Rapport

Cyber-threat analysis for Cyber-Physical Systems

Technical report for Package 4, Activity 3 of ELVIRA project.

Technical Report HS-IIT-18-004

Editor: Yacine Atif

2018-08-25

Cyber-threat analysis for Cyber-Physical Systems

Technical report for Package 4, Activity 3 of ELVIRA project.

Authors

Yacine Atif (University of Skövde)

Yuning Jiang (University of Skövde)

Manfred Jeusfeld (University of Skövde)

Jianguo Ding (University of Skövde)

Birgitta Lindström (University of Skövde)

Sten F. Andler (University of Skövde)

Christoffer Brax (Combitech)

Daniel Haglund (Combitech)

Björn Lindström (Combitech)

EXECUTIVE SUMMARY

This document reports a technical description of ELVIRA project results obtained as part of Work-package Activity 4.3 entitled “Cyber-threat analysis for Cyber-Physical Systems”. ELVIRA project is a collaboration between researchers in School of IT at University of Skövde and Combitech Technical Consulting Company in Sweden, with the aim to design, develop and test a testbed simulator for critical infrastructures cybersecurity.

Smart grid employs ICT infrastructure and network connectivity to optimize efficiency and deliver new functionalities. This evolution is associated with an increased risk for cybersecurity threats that may hamper smart grid operations. Power utility providers need tools for assessing risk of prevailing cyberthreats over ICT infrastructures. The need for frameworks to guide the development of these tools is essential to define and reveal vulnerability analysis indicators. We propose a data-driven approach for designing testbeds to evaluate the vulnerability of cyberphysical systems against cyberthreats. The proposed framework uses data reported from multiple components of cyberphysical system architecture layers, including physical, control, and cyber layers. At the physical layer, we consider component inventory and related physical flows. At the control level, we consider control data, such as SCADA data flows in industrial and critical infrastructure control systems. Finally, at the cyber layer level, we consider existing security and monitoring data from cyber-incident event management tools, which are increasingly embedded into the control fabrics of cyberphysical systems.

Table of Contents

1 Introduction

Cyberphysical systems comprise networks of control elements that employ advanced monitoring and communication technologies to deliver reliable and secure industrial or critical-infrastructure operations. Smart grid employs cyberphysical systems in an evolution from ageing power-delivery systems, in order to optimize and protect electricity delivery operations. These processes could be facilitated by the analysis of data that originate from the different layers composing the cyberphysical systems in smart grid architectures. Figure 1 shows an overview of dynamic data-flows across smart grid layers, which include SCADA as an instance of cyberphysical systems to maintain a continuous and instantaneous balance between generation and load of power. Data is organized into time-synchronized instances sampled from several sources, and involving a range of contemporary sensors [1]. Data flows are produced by measurement components such as SCADA Remote Terminal Units (RTUs), which transmit telemetry data from sensing devices that are associated with power physical-components to a Master Terminal Unit (MTU) system. Commands from the master supervisory system are conveyed back to connected physical power components to close the control loop process. Phasor measurement units (PMUs) measurements on the other hand, provide another source of data in the form of synchronized information about the magnitude of power signal wave (called phasors) across the power-grid using a common time-source for synchronization, retrieved generally from a Global Positioning System (GPS) receiver [2].

