Cyber-Threat Intelligence Architecture for Smart-Grid Critical Infrastructures Protection

Yacine Atif[1], Jianguo Ding[1], Birgitta Lindström[1], Manfred Jeusfeld[1], Sten F. Andler[1], Yuning Jiang[1] Christoffer Brax[2], Per M. Gustavsson[2]

[1] School of Informatics, University of Skövde, Sweden
{Yacine.Atif, Jianguo.Ding, Birgitta.Lindstrom, Manfred.Jeusfeld, Sten.F.Andler}@his.se
[2] CombiTech AB, Skövde, Sweden
{christoffer.brax, per.m.gustavsson}@combitech.se

Abstract. Critical infrastructures (CIs) are becoming increasingly sophisticated with embedded cyber-physical systems (CPSs) that provide managerial automation and autonomic controls. Yet these advances expose CI components to new cyber-threats, leading to a chain of dysfunctionalities with catastrophic socio-economical implications. We propose a comprehensive architectural model to support the development of incident management tools that provide situation-awareness and cyber-threats intelligence for CI protection, with a special focus on smart-grid CI. The goal is to unleash forensic data from CPS-based CIs to perform some predictive analytics. In doing so, we use some AI (Artificial Intelligence) paradigms for both data collection, threat detection, and cascade-effects prediction.

Keywords: critical infrastructures, cyber-threat, situation awareness, smart-grid, machine-learning, artificial intelligence, multi-agent systems

1 Introduction

Critical infrastructures (CIs) include assets that are essential to societal functions. However, natural disasters, malicious attacks and criminal activities represent potential threats that can disrupt this backbone of national economies. Power grid is a CI example, which is distinguished by the complexity of its network and rising concerns over cyber-attack threats. A hypothetical cyber-attack scenario by Lloyd's of London in a joint effort with the University of Cambridge's Centre for Risk Studies predicts almost 100 million US citizens would be plunged in a blackout [13] following the cascading-effect of some initial trigger. Attacks could be initiated in the form of trojans spreading through the network and compromising power-control stations, in several geographical locations. The limitations of classical power-network led to the evolving smart-grid which transforms traditional power-systems into an information system which can predict and intelligently respond to energy-demand [5].

The smart-grid communication architecture connects an enormous number of electrical devices, to transport different classes of data. This communication

infrastructure also includes the sensing-devices used to control various power-grid equipments and monitor related environmental-measures [10]. This intricate infrastructure is subject to failure risks that range from natural causes to deliberate attacks. Indeed, data exposure into cyberspace may lead to breach incidents despite the security-mechanisms employed at the control-level by systems such as the Supervisory Control and Data Acquisition (SCADA) [2] and the adoption of proprietary network protocols specifically for the smart-grid at the data-communication level, such as Home Area Networks (HANs), Building Area Networks (BANs), Industrial Area Networks (IANs) [19]. This lack of immunity against threats that could spread across sprawling transmission lines of such a vital CI, calls for new architectural models to support the evolution of new situation-awareness and incident-management systems that predict suspected failures, and support real-time decisions, which prevent or alleviate cascading-effects.

There are several situation-awareness models discussed in the literature. In this paper, we advocate Mica Endsley approach, which is one of the most popular and widely accepted by the research community [3]. This model, illustrated in Fig. 1, comprises three levels within the situation awareness phase to support decision-making process, as a precondition for the action impacting CI components: perception, comprehension and projection. Following this mode, a potential threat should draw the attention of CI operators in the perception level. Subsequently, the nature of the threat is differentiated to comprehend its features and damage expectations. Finally, a projected-plan of the cascading-effects is predicted to anticipate further consequences of the threat. The resulting new situation is returned by a loop-back control process to continue assessing the dynamic situation of CI. Based on this situation-awareness model, we develop a threat-notification and identification approach to perceive and comprehend the nature of the threat. Our approach uses spatial and temporal measurements reported by cyber-physical elements embedded within substations of the smart-grid. In doing so, we classify reported data into threat or non-threat data. A threat modeler follows to analyze further data features in order to predict threat consequences and plausible cascading-chain scenarios. Then, a threat-evolution model projects the cascading-effects across a single-dimensional time-line to establish a cascading-schedule with decision-points for operators to intervene. This work is distinguished by its architectural modules which facilitate the development of data-intensive techniques across the entire spectrum of CI protection. These modules streamline data-collection, threat identification and cascading-chain prediction in cyber-physical-augmented CIs, such as the smart grid.

