ADVANCES IN BUILDING ENERGY RESEARCH, 2017
https://doi.org/10.1080/17512549.2017.1325401

An innovative soft computing system for smart energy grids cybersecurity

Konstantinos Demertzis, Lazaros S. Iliadis and Vardis-Dimitrios Anezakis

Department of Forestry and Management of the Environment and Natural Resources, Lab of Forest-Environmental Informatics and Computational Intelligence, Democritus University of Thrace, Orestiada, Greece

The upgrade of energy infrastructures by the incorporation of communication and Internet technologies might introduce new risks for the security and for the smooth operation of electricity networks. Exploitation of the potential vulnerabilities of the heterogeneous systems used in smart energy grids (SEGs) may lead to the loss of control of critical electronic devices and, moreover, to the interception of confidential information. This may result in the disruption of essential services or even in total power failures. Addressing security issues that can ensure the confidentiality, the integrity, and availability of energy information is the primary objective for a transition to a new energy shape. This research paper presents an innovative system that can effectively offer SEG cybersecurity. It employs soft computing approaches, fuzzy cognitive maps, and a Mamdani fuzzy inference system in order to model overall security level. Three of the 27 scenarios considered herein have low overall security level, 21 of them have middle overall security, whereas only 3 are characterized as secure. The system automates the strategic planning of high security standards, as it allows a thorough audit of digital systems related to potential infrastructures and it contributes towards accurate decision-making in cases of threats.

ARTICLE HISTORY
Received 26 January 2017
Accepted 20 February 2017

KEYWORDS
Smart energy grids; smart grids domains; smart grid cybersecurity; logical interface categories; fuzzy cognitive maps; Mamdani fuzzy inference system; fuzzy rules

1. Introduction

1.1 Smart energy grids

The transition and upgrade of old electricity network infrastructures to a new smart and interactive management and distribution scheme is one of the most essential contemporary tasks globally. The smart energy grids (SEGs) use the most modern digital technology for monitoring, transferring, and organizing electricity from all the production sources, to address the varying needs of users. Coordination and anticipation of the market's needs, combined with the potentials of producers, system operators, consumers, and other market entities, are one of the main tasks performed by the SEGs. In this way, all parties

CONTACT Vardis-Dimitrios Anezakis ✉ danezaki@fmenr.duth.gr Department of Forestry and Management of the Environment and Natural Resources, Lab of Forest-Environmental Informatics and Computational Intelligence, Democritus University of Thrace, 193 Pandazidou st., 68200 Orestiada, Greece

© 2017 Informa UK Limited, trading as Taylor & Francis Group

are functioning optimally, by minimizing the cost and the environmental impact and by maximizing the adaptability, stability, and reliability of the overall network.

1.2 Literature review and motivation-innovation

It is a fact that many and significant research efforts have been published in the literature on the application of soft computing techniques. Some of them are using Fuzzy Logic (Ahmad & Baig, 2012; Wang, Wang, Ma, & Yao, 2013), whereas others employ Machine Learning (Baig, 2011; Zhang, Wang, Sun, Green, & Alam, 2011) in order to analyse security issues in SEGs (Kumar & Hussain, 2014; Li et al., 2012). It is a fact that the utilization of graph theory concepts, of fuzzy cognitive maps (FCMs) and Expert Systems (Mohagheghi, 2014), offers a solution capable to reveal weak links and vulnerabilities of automation systems. However, they can potentially become more exposed to partial internal failure or external damage.

A case has been studied on the IEEE 34-bus test distribution system, to show the efficiency of the proposed scheme. Mohagheghi (2010) explores such applications that arise from the employment of the standard IEC 61850. According to this research, the integrity of the data is checked across the substation and it can be verified by considering the quality and validity indices which are available from different devices and control/protection functions. This study uses FCMs that derive relationships and associations between various functions within the substation and determine a level of confidence on the available data.

Furthermore, Kottas et al. (2015) propose fuzzy cognitive networks to predict and perform the necessary actions for supplying different ancillary services to the grid, such as fast active power compensation, voltage, frequency regulation, and back-up supply. Additionally, Wang, Chen, and Chen (2016) make a qualitative analysis of the main factors affecting intelligent power distribution networks and Wireless Sensors networks, by building FCMs based on the data transmission performance index. Moreover, they propose an approach to dynamically evaluate variables that determine the routing path and adjust the network parameters, according to the inference of the FCMs. Finally, they conduct a simulation experiment on the proposed method and they analyse the performance of data transmission.

Furthermore, Jurado, Nebot, Mugica, and Avellana (2015) compare the accuracy of different Machine Learning methodologies for hourly energy forecasting in buildings. The main goal of this work is to demonstrate the performance of these models and their scalability for different consumption profiles.

Silva, Knak Neto, Abaide, and Bernardon (2015) present a methodology based on Neuro-fuzzy controllers producing grid indices, used to evaluate the system operability, its intelligence level, and its regulatory standards.

Coelho et al. (2016) propose a novel hybrid evolutionary fuzzy model with parameter optimization. Computational results show that the proposed framework is suitable for short-term forecasting over micro-grids and large-grids, being able to accurately predict data in a short computational time.

Also Hosseini, Bathaee, Abedini, Hosseina, and Fereidunain (2014) present a new approach to detect false data injection attack in a database management system of a smart grid network, and they attempt to estimate the voltage of buses using Neuro-fuzzy controllers.

Koraz and Gabbar (2016) present a multilevel safety hierarchical control of a micro energy grid (MEG). A three-level hierarchical control scheme for the MEG is offered with the use of an adaptive network-based fuzzy inference system.

Rahman, Oo, Mahmud, and Pota (2016) present an innovative agent-based security scheme for identifying the potential impacts of cyber attacks on smart grid protection systems. The proposed scheme identifies the malicious cyber attacks by utilizing the cyber and physical properties of power systems.

Xie, Stefanov, and Liu (2016) discuss critical vulnerabilities of a smart grid that can be exploited for physical and cyber intrusions. A comprehensive survey is conducted on the state-of-the-art research to enhance the physical and cybersecurity in a smart grid environment. Tazi, Abdi, and Abbou (2015) introduce cyber-physical defence algorithms and summarize the results of their performance evaluation. Finally, Rawat and Bajracharya (2015) provide a comprehensive study of challenges in smart grid security. They concentrate on the problems and their corresponding solutions. This paper offers a more thorough understanding of smart grid security and the research trends in this topic.

In all, simulations performed by many researchers all lead to the same conclusion: 'Security of the smart grid depends on the combined physical and cyber security'.

1.2.1. Motivation for this research

Nowadays, 'Logical Interface Categories' (LICs) are controlled manually. The motivation for this research is the development of a realistic innovative system, towards the optimization of decision-making, aiming to offer enhancement of the design, analysis, management, and support of the digital SEGs security. Given the complexity of the heterogeneous interconnected systems and the high availability requirements of general infrastructure, the development of smart, innovative, and integrated SEG digital security systems is a necessity. Essentially the smart energy grid cybersecurity (SEG-CYS) facilitates and significantly simplifies the analysis and optimal decision-making in cases of threats. It presents the safety level changes in logical connections between the individual systems in a real-time mode. This is achieved based on predefined security levels set (security baselines).

The basic idea of this modelling effort includes the use of FCMs (Papageorgiou & Salmeron, 2013; Salmeron & Froelich, 2016; Vidal, Salmeron, Mena, & Chulvi, 2015). FCMs are based solely on the factors and measures set by the standardization bodies of SEGs as they emerge from the correlation analysis of the real needs and not from the experts' opinions which are usually applied in such cases. In fact, herein we employ existing knowledge regarding the interaction causality between the risk factors related to the interconnected SEGs' systems. Moreover, the use of a Mamdani fuzzy inference system (MFIS) based on a set of fuzzy rules (FR) under actual scenarios of natural and logical connections is an interesting novelty that improves the quality and value of the proposed model (Chaudhari & Patil, 2014; Guney & Sarikaya, 2009; Jang, Sun, & Mizutani, 1997; Mamdani & Assilian, 1975). The learning – generalization ability in the proposed system is achieved under a set of scenarios, in a way that the necessary FR acquire the status of 'permanent' ones, optimizing the overall level of security. FCMs and the MFIS not only model the overall security, but they also estimate how it is affected by changes and deviations from the security baseline, for each LIC.