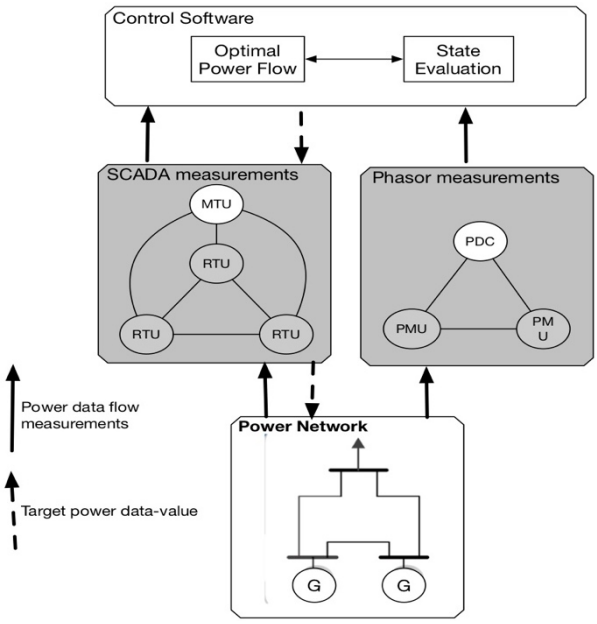

Figure 1: Smart Grid system diagram

These measurements are used to estimate power-grid state by the SCADA software level to derive optimal power-flow parameters. Hence, power management systems rely on data to monitor and operate power grids. However, data is transmitted across information technology infrastructures and employing microprocessor-based computational nodes. These structures are prone to potential vulnerabilities, which could be exploited by a wide range of notorious cyberthreats. Figure 2 shows a possible scenario induced by false-data injection threat, at some level of the SCADA control loop.

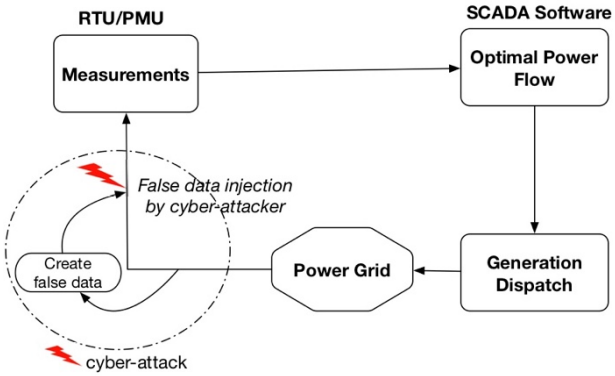

Figure 2: Cyberphysical system vulnerability

These opportunistic threats evolved into major issues with actual nation-wide incidents [3], which can cascade into detrimental consequences to crucial societal functions. The Ukraine Blackout in 2015 was caused by a synchronized and coordinated cyber-attack that affected over 200,000 individuals for several hours . Hence, it is important to assess cyberphysical systems infrastructures such as prevailing smart grids to evaluate their vulnerability index and alleviate concerns over cyberthreats. Grid operators need to gauge investments into security measures against vulnerability indexes to optimize the value of investment. Prevention against malicious cyberthreats such as malware or false-data injection has increased recently due to the above mentioned incidents and more recent ransomware ones. Due to the vital domains where these cyberphysical systems are deployed online, the security analysis of these systems are evaluated offline using actual data logs from live or simulated infrastructures. In this paper, we discuss vulnerability metrics, and their impact of cyber-attack prevention. Cyberthreats to cyberphysical systems are distinguished by their multidimensional attributes, which similarly call for analysis methodologies that encompass multidimensional elements, including physical, control and cyber elements. The main contribution of this paper is the specification a smart-grid security-prevention approach, which includes vulnerability assessment methodologies derived from power, control and cyber elements that make the grid layers. A testbed may use this specification to enable a co-simulation of these elements and related-operations for evaluating the vulnerability of an infrastructure model.

Vulnerability analysis may also enable a learning-continuum to raise awareness and readiness levels through simulation games that lead to progressive developments of new skills and joint-strategies. The multi-layered architecture and threat scenario repository of vulnerability-analysis testbed captures various data-flows for threat intelligence to support decision-making in security investments. Towards this objective, we contribute a vulnerability assessment model which includes a vulnerability metric to leverage data from cyberphysical systems' control and monitoring processes for security mechanisms. In doing so, we address the major challenge induced by the lack of direct mappings between threat patterns and security event logs in cyberphysical systems. It is a significant task to map collections of unrelated events inferred from dynamic cyberphysical systems' data to threat patterns because both accounts of information are described in unstructured data. The results, are derived attack-scenarios' awareness that empowers security analysts' competencies. The provided support automatically gather and cluster analysis data to reduce information-overload effects and hence reduces analysts' time to evaluate potential vulnerabilities. In addition, a correlation between evidences and known threat patterns is automatically suggested, along with mitigation recommendations.