Critical infrastructures such as energy-related services have become increasingly dependent on cyber-physical systems to facilitate communication, but at the same time they became vulnerable to cyber-attack threats. Data stores and analysis mechanisms emerged as a promising countermeasure approach to alleviate induced-damages from these threats [7]. Defeating cyber-attacks require judicious data architectures to harness multidimensional complexities prevailing in CIs. The architectural model discussed in this paper focuses particularly on

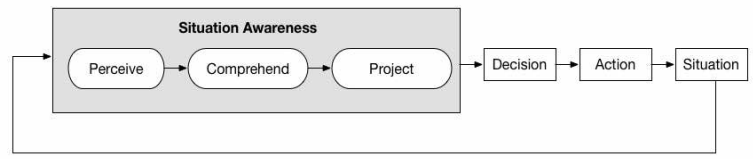

Fig. 1: Situation awareness model [3]

recognizing cyber-attacks which may deliberately incapacitate a smart-grid or related assets resulting in dysfunctions on dependent CIs. The proposed architecture organizes data to support context-aware decision-making, when designing prevention (in off-line simulations) or recovery (in online -real-time- deployment) plans for emergency-response to evolving threats. The remaining sections of this paper are organized as follows. Section 2 presents some background and state the problem discussed in this paper. Section 3 reveals a cyber-physical-model for smart-grid CI. Section 4 shows our reflection of situation-awareness modeling for CI protection, following Endsley's road-map introduced earlier in this paper. This section includes our threat identification and evolution approaches. Finally, we conclude the paper in Section 5 with a summary of results and some of our planned future works.

2 Background and related works

2.1 Contemporary threats to critical infrastructures

Threat triggers are bound to infect CI components in what is known as cascading effects, which gradually increase the magnitude of damages across CI and dependent operations. Threat evolution models involve procedures to minimize the disruptive outcomes from CI components' failure and accelerate recovery. However, the desired resilience index comes at some cost thresholds that decision-makers need to weight to change the course of cascading events following a detected failure [20]. The high degrees of interdependencies generally make CI systems more efficient under normal operations but more vulnerable to cascading-effects when a threat-failure occurs [14]. Incident management includes organizational and operational readiness, to shift the course of CI threats. This requires a situation awareness and understanding of CI resources, their temporal attributes to withstand threats and their geospatial distribution to assess the scale of threat infection. Hence, an increasing focus on incident management methodologies and supporting tools to empower decision-makers situating key points in the incident evolution, is being addressed by the research community to support crisis management around CIs [12, 8, 16]. Nevertheless, CI protection is a relatively new area of research, whereby contemporary cyber-attacks and natural disasters have shown that the impact of threats on CIs are analyzed through offline or real-time simulation tools to predict outcomes and deploy countermeasures [16]. Earlier studies revealed that threats and vulnerabilities in CI systems show two important trends in methodologies and modeling. A first

one relates to the identification of methods, and techniques to describe the current state of CI, whereas the second trend manages the dynamic evolution of CI systems by means of simulation techniques including systems dynamics, Monte Carlo simulation, and multi-agent systems [22]. We address both trends in this paper, as they are interrelated in a holistic architectural approach to CI security monitoring.

2.2 Smart-grid monitoring

Smart-grid is an example of CI that weaves power-components and embedded data to derive information across two-way cyber-communication technologies. Computational intelligence uses this data to supply algorithms, architectures and applications needed for the development of smart grid-related operations.

