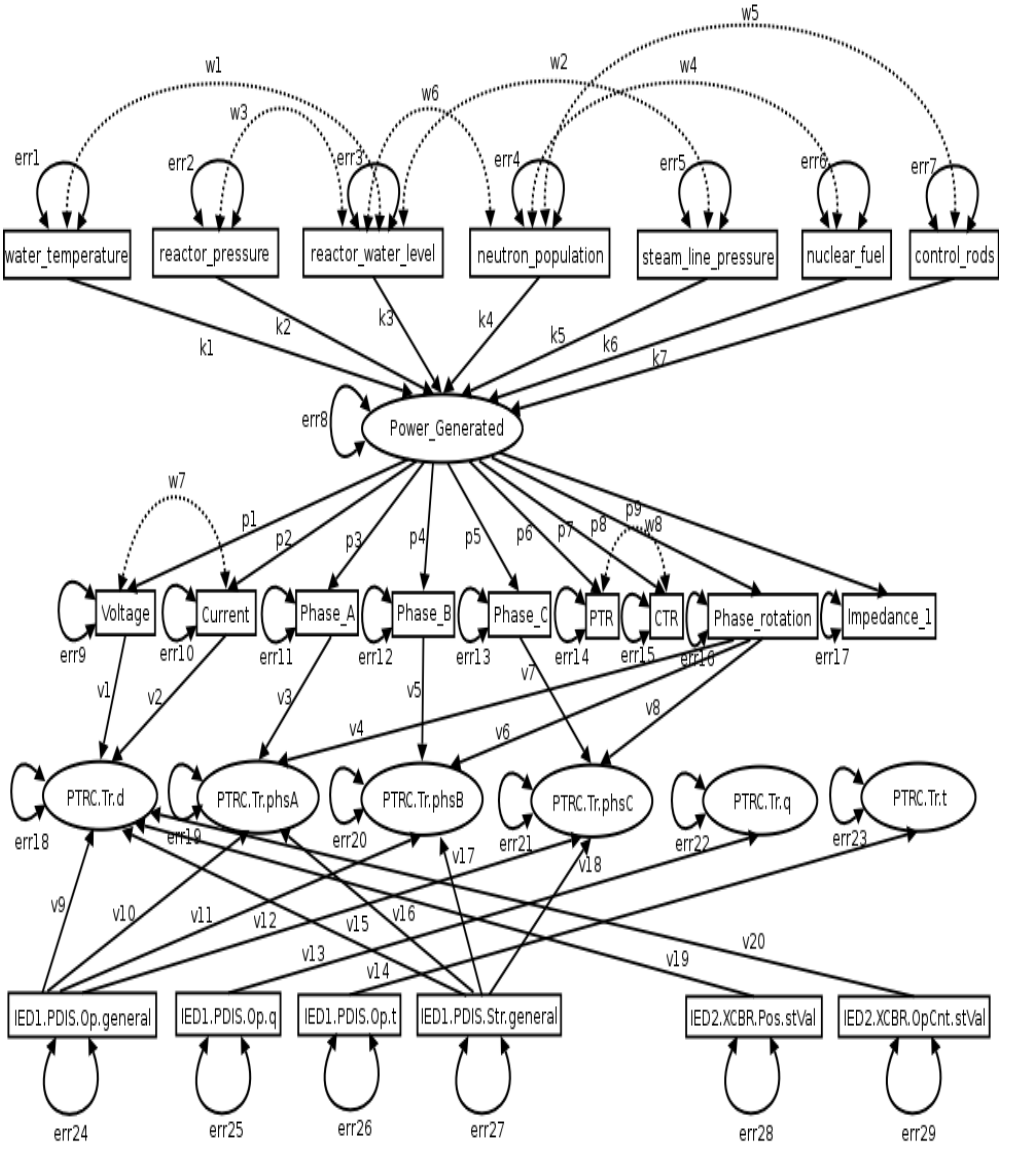


Figure 3. Excerpt of the RAM format path diagram for a PTRC logical node

```
PTRC.Tr.d = v1 * Voltage + v2 * Current + v9* IED1.PDIS.Op.general
            + v15 * IED1.PDIS.Str.general + v19 * IED2.XCBR.Pos.stVal
            + v20 * IED2.XCBR.OpCnt.stVal + err18
PTRC.Tr.phsA = v10 * IED1.PDIS.Op.general + v16 * ED1.PDIS.Str.general
            + err19
PTRC.Tr.phsB = v11 * IED1.PDIS.Op.general + v17 * ED1.PDIS.Str.general
            + err20
PTRC.Tr.phsC = v12 * IED1.PDIS.Op.general + v18 * ED1.PDIS.Str.general
            + err21
PTRC.Tr.q = v13 * IED1.PDIS.Op.q + err22
PTRC.Tr.t = v14 * IED1.PDIS.Op.t + err23
Power_Generated = k1 * water_temperature + k2 * reactor_pressure
            + k3 * reactor_water_level + k4 * neutron_population
            + k5 * steam_line_pressure + k6 * nuclear_fuel
            + k7 * control_rods + err8
```

Table 1. Excerpt of the structural submodel for a PTRC logical node

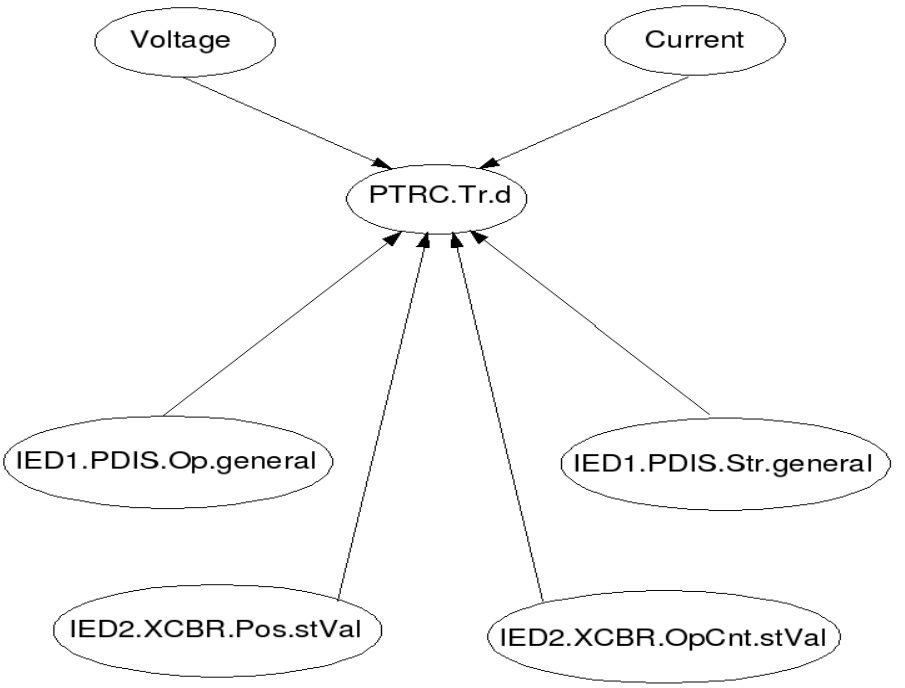
The estimation of the model is further refined by calculating modification indexes. Such indexes eventually indicate that a better fit could be achieved by performing defined modifications on the model specification, such as for example freeing one or more of the covariances. The estimation of the structural equations model for a logical node provides regression coefficients and covariances which quantify the causal relations between the logical node in question and other logical nodes which eventually interact with the former as part of one or more legitimate communication flows. Informally speaking, if in a given legitimate communication flow data x in logical node A is causally affected by data y in logical node B and data z in logical node C, then estimation of the structural equations model for node A allows for calculating a likely value of x given y and z.

The way logical node B and logical node C affect x in logical node A is through transmission of one or more PICOMs. A read operation from logical node B and logical node C could be initiated, allowing A to get y and z via a received PICOM, and then update the value of x being based on the read values of y and z. As another example, a write operation could be initiated on A, calculating in place a new value of x upon y and z from B and C respectively, and sending the new value of x to A via a PICOM. Hence construction and estimation of structural equations models for each one of the logical nodes taking part in a legitimate communication flow provides the capability to estimate the content of PICOMs exchanged.

