A Sustainable Dispositional and Situational Security Awareness Model for Smart Grids

Abubakar Sadiq Sani*, Dong Yuan†, Yahaya Lawal ‡, George Loukas*, and Zhao Yang Dong§
* School of Computing and Mathematical Sciences, University of Greenwich, London, United Kingdom
Email: [s.sani, g.loukas]@greenwich.ac.uk
† School of Electrical and Information Engineering, The University of Sydney, Sydney, Australia
Email: dong.yuan@sydney.edu.au
‡ Oracle Corporation, Texas, United States
Email: yahaya.lawal@oracle.com
§ Department of Electrical Engineering, City University of Hong Kong, Hong Kong
Email: zydong@ieee.org

***Abstract*—The continuous introduction of emerging technologies such as Artificial Intelligence (AI) in smart grids has improved the reliability of operations and communication among components in the grids. However, such technologies can become unsustainable and further introduce security vulnerabilities. Any potential impact of security attacks on a smart grid component such as a sensor, either through internal or external adversaries, may lead to a breakdown of operations in the grids. Additionally, the large number of components along with their dependencies on emerging technologies may hinder the ability of grid operators to sustainably identify security flaws. Note that sustainability (of smart grid security) in this work refers to the ability to mitigate security vulnerabilities or attacks without overdependence on grid operators or emerging technologies that introduce high computational overheads. In this paper, we propose a sustainable dispositional and situational security awareness model through the utilization of a Fuzzy Cognitive Map (FCM) to effectively reveal and mitigate security vulnerabilities in the smart grids without overdependence on emerging technologies. We conducted some case studies on a Supervisory Control and Data Acquisition (SCADA) system to show the usefulness of our model.**

***Index Terms*—smart grids, sustainability, dispositional and situational security awareness, Fuzzy Cognitive Map, security**

I. Introduction

Smart grids are equipped with several components such as sensors, actuators, and controllers which can be operated, monitored, and controlled from remote locations [1]. The utilisation of emerging technologies such as Artificial Intelligence (AI) in the grids has greatly provided insights into grid operations for enhanced reliability and productivity (see, e.g., [2]). A Supervisory Control and Data Acquisition (SCADA) system is usually deployed to monitor and control the activities in the grids. The SCADA system can utilise emerging technologies for enhanced insights into the grid operations; however, any security attacks during the operations can affect the services provided by the grids. Besides, a lack of sustainability of such technologies may hinder the continuous mitigation of security vulnerabilities and attacks in the grids. In this work, sustainability focuses on mitigating security vulnerabilities or attacks with limited dependence on grid operators or high computational overheads-based emerging technologies. Note that sustainability in this work refers to the ability to mitigate security vulnerabilities or attacks without overdependence on grid operators or emerging technologies that introduce high computational overheads.

In this work, the act of using smart grid components' external attributes such as time to observe the components in the grid can be referred to as situational awareness. The need for dispositional awareness is introduced in this work to use internal attributes such as data size to observe the behaviour of the components. In this case, both situational awareness and dispositional awareness mechanisms can be applied to identify and mitigate security vulnerabilities and attacks in the grids without overdependence on emerging technologies, which can become unsustainable and further introduce security vulnerabilities.

While several approaches for smart grid security awareness have been proposed, these approaches such as the secure data awareness model [3] and situational awareness mechanism [4] have different advantages and limitations. For example, the solutions presented in [3] and [4] do not support integrated dispositional and situational awareness. Wang et al. [5] proposed a distributed intelligence solution for online situational awareness in power grids. Wu et al. [6] proposed a security situational awareness mechanism to predict attacks on the smart grid before damages. Xi et al. [7] introduced a comprehensive network security situation awareness tool to identify network security situations. This tool uses a fusion of network information to make a quantitative assessment of network security situations. However, the solution in [5], mechanism in [6], and tool introduced by [7] do not provide security control and are unsustainable for grid operators due to their computational complexities. Zhai et al. [8] proposed a dynamic security assessment framework for small-signal stability in the power grids. The proposed framework provides situational awareness

for human operators in the grids. However, the framework is unstainable due to the high computational overheads. Jin et al. [9] proposed an optimization-based graphical boundary defence mechanism to identify data manipulation in a power system. The proposed mechanism enhances situational awareness of the grid; however, it does not provide integrated dispositional and situational security awareness capable of providing security control against cyber threats.