2. Theoretical background

2.1 Conceptual model and domains

Based on the operating framework for SEGs, standardization bodies adopted a model of partial decomposition of the energy cycle in individual primary branches. This was achieved based on the mapping and demarcation of the procedures and responsibilities in a clear objective manner. This is essential in order to classify the involved parties based on infrastructure evaluative criteria, on institutional motivations and aspirations, and, finally, on objectives and specific functions.

This idealized shape (named Conceptual Model) is based on the diversity of each sector's functions. It is a tool that provides the basis for the description or analysis of the interoperability of standards of current architectures. It comprises seven basic domains, namely, *Bulk Generation, Transmission, Distribution, Customer, Service Provider, Operations, and Markets*.

A smart grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other *actors* with similar objectives. The various actors are needed to transmit, store, edit, and process the information needed within the smart grid. To enable smart grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 1. Actors are devices, systems, or programmes

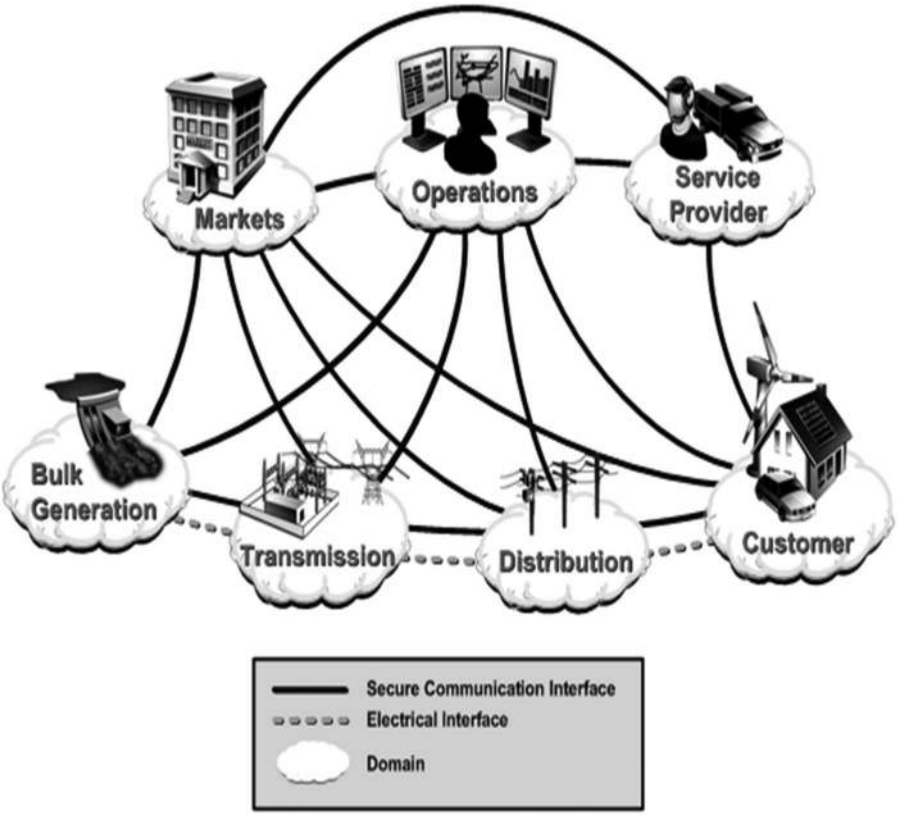

Figure 1. Smart energy grid framework (NISTIR 7628, 2010).

that make decisions and exchange information necessary for executing applications within the smart grid (National Institute of Standards and Technology Interagency Report, NISTIR, 7628, 2014).

The physical interconnection of the electrical interfaces follows the path: *Bulk Generation, Transmission, Distribution,* and *Customer*, in a relation point to point. On the other hand, the logical interconnection of the communication interfaces is scheduled by the involvement of all parts in a relation point to multipoint.

2.2 Introduction of new vulnerabilities

The main innovation of the SEGs is the integration of digital means and the extended use of the most modern telecommunication infrastructures, such as *Fibre Optics, Broadband over Power Line, WiMax, WiFi,* and *Zigbee*, which allow bidirectional communication between sophisticated systems. This layering and architecture modelling increases the complexity of the system and introduces asymmetric threats.

The incorporation of these technologies converts the previously isolated and closed networks of power control systems into networks accessible to the public. Cyber threats such as malware, spyware, and computer viruses currently threatening computer and communication networks and additionally the introduction of new technologies and services such as smart metres, sensors, and distributed access points can create new vulnerabilities in the architectures of SEGs.

The assumptions underlying the implementation of comprehensive security architectures in SEGs require ensuring an iterative review process at regular intervals in order to cope with new threats and vulnerabilities, plus the belief that all SEG systems are potential targets. It is necessary to use the minimum amount of resources in order to mitigate the consequences of security breaches. It is a fact that there is no magical overall security architecture applied in any case, capable of protecting in all Logical Interfaces of all the SEGs domains.

2.3 Logical interface categories

As it is obvious, heterogeneous systems making up the SEGs and those inherited from the existing structures, include a huge number of different interfaces with different security features and requirements. An architectural standardization system, should organize these interfaces based on the characteristics that could affect safety requirements. So in order to create a robust background and a single way of reference, individual logical interfaces which show similar safety profiles are grouped by SEG standards organizations, at 22 LICs. The LICs are the development guidelines in cybersecurity strategies and the fundamental way to control and assess potential risks, such as logical interfaces and interconnections between control systems within the same or different organizations.

These security-related LICs are defined based on attributes that could affect the security requirements. These LICs and the associated attributes can be used as guidelines by organizations that are developing a cybersecurity strategy and implementing a risk assessment to select security requirements (National Institute of Standards and Technology Interagency Report, NISTIR, 7628, 2014). This information may also be used by vendors and integrators as they design, develop, implement, and maintain the security

Table 1. Logical interfaces and categories.

Logical interface category	Logical interfaces
1. Interface between control systems and equipment with high availability with computing and/or bandwidth constraints	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
2. Interface between control systems and equipment without high availability, but with computing and/or bandwidth constraints	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
3. Interface between control systems and equipment with high availability, without computing and/or bandwidth constraints	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
4. Interface between control systems and equipment without high availability, without computing or bandwidth constraints	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
5. Interface between control systems within the same organization	U9, U27, U65, U66, U89
6. Interface between control systems in different organizations	U7, U10, U13, U16, U56, U74, U80, U83, U87, U115, U116
7. Interface between back office systems under common management authority	U2, U22, U26, U31, U63, U96, U98, U110
8. Interface between back office systems not under common management authority	U1, U6, U15, U55
9. Interface with B2B connections between systems usually involving financial or market transactions	U4, U17, U20, U51, U52, U53, U57, U58, U70, U72, U90, U93, U97
10. Interface between control systems and non-control/corporate systems	U12, U30, U33, U36, U59, U75, U91, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters	U111
12. Interface between sensor networks and control systems	U108, U112
13. Interface between systems that use the AMI network	U8, U21, U25, U32, U95, U119, U130
14. Interface between systems that use the AMI network with high availability	U8, U21, U25, U32, U95, U119, U130
15. Interface between systems that use customer (residential, commercial, and industrial) site networks	U42, U43, U44, U45, U49, U62, U120, U124, U126, U127
16. Interface between external systems and the customer site	U18, U37, U38, U39, U40, U88, U92, U100, U101, U125
17. Interface between systems and mobile field crew laptops/equipment	U14, U29, U34, U35, U99, U104, U105
18. Interface between metering equipment	U24, U41, U46, U47, U48, U50, U54, U60, U64, U128, U129
19. Interface between operations and decision support systems	U77, U78, U134
20. Interface between engineering/maintenance systems and control equipment	U11, U109
21. Interface between control systems and their vendors for standard maintenance and service	U5
22. Interface between security/network/system management consoles and all networks and systems	U133 (includes interfaces to actors 17, 12, 38, 24, 23, 21, 42, 44, 43, 41, 19, 34)

requirements. Table 1 includes a listing of all logical interfaces by category and their corresponding descriptions.