Depending on the type of faults sensed by IEDs, the type of monitoring tasks carried out, or the actual state of an electrical substation in the moment of fault detection or polling, a logical node may take part in a large number of legitimate communication flows, and many other logical nodes may exhibit causality relations with the logical node in question. In an electrical substation, as in other fields where intrusion detection is being employed, deterministically discerning between legitimate traffic and attack traffic results to be a source of overwhelming false positives. Consequently we use the probability theory to probabilistically estimate the legitimacy or abnormality of both physical and logical IEC 61850 traffic.

For each logical node we developed a BBN to model the probability distribution of each one of its data attributes. Fig. 4 depicts part of the BBN model for the PTRC logical node in the example application of the GSE model mentioned earlier in this section. Note that the BBN model for the PTRC logical node in question is provided for illustration purposes only. We used the MSBNx tool to estimate such probability distributions through probability calculus and the Bayes theorem relying on information gathered via structural equations models and legitimate communication flows developed as shown earlier in this section. In order to add a causal interpretation to the graphical structure of each one of the BBN models developed, we followed the link between structural equations models and BBNs as defined in [3].

Causal interpretation of the BBN model of each logical node allows for deriving information regarding direction in each possible interaction between logical nodes. Direction information in turn appears to be quite relevant to a thorough characterization of legitimate communication flows. As shown in Fig. 4, each BBN node with no parents represents an exogenous variable of the associated structural equations model. Further, each BBN node and its direct parent nodes, i.e. *PTRC.Tr.d* and its parent nodes in the case of the model depicted in Fig. 4, represent variables involved in the interactions between a logical node for which the BBN model has been developed, i.e. *PTRC* in our example, and other logical nodes. With these two properties the BBN model of each one of the logical nodes reflects the causal structure of IEC 61850 communications in an electrical substation.



						PTRC.Tr.d		
Volt.	Cur.	Op.Gen.	Str.gen.	Pos.stVal	OpCnt.stVal	d1	d2	d3
v1	c1	og1	sg1	ps1	os1	0.5	0.25.	0.25
v2	c2	og2	sg2	ps2	os2	0.0	0.0	1.0
v3	c3	og3	sg3	ps3	os3	0.5	0.5	0.0

Figure 4. Excerpt of the BBN model for the PTRC logical node

We used the SAN formalism to unify and complement the information gathered via analysis of communication flows and construction of structural equations and BBNs. For each logical node we built an atomic SAN model (see Fig. 5 for an example) where most of the places represent data attributes, instantaneous activities represent ACSI services, activity case distributions represent probability distributions calculated through BBNs, enabling predicates of input gates represent conditions for a defined logical node to access data attributes of the logical node being modeled, and output functions in output gates represent the result of calling an ACSI service on the logical node being modeled.

While all this information is already available in legitimate communication flows, structural equations models, and BBNs separately and statically for each logical node, for validation purposes it was necessary to put all the pieces together and analyze the dynamic behavior of the proposed approach. We used the *Join* operation [11] to compose atomic SAN models into models of logical devices. Models of logical devices in turn were composed into models of physical devices (see Fig. 6 for an example).