Smart grid data is typically communicated in intervals format. For example, smart meter records consumption of electric energy in intervals of an hour or less and communicates that information, at least daily back to the utility for monitoring and billing. Power systems employ synchronized sampling and measurements with monitoring and control devices operated by SCADA-like systems. Power measurements are derived from several samples, that are associated with a data-window spanning the sample set. Simultaneous such measurements may be considered with several voltages and currents over the same data-window to form a consistent picture of the power network. This operation facilitates power-network monitoring, protection and control functions, as well as tracking dynamic phenomena that may threaten power networks. Simultaneous measurements can be obtained by synchronizing sampling-clocks across the power system, at each substation measurement site [18]. Sensing devices monitor the power flowing over the grid and take snapshots of currents and voltages. Time synchronized data could be correlated with each other from all sensors (across substations) to analyze interval-based power-system events, for clustering them into patterns in order to isolate faults and threat-triggers.

Interval-based events are characteristic for utility services such as the power grid. The power grid is a system to deliver electrical energy from power plants to customers. The energy measured in kilowatt hours (kWh) is the integral of the power (kW) over time. Hence, one can sub-divide time into intervals units such as hours and monitor the delivery of energy in the grid via these discrete units. The introduction of smart meters at the consumer premises contributes to the transmission of such interval-based measurements to grid operators. The smart management of the power grid does however also create new vulnerabilities, e.g. by manipulated event messages from smart-meters and other sensors in the power-grid.

2.3 Data analytics for critical infrastructure protection

Clustering sampled interval-based power-data could contribute to accurate diagnosis/prognosis as well as superior levels of situational awareness over smart

grids, in support of operational resilience upon contingencies and malicious attacks[4]. Traditional clustering methods are unsupervised and aim at finding patterns based on features in the data set [1]. A feature can usually be represented as a multi-dimensional vector $\vec{V_i} = (x_1^i, x_2^i, ..., x_n^i)$, and a label $l_k \in L$ is assigned to $\vec{V_i}$ depending on the distance metric used among feature vectors. In smart-grid context, multidimensional data vector could refer to voltage, current phasors, and frequency measurements at some substation, whereas labels could refer to anomaly detection levels corresponding to deviations from expected values. The process of labeling data forms clusters that could be mapped to benchmarked classification of anomaly schemes.

3 Data architecture for cyber-physical-based critical-infrastructures protection

We investigate the integration of software agents to testbed CI security, using a multi-agent system architecture around the Blackboard paradigm for the development of a CI analysis toolkit, in the context of power-plant related scenarios [11] that automate a number of security controls, including preventive and recovery controls. These cornerstone modules to support situation-awareness [21] in smart-grid infrastructures provide cyberattack diagnosis, as illustrated further in Fig. 2. From top to bottom, the smart grid architecture could be layered into four blocks: information, data, sensing/actuating devices and physical-power components that make-up the actual power-equipment. Horizontally, power transmission is carried out by enterprise grid infrastructures, covering various geographical territories -possibly interconnecting separate grids-, across increasingly deregulated markets. This level includes high-voltage, long-range lines for transmission and medium- to low-voltage lines for distribution and electrification across various national districts.