2.4. Security properties and availability impact levels

The introduction of new digital components is combined with weaknesses or heterogeneities inherited from the existing structures. An architecture in SEGs can be considered as secure if it meets three crucial properties of security: *Confidentiality, Integrity, and Availability* (CIA). These features are analysed as follows (Cirincione, Krishnamurthy, La Porta, Govindan, & Mohapatra 2010; Drtil 2013; Samonas & Coss 2014; Sattarova Feruza & Kim 2007):

(i) Confidentiality: Preserving authorized restrictions on information access and disclosure. Unauthorized disclosure of information could be expected to have a **Low** (L) (*limited*) or **Moderate** (M) **(***serious***)** or **High** (H) **(***severe or catastrophic***)** adverse effect on organizational operations, organizational assets, or individuals.

(ii) Integrity: Guarding against improper information modification or destruction. Unauthorized modification or destruction of information could be expected to have an L or M or H adverse effect on organizational operations, organizational assets, or individuals.

(iii) Availability: The most important security objective for the reliability of a power system. It means ensuring timely and reliable access and use of information. The disruption of access or use of information could be expected to have an L or M or H adverse effect on organizational operations, organizational assets, or individuals.

The impact levels (L, M, and H) presented in Table 2 address the impacts on the nationwide power grid, particularly with regard to grid stability and reliability. Each of the three impact levels (i.e. low, moderate, and high) is based upon the expected adverse effect of a security breach upon organizational operations, organizational assets, or individuals. The initial designation of impact levels focused on power grid reliability (National Institute of Standards and Technology Interagency Report, NISTIR, 7628, 2014).

2.5. Levels of conceptual interoperability

Interoperability is the potential of two or more systems, devices, applications, or networks to exchange and use information easily, securely, and efficiently, with little or no user intervention. It requires interfaces fully and publicly documented, linked, and operating without restrictions on access or barriers to implementation. The levels of interoperability are related to the general configuration based on evaluative investigation criteria (EIC). These EIC are designed to identify the degree of heterogeneity resulting from any

Table 2. Impact levels definitions.

CIA	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Availability Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

communication of disparate systems. The stratification of the interoperability is done with a down-up approach and it includes the following levels:

(1) Level 0, No Interoperability. In this level, there is no available communication and the system is considered isolated.

(2) Level 1, Technical Interoperability. A communication protocol succeeds the data interchange between participating systems at a digital data level (exchange bits and bytes).

(3) Level 2, Syntactic Interoperability. A protocol defines and manages the information exchange process with an acceptable common data format.

(4) Level 3, Semantic Interoperability. The interchange application content of the heterogeneous systems is specifically defined and the data are shared.

(5) Level 4, Pragmatic Interoperability. The data are understood by all participating systems.

(6) Level 5, Dynamic Interoperability. Due to the fact that the system operates on a long-term basis, its situation might have changed something that affects the assumptions and limitations related to communication or interchanged data. If the systems have achieved dynamic interoperability, they are able to understand the state changes that occur in the parallel system and they can adapt and potentially benefit, rearranging their structure.

(7) Level 6, Conceptual Interoperability. When the theoretical design and operation models are based on documented methods that enable the interpretation and evaluation of their heterogeneous systems complementing one frame, then these systems are considered fully aligned and achieve interoperability on a conceptual level.

3. Methods and materials

3.1 Fuzzy cognitive maps

Unlike the majority of complex dynamic systems characterized by non-linearity and high uncertainty, the FCMs use advanced learning techniques in order to choose appropriate weights for the causal connections between the examined variables. This is done in order to rationally capture the essence of the problem. Combining the theoretical background of fuzzy logic, they cover the needs for the comparison and characterization of reference sets in modelling and solving complex problems for which there is no precise mathematical model.

In a FCM model, the nodes are linked together by edges. Each edge connects two nodes, and describes the change in the activation status value of one node, which is used to configure the activation status value of the other interconnected node. The direction of the edge node implies who influences whom, with the sign of the causality relationship being positive if there is a direct relationship to influence, and negative in the case of a trade-off effect. Finally, it equals to zero if the two nodes are uncorrelated. Causal relations typically defined by experts are described by using fuzzy linguistic variables and they are fuzzified using membership functions (Groumpos, 2012; Papageorgiou & Groumpos, 2005). In this way, the linguistics are transformed to real numbers in the interval $[-1,1]$ (Figure 2).

The SEG-CYS modelling approach can have a potential application in several scenarios. It actually incorporates FCMs and procedures that achieve the forecast or estimation of

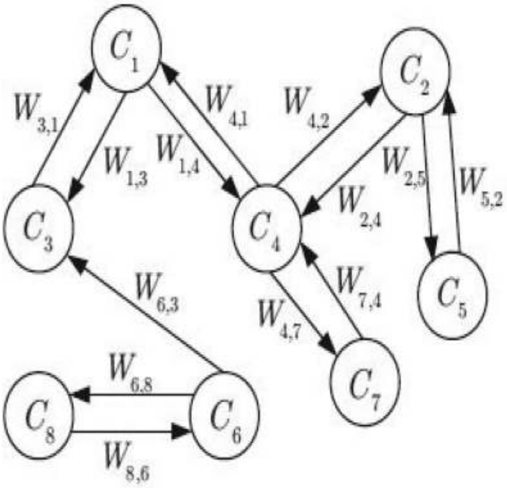

Figure 2. Construction of a FCM with nodes and weights.

the relative change in the overall level of security under the Mental Modeler software (http://www.mentalmodeler.org/scenario/).

3.2 MFIS and FR

Fuzzy logic is a modelling attempt close to the human way of thinking and inference. It provides approximate reasoning mechanisms and inference/decision-making, since the human brain tends to make the approximate reasoning based on qualitative perception criteria.

In an MFIS, human knowledge is illustrated in the form of fuzzy *IF/THEN* rules (FR). The FR are a mechanism of knowledge representation, which is reflected in the hypothetical proposals, analogous to the human way of thinking. The fuzzy sets expressing verbal terms are combined together and they create FR, representing the available knowledge. They are described as follows:

IF x is A (antecedent) *THEN y is B* (consequent),

where *A* and *B* are fuzzy sets (linguistics) corresponding to parameters *x* and *y* which are defined in the universe of discourse *X* and *Y*, respectively. The expressions ' *x* is *A* and *y* is *B*' are fuzzy proposals. The fuzzy rule defines a fuzzy implication relation (between the parameters *x* and *y*). The implication relation correlates the truth level of the antecedent to the corresponding truth of the consequent. It is a fact that *x* belongs to the fuzzy set *A* with a degree of membership, and the same stands between *y* and *B*. Finally, the fuzzy consequent is defuzzified by a defuzzification function and we obtain a crisp value, which is the final numeric result. Its benefit is that it can be handled by a computational approach or a sensor (Iliadis, 2008).

The development of the MFIS based on the corresponding FR has been done under the Matlab platform that offers an integrated fuzzy systems' development analysis and visualization environment (http://www.mathworks.com/) (Figure 3).

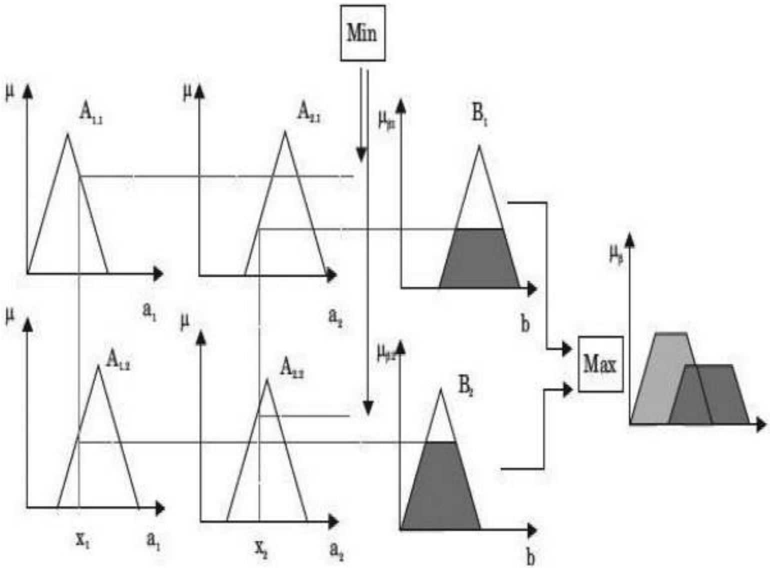

Figure 3. Max–Min inference for the Mamdani model (Saboya, da Glória Alves, & Dias Pinto, 2006).