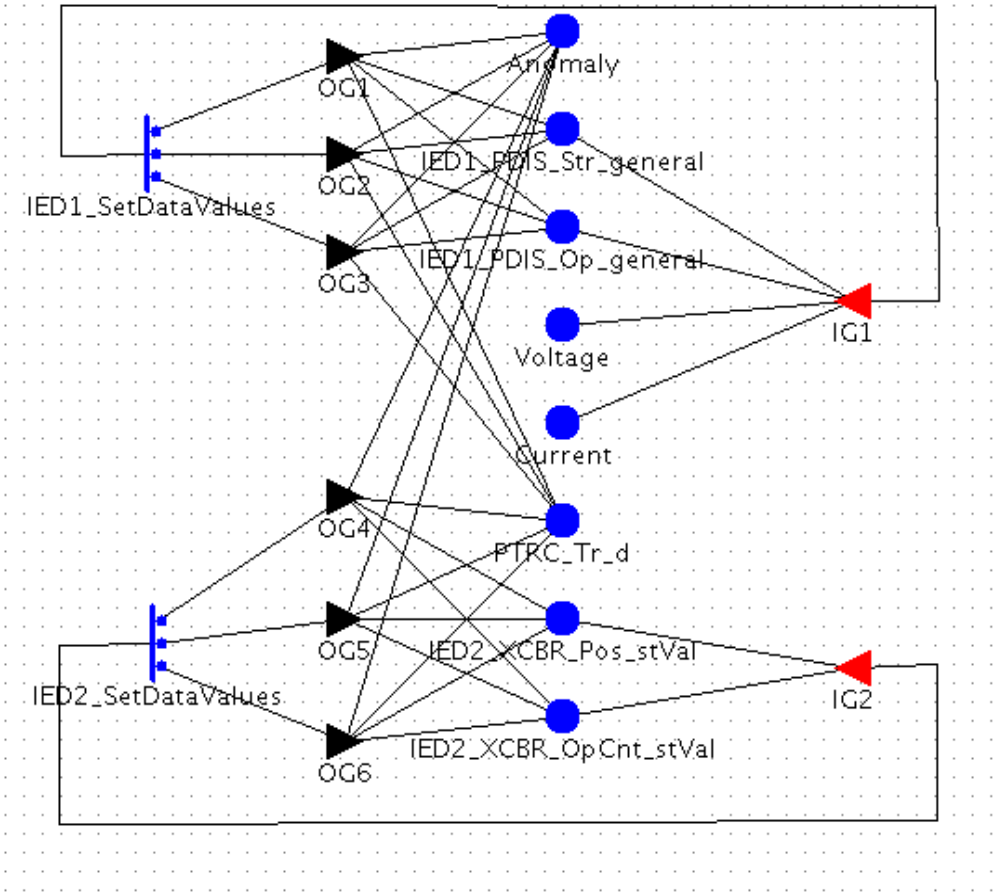


Figure 5. Excerpt of the SAN atomic model developed for the PTRC logical node

The composition of SAN models can go further by composing models of physical devices into models of bays, and so on until covering the whole substation network. The resulting composed model can then be solved in order

to allow for studying the behavior of the SANs, which in fact corresponds to the behavior of the intrusion detection approach proposed in this paper.

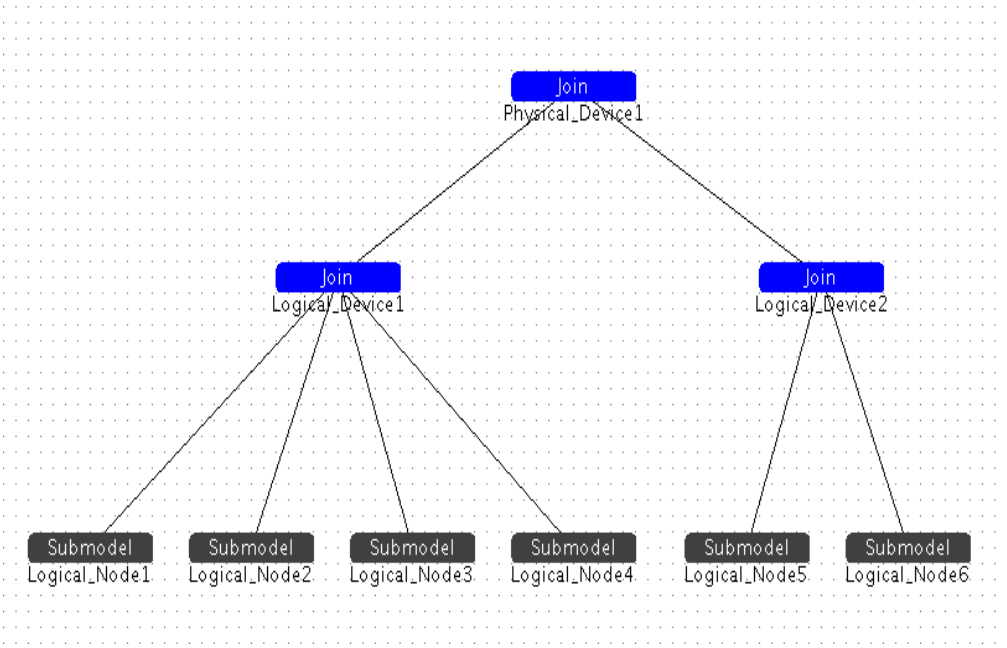


Figure 6. Example of a composed SAN model of an IED

We propose an experimental feature of the intrusion detection approach discussed in this paper, namely the capability to probabilistically quantify the involvement of each logical node in IEC 61850 traffic, which is supposed to flow over the duration of a defined interval of time Δ through legitimate communication flows associated with protection functions, and which is triggered in response to detection of the corresponding faults in electrical substation components. With quantification of a logical node involvement under the aforementioned conditions we mean an estimation of the frequency of invocation of ACSI services in the logical node under consideration on behalf of other logical nodes, and the likelihood that after an ACSI service invocation data attributes in the node under consideration will have certain defined values.