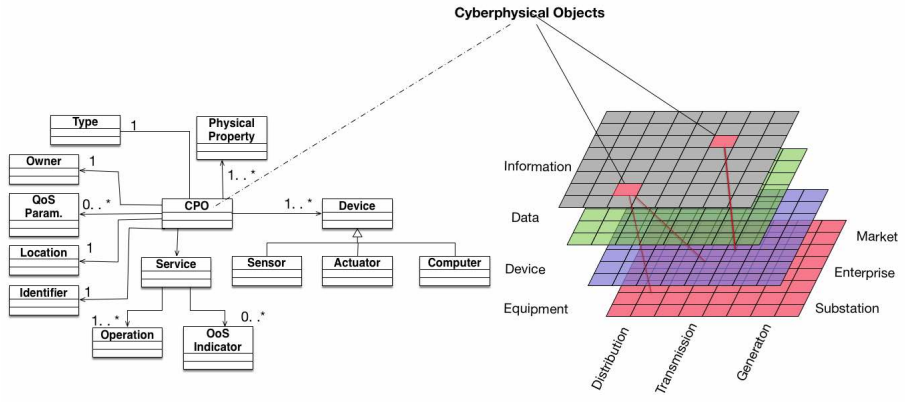

Fig. 2: Data architecture

In cyber-physical systems (CPSs), it is the data that are valuable for end-use: hardware, devices and communication technologies are ideally hidden from interfacing applications. To inter-operate with diverse applications, a metadata layer filters out the data across CI components such as smart-grid substations to bridge with a new range of services including situation-awareness. This architectural approach offers new levels of remote monitoring services that assimilate multi-scale data fusion to capture the true CI state. Fig. 3 shows this modeling approach of CPS as an aggregation of modular and interacting cyber-physical Objects (CPOs). This data abstraction aims to shield CI-related hardware/system from digital intrusions beyond advertised CI component's metadata assets.

CPS modeling for CI protection includes computational entities as well, driven by cooperating and distributed software agents which oversee CPOs' interconnection and report grid components' status indicators on a common deliberating-structure that facilitates multi-scale fusion. This process is streamlined through knowledge sources (KSs) fed by preplanned expert knowledge-representation in the form of rules to handle threat identification and evolution. Fig. 4 illustrates a Blackboard-based framework where different types of agents cooperate to deliberate on situational awareness and related decision-making operations [6, 9]. Reporting agents trigger events which are maintained (and possibly ranked) until the agents executing KS activations are scheduled. As an executing agent reflects the advocated inference on the Blackboard, KS-execution cycle resumes, given the new inference that might trigger other KSs. All agents report their observations and intermediate results onto the blackboard, whereas other agents can fuse these results with other reported data to elaborate situation awareness and potential preventive plans for CI protection.

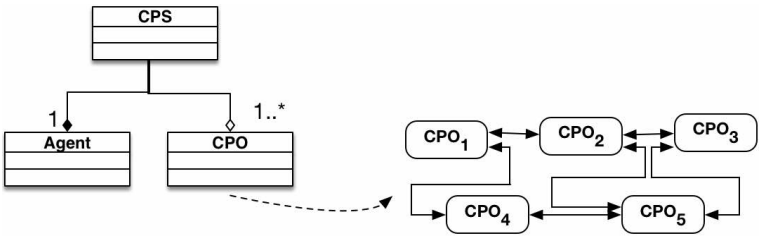

Fig. 3: cyber-physical system modeling of CI

Following Endsley's model discussed earlier in the introduction and illustrated in Fig. 1, control components *watch* the blackboard to perceive data, looking for an opportunity to apply KS expertise. When a pattern is detected, the corresponding KS is enacted by a handling agent which records its outcomes on the blackboard allowing other KSs to be enacted. This is the second step in Endsley's model to comprehend the threat. This framework appears particularly suitable as a simulation tool for evaluating and preventing cascading-effect scenarios that may be triggered by cyber-attack threats targeting smart-grids, for example.