4. Architecture of the SEG-CYS

The design of the system's architecture was performed by using the initial identification of security baselines, for each LIC based on the *Impact Levels* (ILs) of CIA, as they were set by the standardization bodies. The proposed system should capture the existing knowledge, regarding the interaction–causal relationships between risk factors of the interconnected SEG systems (Figure 4).

The algorithmic steps are described below: In the first stage, all the FCM connections and interaction points are represented in the FCM.

Step 1 (Modelling): It includes the design of the FCM by introducing and connecting all correlated *CIA ILs* of every *LIC*. The security baselines of the *IL* cases of the CIA for the 22 LICs are presented in Table 3. The FCM produces the relative changes in the potential *IL* cases of the CIA for all LICs based on the security baselines.

The FCM algorithm performs the simulation of nodes' interaction. This is done by performing iterative calculations of the new interaction values corresponding to each node. The new interaction value of a node $\boldsymbol{n_i}$ depends on the values of the nodes with starting edges that point to node $\boldsymbol{n_i}$. Transfer functions are used to transform the result of the sum of the product of the node activation values. This calculates the new value of each node and the corresponding weight of the connecting edge, while this converts the actual value of each variable in the modelled system in the interval [−1,1].

Step 2 (Boundaries): It includes the fuzzification of the numerical crisp values of the relative changes obtained by the FCM. This is done by employing three consequent triangular membership functions (in Matlab) in order to classify the security of each subsystem in three classes (linguistics), namely, *Low (L), Middle (M),* and *High (H)* security. In the end of this process, all of the crisp numerical values of the relative changes are assigned to boundaries of the triangular membership functions. As we have already mentioned, the subsystems are classified in the three above linguistics.

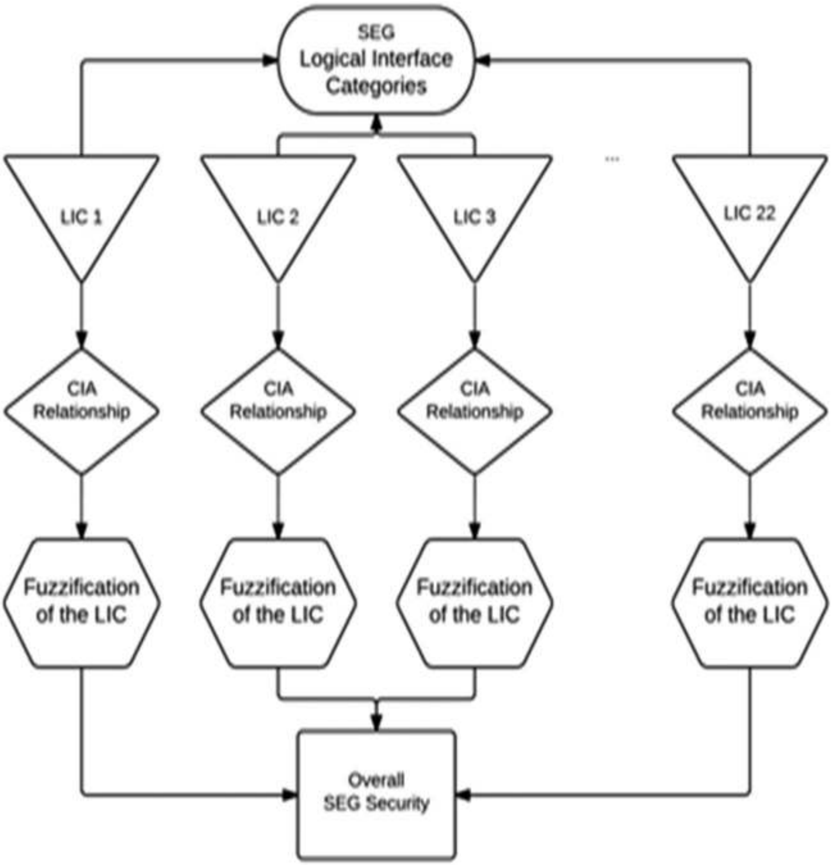

Figure 4. Architecture of SEG-CYS.

Additionally, the fuzzy Mamdani implication relation is used for building rules in order to extract the overall security, by considering all of the subsystems. More specifically, the *max–min* Mamdani fuzzy relation is used. This relation receives the smallest degree of participation of the fuzzified values and produces the degree of fulfilment of each rule. *The degree of fulfilment of the rule indicates the importance of the result of the rule.*

The centroid defuzzifier is used to convert the conclusions drawn by the inference mechanism, in real crisp numbers, corresponding to real-world concepts related to the case.

Table 3. Smart grid impact levels.

LIC	Co	In	Av	LIC	Co	In	Av
1	L	H	H	12	L	M	M
2	L	H	M	13	H	H	L
3	L	H	H	14	H	H	H
4	L	H	M	15	L	M	M
5	L	H	H	16	H	M	L
6	L	H	M	17	L	H	M
7	H	M	L	18	L	H	L
8	H	M	L	19	L	H	M
9	L	M	M	20	L	H	M
10	L	H	M	21	L	H	L
11	L	M	M	22	H	H	H

Step 3 (Scenarios): The third step includes the fuzzification of the 22 LICs, obtained by extensive testing under a variety of scenarios (27 potential cases of CIA *IL*).

A FIS has been developed with detailed FR. This is done in order to examine how a change in one interface affects all of the security SEGs. This methodology reclaims and automates the adjustment of the knowledge base resulting from the FCM. In this system, the original interconnections of each *LIC* is assigned three fuzzy categories (*min, middle, and max*) using triangular membership functions, thus creating the conditions for decision-making under uncertainty.

To derive the overall security degree for each potential *IL* case of the CIA and for the 22 subsystems, a set of fuzzy Mamdani rules is created. The developed rules follow the 27 potential *IL* cases of the CIA, for the 22 *LICs*. The inputs to the rules are the values of the relative changes in the 22 LICs corresponding to the *IL* cases of the CIA. The output of each rule is a value in the interval [0,1] and it offers the final classification, based on the obtained overall security.

4.1 SEG-CYS algorithm

The basic modelling methodology of the SEG-CYS includes three distinct stages, namely, Modelling, Grid, and Scenarios. The proposed algorithmic process involves seven distinct steps, which are discussed below:

In the first stage (Modelling), a FCM is constructed for the estimation of the relative changes in the *IL* cases for each LIC.

(1) The security baselines of the IL cases of the CIA for the 22 LICs are presented in Table 3 and they are interconnected by synapses and named accordingly.

According to Table 3, LICs 7, 8, 13, 14, 16, and 22 have a high impact level for confidentiality, because of the type of data that needs to be protected (sensitive customer energy usage data, and critical security parameters).

(2) The design of the FCM by introducing and connecting all correlated CIA of every LIC (Figure 5).

(3) All different interconnections and the corresponding influence degrees of potential *IL* cases (L), (M), and (H) of CIA from the 22 *LICs* are represented.

(4) The FCM produces the relative changes in the potential *IL* cases of the CIA for all LICs based on the security baselines. This modelling aims to estimate the relative changes in the IL cases for each LIC. This means that if an interconnection between an LIC changes, the system is capable to forecast the IL for the CIA of the LIC. The total potential IL cases for the CIA of every LIC are $3^3 = 27$.

