Intrinsically Resilient Energy Control Systems

Frederick Sheldon
Oak Ridge National Laboratory
Oak Ridge, TN 37831, U.S.A.
+1-865-576-1339
sheldonft@ornl.gov

Jingshan Huang
University of South Alabama
Mobile, AL 36688, U.S.A.
+1-251-460-7612
huang@usouthal.edu

Jiangbo Dang
Siemens Corporation
Princeton, NJ 08540, U.S.A.
+1-609-734-3656
jiangbo.dang@siemens.com

Daniel Fetzer
Oak Ridge National Laboratory
Oak Ridge, TN 37831, U.S.A.
+1-865-574-3312
fetzerdt@ornl.gov

Stuart Goose
Siemens Corporation
Berkeley, CA 94704, U.S.A.
+1-510-665-1330
stuart.goose@siemens.com

Jonathan Kirsch
Siemens Corporation
Berkeley, CA 94704, U.S.A.
+1-510-665-1339
jonathan.kirsch@siemens.com

David Manz
Pacific Northwest National Laboratory
Richland, WA 99354, U.S.A.
+1-509-372-5995
david.manz@pnnl.gov

Thomas Morris
Mississippi State University
Mississippi State, MS 39762, U.S.A.
+1-662-325-3199
morris@ece.msstate.edu

Dong Wei
Siemens Corporation
Princeton, NJ 08540, U.S.A.
+1-609-734-3525
dong.w@siemens.com

ABSTRACT

To preserve critical energy control functions while under attack, it is necessary to perform comprehensive analysis on the root cause and impact of an ongoing cyber intrusion without sacrificing the availability of energy delivery. In this position paper, we present a proof of concept of an intrinsically resilient energy control system, with the ultimate goal of ensuring availability/resiliency of energy delivery functions, along with the capability to assess root causes and impacts of cyber intrusions.

Keywords

cybersecurity, energy control system, root cause analysis, intrusion-tolerant SCADA, ontology, knowledge base, semantic annotation, data integration, situational awareness.

1. INTRODUCTION

Our energy infrastructure depends on energy delivery systems comprised of complex and geographically dispersed network architectures with vast numbers of interconnected components. These systems provide critical functions to provide information and automated control over a large, complex network of processes that collectively ensure reliable and safe production and distribution of energy. The energy utilities are modernizing these vast networks with millions of smart meters, high speed sensors, advanced control systems, and a supporting communications infrastructure. This additional complexity brings benefits, but also increases the risks of cyber attacks that could potentially disrupt our energy delivery. These systems must maintain high availability and reliability even when under attack. After a security incident has been detected, the incident response team needs the ability to investigate and determine the root cause, attack methods, consequences, affected assets, impacted stakeholders, and other information to inform an effective response. The response team needs this information in the short term to contain or eradicate the attack, recover compromised equipment, and restore normal operation. In the longer term, the team needs to determine counter-measures to prevent recurrence and possibly collect evidence to prosecute intruders. This analysis and response must be done without interrupting the availability of the energy delivery systems. To address the aforementioned challenges, we present in this position paper the design of *InTRECS*, an <u>In</u><u>T</u>rinsically <u>R</u>esilient <u>E</u>nergy <u>C</u>ontrol <u>S</u>ystem. The ultimate goal of InTRECS is to provide tools and technologies to ensure the availability/resiliency of energy delivery functions, along with the capability to assess root causes and impacts of cyber intrusions. The rest of the paper is organized as follows. Section 2 describes the overall architecture of InTRECS and design details for each subsystem. Section 3 concludes with future research directions.

2. INTRECS ARCHITECTURE

2.1 System Overall Architecture

Figure 1 illustrates the overall architecture of InTRECS, which is decomposed into six subsystems: *Intrusion-Tolerant SCADA (InTRADA)*, *Cybersecurity Ontologies and Knowledge Base for Energy Delivery Systems (CoEDS)*, *Semantic Data Integration and Processing (SeDIEP)*, *Root Cause and Impact Analysis (RoCIA)*, *Dashboard Analytics and Situation Awareness (DaSA)*, and *Test and Evaluation (TnE)*. InTRECS will be constantly active to intrinsically provide resiliency, i.e., correct operations and excellent performance. At the same time, a DaSA GUI will guide end users to generate queries out of data derived from diverse sources. Query results, e.g., the root cause, extent, and impacts of the cyber intrusion, can then be provided back to end users. InTRECS will also push security alerts up to end users. Both query results and alerts are regarded as semantic decision support to end users because they extensively utilize Semantic Web technologies, namely, domain ontologies, resource description framework (RDF) triples from semantic annotation, and inferences & analysis performed at the semantic level.