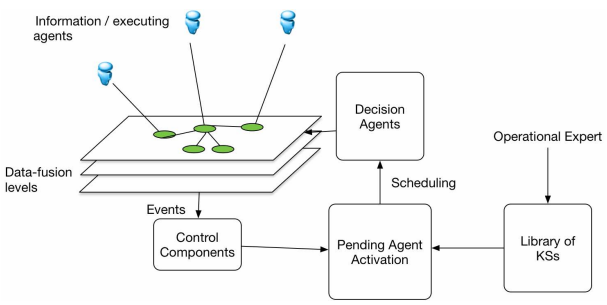

Fig. 4: Blackboard-based data fusion

4 Threat identification and evolution management

The next step of situation awareness following threat perception and identification, is threat projection into the future (Fig. 1). In CPS-based CIs such as smart grids, each component may include multi-dimensional inputs from external or internal sources of the cyber, physical and social dimensions [15]. Each dimension may contain several inputs with different quantitative contributions to the system functions. This data is further interpreted at multiple abstraction levels. The goal is to detect event-initiators and subsequent dependency-chains. To detect event-initiators, we adopt a machine-learning technique to spatiotemporal interval-data streamed onto the first level of the Blackboard structure. To evaluate the evolution of the detected incident, KS rules reason around the threat event and infer new data onto the blackboard

Threat detection is facilitated by a match between some patterns which are the premises of a KS rule in our proposed framework. This inference predicts the level of damage from the current CI key-point situation to another key-point dictated by the KS-inferred course of cascading effects. Stated otherwise, this problem is about how to select KS rules to meet certain criteria among a number of candidate rules with various attributes, such as (external) threat type, (internal) vulnerability level and exposure rate of that vulnerability with respect to the perceived threat. Formally, given a threat type T_i for which a particular CPO in a CI has a vulnerability value to that threat V_i and an exposure assessment E_i, the incurred damage inferred by KS rule is D_i.

$$T_i \times V_i \times E_i \rightarrow D_i \tag{1}$$

For example, given a certain threat-type causing a grid node voltage to be outside well-defined ranges, that affect some vulnerable equipment within that node. The equipment may be supported by features to sustain current magnitudes up to certain ratings, beyond which the equipment's vulnerability becomes exposed to the voltage surge. If this condition is met, then other nodes linked to this node in the grid are expected to be affected by the damage. The magnitude of damage may be translated into power-loss, people affected and time to recover.

However, CPO data reported to the blackboard structure by corresponding CPS agent have particular characteristics: they tend to be geotagged and includes numeric and discrete time series information. Spatiotemporal data differs however from traditional time series data, as they are not reduced to points associated with timestamps, but their scope extends to a vector of values representing CPO readings at some periodic time-instants. This is typical for CI monitoring, where CPO readings are periodically collected and analyzed. We consider data a sequence of state points in the space covered by CPS agents, which reflect successive CI measurements over a continuous time interval, periodically. CI spatiotemporal data analysis represents both time and space dimensions, whereas traditional time-series data is linked to a single homogenous domain. Next, we discuss our methodology to model these data before revealing a clustering methodology across multiple level of domains, in order to identify threat types and triggering issues.

KS rules cluster spatiotemporal data to infer some ground truth about an evolving threat targeting CPOs. This process allows patterns identification from CPS data to help CI operators make informed decisions. Using this approach, CPS data can be labelled and issues can further be explored within a narrowed solution domain to cope with threats diversity as illustrated in Fig. 5. This figure shows that threats are identified via their features to aggregate threat evidences using expert domain knowledge about the features used to characterize potential threats. Subsequent levels consist in fusing these evidences on the blackboard, based on weighted and averaging operators. This level of fusion across candida‘xte threat features isolate issues and advocate remedies from KSs to alleviate incurred damages at threat identification level. However, threats or some of its impacts may still evolve across CI and could only be identified based on evolution patterns, in which case a process clustering approach is advocated. This approach aims at identifying a threat-evolution through the discovery of correlations between a range of predicted cascading chains.