Regarding the first LIC as security baseline, the IL for the CIA has been set as follows: *Confidentiality - Low, Integrity - High, and Availability - High* (LHH). In the case of LIC_1 modelling with a FCM and for the security baseline LHH, the relative change was set to 0. The security baseline LHH is the initial state of LIC1 and for this reason, we have assigned it the value of 0. In Table 3, the initial states of LICs are presented. Table 4 contains the numerical values of the relative changes in the 27 IL cases that have emerged based on FCM mapping when the security baseline is LIC1.

For each connected LIC of the FCM, the initial state of the CIA can take either of the three linguistics (L, M, or H). For example, for LIC_1 the initial state of CIA is LHH. In the FCM mapping, the three above linguistics are described by using the symbols + or −.

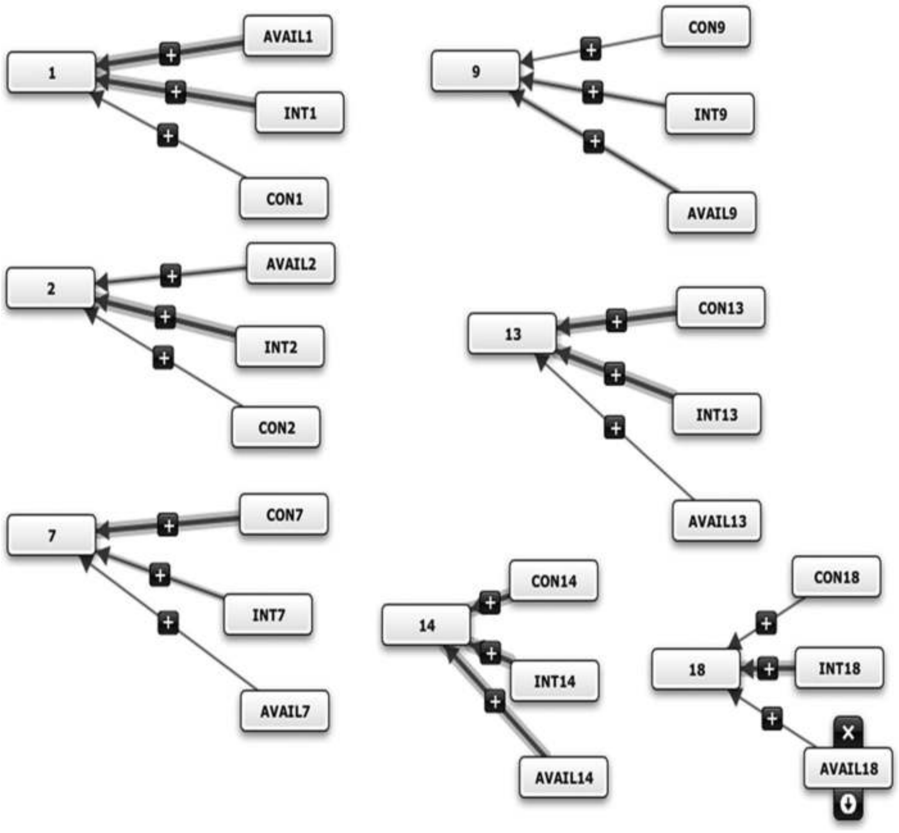

Figure 5. The primary causal interconnections of the different IL cases of CIA for some LICs during the Modelling process.

The low is assigned the symbol (+), the middle (+ +), and the high (+ + +). We examined for each LIC all combinations of the three linguistics (L, M, and H) of the CIA (see Table 4). All the relative changes are estimated to the initial state. Totally $3^3 = 27$ scenarios are created for each LIC. For the calculation of the 27 scenarios in the closed interval [−1,1], the hyperbolic tangent (tanh) function has been used. The same approach is used for all of the LICs.

Table 4. The relative changes in 27 IL cases of CIA when the security baseline is LIC1.

Impact level cases	Con	Int	Av	Relative change	Impact level cases	Con	Int	Av	Relative change
1	L	L	L	−0.25	15	M	M	H	−0.05
2	L	L	M	−0.19	16	M	H	L	−0.09
3	L	L	H	−0.1	17	M	H	M	−0.05
4	L	M	L	−0.19	18	M	H	H	0.01
5	L	M	M	−0.14	19	H	L	L	−0.21
6	L	M	H	−0.06	20	H	L	M	−0.15
7	L	H	L	−0.1	21	H	L	H	−0.07
8	L	H	M	−0.06	22	H	M	L	−0.15
9	L	H	H	0	23	H	M	M	−0.11
10	M	L	L	−0.14	24	H	M	H	−0.03
11	M	L	M	−0.18	25	H	H	L	−0.07
12	M	L	H	−0.09	26	H	H	M	−0.03
13	M	M	L	−0.18	27	H	H	H	0.02
14	M	M	M	−0.13					

In the second stage (Boundaries), the FIS is constructed under the Matlab environment.

(5) The numerical crisp values of the relative changes are used as boundaries in order to classify the security of each subsystem in one of the three following linguistics, namely, *Low, Middle,* and *High*. This happens in order to fuzzify the numerical crisp values of the relative changes in all the potential *IL* cases for each LIC.

(6) Three consequent triangular fuzzy membership functions are constructed under the Matlab environment in order to classify the security of each subsystem.

The security categorization of the first LIC from the application of all potential *IL* cases of the CIA (scenarios – deviations) is presented in Table 5. The same approach is used for all of the LICs.

The largest relative changes from the original connections provide lower security. However, changes greater than the initial links or near to the security baseline give higher security levels.

In the third stage (Scenarios), a FIS has been developed with detailed FR.

(7) The fuzzy Mamdani implication relation is used for building rules in order to extract overall security. This has been done in order to derive the overall security of each IL case of the CIA for the 22 subsystems. It includes the values of the relative changes in the 22 LICs from the potential *IL* cases (27*22). This is done based on the changes in the LICs' interfaces. The inputs to the rules are the numerical crisp values of relative changes, which are used as boundaries of the 22 LICs corresponding to the *IL* cases of the CIA (see Table 6).

The range of the numerical crisp values from the relative changes in the 27 *IL* cases of the CIA for all of the LICs is presented in Table 7.

Table 5. Fuzzification of the relative changes in the 27 IL cases of CIA for the 1st LIC.

Impact level cases of CIA	Values of relative change	Max	Middle	Min	Security	Difference from security baseline
LLL	−0.25	1	0	0	Low	High
LLM	−0.19	0.44	0.30	0	Low	High
LLH	−0.1	0	0.86	0	Middle	Medium
LML	−0.19	0.44	0.30	0	Low	High
LMM	−0.14	0	0.77	0	Middle	Medium
LMH	−0.06	0	0.49	0.26	Middle	Medium
LHL	−0.1	0	0.86	0	Middle	Medium
LHM	−0.06	0	0.49	0.26	Middle	Medium
LHH	0	0	0	0	Security Baseline	
MLL	−0.14	0	0.77	0	Middle	Medium
MLM	−0.18	0.35	0.4	0	Middle	Medium
MLH	−0.09	0	0.77	0	Middle	Medium
MML	−0.18	0.35	0.4	0	Middle	Medium
MMM	−0.13	0	0.86	0	Middle	Medium
MMH	−0.05	0	0.4	0.35	Middle	Medium
MHL	−0.09	0	0.77	0	Middle	Medium
MHM	−0.05	0	0.4	0.35	Middle	Medium
MHH	0.01	0	0	0.91	High	Low
HLL	−0.21	0.63	0.12	0	Low	High
HLM	−0.15	0.07	0.67	0	Middle	Medium
HLH	−0.07	0	0.58	0.17	Middle	Medium
HML	−0.15	0.07	0.67	0	Middle	Medium
HMM	−0.11	0	0.95	0	Middle	Medium
HMH	−0.03	0	0.21	0.53	High	Low
HHL	−0.07	0	0.58	0.17	Middle	Medium
HHM	−0.03	0	0.21	0.53	High	Low
HHH	0.02	0	0	1	High	Low

Table 6. The boundaries of the triangular membership functions from the 27 IL cases of CIA for each LIC.