As an instance, assume that logical node *PDIS* is supposed to access the fault locator logical node (*RFLO*) through the *SetDataValues* ACSI service along a legitimate communication flow associated with the distance protection function. We probabilistically estimate the values of two variables. The first variable is the total number of calls to *SetDataValues* in *RFLO* on behalf of

PDIS logical node over the duration of a defined interval of time Δ. Let P denote the set of all data attributes in the logical node *RFLO*, $M = \{x \mid x \in N\}$ the set of all possible values of those data attributes, and $F = \{f \mid f : P \rightarrow M\}$. Staying within our example, the second variable that we estimate is the likelihood of each element of F being in place after a call to *SetDataValues* has been issued in *RFLO* on behalf of *PDIS*.

In our approach we generally use the activity-marking oriented reward structure as provided in [20] to encode these variables. We refer to the former as ACSI service request frequency, and to the latter as logical node instantiation likelihood. ACSI service request frequency is encoded as an impulse reward, while logical node instantiation likelihood is encoded as a rate of reward. Both of these variables are defined as belonging to the Interval-of-Time category [20] and each one of them represents the total reward accumulated during an interval of time Δ for the respective phenomenon they represent. The estimation of ACSI service request frequencies and logical nodes instantiations likelihoods via SAN modeling is driven by a characterization of faults on the physical components of the electrical substation.

In this regard we draw from power system research on probabilistic estimation of the failure rate of physical components such as transformers and circuit breakers of an electrical substation [9, 15, 27]. One of the techniques that has been investigated as a means of estimation of failure rates is condition data monitoring and aggregation. The research work discussed in [15] uses power transformer condition data gathered via distributed data sources such as sensors that measure concentration of several gasses, oil temperature, winding temperature, etc., to develop Hidden Markov Models which in turn use those condition data to estimate the failure rate of the power transformer under consideration. The task of the work discussed in [15] is the estimation of substation equipment failure rate to be used in system level simulation tools for the purpose of transmission reliability.

The research work discussed in [9] extends the use of the condition monitoring technique to estimate the failure rate of circuit breakers, while the research work discussed in [27] applies the BBN formalism along with condition monitoring to calculate the failure rate of power transformers. We augment the SAN models developed by the work described so far with an atomic model for each substation equipment. In such SAN models failures are represented by timed activities, equipment condition variables along with other related variables are represented by places, conditions representing deterioration are represented by enabling predicates of input gates, and failure

modes are represented by activity cases. The time distribution functions of timed activities representing substation equipment faults implement the contribution provided in [9, 15, 27] to estimate the rates of those activities upon the number of tokens found in each place in the moment of estimation. As to IEC 61850 traffic generated by monitoring functions, it is straightforward to include them in the modeling process. The monitoring rate is usually periodic, and is statically defined in IED configurations.

The validation of the proposed intrusion detection approach includes measuring the performance of its efficiency via two main variables commonly used by DARPA as IDS evaluation metrics, namely probability of detection (*Pb*) and false alarm rate (*Fa*). In our SAN models these two variables were encoded as rates of reward belonging to the Instant-of-Time category according to the activity-marking oriented reward structure [20]. Both of these variables denote the reward at a particular time *t*. We measured via simulation the value of *Pb* for known attack techniques in several attack scenarios by solving the SAN models with Möbius. The observed effects of such attacks were deviations from legitimate communication flows, abnormal ACSI service request frequencies, selection of instantaneous activity cases denoting a quite minimal or in some instances a zero probability of PICOM data legitimacies along with quite low logical node instantiations likelihoods.