CSIIRW 8, Jan. 8 - 10, 2013, Oak Ridge, TN, USA
ACM 978-1-4503-1687-3/12/10.

The submitted manuscript has been authored by contractors of the U.S. Government (USG) under contract DE-AC05-00OR22725. Accordingly, the USG retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for USG purposes.

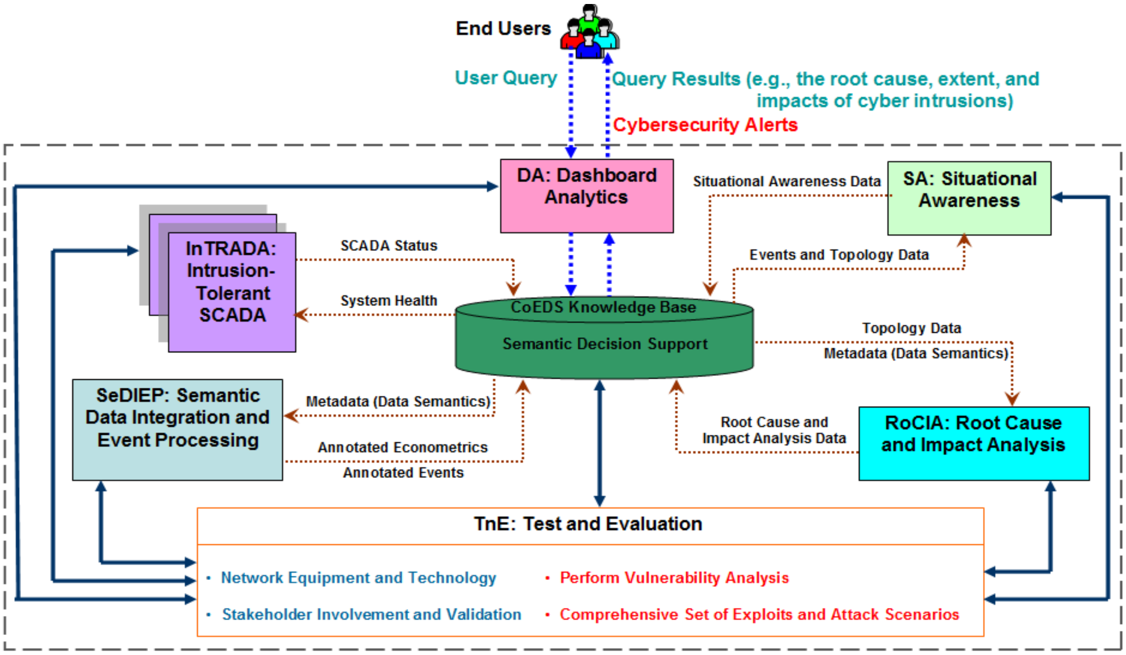
End Users
User Query
Query Results (e.g., the root cause, extent, and impacts of cyber intrusions)
Cybersecurity Alerts
DA: Dashboard Analytics
Situational Awareness Data
SA: Situational Awareness
InTRADA: Intrusion-Tolerant SCADA
SCADA Status
System Health
Events and Topology Data
CoEDS Knowledge Base
Semantic Decision Support
Topology Data
Metadata (Data Semantics)
SeDIEP: Semantic Data Integration and Event Processing
Metadata (Data Semantics)
Annotated Econometrics
Annotated Events
Root Cause and Impact Analysis Data
RoCIA: Root Cause and Impact Analysis
TnE: Test and Evaluation
Network Equipment and Technology
Stakeholder Involvement and Validation
Perform Vulnerability Analysis
Comprehensive Set of Exploits and Attack Scenarios

Figure 1. Overall architecture of InTRECS system.