LIC	Low security	Medium security	High security
LIC 1	[−0.358 −0.25 −0.142]	[−0.223 −0.115 −0.007]	[−0.088 0.02 0.128]
LIC 2	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 3	[−0.358 −0.25 −0.142]	[−0.223 −0.115 −0.007]	[−0.088 0.02 0.128]
LIC 4	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 5	[−0.358 −0.25 −0.142]	[−0.223 −0.115 −0.007]	[−0.088 0.02 0.128]
LIC 6	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 7	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 8	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 9	[−0.14 −0.06 0.02]	[−0.04 0.04 0.12]	[0.06 0.14 0.22]
LIC 10	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 11	[−0.14 −0.06 0.02]	[−0.04 0.04 0.12]	[0.06 0.14 0.22]
LIC 12	[−0.14 −0.06 0.02]	[−0.04 0.04 0.12]	[0.06 0.14 0.22]
LIC 13	[−0.358 −0.25 −0.142]	[−0.223 −0.115 −0.007]	[−0.088 0.02 0.128]
LIC 14	[−0.37 −0.27 −0.17]	[−0.245 −0.145 −0.045]	[−0.12 −0.02 0.08]
LIC 15	[−0.14 −0.06 0.02]	[−0.04 0.04 0.12]	[0.06 0.14 0.22]
LIC 16	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 17	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 18	[−0.262 −0.17 −0.078]	[−0.147 −0.055 0.037]	[−0.032 0.06 0.152]
LIC 19	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 20	[−0.28 −0.18 −0.08]	[−0.155 −0.055 0.045]	[−0.03 0.07 0.17]
LIC 21	[−0.262 −0.17 −0.078]	[−0.147 −0.055 0.037]	[−0.032 0.06 0.152]
LIC 22	[−0.37 −0.27 −0.17]	[−0.245 −0.145 −0.045]	[−0.12 −0.02 0.08]

The output of each rule is obtained by three triangular membership functions (min, middle, and max) with crisp numerical values in the closed interval [0,1] (Table 8).

After the examination of all the scenarios, we obtained the overall security category (OSCAT) of each subsystem under consideration (Table 9).

Table 7. The range of the numerical crisp values of the relative changes. The values of the 27 IL cases of CIA for all LICs.

IL cases of CIA	Range for all LICs	IL cases of CIA	Range for all LICs
LLL	[−0.27 −0.06]	MMH	[−0.11 0.06]
LLM	[−0.23 −0.03]	MHL	[−0.1 0.04]
LLH	[−0.13 0.02]	MHM	[−0.07 0.06]
LML	[−0.22 −0.03]	MHH	[−0.03 0.11]
LMM	[−0.18 −0.09]	HLL	[−0.21 −0.02]
LMH	[−0.15 0.05]	HLM	[−0.15 0.01]
LHL	[−0.13 0.02]	HLH	[−0.08 0.06]
LHM	[−0.1 0.05]	HML	[−0.15 0.01]
LHH	[−0.07 0.1]	HMM	[−0.11 0.04]
MLL	[−0.22 −0.05]	HMH	[−0.03 0.09]
MLM	[−0.18 −0.02]	HHL	[−0.07 0.06]
MLH	[−0.15 0.04]	HHM	[−0.03 0.09]
MML	[−0.18 −0.02]	HHH	[0.02 0.14]
MMM	[−0.13 0.01]		

Table 8. The boundaries of overall security classification (output of each rule).

Linguistics of overall security classification	Boundaries of the triangular membership functions
Low	[−0.4 0 0.4]
Middle	[0.1 0.5 0.9]
High	[0.6 1 1.4]

Table 9. Overall security classification (OSC) by applying the IL cases of CIA related to the 22 LICs.

27 IL cases	22 LICs																						OSC
CIA	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	
LLL	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	0.13 (L)
LLM	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	0.16 (L)
LLH	M	M	M	M	M	M	L	L	M	M	M	M	M	M	M	L	M	L	M	M	L	M	0.5 (M)
LML	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	M	L	L	M	L	0.37 (M)
LMM	M	M	M	M	M	M	L	L		M			M	M		L	M	M	M	M	M	M	0.48 (M)
LMH	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	0.5 (M)
LHL	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M		M	M		M	0.5 (M)
LHM	M		M		M		M	M	M		M	M	M	M	M	M		H			H	M	0.5 (M)
LHH		H		H		H	M	M	H	H	H	H	M	H	H	M	H	H	H	H	H	H	0.65 (M)
MLL	M	L	M	L	M	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	0.16 (L)
MLM	M	L	M	L	M	L	M	M	L	L	L	L	M	M	L	M	L	L	L	L	L	M	0.38 (M)
MLH	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	0.5 (M)
MML	M	M	M	M	M	M	M	M	L	M	L	L	M	M	L	M	M	M	M	M	M	M	0.47 (M)
MMM	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	0.5 (M)
MMH	M	M	M	M	M	M	M	M	M	M	M	M	M	H	M	M	M	M	M	M	M	H	0.5 (M)
MHL	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	H	M	M	H	M	0.5 (M)
MHM	M	H	M	H	M	H	M	M	M	H	M	M	M	H	M	M	H	H	H	H	H	H	0.5 (M)
MHH	H	H	H	H	H	H	M	M	H	H	H	H	H	H	H	M	H	H	H	H	H	H	0.85 (H)
HLL	L	L	L	L	L	L	M	M	L	L	L	L	M	M	L	M	L	L	L	L	L	M	0.3 (M)
HLM	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	0.48 (M)
HLH	M	M	M	M	M	M	H	H	M	M	M	M	M	H	M	H	M	M	M	M	M	H	0.5 (M)
HML	M	M	M	M	M	M			M	M	M	M	M	M	M		M	M	M	M	M	M	0.5 (M)
HMM	M	M	M	M	M	M	H	H	M	M	M	M	M	H	M	H	M	M	M	M	M	H	0.5 (M)
HMH	H	M	H	M	H	M	H	H	H	M	H	H	H	H	H	H	M	H	M	M	H	H	0.51 (M)
HHL	M	H	M	H	M	H	H	H	M	H	M	M		H	M	H	H	H	H	H	H	H	0.73 (M)
HHM	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	0.84 (H)
HHH	H	H	H	H	H	H	H	H	H	H	H	H	H		H	H	H	H	H	H	H		0.84 (H)

5. Results

Table 9 contains the 22 LICs and the 27 potential *IL* cases of the CIA that may arise. It presents the overall security classification (OSC) of the SEGs based on the three linguistics *low (L), middle(M)*, and *high (H)*. Three out of the 27 *IL* cases that are considered have *low* overall security (LOS) level, 21 of them have *middle* overall security (MOS), and 3 *high*.

Attempting a thorough analysis and explanation of Table 9, we observe that three *IL* cases provide LOS. From these, two IL cases of CIA (LLL and LLM) provide absolute LOS for all of their subsystems. On the other hand, one IL case of the CIA (MLL) is assigned MOS for some of their subsystems without affecting the overall LOS at all.

It is a fact that 21 IL cases of CIA show MOS. A subset of six *IL* cases of the CIA (out of the 21) have MOS in all of their subsystems (LMH, LHL, MLH, MMM, HLM, and HML), whereas six exhibit some LOS subsystems (LLH, LML, LMM, MLM, MML, and HLL) and nine MOS *IL* cases of CIA (out of the 21) include some High Overall Security (HOS) subsystems (LHM, LHH, MHH, MHL, MHM, HLH, HMM, HMH, and HHL).

Finally three scenarios are characterized by HOS. From them, two (HHM and HHH) provide exclusively HOS subsystems. On the other hand, one IL case of the CIA (MHH) provides MOS to the minority of their subsystems.

The most important fact is the visualization of the overall security of SEGs. It also enables the administrators of these systems to calculate changes in the overall level of security that can be derived from the change in the IL cases of the CIA of some LICs. This feature significantly strengthens and fortifies the overall system and provides significant opportunities for making valid and optimal decisions.

6. Using our approach in real world

It is important to present an application case of our system-model under a hypothetical scenario. This would provide insights towards a better understanding of its contribution.