Fa was also measured via simulation by encoding substation equipment condition data as tokens in the associated places and solving the SAN models with Möbius.

4. Conclusion and Future Work

IEC 61850, as a model-driven industrial protocol for substation automation, represents a new way of thinking which acknowledgeably is changing the way electrical substations are designed and deployed. On the other hand, there are various security considerations in IEC 61850 design and implementations. As any other industrial protocol, IEC 61850 may be subject to attacks carried out over the network. Currently several security capabilities for IEC 61850 profiles are under development in various research bodies, and intrusion detection is an integral part of such capabilities. Examples of research efforts on IEC 61850 security include security standards such as IEC TS 62351 devised by group 15 within the technical committee 57 of the International Electrotechnical Commission, which covers also intrusion detection to some degree.

In this paper we discussed a mathematical approach to detection of attacks on IEC 61850 implementations. We used the *sem* package within the R software for statistical computing to construct structural equations models estimating the causality relations between variables of electrical substation and nuclear power plant operation. We then employed BBNs via the MSBNx tool to probabilistically model legitimate data flows and potential attack data flows along with characteristics of legitimate and attack PICOM data frames, respectively. We used the Möbius tool to build SAN models of substation operation based on causality and probability information calculated as previously described. The SAN models built upon information provided by structural equations models and BBN models along with their solution are used to derive intrusion detection rules implementable in electrical substations.

As a future work we will further investigate through multivariate statistics the causal relations between the mechanical operation of substation physical components, the operation of nuclear power plant physical components, and protection and power regulating functions carried out by IEC 61850 based IEDs. Our work so far has focused on detection of application level attacks on IEC 61850 implementations. We will investigate on how to exploit and possibly refine the model based intrusion detection approach described in this paper in order to provide capabilities of detection of attacks on transport, network, and data link layers. We plan to experiment with coding intrusion detection rules constructed through the research work discussed in this work in what is referred to as an executable architecture definition language [7, 8] and deploying them on a complex event processing (CEP) engine. Such an engine is designed to act within a few milliseconds, consequently it is quite suitable to our needs as it provides architectural support for real-time detection capabilities in a distributed control environment.

About the Authors – Roy H. Campbell is the Sohaib and Sara Abbasi Professor of Computer Science at the Siebel Center for Computer Science at the University of Illinois, Urbana-Champaign, USA. He has supervised the completion of forty Ph.D. dissertations, and is the author of over two hundred and fifty research papers on security, programming languages, software engineering, operating systems, distributed systems, and networking. His research includes security of the electric power grid, Gaia project on active spaces, and mobile computer operating systems. Professor Campbell is Director of the University of Illinois Center of Academic Excellence in Information Assurance Education, and a member of the Information Trust Institute. He is a member of the ACM and an IEEE Fellow.

Julian L. Rrushi is a visiting research scholar at the Department of Computer Science, University of Illinois at Urbana-Champaign, USA, and a final year PhD candidate in Computer Science at Università degli Studi di Milano, Italy. His research interests lie in cyber security of the electric power infrastructure, with focus on intrusion detection in nuclear power plants. Rrushi has been an (ISC)² scholarship recipient for the years 2005 and 2007, and has carried out research at the Joint Research Center of the European Commission in Ispra, Italy.

Acknowledgment

We thank Microsoft Research for providing the MSBNx tool, the PERFORM Performability Engineering Research Group at the University of Illinois at Urbana-Champaign for providing the Möbius tool, Schweitzer Engineering Laboratories for providing through the TCIP center of the Information Trust Institute at the University of Illinois at Urbana-Champaign most of the electrical substation equipment used during our experiments, and the R Development Core Team for providing the R software for statistical computing. Julian Rrushi was supported on a research scholarship from (ISC)².

Any opinions, findings and conclusions expressed in this paper are those of the authors and do not necessarily represent the views of the aforementioned organizations.

References

[1] K. Albanowski, and D.J. Dionne, “Embedded Linux Microcontroller Project”, http://www.uclinux.org

[2] D.D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J.MDoyle, and W.H. Sanders, “The Möbius Framework and Its Implementation”, IEEE Transactions of Software Engineering, vol. 20, no. 10, pp. 956-969, October 2002.