The remaining sections of this document are organized as follows: Section 2 presents some relevant background and discusses some related works. Section 3 reveals a methodological approach to vulnerability analysis for cyberphysical systems, with focus on a smart-grid infrastructures. Section 4 describes the testbed framework design, and provides an overview of some relevant algorithms that contribute to vulnerability analysis and visualization. Section 5 concludes the paper with a summary of the proposed work and some follow-up work suggestions.

2 Background and related works

In smart-grid, power network state *x* is inferred from flow-measurements *y*, and power network model *M* using some power transformation model such as:

$$y=Mx+e \quad (1)$$

In the above model, *x* is a vector representing the state of power-network buses and *y* is a vector representing collected data. However, inaccurate measurements resulting from failing control elements such as RTUs (or Remote Terminal Units) and communication network failures are common in SCADA control-networks, and modeled as an error-vector *e*, in the power network state evaluation model of Equation 1. Hence, power network state is determined by resolving Equation 1.

2.1 Vulnerability assessment

According to the definitions and countermeasures provided by ISO/IEC 27005 and ISO/IEC 15408-1: 2009 standard, threat, risk, asset and vulnerability are the essential taxonomy concepts depicted in Figure 3, which is modified from Lehto's diagram [4]. The links between the concepts show the relationship between them. Namely, infrastructure owners need to be aware of potential infrastructure vulnerabilities to gauge investments into countermeasures, as indicated earlier. Threat actors generate threats using exploit vectors. To accomplish such malicious act, threat actors need to develop a certain level of awareness about exploit-vectors to plan the threat injection. A threat materializes into attack vectors which could disrupt some infrastructure assets. Vulnerabilities induce risks to the assets with plausible service disruptions.

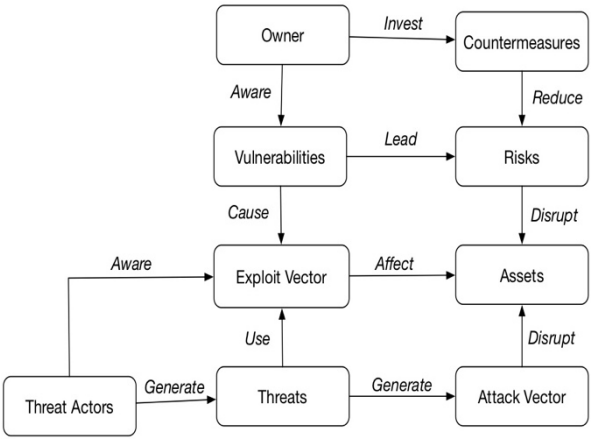

Figure 3: Concepts and relationships.

Vulnerability is defined as "weakness of an asset or control that can be exploited by a threat" according to ISO/IEC 27000:2009. Based on this definition, three aspects need be considered when conducting vulnerability analysis. Those three aspects are 1) type of the threat, 2) probability of acquiring related exploits, and 3) the victim assets that might be involved, separately. Vulnerability is also associated with the minimum number of measurements that ought to be corrupted by an attacker in order for the attack to remain unnoticed (i.e. stealth attack). Measurements can originate from control, cyber or phasor data. A combined stealth-attack may use these different data sources to drive an attack vector *a* into affecting the estimated power-state vector *x* that may be shifted by the attack into $x' = x+a$ [5].

2.2 Cyber Threats for smart grids

Cyber-threats are usually classified through the information about threat actors, as well as exploit and attack vectors [4]. A threat actor is any person or thing or organization that cause or transmit a threat [6]. Common threat actors include cyber criminals, terrorists, hackers, etc. An attack vector is a path by which an attacker engages into a malicious outcome, whereas an exploit vector represents the available means or opportunistic gaps that make such an engagement possible. Typical cyberthreats to smart-grid infrastructure originate at the three layer levels of smart-grid architecture, as shown in Figure 4.