Assume a microgrid consisting of solar panels, a small wind turbine, batteries, controlled loads, and controlled interface to the local network of Low Voltage (LV). The batteries, the solar panels, and the wind turbine are connected to the alternating voltage network through DC/AC (Alternating Current/Direct Current) power converters. The inverters are properly controlled to allow the operation of the system either to the interconnected XT network (grid-tied) or to an autonomous (island) function through a fast jump from one state to another. The central element of the microgrid is the battery inverter, which regulates the voltage and the frequency when the system operates in standalone mode, taking control of active and inactive power.

The battery inverter consists of a DC/DC converter and a voltage source. Both of them are operating in the bidirectional power flow mode, thereby allowing the charging and discharging of the batteries. The DC/DC converter provides constant 380 V DC voltage at the input of the DC/AC inverter. The high-frequency transformer, which operates at 16.6 kHz, provides electrical isolation between the battery and the network. A single-phase inverter is connected to the AC microgrid (ACMIC). The inverter is powered by photovoltaic power within 2.1 KW, located in the installation of the microgrid space. The ACMIC with three single-phase battery inverters is constantly evolving with the connection of new seepages.

The inverter comprises three WiFi interfaces with CIA of low security LML, an Ethernet with CIA MLH of medium security, and a Zigbee with CIA of high security HMH.

As the following system works with dynamic interoperability, its situation may change frequently, modifying its overall safety.

However, if these interfaces in the microgrid are modified, then the CIA of every interconnection changes and hence the whole microgrid security level becomes completely different. If FCMs consider all of the CIA change scenarios at each interface, we obtain $3^3 = 27$ scenarios of relative change in the initial security situation of each interface. Totally 27*3 = 81 scenarios were built for the three interfaces. After the fuzzification of the crisp relative change values of each interface in the closed interval [−0.05, 0.05], three risk linguistics (low, medium, and high) were used to characterize the security level of each interface in each scenario.

In this way, we manage to estimate the security provided by each interface for each CIA scenario, while by the use of the fuzzy inference Mamdani system, we obtain the overall security of the network for all of the scenarios in all three interfaces.

For example, the initial WiFi security is assigned an LML value for the CIA, which is interpreted as low security for all three interfaces. In the LML scenario, the Ethernet modifies its security level by −0.03 from its initial CIA state, whereas the Zigbee by −0.04, which are both interpreted as passing to low network security. The 27 CIA scenarios constructed for the three interfaces are shown in Table 10, giving in each case the overall security of the microgrid. The CIA scenarios with the lowest overall security are the LLL and LML, whereas the HHH offers the highest potential security level.

Table 10. Overall security by applying the IL cases of the 27 CIA related to the three (WiFi, Ethernet, and Zigbee) LICs.

27 IL cases	3 LICs			Overall security
CIA	WiFi	Ethernet	Zigbee	
LLL	M	L	L	0.13 (L)
LLM	M	M	L	0.5 (M)
LLH	M	M	M	0.5 (M)
LML		L	L	0.13 (L)
LMM	M	M	M	0.5 (M)
LMH	M	M	M	0.5 (M)
LHL	M	M	M	0.5 (M)
LHM	M	M	M	0.5 (M)
LHH	M	H	H	0.854 (H)
MLL	M	M	L	0.5 (M)
MLM	M	M	M	0.5 (M)
MLH	M		M	0.5 (M)
MML	M	M	M	0.5 (M)
MMM	M	M	M	0.5 (M)
MMH	M	H	H	0.854 (H)
MHL	M	M	M	0.5 (M)
MHM	M	H	M	0.5 (M)
MHH	M	H	H	0.854 (H)
HLL	M	M	M	0.5 (M)
HLM	M	M	M	0.5 (M)
HLH	M	H	H	0.854(H)
HML	M	M	M	0.5 (M)
HMM	M	M	H	0.822 (H)
HMH	M	H		0.847 (H)
HHL	M	M	H	0.822 (H)
HHM	M	M	H	0.822(H)
HHH	H	H	H	0.87 (H)

7. Conclusions

A highly reliable hybrid system that automates and facilitates the planning, monitoring, managing, and obtaining of an optimal resolution of the security systems of SEG is presented in this research paper. It is an artificial intelligence computer security technique (Demertzis & Iliadis, 2014a, 2014b, 2014c, 2014d; Demertzis & Iliadis, 2015a, 2015b) which provides smart mechanisms for the supervision and categorization of energy networks, and it creates the essential conditions for active security in an architectural design. Moreover, it allows a detailed analysis of the management methods of SEGs and it optimizes decision-making in cases of threats or risks.

Attempting a thorough analysis, it is easy to understand that the proposed system simplifies the very complex problem of digital SEGs' security. The employment of a FCM reflects and models each of the 22 LICs in relation with the *ILs* of the CIA. The integration of these 22 categories creates a basic framework, which is the basic foundation for building an architectural design based on realistic security rules. Also, the use of the FIS and the adoption of FR created a high-level safety controller, which allows almost visual deciding on any possible interface change scenario and how this change affects the overall level of security in all of the SEG domains.

The proposed system controls the overall security due to the dynamic interoperability, by creating automated control capabilities for updating the network structure as a result of the incurred changes. What is needed to achieve the control is to map the network systems and the CIA and to consider how any change in the system affects the overall safety.

As future directions that can improve the proposed model, we are going to plan the addition of a heuristic optimization method in FCM procedures, such as genetic algorithms or swarm intelligence. Also, it would be interesting to employ a system with Fuzzy Association Rules, which could improve the dynamics of the system, by identifying more precisely the logical relationships which present a high risk and require special handling.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Ahmad, S., & Baig, Z. A. (2012). Fuzzy-based optimization for effective detection of smart grid cyber-attacks. *International Journal of Smart Grid and Clean Energy*, *1*(1), 15–21. Retrieved from http://www.ijsgce.com/uploadfile/2012/1011/20121011122129685.pdf

Baig, Z. A. (2011, October). *On the use of pattern matching for rapid anomaly detection in smart grid infrastructures*. IEEE international conference on smart grid communications. Proceedings of smart grid communication, (pp. 214–219), Brussels, Belgium. doi:10.1109/SmartGridComm.2011.6102321

Chaudhari, S. R., & Patil, M. E. (2014). Comparative analysis of fuzzy inference systems for air conditioner. *International Journal of Advanced Computer Research*, *4* (4). (ISSN (Print): 2249–277 ISSN (Online): 2277-7970)

Cirincione, G., Krishnamurthy, S., La Porta, T. F., Govindan, R., & Mohapatra, P. (2010). *Impact of security properties on the quality of information in tactical military networks*. Proceedings – IEEE military communications conference MILCOM, San Jose, CA, 31 Oct–3 Nov, 2010, art. no. 5680438, pp. 1–6. doi:10.1109/MILCOM.2010.5680438

Coelho, V. N., Coelho, I. M., Coelho, B. N., Reis, A. J. R., Enayatifar, R., Souza, M. J. F., & Guimarães, F. G. (2016). A self-adaptive evolutionary fuzzy model for load forecasting problems on smart grid environment. *Applied Energy*, *169*, 567–584.

Demertzis, K., & Iliadis, L. (2014a). A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification. *In: E-Democracy, Security, Privacy and Trust in a Digital World. Communications in Computer and Information Science*, *441*, 11–23. doi:10.1007/978-3-319-11710-2_2

Demertzis, K., & Iliadis, L. (2014b). Evolving computational intelligence system for malware detection. *In: Advanced Information Systems Engineering Workshops, Lecture Notes in Business Information Processing*, *178*, 322–334. doi:10.1007/978-3-319-07869-4_30

Demertzis, K., & Iliadis, L. (2014c, April). *Bio-inspired hybrid artificial intelligence framework for cyber security*. Springer proceedings 2nd conference on CryptAAF: Cryptography network security and applications in the armed forces (pp. 161–193). Athens: Springer. doi:10.1007/978-3-319-18275-9_7

Demertzis, K., & Iliadis, L. (2014d, November). *Bio-inspired hybrid intelligent method for detecting android malware*. Proceedings of the 9th KICSS 2014, knowledge information and creative support systems (pp. 231–243), Cyprus. ISBN: 978-9963-700-84-4

Demertzis, K., & Iliadis, L. (2015a, April). *Evolving smart URL filter in a zone-based policy firewall for detecting algorithmically generated malicious domains*. Proceedings SLDS (Statistical Learning and Data Sciences) conference LNAI (Lecture Notes in Artificial Intelligence) (Vol. 9047, pp. 223–233). Berlin: Springer, Royal Holloway University London, UK. doi:10.1007/978-3-319-17091-6_17

Demertzis, K., & Iliadis, L. (2015b, September). *SAME: An intelligent anti-malware extension for android ART virtual machine*. Proceedings of the 7th international conference ICCCI 2015, Lecture Notes in Artificial Intelligence (LNAI) (Vol. 9330, pp. 235–245). Madrid, Spain. doi:10.1007/978-3-319-24306-1_23

Drtil, J. (2013). Impact of information security incidents theory and reality. *Journal of Systems Integration*, *4*(1), 44–52. doi:10.20470/jsi.v4i1.144

Groumpos, P. P. (2012, June). *Mathematical modeling of control using fuzzy cognitive maps: Challenging issues*. Proceedings of the IASTED international conference and applications (pp. 197–204), Crete, Greece.