Having a sustainable security operating procedure consisting of security events and remedial security actions to be followed by grid operators in cases of any security vulnerabilities or attacks is important for smart grids. Thus, we propose a sustainable dispositional and situational security awareness model that is capable of providing knowledge of security vulnerabilities and actioning remedial security actions in the smart grids. The proposed model is designed based on Fuzzy Cognitive Map (FCM) [10], which utilises a combination of expert knowledge and Hebbian learning algorithm [11] for security analysis and pattern classification, respectively, in this work. The Hebbian learning algorithm is one of the simplest algorithms in the neutral network. Our key contributions in this work are as follows: (I) We propose security functions such as security disposition, security situation, security modeling, and security control for detecting and mitigating security vulnerabilities and applying countermeasures. (II) We present two case studies to illustrate the usefulness of our model in achieving sustainable security awareness in the grids.

II. Preliminaries

In this section, we present a brief description of FCM, which represents the underlying mechanism for constructing our model.

A. FCM

In FCM, nodes and edges are used as variable concepts and casual connections respectively. In general, FCM is used for logical reasoning and knowledge representation of concepts (e.g., components) and their relationships. It has been applied to model intrusion detection systems, utility automation systems, and energy management systems, to name a few. A simple illustration of the FCM is presented in Fig. 1. This figure shows that two nodes or components, N_i and N_j, are connected by a causal link weight W_{ji}. A simple FCM rule can be expressed as

$$A_i^{(t+1)} = f(A_i^{(t)} + \sum_{j=1,\neq i}^{n} A_j^{(t)} W_{ji}), \tag{1}$$

where $A_i^{(t+1)}$ is the value of N_i at time $t+1$, W_{ji} is the weight of the edges or interconnection between nodes N_j and N_i, and f is the threshold function that compresses results in the interval of $[0, 1]$. Note that in what follows we use the term "node" to refer to a smart grid component like a sensor and therefore the "user" and "component" terms are often used interchangeably.

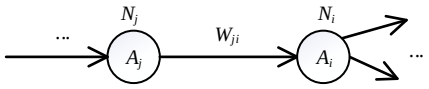

Fig. 1. A simple illustration of a Fuzzy Cognitive Map.

B. FCM Training

In this section, we describe how the FCM works in this paper.

1) Weight Initialisation via Expert Knowledge: Expert knowledge in smart grid security is required for building the FCM and assigning initial weights in this work. This approach should not be considered a weak link of the FCM because the nodes and their relationships clearly show how one node influences another interconnected node. The expert knowledge is considered one step ahead of all the relationships and impacts among all components because it uses the available data to determine the initial weights. In this work, data from a SCADA system is used to support the expert knowledge.

2) Weight Adjustment via Hebbian Learning: The weights of the FCM are adjusted using the Hebbian learning algorithm as a result of impacts from variations of events. Changes at each iteration step in the FCM trigger the FCM thereby adjusting the weights. In this work, some impacts can lead to security vulnerabilities that can affect smart grid operations.

Please note that while expert knowledge is restricted to deriving local and first-time relationships for assigning the initial weights, the Hebbian learning algorithm is used for fine-tuning the weights and then determining the overall relationships in the FCM.

III. Smart Grid Architecture and Basic Security Requirements for Security Awareness

A simple smart grid architecture is presented in Fig. 2 to show the communications among smart grid components. The figure shows that all internal communications are carried out over a Local Area Network (LAN) while external communications are over a Wide Area Network (WAN). Other components presented in the figure include SCADA client/server, network switch, Network Intrusion Detection System (NIDS), Firewall, Historian, servers, workstations, sensors, controllers, and an Intelligent Electronic Device (IED). The data exchanged between the components must be prevented from unavailability, unauthorised reading, and unauthorised modification. In this work, the basic security requirements for security awareness to enhance the security of data exchange among the components are as follows: (I) Availability: This requirement ensures that components and data are available to the components. (II) Integrity: This requirement ensures that the components and data are prevented from unauthorised modification. (III)