2.2 InTRADA

The InTRADA subsystem represents a new way of thinking about the security and availability of SCADA. Existing approaches to SCADA security aim to *prevent* attacks, but we believe it is impossible to prevent all attacks. Therefore, InTRADA complements existing security technologies by aiming to *survive* attacks that manage to breach the security perimeter or originate from a malicious insider. To achieve this goal, InTRADA applies our Prime intrusion-tolerant replication technology [2] to the SCADA Master application [4]. We run several copies, or *replicas*, of the SCADA Master application and synchronize them using our Prime-based replication engine. Collectively, the replicas implement a *logical* SCADA Master that provides correct service and achieves its expected level of performance even if a subset of the replicas is experiencing a malicious cyber attack. InTRADA involves two key pieces. (i) An existing SCADA Master will be integrated with our Prime replication engine to make it survivable. (ii) An existing Remote Terminal Unit (RTU) will be integrated with our intrusion-tolerant libraries so that it can securely interact with the replicated SCADA Master.

2.3 CoEDS

We propose to develop a Knowledge Base (KB) upon Cybersecurity Ontologies for Energy Delivery Systems (CoEDS). The KB will contain (i) CoEDS domain ontologies, (ii) an RDF repository, (iii) a SPARQL RDF query engine, and (iv) an inference engine. Through automated data integration and logic reasoning rendered by Semantic Web techniques, CoEDS KB will be able to provide a unified and consistent data layer for analyzing data *at the semantic level*. It will thus assist end users to effectively obtain real-time decision support, so that they can (i) obtain health status updates of SCADA replicas, (ii) analyze and better understand the root cause, extent, and impacts of an attack, (iii) acquire situational awareness, and (iv) recommend courses of action. CoEDS KB will actively exchange information with other subsystems of InTRECS on a regular basis.

- InTRADA receives system health and status information from CoEDS KB, and incorporates such knowledge to enhance its fault-detection algorithms. This will enable InTRADA to more rapidly reconfigure itself in the event of a cyber attack by helping it distinguish between performance faults caused by a malicious application and by more benign issues such as transitory network problems. InTRADA sends to CoEDS KB status updates regarding the health of the replicas, hence providing data for future cyber attack analysis.
- SeDIEP obtains the data semantics, i.e., ontological metadata, from CoEDS KB and utilizes such metadata during the automatic semantic annotation. Annotated data, including cybersecurity econometrics, dynamic events, etc., are stored back into CoEDS KB to construct and continuously update the central data repository in the KB.
- CoEDS KB provides RoCIA with topology data as well as the data semantics essential for performing root cause and impact analysis. RoCIA supplies CoEDS KB with root cause and impact analysis data, including attack signatures, attack locations, exploits, consequences, countermeasures, model parameters, network components, security requirements, threats, vulnerabilities, and stakeholders.
- CoEDS KB furnishes DaSA with dynamic events and electric grid components and topology data, both of which are in an annotated form. DaSA sends back situational awareness data to CoEDS KB. In addition, the KB also provides the Correlation Layers for Information Query and Exploration (CLIQUE) and Traffic Circle, two visual analytics tools in DaSA, with interoperability for behavior model-based anomaly detection.

2.4 SeDIEP

According to the formal domain knowledge, including a global metadata model, defined in CoEDS ontologies, heterogeneous data sources can be annotated and seamlessly integrated into a central RDF data repository, which will serve as a unified and consistent data layer for data analytics applications. SeDIEP has three major components: (i) *Semantic TagPrint*, (ii) *Semantic Knowledge Management Tool* (SKMT), and (iii) *Event Engine*. Semantic TagPrint is an automated semantic tagging engine that annotates structured data and free text using ontological entities from CoEDS ontologies. SKMT manages heterogeneous data sources for semantic annotation and integration. Event engine feeds the semantic tagging engine with dynamic events. It also generates alerts with the support from CoEDS through modified RDF queries and the semantic reasoning.

With SeDIEP, heterogeneous data sources will be annotated and seamlessly integrated into a central RDF data repository based on CoEDS ontologies. This data repository will serve as a unified and consistent data layer for further analyzing data at the semantic level. Our core technologies can substantially reduce design-to-execution time for application domains of data integration, visualization, analysis, and search.