Guney, K., & Sarikaya, N. (2009). Comparison of Mamdani and Sugeno fuzzy inference system models dor resonant frequency calculation of rectangular microstrip antennas. *Progress in Electromagnetics Research B*, *12*, 81–104.

Hosseini, H., Bathaee, S., Abedini, A., Hosseina, M., & Fereidunain, A. (2014). Defending false data injection attack on smart grid network using neuro-fuzzy controller. *Journal of Intelligent and Fuzzy Systems*, *27*, 1457–1467. doi:10.3233/IFS-131112

Iliadis, L. (2008). *Intelligent information systems and applications in risk estimation*. Thessaloniki, Greece: A. Stamoulis. ISBN: 978-960-6741-33-3

Jang, J. S. R., Sun, C. T., & Mizutani, E. (1997). *Neuro-fuzzy and soft computing: A computational approach to learning and machine intelligence*. Upper Saddle River, NJ: Prentice-Hall.

Jurado, S., Nebot, À., Mugica, F., & Avellana, N. (2015). Hybrid methodologies for electricity load forecasting: Entropy-based feature selection with machine learning and soft computing techniques. *Energy*, *86*, 276–291.

Koraz, Y., & Gabbar, H. A. (2016, August). *Hierarchical safety control for micro energy grids using adaptive neuro-fuzzy decision making method*. 4th IEEE international conference on smart energy grid engineering (pp. 131–136). SEGE 2016, art. no. 7589513.

Kottas, T., Stimoniaris, D., Tsiamitros, D., Kikis, V., Boutalis, Y., & Dialynas, E. (2015). *New operation scheme and control of smart grids using fuzzy cognitive networks*. IEEE Eindhoven PowerTech, PowerTech 2015, art. no. 7232563.

Kumar, V., & Hussain, M. (2014, December). *Secure communication for advance metering infrastructure in smart grid*. Annual IEEE India conference (INDICON) (pp. 207–212), India. doi:10.1109/INDICON.2014.7030600

Li, X., Liang, X., Lu, R., Shen, X., Lin, X., & Zhu, H. (2012). Securing smart grid: Cyber-attacks, countermeasures and challenges. *Cyber Security for Smart Grid Communications, IEEE Communications Magazine*, *50*, 38–45. doi:10.1109/MCOM.2012.6257525

Mamdani, E. H., & Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies*, *7*, 1–13.

The MathWorks. Retrieved from http://www.mathworks.com/

The MentalModeler. Retrieved from http://www.mentalmodeler.org/scenario/

Mohagheghi, S. (2010). A fuzzy cognitive map for data integrity assessment in a IEC 61850 based substation. *Power and Energy Society General Meeting*, 1–7. doi:10.1109/PES.2010.5588058

Mohagheghi, S. (2014). Integrity assessment scheme for situational awareness in utility automation systems. *IEEE Transactions on Smart Grid*, *5*, 592–601. doi:10.1109/TSG.2013.2283260

NISTIR 7628. (2010). *Introduction to NISTIR 7628, Guidelines for smart grid cyber security* (pp. 1–20). The Smart Grid Interoperability Panel Cyber Security Working Group.

NISTIR 7628. (2014). *Guidelines for smart grid CyberSecurity: Smart grid cyber security strategy, Architecture, and high-level requirements*. The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, National Institute of Standards and Technology, U.S Department of Commerce, Interagency Report 7628 (NISTIR7628), 1, 290. doi:10.6028/NIST.IR.7628r1

Papageorgiou, E. I., & Groumpos, P. P. (2005). A new hybrid method using evolutionary algorithms to train fuzzy cognitive maps. *Applied Soft Computing*, *5*, 409–431. doi:10.1016/j.asoc.2004.08.008

Papageorgiou, E. I., & Salmeron, J. L. (2013). A review of fuzzy cognitive maps research during the last decade. *IEEE Transactions on Fuzzy Systems*, *21*(1), 66–79.

Rahman, M. S., Oo, A. M. T., Mahmud, M. A., & Pota, H. R. (2016). *A multi-agent approach for security of future power grid protection systems*. IEEE Power and Energy Society general meeting, Boston, 17–21 July, 2016, art. no. 7741880. doi:10.1109/PESGM.2016.7741880

Rawat, D. B., & Bajracharya, C. (2015 June). *Cyber security for smart grid systems: Status, challenges and perspectives*. Conference proceedings, IEEE SOUTHEASTCON, Fort Lauderdale, FL, 9-12 April 2015, art. no. 7132891. doi:10.1109/SECON.2015.7132891

Saboya, Jr, F., da Glória Alves, M., & Dias Pinto, W. (2006). Assessment of failure susceptibility of soil slopes using fuzzy logic. *Engineering Geology*, *86*(4), 211–224. doi:10.1016/j.enggeo.2006.05.001

Salmeron, J. L., & Froelich, W. (2016). Dynamic optimization of fuzzy cognitive maps for time series forecasting. *Knowledge-Based Systems*, *105*, 29–37.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), ISSN:1551-0123

Sattarova Feruza, Y., & Kim, T. H. (2007). It security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Silva, L. N., Knak Neto, N., Abaide, A. R., & Bernardon, D. (2015 November). *Intelligent methodology to distribution systems diagnostic in smart grids perspective*. Proceedings of the universities power engineering conference, Science Centre, Faculty of Computing, Engineering and Sciences, Staffordshire University, Stoke-on-Trent, United Kingdom, 1–4 Sep 2015, art. no. 7339935. doi:10.1109/UPEC.2015.7339935

Tazi, K., Abdi, F., & Abbou, M. F. (2015 December). *Review on cyber-physical security of the smart grid: Attacks and defense mechanisms*. Proceedings of 2015 IEEE international renewable and sustainable energy conference, IRSEC 2015, Marrakech, Morocco, art. no. 7455127. doi:10.1109/IRSEC.2015.7455127

Vidal, R., Salmeron, J. L., Mena, A., & Chulvi, V. (2015). Fuzzy cognitive map-based selection of TRIZ trends for eco-innovation of ceramic industry products. *Journal of Cleaner Production*, *107*, 202–214.

Wang, J., Chen, Y., & Chen, M. (2016). Research on real-time and reliability of intelligent distribution network WSNs based on fuzzy cognitive map. *Chinese Journal of Sensors and Actuators*, *29*(2), 213–219.

Wang, J., Wang, Q., Ma, W. Q., & Yao, D. H. (2013, March). *Fuzzy knowledge representation and reasoning of the smart grid. based on medium logic and its application*. Proceedings of the 2nd international conference on computer science and electronics engineering (ICCSEE) (pp. 2786–

2789), China. Paris: Atlantis Press. Retrieved from http://www.atlantis-press.com/php/download_paper.php?id=5126

Xie, J., Stefanov, A., & Liu, C. C. (2016). Physical and cyber security in a smart grid environment. *Wiley Interdisciplinary Reviews: Energy and Environment*, *5*(5), 519–542.

Zhang, Y., Wang, L., Sun, W., Green, R. C., & Alam, M. (2011). Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*, *2*, 796–808.