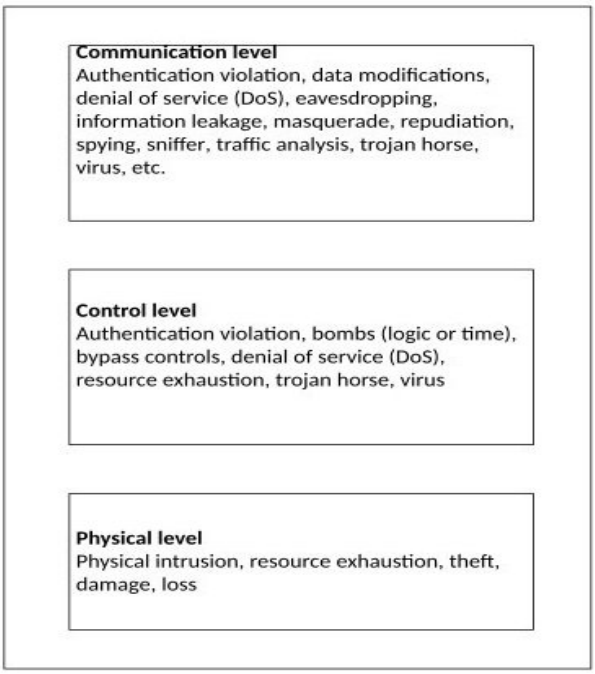

Figure 4: Three-level cyberthreat types for smart-grids

In this paper, data reported from multiple smart-grid component levels, including physical, control, and cyber layers are used to evaluate assets' vulnerability to cyberthreats such as the ones shown in Figure 4. Data at the physical layer, may originate from power inventory and digital fault recorders (DFRs) [7]. At the control level, data may originate from SCADA [8] about power-flow from RTU sensors, and control-commands from MTU (Master Terminal Unit), as well as Phasor Measurements Unit (PMU) data [9] from synchrophasor. Finally, at the cyber layer level [10], we consider data from cyber-incident event management tools, which are increasingly embedded into smart grid fabrics. The combination

of these data-sources to compute vulnerability is both typical and original, when applied to cyberphysical systems, such as those employed in smart-grids.

3 Methodological approach to vulnerability assessment

Vulnerability index in smart-grid is determined by a sequence of data instances where a region of similarities that may be a consequence of functional relationships match exploit-vector patterns. Numerous sequences may be aligned by algorithms. Cybersecurity contingency is further optimized considering the outcome of vulnerability analysis against cybersecurity budget. A ranked set of issues is worked out to allocate investment into prioritized weaknesses. The need and potential of similarity analysis to match archetype patterns of cyberthreats allows a quantification of vulnerability by applying an indicator-based clustering analysis, where the initial centers indicate the features of well-known threat patterns.

3.1 Vulnerability metric

A vulnerability metric starts by elaborating an evolving inventory of data collection about new information on existing threat alerts or attack trends via their corresponding exploit vectors, to create data models of known patterns. These source exploit-vectors may originate from security alerts from national cybersecurity organizations or security product-vendors, as well as security alerts from critical infrastructure industry or known threat classification [11]. These may include feeds from US-CERT (United States Computer Emergency Readiness Team) alerts, NVD (National Vulnerability Database) feeds, Common Attack Pattern Enumeration and Classification (CAPEC), and CVE (Common Vulnerability and Exposure) list. These publicly available repositories provide a comprehensive dictionary and classification taxonomy of known attack patterns that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.

Gathered attributes from threat exploit-vectors are employed in a machine-learning process based on cluster analysis for quantifying vulnerability. Each cluster may contain the multidimensional information describing the threat features via their representative exploits vector. These attributes form an account of exploits chronologically organized into a vector-pattern, indicating the level of required-knowledge about each exploit for the threat to materialize. The resulting exploits vector conveys a method that a given threat to compromise the target. For example, an exploit vector may include access to admin credentials, and remote execution service to instantiate a DDoS threat.

Clusters of data labelled I_i act as a reference for vulnerability index *i*, referring to a specific thread model and represented by the corresponding exploit-vector, which acts as the cluster centroid. On the other hand, time-synchronized interval-data are first classified in order to isolate normal data from threat-prone data. Measurements vector V_i belongs to a cluster labelled I_i if its similarity value to the representative exploit-vector of Cluster I_i is smaller than any other value of the other cluster exploit-vectors. Each data-vector is evaluated with respect to its distance from the associated cluster centroid V_i, using Euclidean cosine similarity, where vector-attributes refer to exploit-instances relevant to threat *i*. Only angular-distances lower than $\pi/2$ are considered in clusters, so that the cosine is confined between 0 and 1, in the following similarity measure:

$$d(\vec{V}_i,\vec{V}_j)=\cos(\vec{V}_i,\vec{V}_j) \quad (2)$$

In the above equation, V_j, is worked-out by the cyber-incident management (i.e. SIEM) following a fusion-process of data account from other data-sources of the cyberphysical system structure. Any instance of the *n* exploits in V_i, that is not observed in the collected data reported by SIEM, is set to zero in V_j. Both vectors share the same set of vocabularies, which originate from the text used in both incident management reports and public threat-pattern repositories. Hence, the above equation measures the progression towards a vulnerable-state represented by the exploit-attributes of Vector V_i, considering term frequencies in both incident-events and pattern vectors. The top-k events ranked with respect to their proximity to pattern-vectors, provide an overview on vulnerability evolution. Subsequently, the vulnerability index to Threat *i*, is determined by:

$$X_i=\frac{\sum_{j=1}^{j=k} d(\vec{V}_i,\vec{V}_j)}{k} \quad (3)$$

Vulnerability index is a score of awareness about an exploit by an entity which originates from a given threat pattern. The score expresses an affinity distance with a threat profile to indicate the probability that a particular node is exposed to a targeted cyber-threat. This approach to vulnerability could be mapped to CVSS (Common Vulnerability Scoring System) standard, which defines vulnerability as a function of exploitability [12].

3.2 Vulnerability analysis

Smart-grid architecture data flows are typically communicated in intervals format, where synchronized sampling and measurements are reported by monitoring and control-devices operated at SCADA, PMUs, DFRs and cyber-incident monitoring system levels. Measurements observed within a common time-window are considered to form a consistent picture of the smart grid. The goal of vulnerability analysis is to detect and rank security weaknesses as part of a risk management inventory. This is facilitated by testbed to give an indication on tpossible security issues in the form vulnerability indexes with respect to specific threats.

In the proposed data approach, physical-process (i.e. power) data is first classified to discriminate abnormal data. Subsequent analysis determine key relationships from data emerging from cyber-incident system sources which could lead to the discovery of vulnerability instances as illustrated in Figure 5. In the proposed system approach, events data are gathered from multiple sources and related to each other via temporal attributes and events' chronology, to investigate their mapping with known threat patterns. The goal is to identify the top-k of most similar security events within a threat-pattern of clustered data, which can track a specific progression into a vulnerable state, defined in the above-mentioned public repositories. The set of events is presented to analysts in the form of dashboard along with recommendations extracted from the same repositories reporting known incidents and mitigation practices. The analysts can then assess the security accounts and recommendations, and automatically build a report, which is going to be used for calculating returns on security investments.