- *Meaningful data.* Our system will annotate terms in text with their corresponding concepts in CoEDS ontologies by finding their meanings and analyzing their context.
- *Scalability.* Indexed data are stored and managed in a repository. Collected and initially processed data can be incrementally analyzed and indexed.
- *Easy integration.* Various data sources can be seamlessly integrated along with their semantic indexes.
- *Flexible use of data.* Semantic data can be application independent. Therefore, indexes can be consumed and manipulated by any other energy control system (ECS) security applications.

2.5 RoCIA

After a security incident has been detected, the incident response team needs the ability to investigate and determine the root cause, attack methods, extent/consequences, affected assets, impacted stakeholders, the identity of the attackers, and other information to inform an effective response. The response team needs such information in the short term to contain or eradicate the attack, recover compromised equipment, and restore normal operations. The team also needs to determine counter-measures to prevent recurrence and possibly collect evidence to legally prosecute the offenders without interrupting the availability of an energy delivery system (EDS). SeDIEP and CoEDS subsystems will continuously collect and store network traffic and other relevant data. RoCIA will use collected data in CoEDS to provide an effective ontology-based reasoning tool to automatically detect suspicious activity and support post-incident investigation. In addition, RoCIA can identify assets and stakeholders affected by an attack as well as economic impacts to those stakeholders. RoCIA may also provide the intrusion detection system (IDS) functionality to alert personnel and other components about suspected attacks.

RoCIA will provide a Health Monitor Service (HMS) to continuously monitor SCADA components and process activities to detect faults and other abnormalities. Every process system has process variables that are used to control these processes. Values of running processes can be compared to the model with deviations identified as faults [HIE09]. RoCIA will also continuously monitor incoming data for other potential anomalies, or for traffic that matches known attack patterns. These faults will trigger alerts of a possible cyber intrusion.

RoCIA will provide an Investigation Lab (IL) to allow an incident response analyst to open an investigation, and to use a graph-based interface to search available evidence and thus determine the root cause of an incident. Analysts will be able to begin an investigation using alerts identified by the system, followed by constructing a graph of related information. We will also provide a timeline view to allow users to view events in chronological order. RoCIA IL will help analysts determine the root cause of the attack, affected assets, and stakeholders. Also, IL will provide tools that use the Cyber Security Econometrics System (CSES) model to calculate economic impacts of the attack [AIS10, SHE09]. IL will allow analysts to document their findings, lessons learned, and response actions for the attack.

2.6 DaSA

To be a complete solution that has the commercial viability, we need to integrate features in Dashboard Analytics and Situational Awareness (DaSA). We plan to develop tools to help ECS end users and analysts to see and be in command of their data in ways that are previously not possible. In addition, such tools will be customized to integrate with CoEDS KB, resulting as Dashboard Analytics and Situational Awareness capability for energy delivery ECS end users.

We propose to design a visual analytics tool to display high-level overviews of network traffic using a new behavioral, model-based anomaly detection technique. This tool will build models for learning and classifying expected behaviors on individual hosts on a network and then compare these modeled behaviors to real-time streaming data to generate early indicators of “off-nominal” network activities. The effectiveness of such a tool will be enhanced by visualization features that allow analysts to compare anomalous activities to normal conditions. Users can navigate through their data temporally, viewing time periods as short as a few minutes or as long as several years. As a result, this tool will help analysts to see departures from normal behaviors at any time scale so that users can drill down to view detailed displays of network activities and spot control system machines, buildings, facilities, or other sources of traffic behaving anomalously.

Considering that visualizations of aggregate network activities are often not detailed enough for analysts to spot subtle changes in communication patterns within large data sets, which may signal malicious behavior, we also propose to develop a second visual analytics tool, which will display raw network traffic through multiple time-based views, and with up to hundreds of millions of communication events in a single view. This second tool will enable analysts to see individual communication patterns that appear suspicious, and will be extended to support InTRECS toward providing a revolutionary improvement in situational awareness for energy management system (EMS) end users.

Note that both tools will accommodate streaming data. As new network transactions occur, our tools will display them on a moving timeline. Consequently, analysts can dynamically zoom through data spanning months or years in just seconds. Moreover, the tool will also allow for sophisticated filters that highlight important patterns in the traffic.