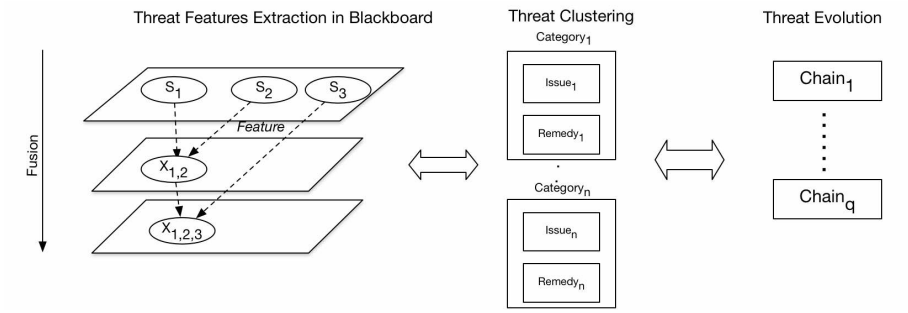

Fig. 5: Threat information models

4.1 Threat Identification

Clustering is a common technique to extract patterns from data in order to identify CI threats [17]. However, dealing with time-interval based data requires specific considerations. For example, CPS data of a power grid CI may drive interval-based measurements collected by an agent from substation CPSs. To subsume the multidimensional values of spatiotemporal data, a clustering approach across multiples euclidian spaces is recommended. There are several extensions of traditional clustering methods to spatial-temporal domains, although they still focus on time-series data.

A spatiotemporal-interval data clustering problem is defined as a set of data points P and a finite set of labels L. Each data point P is associated with at least two attributes. One represents temporal information, whereas the other represents spatial information. The goal is to assign each data point a label $l(p) \in L$. Label selection is based on an objective function $\mathcal{F}(l)$ with preset similarity thresholds among the data points:

$$\mathcal{F}(l) = \mathcal{F}_s(l) + \mathcal{F}_t(l) \tag{2}$$

where the first member of the equation represents the spatial similarity of data and the second member represents the temporal similarity of the data points, which is associated to a fixed period of time that map interval-data samples. The objective function has two terms, the first term captures the spatial information of the threat, and the second term is expected to be associated with a time-interval based data representing CI state over a period of time.

4.2 Threat evolution

We propose an architectural model illustrated in Fig. 7 to identify sequences of cascading-effect steps as part of a Threat Evolution (TE) model. Each sequence corresponds to processes that are identified as plausible members of a cascading failure from among steps belonging to streams of steps, each describing a CPS instance failure expectation in CI, given a perceived threat. This expectation is described in terms of minimum failure time, which is the Minimum Length of Failure (MLF) i.e time between failure occurring at CPS level and recovery, as well as Earliest Time of Occurrence (ETO) and Resilience Time (RT) during which the threat could be absorbed before propagating to other CPSs. A cascade failure sequence is thus modeleled as a temporal graph, shown in Fig. 6, where vertices refer to incident ETOs, whereas edges refer to the minimum propagation time between two incidents.

Accordingly, following an identified incident threat T_i, CPS failure at a node j that is vulnerable to threat T_i from a neighbouring failure of a node k, is expected to occur at ETO_j, where: $ETO_j = ETO_k + RT_{ij} + t_{kj}$. RT_{ij} is defined as the resilience of CPS_j to threat T_i, and derived as a function of that CPS vulnerability and exposure to a given threat. That is:

$$RT_{ij} = f_{T_i}(V_{ij}, E_{ij}) \tag{3}$$

E_{ij} refers to exposure level of CPS_j to threat i. In a simulation scenario setup, RT_{ij} could be configured to evaluate the threat evolution under different vulnerability and exposure settings in order to assess the level of preparedness and induced costs. Alternatively, a normalized resilience index R_{ij} of CPS_j to Threat i, can be expressed as:

$$R_{ij} = \frac{RT_{ij}}{\sum_{n=1} RT_{in}} \tag{4}$$

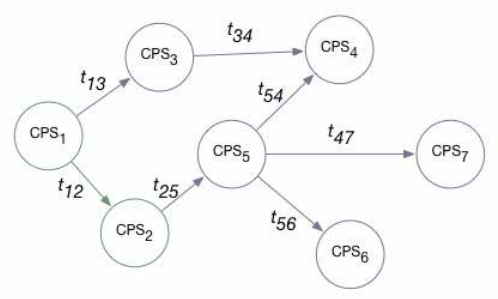

Fig. 6: Temporal graph of a cascade failure

The identification of a cascade schedule contributes to situation awareness, and is determined through feature values associated with each candidate sequence of steps. These feature values are submitted to a predictor module, as input to generate indicative values on whether a candidate sequence could be part of TE chain. In doing so, the set of candidate sequences is divided into positive ones that are deemed comprised within the evolving threat and a negative subset of steps that are not typically triggered by TE. This approach creates a model of threat-evolution based on sequences of steps corresponding to TE features. Each step is associated with a CPS. A cascade modeler may employ a pattern of steps involved in TE. This module infers a graph depicting a cascading-effect scenario. This scenario model may include additional parameters that influence the behaviour of this graph-based representation of TE.

The threat modeler subsystem module takes in input in the form of identified threat incidents, and uses threat-specific infection propagation rules to elaborate candidate failure propagation scenarios. Using these infection propagation rules from dedicated KSs, the analysis engine captures the sequence of cascading effects in the form of a temporal graph. Each graph may have multiple interpretations corresponding to cascade scenarios. Each scenario provides a different perspective on how the threat may propagate based on individual CPS vulnerability and exposure assessments with respect to identified threats.

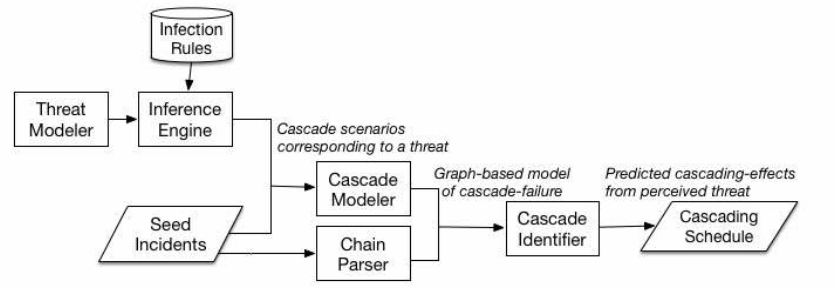

Fig. 7: Cascade failure model

5 Conclusion

We presented a data-oriented architectural abstraction for cyber-threat intelligence to protect critical infrastructures, such as smart power-grids. We showed how this architecture facilitates the integration of machine-learning techniques to identify threats, and predict its cascading-effects. We also elaborated on the capacity of the proposed architecture to deliver a comprehensive level of situation awareness as part of corresponding decision-support tools. We plan to validate further the proposed architecture through a simulation-tool that reveals decision-points along a predicted situation-awareness timeline to assess CI resilience against cyber-attack threats.

Acknowledgments. This work is supported by EU: Internal Security Fund (ISF) A431.678-2016.

References

1. Aggarwal, C.C., Reddy, C.K.: Data Clustering. Algorithms and Applications, CRC Press (Aug 2013)
2. Colbert, E.J.M., Kott, A.: Cyber-security of SCADA and Other Industrial Control Systems. Springer (Aug 2016)
3. Endsley, M.: Situation Awareness in Dynamic Human Decision Making: Theory and Measurement. University of Southern California (1990)
4. Giannakis, G.B., Kekatos, V., Gatsis, N., Kim, S.J., Zhu, H., Wollenberg, B.F.: Monitoring and optimization for power grids: A signal processing perspective. IEEE Signal Processing Magazine 30(5), 107–128 (Sept 2013)
5. Guérard, G., Amor, S.B., Bui, A.: A Complex System Approach for Smart Grid Analysis and Modeling, Frontiers in Artificial Intelligence and Applications, vol. 243. IOS Press (2012)
6. Hayes-Roth, B.: A blackboard architecture for control. Artif. Intell. 26(3), 251–321 (Aug 1985), http://dx.doi.org/10.1016/0004-3702(85)90063-3
7. Hurst, W., Merabti, M., Fergus, P.: Big data analysis techniques for cyber-threat detection in critical infrastructures. In: 2014 28th International Conference on Advanced Information Networking and Applications Workshops. pp. 916–921 (May 2014)