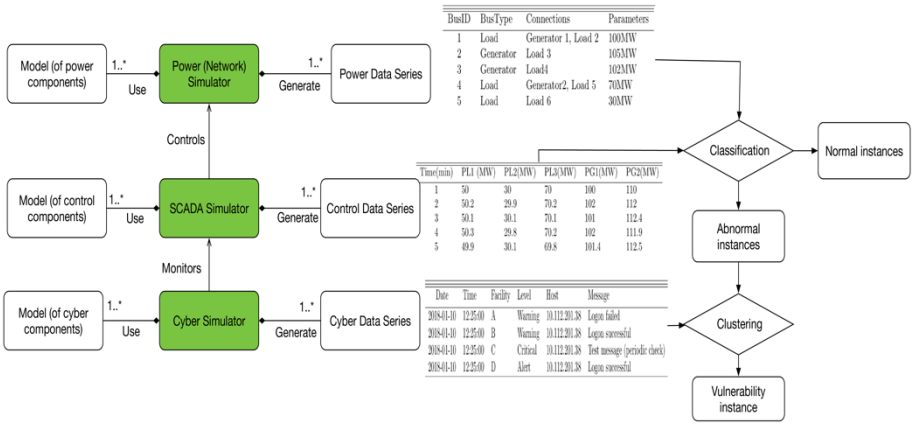

Figure 5: Data analysis in a smart-grid co-simulation testbed

Patterns identification drive available data from power topology, control processes, and cyber-incident logs to support decision-making in investment for smart-grid security. The co-simulation framework of a testbed can automate the data-generation process used for further investigation. Intrusion instances are preliminary determined from beyond-normal variations of power-flow instances, where transient behaviors can be recognized by a set of differential equations [13]. The power network topology and related asset data are used to determine sustainable thresholds of power components, which are contrasted against power-flow variation instances to isolate candidate intrusion instances. These data series are then correlated with log data from cyber-incident reports where timestamps are used to match incident and intrusion event occurrences in order to assert vulnerability states. A vulnerability index is subsequently derived and feedback to system operators so that they can alleviate the risk in their current control practices. Further analytics can be gathered and analyzed to root-out vulnerability issues along cyberphysical system exploit vectors, such as smart grid as illustrated in Figure 6. The data sources conglomerate Digital Fault Recorders (DFRs) that are embedded into the physical power-grid to report disturbances, along with phasor data from PMUs, control data from SCADA and cyber-incident data from a security event management system.

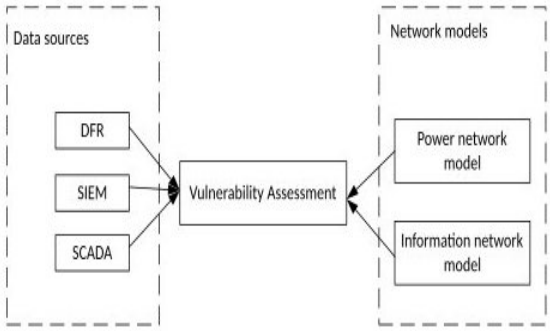

Figure 6: Data sources for vulnerability assessment

4 Testbed for vulnerability assessment

Vulnerability analysis is a procedure for cyber-threat evaluation performed by a scanning testbed using log data from a smart-grid infrastructure offline. It is an alternative to integrate the vulnerability scanning tool online into an operating smart-grid system because of the reluctance of smart-grid operators to develop adverse effects on a critical live system. Therefore, a testbed abstracts complex structures of smart-grids to replicate only the relevant processes for evaluating and identifying vulnerability to cyberthreats that could evolve into potentially adverse behaviors of smart-grid's interacting cyber-physical systems, when exposed to an actual cyber-attack. Hence, risk assessment plans can be elaborated and tested using data that mimic dynamic processes of real-word environments, Data is typically time-stamped and revolves around a multiagent-based system of the testbed architecture show in Figure 7. Data can be supplied offline via log repositories or generated through a simulation model of the smart-grid infrastructure, which includes a scenario player and an emulation of cyberphysical components, involved in a co-simulation framework. However, the simulation model is outside the scope of this paper, and the proposed vulnerability framework assumes the availability of supplied source-data to focus on the vulnerability analysis model of Figure 7, which illustrates the position of that module in the overall testbed architecture.