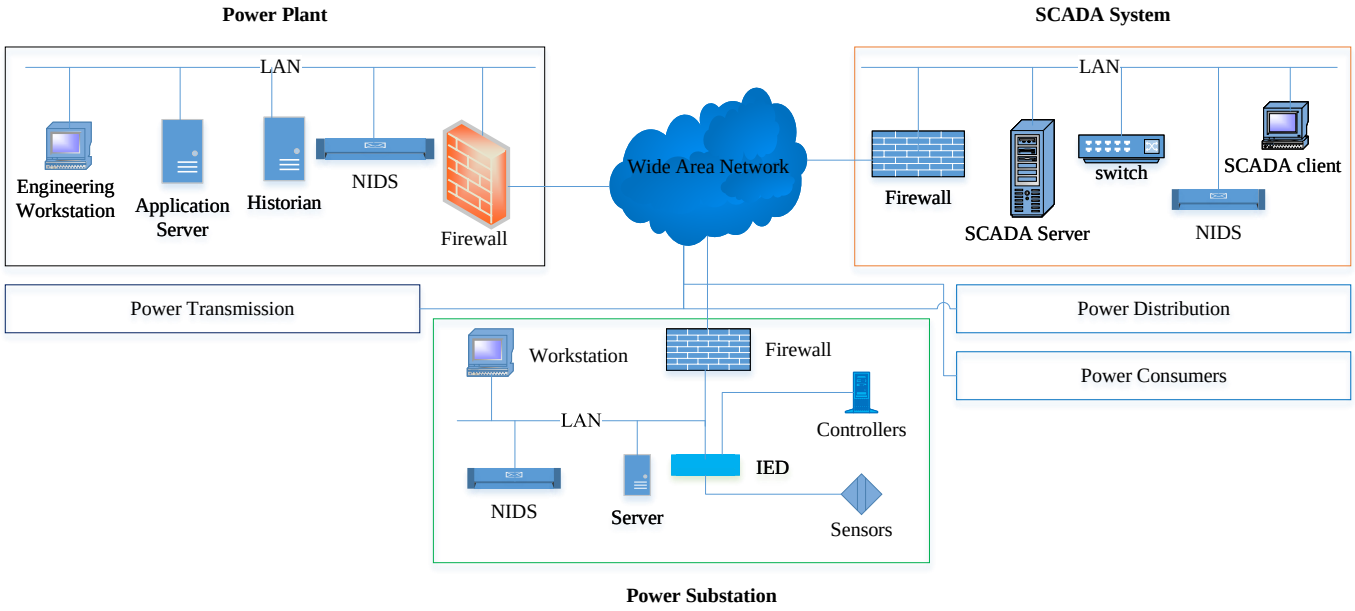

Fig. 2. A simple illustration of a smart grid architecture. Abbreviations: LAN - Local Area Network; NIDS - Network Intrusion Detection Ssytem; SCADA: Supervisory Control And Data Acquisition; IED: Intelligent Electronic Device.

Confidentiality. This requirement ensures that the components and data are prevented from unauthorised disclosure.

Considering Fig. 1, determining the initial weights of components in Fig. 2 is considered the first step in developing the structure of an FCM in this work. While expert knowledge is used to determine the weights, the Hebbian learning algorithm is used to adjust the weights in an automated fashion.