8. Hurst, W., MacDermott, Á.: Evaluating the effects of cascading failures in a network of critical infrastructures. International Journal of System of Systems Engineering 6(3), 221–236 (2015)
9. Jiawen, T., Shoushi, X.: Application of knowledge-based systems in multisensor data fusion. In: Proceedings of the 3rd World Congress on Intelligent Control and Automation (Cat. No.00EX393). vol. 1, pp. 351–354 vol.1 (2000)
10. Kuzlu, M., Pipattanasomporn, M., Rahman, S.: Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks 67, 74 – 88 (2014)
11. Leszczyna, R.: Agents in Simulation of Cyberattacks to Evaluate Security of Critical Infrastructures. In: Multiagent Systems and Applications, pp. 129–146. Springer Berlin Heidelberg (2013)
12. Lindström, J., Lindström, P., Lönnermark, A., Svensson, S.: Tactical First Responder Operations and Effects of Human Activities on the Course of Events. Deliverable Number: D3.1, CascEff Project: Modelling of dependencies and cascading effects for emergency management in crisis situations (2015)
13. Lloyd's: Emerging risk report. Tech. rep., Security and Society, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf (2015)
14. Lönnermark, A., Lange, D.: Cascading effects during incidents: CascEff. 26th European Safety and Reliability Conference (2016)
15. Luiijf, H., Nieuwenhuijs, A.: Extensible threat taxonomy for critical infrastructures. International Journal of Critical Infrastructures 4(4), 409–417 (2008), http://EconPapers.repec.org/RePEc:ids:ijcist:v:4:y:2008:i:4:p:409-417
16. MacDermott, Á., Hurst, W., Shi, Q., Merabti, M.: Simulating critical infrastructure cascading failure. In: 2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation. pp. 324–329 (March 2014)
17. Oliva, G., Panzieri, S., Setola, R.: Identifying critical infrastructure clusters viaâ spectral analysis. In: Rome, E., Theocharidou, M., Wolthusen, S. (eds.) Critical Information Infrastructures Security: 10th International Conference, CRITIS 2015, Berlin, Germany, October 5-7, 2015, Revised Selected Papers. pp. 223–235. Springer International Publishing, Cham (2016)
18. Phadke, A.G., Pickett, B., Adamiak, M., Begovic, M., Benmouyal, G., Burnett, R.O., Cease, T.W., Goossens, J., Hansen, D.J., Kezunovic, M., Mankoff, L.L., McLaren, P.G., Michel, G., Murphy, R.J., Nordstrom, J., Sachdev, M.S., Smith, H.S., Thorp, J.S., Trotignon, M., Wang, T.C., Xavier, M.A.: Synchronized sampling and phasor measurements for relaying and control. IEEE Transactions on Power Delivery 9(1), 442–452 (Jan 1994)
19. Sato, T., Kammen, D.M., Macuha, M., Duan, B., Zhou, Z., Wu, J., Tariq, M., Asfaw, S.A.: Smart Grid Standards. Specifications, Requirements, and Technologies, John Wiley & Sons (Apr 2015)
20. Thurlby, R., Warren, K.: Understanding and managing the threat of disruptive events to the critical national infrastructure. Journal of Facilities Management 12(3), 231–246 (Aug 2014)
21. Tsegaye, T., Flowerday, S.: Controls for protecting critical information infrastructure from cyberattacks. In: World Congress on Internet Security (WorldCIS-2014). pp. 24–29 (Dec 2014)
22. Yusta, J.M., Correa, G.J., Lacal-Arántegui, R.: Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy 39(10), 6100–6119 (Oct 2011)