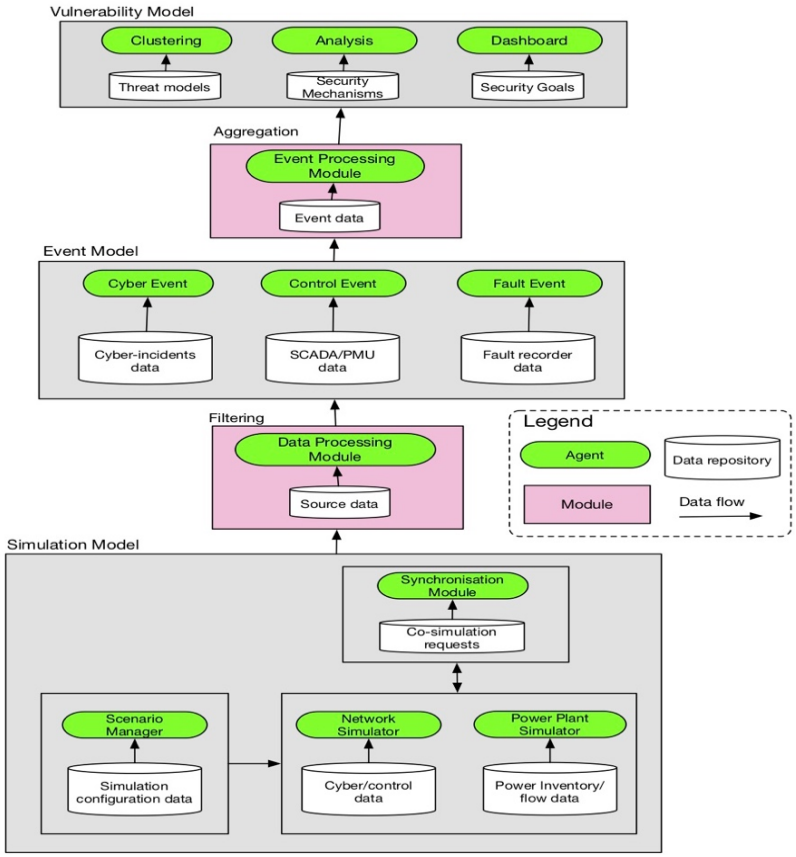

Figure 7: Testbed architecture

Each testbed agent keeps a fixed time-window size OUTPUT buffer of data, which is continuously replenished by sources to connected log-data repositories. The agents we consider in the scope of this paper are the Clustering, Analysis and Dashboard agents. An agent signals an event to express the need for synchronization to the testbed scheduler by placing a request into the scheduler request-queue.

The testbed scheduler retrieves the OUTPUT buffer data from the corresponding source agent, as well as current agent-time and state. Then, the retrieved buffer data is delivered to a destination agent's INPUT Buffer. The scheduler's queue ensures that no agent request for Input/output goes unattended. Hence, agents interact with each other by exchanging event messages via the scheduler. Outputs from an agent become inputs for other agents. The agent state is updated by external input events (inputs) and internal events. Each event is considered instantaneous or "atomic" (i.e. no duration). Events change the state and an agent stays in a state until either it receives an input, or a predetermined amount of time elapses. A class diagram model of an agent is described in Figure 8, following the BDI (Belief-Desire-Intention) framework [14].

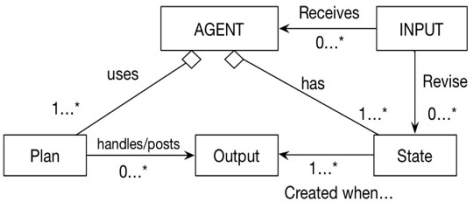

Figure 8: Agent structure

4.1 Clustering agent

A machine learning algorithm based on k-Nearest-Neighbour ((k-NN), which is amongst the simplest approaches to supervised learning and which does not require prior knowledge about data dimensionality [15] forms the clustering agent activity. This agent evaluates the top-k related events data from log data to given threat patterns. The agent's input consists of data-streams segmented into time-windows, used to determine the threat category that is nearest to this input data. The proposed multi-agent environment collects data streams from source agents in the testbed, and identifies the clusters where the new records are added using the previously mentioned similarity metric in Equation 2.

4.2 Analysis agent

The analysis agent determines the vulnerability index to given threats using the formulation expressed earlier in Equation 3, within a given time-window as well as the evolution of vulnerability indexes across a sequence of time-windows. The size of the time window and observed sequences are parameters set by security analysis. The output values are shared with dashboard agent for visualization of vulnerability-index evolution.

4.3 Dashboard agent

Dashboard agent is used to visualize vulnerability-evolution across threat-patterns. Index values are used to prioritize security investments and to facilitate risk management. A flowchart containing risk elements and index values is horizontally represented by the dashboard agent. When OUTPUT data from analysis is delivered to dashboard INPUT buffer, the dashboard elaborates initial risks and the corresponding measures retrieved from published repositories to alleviate those risks. A comprehensive view of the interactions between threats, vulnerabilities and risks uses the Risk

Reduction Overview (RRO) threat modelling technique. RRO has been used as an effective visualization method within the last decade, by comparison to other risk-management visualization methods such as Attack Countermeasure Trees (ACT) [16] and Attack Trees [17]. And RRO is proven to provide an intuitive overview of the coherence of risks and measures [18]. Hence, the adoption of this technique as the corer module of dashboard agent.