IV. Sustainable Dispositional and Situational Security Awareness Model

In this section, we present our proposed model for sustainable dispositional and situational security awareness in smart grids as shown in Fig. 3. The model consists of security functions such as security disposition, security situation, security modeling, and security control. A brief description of the functions is given below:

A. Security Disposition

This function captures and analyses the dispositional attributes (i.e., data sizes) associated with components with the support of the FCM's expert knowledge and Hebbian learning algorithm, respectively. Let SD_i be the security disposition function at time $t-1$. $SD_i^{(t-1)}$ is given as

$$SD_i^{(t-1)} = \sum_{j=1,\neq i}^{n} W_{ij} A_j^{(t-1)} \tag{2}$$

where $SD_i^{(t-1)}$ is the security disposition function of components at time $t-1$, $A_j^{(t-1)}$ is the value of node N_j at time

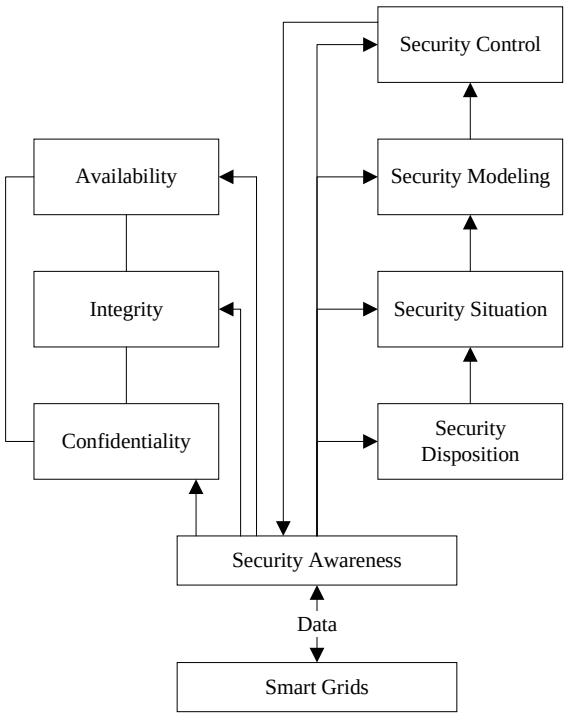

Fig. 3. Sustainable Dispositional and Situational Security Awareness Model-simple illustration of a smart grid architecture.

$t-1$, and W_{ij} is the value of the weight between nodes N_i and N_j. Note that the Hebbian learning algorithm is defined as $W_{ij}^* = \alpha.W_{ij}$, where α is a learning rate parameter and W_{ij}^* is the value of the adjusted weight between nodes N_i and N_j.

Remarks: In this work, we heuristically determine that α of 0.1 in the weight adjustments produces the best results for accuracy due to a fundamental tradeoff between high performance and low delay in the learning process. If the learning process is too high, it leads to high delays, heavyweight computations, and instability in the interconnections among the components. Thus, achieving availability, confidentiality, and integrity in a manner that minimises delays or computations is within the constraints of such a learning process. Note that the learning process ensures the long-term applicability and sustainability of our solution in the real world.

B. Security Situation

This function captures and analyses the situational attributes (i.e., data availability time) associated with the components' data sizes with the support of the expert knowledge and Hebbian learning algorithm, respectively. Please note that the data availability time of a node represents the time a data size of the node becomes available in the grids. Let SS_i be the security situation function at time t. $SS_i^{(t)}$ is given as

$$SS_i^{(t)} = \sum_{j=1,\neq i}^{n} W_{ij} A_j^{(t)} TA_j^{(t)} \tag{3}$$

where $SS_i^{(t)}$ is the security situation function of components at time t, $A_j^{(t)}$ is the value of node N_j at time t, and $TA_j^{(t)}$ is the data availability time value of node N_j at time t.

C. Security Modeling

This function uses the combination of the security disposition and security situation functions to identify possible security compromises associated with the components. Specifically, it investigates the data size and data availability time associated with the components to ensure that the associated values are within range. If the values are out of range, it notifies the security control function to reset the out-of-range values to the actual values. Please note that out-of-range values can be seen as a result of data manipulation by adversaries or disgruntled operators in the grids. Let SM_i be the security modeling function at time $t+1$. $SM_i^{(t+1)}$ is given as

$$SM_i^{(t+1)} = \sum_{j=1,\neq i}^{n} W_{ij} A_j^{(t+1)} TA_j^{(t+1)} \geq \sum_{j=1,\neq i}^{n} W_{ij} A_j^{(2t-1)} TA_j^{(2t-1)} \tag{4}$$

where $SM_i^{(t+1)}$ is the security modeling function of components at time $t+1$, $A_j^{(t+1)}$ is the value of node N_j at time $t+1$, $TA_j^{(t+1)}$ is the data availability time value of node N_j at time $t+1$, $A_j^{(2t-1)}$ is the value of node N_j at time $2t-1$, which represents the time associated with the security disposition and security situation functions, and $TA_j^{(2t-1)}$ is the data availability time value of node N_j at time $2t-1$.