2.7 TnE

We plan to provide TnE validation testing, which includes a comprehensive set of experimentation, testing, and assessment. Our research team has active, directly funded research projects with numerous entities, e.g., Pacific Gas and Electric Company (PG&E), Entergy Corporation, the Tennessee Valley Authority (TVA), and the Electric Power Research Institute (EPRI). These entities will be engaged to help demonstrate and validate InTRECS outcomes.

Our testbed will be a remotely configurable, flexible, and multi-user resource that provides an experimentation facility for power system research. The testbed will be designed to enable a wide range of experimentation, both in scale and of types, by combining virtual, emulated, simulated, and physical equipments. Capabilities to be provided by the testbed will include:

- *SynchroPhasor research.* We will provide access to physical phasor measurement units (PMUs) from a variety of leading commercial vendors. In addition, PMU hardware and software development kits will be provided to enable testing of cutting-edge solutions on real platforms.
- *Automated metering infrastructure research.* The testbed is able to integrate Automated Metering Infrastructure (AMI) equipment, Itron Meters for example.
- *Energy management system.* A clone of operational energy management system (EMS) will be provided for experimentation. Archived, real-world data that are streamed will be available for replay.
- *VMware virtual environment.* A virtual environment will be made available to provide the scalability necessary to perform a wide range of experimentation (our preliminary design is up to 250 virtual equipment nodes).
- *Network emulation.* Control systems utilize the full range of communication media. The testbed will thus provide a network emulation capability that can emulate LAN, WAN, and wireless communication media.
- *Simulation cluster.* The testbed will provide a small, high-performance computing cluster for running power system simulations.

We will also implement vulnerabilities to investigate the impact of cyber attacks on physical systems. Taxonomies will be developed that group attacks by methods of delivery and impacts on physical systems. From these taxonomies we will further investigate cybersecurity intrusion detection, system protection, and attack resilience technologies.

In addition, we believe that demonstration and execution of the testing should be performed both locally and remotely, and we plan to utilize RSA SecurID VPN tunnels to provide connectivity. As a result, our testbed will be federated with other external testbeds, which provides the potential to grow and expand beyond the equipment and capabilities to other Federally Funded Research and Development Centers (FFRDCs) or research organizations and their equipment.

3. CONCLUSION

To preserve critical energy control functions while under attack, it is necessary to perform comprehensive analysis on the root cause, extent, and impacts of cyber intrusions without sacrificing the availability of energy delivery. We proposed to develop InTRECS, an intrinsically resilient energy control system, to address these challenges. In summary, InTRECS technology will (i) significantly benefit the energy infrastructure cybersecurity industry compared with state-of-the-art technologies/products that exist today; (ii) address an important cyber intrusion resiliency gap; and (iii) provide considerable technical, operational, and environmental performance improvements, cost savings, and societal benefits. An immediate future research direction is to implement subsystems described in this position paper.

4. ACKNOWLEDGMENTS

This research was partially supported through the U.S. Department of Energy (DOE) Higher Education Research Experiences (HERE) program for Faculty at the Oak Ridge National Laboratory, Oak Ridge, Tennessee, sponsored by the U.S. Department of Homeland Security (DHS).

5. REFERENCES

[1] Aissa, A.B., Abercrombie, R.K., Sheldon, F.T., and Mili, A. 2010. *Quantifying security threats and their potential impacts: a case study*. Innovations in Systems and Software Engineering, Vol. 6, No. 4, pp. 269-281.

[2] Amir, Y., Coan, B., Kirsch, J., and Lane, J. 2011. *Prime: Byzantine Replication Under Attack*. IEEE Transactions on Dependable and Secure Computing, Vol. 8 Issue 4.

[3] Hieb, J., Graham, J., and Guan, J. 2009. *An Ontology for Identifying Cyber Intrusion Induced Faults in Process Control Systems*. Critical Infrastructure Protection III, IFIP AICT 311, pp. 125-138.

[4] Kirsch, J., Goose, S., Amir, Y., and Skare, P. *Toward Survivable SCADA*. Proc. 7th Annual Cyber Security and Information Intelligence Research Workshop, Oak Ridge, TN, October 2011.

[5] Sheldon, F.T., Abercrombie, R.K., and Mili, A. 2009. *Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission*. Proc. the 42nd Hawaii International Conference on System Sciences.