5 Conclusion

A data-driven approach to vulnerability assessment is proposed to support a security testbed for cyber-physical system. Security-prevention schemes are developed as a consequence of plausible threats and related exploit-vectors. Given the nature of cyberphysical systems, data-flows generated from different both process, control and cyber levels are involved to assert vulnerability. A data-oriented vulnerability metric and an analytical vulnerability analysis based on a machine-learning technique are discussed in this paper. The overall multi-agent based architecture of the testbed employing the proposed vulnerability-assessment module is also presented, where we emphasized the role of clustering, analysis and dashboard agents. A case study scenario is being worked-out to validate the proposed approach in a smart-grid context, and hence cyberphysical system illustrations used throughout this paper use this critical infrastructure as instance of cyberphysical system models.

This work presents the first investigation-step into a comprehensive data-driven framework for multi-layered threat analysis with the elaboration of cyberphysical-systems-specific vulnerability metrics. These systems are distinguished from communication-network systems, by their interweaving into the physical process fabric. Our future works includes the elaboration of a case-study scenario to evaluate and refine the proposed vulnerability assessment model, and the integration into a tested under development to simulate the cyberphysical-system perspective of a smart-grid.

6 Acknowledgments

This research has been supported in part by the EU ISF Project A431.678/2016 ELVIRA (Threat modeling and resilience of critical infrastructures), coordinated by Polismyndigheten/Sweden.

7 References

[1] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid – the new and improved power grid: A survey,” *IEEE Communications Surveys Tutorials*, vol. 14, pp. 944–980, Fourth 2012.

[2] K.-S. Cho, J.-R. Shin, and S. H. Hyun, “Optimal placement of phasor measurement units with gps receiver,” in *2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194)*, vol. 1, pp. 258–262 vol.1, Jan 2001.

[3] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 ukraine blackout: Implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, pp. 3317–3318, July 2017.

[4] M. Lehto, “Phenomena in the cyber world,” in *Cyber Security: Analytics, Technology and Automation*, pp. 3–29, Springer, 2015.

[5] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, “Combined data integrity and availability attacks on state estimation in cyber-physical power grids,” in *Proceedings of 7th IEEE International Conference on Smart Grid Communications (SmartGridComm 2016)*, 2016.

[6] L. Marinos and A. Sfakianakis, “Enisa threat landscape-responding to the evolving threat environment,” *ENISA (The European Network and Information Security Agency)(September*

2012), 2012.
[7] E. M. Davidson, S. D. McArthur, J. R. McDonald, T. Cumming, and I. Watt, "Applying multi-agent system technology in practice: automated management and analysis of scada and digital fault recorder data," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 559–567, 2006.
[8] S. A. Boyer, *SCADA supervisory control and data acquisition*. The Instrumentation, Systems and Automation Society, 2018.
[9] K. E. Martin, "Synchrophasor measurements under the ieee standard c37. 118.1-2011 with amendment c37. 118.1 a," *IEEE Transactions on Power Delivery*, vol. 30, no. 3, pp. 1514–1522, 2015.
[10] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE transactions on Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.
[11] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology*, 2018.
[12] P. Mell, K. Kent, S. Romanosky, N. I. of Standards, and T. (U.S.), *The Common Vulnerability Scoring System (CVSS) and its applicability to Federal agency systems [electronic resource] / Peter Mell ; Karen Scarfone ; Sasha Romanosky*. U.S. Dept. of Commerce, National Institute of Standards and Technology Gaithersburg, MD, 2007.
[13] F. Milano and R. Zarate-Minano, "A Systematic Method to Model Power Systems as Stochastic Differential Algebraic Equations," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4537–4544, 2013.
[14] A. S. Rao and M. P. Georgeff, "Bdi agents: From theory to practice," in *In Proceedings of the First International Conference on Mult-agent Systems (ICMAS-95)*, pp. 312–319, 1995.
[15] T. Cover and P. H. theory, "Nearest neighbor pattern classification," *IEEE Transactions on Information Theory*, vol. 13, no. 1, 1967.
[16] A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (act): towards unifying the constructs of attack and defense trees," *Security and Communication Networks*, vol. 5, no. 8, pp. 929–943, 2012.
[17] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.
[18] H. N. J. Havinga and O. D. T. Sessink, "Risk reduction overview," in *International Conference on Availability, Reliability, and Security*, pp. 239–249, Springer, 2014.