TABLE I
STATES OF COMPONENTS

State	Degree of Security Awareness
Healthy	$0.25 \leq State < 1$
Unhealthy	$0 \leq State < 0.25$
Failure	$-1 \leq State < 0$

D. Security Control

This function applies countermeasures to security compromises by resetting the values associated with the components to a healthy state. Without loss of generality, we assume that the healthy states of components lie between 0.25 and 1, the unhealthy states of components lie between 0 and 0.25, and the failure states of components lie between -1 and 0 in this work. Please see Table I for the illustration of the healthy, unhealthy, and failure states of components. Let SC_i be the security control function at time $t+p$, where p is a set of ordered finite numbers for resetting the values of components. $SC_i^{(t+p)}$ is given as

$$SC_i^{(t+p)} = A_i^{(t+1)} + \sum_{j=1,\neq i}^{n} W_{ij} A_j^{(t+p-1)} TA_j^{(t+p-1)} \tag{5}$$

where $SC_i^{(t+p)}$ is the security control function of components at time $t+p$, and $A_i^{(t+1)}$ is the value of node N_i at time $t+1$. Note that: (I) We assume that $p \geq 0.25$; $0.25 \leq SC_i^{(t+p)} < 1$; (II) p is applied to mitigate availability, integrity, and confidentiality vulnerabilities or attacks by ensuring that components are in healthy states.

Remarks: Without loss of generality, our model can be utilised as a software program in smart grid components due to its lightweight computations. Thus, our model can be installed in a Human Machine Interface (HMI) or a distributed server to interface with operators in the grids. Furthermore, the thresholds for healthy and failure states can be experimentally refined via the FCM training and application of our model.

V. CASE STUDIES

A SCADA system is studied in this paper. The basic components of the system include the Master Terminal Unit (MTU), Remote Terminal Unit (RTU), and HMI. Fig. 4 shows the SCADA system with its components. Fig. 5 shows the SCADA components and the security functions. The SCADA components and security functions will be used to determine the nodes and edges of our FCM for the SCADA system.

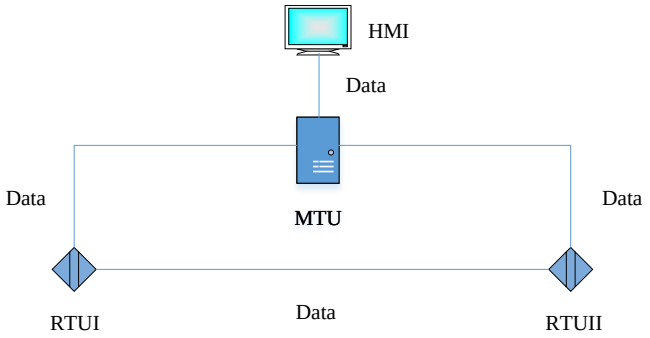

Fig. 4. A Simple SCADA System with communication flow. Abbreviations: RTUI – Remote Terminal Unit I; RTUII – Remote Terminal Unit II; MTU - Master Terminal Unit; HMI - Human Machine Interface. The RTUI and RTUII send information to MTU, and MTU sends all the information to the control centre. The HMI is used by grid operators at the control centre to access grid information.