[3] M.J. Druzdzel, and H.A. Simon, “Causality in Bayesian Belief Networks”, Proceedings of the Ninth Annual Conference on Uncertainty in Artificial Intelligence, pages 3-11, Washington, D.C., July 9-11, 1993.

[4] International Electrotechnical Commission, “IEC TS 62351: Power systems management and associated information exchange - Data and communications security”, 2007.

[5] International Electrotechnical Commission, “IEC 61850: Communication Networks and Systems in Substations”, part 1 through 9, 2004.

[6] G. Leischner, and D. Whitehead, “A View Through the Hacker's Looking Glass”, technical paper of Schweitzer Engineering Laboratories, April 2006.

[7] D.C. Luckham, “The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems”, Addison-Wesley Professional, 1st edition, ISBN 0-201-72789-7, May 2002.

[8] D.C. Luckham, and B. Frasca, “Complex Event Processing in Distributed Systems”, Stanford University Technical Report CSL-TR-98-754, March 1998.

[9] J. McCalley, Y. Jiang, V. Honavar, J. Pathak, M. Kezunovic, S. Natti, C. Singh, and J. Panida “Automated Integration of Condition Monitoring with an Optimized Maintenance Scheduler for Circuit Breakers and Power Transformers”, Final Project Report, Iowa State University, January 2006.

[10] J. F. Meyer, A. Movaghar, and W. H. Sanders, “Stochastic Activity Networks: Structure, Behavior, and Application”, Proceedings of the International Conference on Timed Petri Nets, pp. 106-115, Torino, Italy, July 1985.

[11] J.F. Meyer, and W.H. Sanders, “Specification and Construction of Performability Models”, Proceedings of the Second International Workshop on Performability Modeling of Computer and Communication Systems, Mont Saint-Michel, France, June 1993.

[12] Microsoft Research, “MSBNx: Bayesian Network Editor and Tool Kit”, web: http://research.microsoft.com/adapt/MSBNx/

[13] Modbus Organization, "Modbus Application Protocol Specification", June 2004.

[14] North American Electric Reliability Corporation, "Critical Infrastructure Protection", Reliability Standards, 2006-2007.

[15] J. Pathak, Y. Jiang, V. Honavar, and J. McCalley, "Condition Data Aggregation with Application to Failure Rate Calculation of Power Transformers", Proceedings of the Hawai'i International Conference On System Sciences, Kauai, Hawaii, January 2005.

[16] J. Pearl, "Bayesian Networks: A Model of Self-Activated Memory for Evidential Reasoning", Proceedings of the 7th Conference of the Cognitive Science Society, pp. 329-334, University of California, Irvine, CA, August 1985.

[17] J. Pearl, "Causality: Models, Reasoning, and Inference", Cambridge University Press, ISBN 0521773628, second edition, 2001.

[18] R Foundation, "The R Project for Statistical Computing", web: http://www.r-project.org/

[19] W.H. Sanders, "Construction and Solution of Performability Models Based on Stochastic Activity Networks", doctoral dissertation, University of Michigan, 1988.

[20] W. H. Sanders and J. F. Meyer, "A Unified Approach for Specifying Measures of Performance, Dependability, and Performability", Dependable Computing for Critical Applications, Volume 4 of Dependable Computing and Fault-Tolerant Systems, pp. 215-237, Springer-Verlag, 1991.

[21] Schweitzer Engineering Laboratories, "SEL-421 Instruction Manual", July 2007.

[22] Schweitzer Engineering Laboratories, "SEL-4000 Instruction Manual", February 1997.

[23] US-CERT, "LiveData ICCP Server Heap Buffer Overflow Vulnerability", Vulnerability note VU#190617.

[24] US-CERT, "Takebishi Electric DeviceXPlorer OPC Server fails to properly validate OPC server handles", Vulnerability note VU#926551.

[25] US-CERT, "Invensys Wonderware InTouch creates insecure NetDDE share", Vulnerability note VU#138633.

[26] C. Walter, "FreeMODBUS library", http://www.freemodbus.org/

[27] Z. Zhang, Y. Jiang, and J.D. McCalley, "Bayesian Analysis of Power Transformer Failure Rate Based on Condition Monitoring Information", Iowa

State University, research sponsored by Power Systems Engineering Research Center, USA.