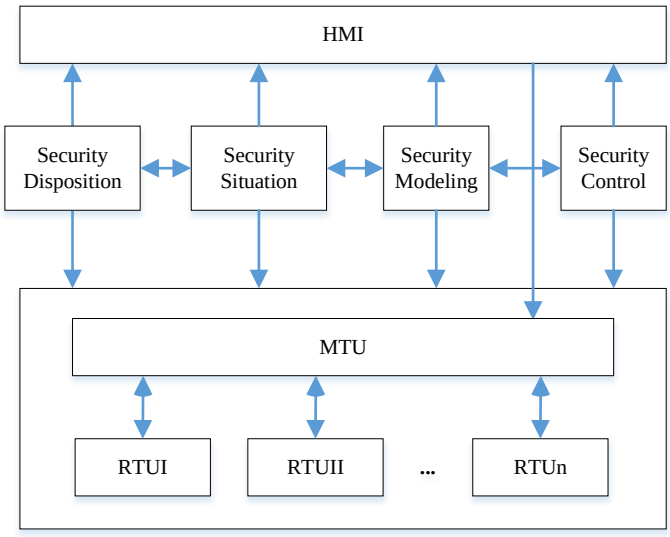

Fig. 5. Diagram of the security functions and communication flow of the SCADA system in Fig. 4. The arrows show the directions of data exchange.

The SCADA system's initial FCM structure with security functions is depicted in Fig. 6. The structure is developed based on the interconnections among the SCADA components. The arrows indicate the direction of impact between the components. For example, MTU → RTUI indicates that MTU has an impact on RTUI or the state of RTUI is affected by the state of MTU. The connections between the components and security functions are calculated using Equations (2), (3), (4), and (5) described in Section IV. Furthermore, Fig. 6 shows the influence of the security functions on the SCADA system to realise the expected security outcomes towards achieving availability, confidentiality, and integrity. We performed our simulations in a MATLAB environment based on the formulations provided

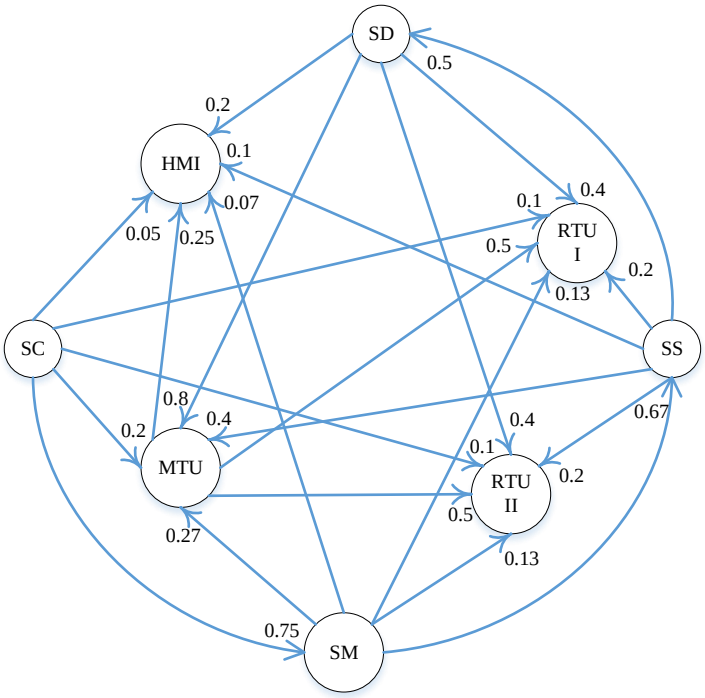

Fig. 6. Initial FCM developed for SCADA system in Fig. 5. Abbreviations: SD - Security Disposition; SV - Security Situation; SM - Security Modeling; SC - Security Control.

TABLE II
SIMULATION RESULTS FROM CASE STUDIES

Case Study	HMI	MTU	RTUII	RTUI
RTUI Performance (1st State)	0.4083	0.8089	0.8075	0.8075
MTU Failure (1st State)	0	–	0	0
MTU Failure (2nd State)	0.4034	0.8035	0.7993	0.7993

in Section IV. Table II presents the simulation results of our case studies based on the weights denoted in Figure 6. The case studies are as follows:

A. *Case Study 1*

RTUI Performance (RTUI initial state = 1). As shown in Table II, RTUI at the first state indicates all components are in healthy states. This shows that the components and their data are available to support grid operations without overdependence on grid operators. Furthermore, the availability of the components for security awareness without relying on heavyweight computations from emerging technologies supports the sustainability of our model.

B. *Case Study 2*

MTU Failure (MTU initial state = -1). We modified the MTU's first state from '0.8089' to '–1'. As shown in Table II, the HMI, RTUI, and RTUII read '0' to mitigate the data integrity attack. At the second state of the components, all the

components return to their healthy states to provide integrity. This shows that our model guarantees that mitigation is correctly applied and is sustainable for security awareness in the grids. Additionally, as our model does not reveal the actual data of the components, this shows that our model supports confidentiality in the grids.

Case studies 1 and 2 show that integrity, confidentiality, and availability security requirements have been met. As the increase in security awareness via the security functions influences the SCADA components, this shows that our model mitigates the security vulnerabilities presented in this paper. Compared with other approaches [4], [5], [6], [7], [8], [9], our model provides security control via resetting the values of components to a healthy state. Please see Section IV-D for more information on security control.

Please note that: (I) Though our model is proven to provide sustainable dispositional and situational security awareness based on the presented security vulnerabilities, other unknown vulnerabilities, which cannot be anticipated, may disrupt the execution of the model, thus, we assume that the model cannot continue if any unknown vulnerabilities disrupt its execution. (II) Providing security awareness for non-security issues such as equipment malfunctioning (as a result of operations in the grids) is not addressed in this paper. In the future, we will consider additional dispositional and situational attributes to provide security awareness for non-security issues.

VI. Conclusion and Future Work

This paper investigates dispositional and situational security awareness towards satisfying availability, confidentiality, and integrity security requirements in smart grids. Existing approaches are not well suited for integrated dispositional and situational security awareness due to their limited functionalities. Additionally, the complexities of the approaches make them unsustainable for the grids. To address this challenge, we presented our FCM-based model that consists of security disposition, security situation, security modeling, and security control functions. We employed a combination of FCM's expert knowledge and the Hebbian learning algorithm to satisfy the security requirements with sustainability. We presented our case studies on a SCADA system to show the effectiveness of our model. In future work, we will introduce new dispositional and situational attributes to optimise the capability of our model and further extend it to include a risk and control matrix.

References

[1] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for Internet of Things-based Energy Internet," Future Generation Computer Systems, 2018.

[2] ABB. ABB and Microsoft collaborate to bring generative AI to industrial applications. [Online]. Available: https://new.abb.com/news/detail/104829/abb-and-microsoft-collaborate-to-bring-generative-ai-to-industrial-applications

[3] A. S. Sani, D. Yuan, and Z. Y. Dong, "SDAG: blockchain-enabled model for secure data awareness in smart grids," in 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2023, pp. 1-5: IEEE.

[4] S. Ghosh, D. Ghosh, and D. K. Mohanta, "Situational awareness enhancement of smart grids using intelligent maintenance scheduling of phasor measurement sensors," IEEE Sensors Journal, vol. 17, no. 23, pp. 7685-7693, 2017.

[5] S. Wang, L. Li, and P. Dehghanian, "Distributed intelligence for online situational awareness in power grids," IEEE Transactions on Power Systems, vol. 37, no. 4, pp. 2499-2515, 2021.

[6] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big Data Analysis based Security Situational Awareness for Smart Grid," IEEE Transactions on Big Data, pp. 1-1, 2016.

[7] R. Xi, S. Jin, X. Yun, and Y. Zhang, "CNSSA: A comprehensive network security situation awareness system," in Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom), United States, 2011, pp. 482-487.

[8] C. Zhai, H. D. Nguyen, and X. Zong, "Dynamic security assessment of small-signal stability for power grids using windowed online Gaussian process," IEEE Transactions on Automation Science and Engineering, 2022.

[9] M. Jin, J. Lavaei, S. Sojoudi, and R. Baldick, "Boundary defense against cyber threat for power system state estimation," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1752-1767, 2020.

[10] B. Kosko, "Fuzzy cognitive maps," International Journal of Man-Machine Studies, vol. 24, no. 1, pp. 65-75, 1986/01/01 1986.

[11] E. Oja, "Neural Networks, Principal Components, and Subspaces," International Journal of Neural Systems, vol. 1, no. 1, pp. 61-68, 1989.