C. Alcaraz, A. Balastegui, and J. Lopez, "Early Warning System for Cascading Effect Control in Energy Control Systems", *5th International conference on Critical Information Infrastructures Security (CRITIS10)*, LNCS vol. 6712, pp. 55-67, 2010.
NICS Lab. Publications: https://www.nics.uma.es/publications

Early Warning System for Cascading Effect Control in Energy Control Systems

Cristina Alcaraz, Angel Balastegui, and Javier Lopez

Computer Science Department - University of Malaga,
29071 - Malaga, Spain
{alcaraz,balaguesti,jlm}@lcc.uma.es

Abstract. A way of controlling a cascading effect caused by a failure or a threat in a critical system is using intelligent mechanisms capable of predicting anomalous behaviours and also capable of reacting against them in advance. These mechanisms are known as Early Warning Systems (EWSs) and this will be precisely the main topic of this paper. More specifically, we present in this paper an EWS design based on a Wireless Sensor Network (using the ISA100.11a standard) that constantly supervises the application context. This EWS is also based on forensic techniques to provide dynamic learning capacities. As a result, this new approach will aid to provide a reliable control of incidences by offering a dynamic alarm management system, identification of the most suitable field operator to attend an alarm, reporting of causes and responsible operators, and learning from new anomalous situations.

Keywords - *Early Warning System, Wireless Sensor Network, Forensic Techniques, Energy Control Systems, SCADA Systems, Cascading Effect.*

1 Introduction

In recent years, electrical energy industry, scientific community and governments are becoming interested in bringing new energy distribution strategies, since these services are fundamental for our economy and social well-being [1]. To be more precise, the most of our critical infrastructures (e.g. transportation systems or communication systems) are highly dependent on electrical energy services to efficiently work and provide their respective services. In other words, a failure (cause) in an energy substation could involve a harmful *cascading effect* (effect) in the business continuity [2]. For this reason, these systems have to trust in other specialized systems, known as SCADA (Supervisory Control and Data Acquisition) systems.

A SCADA system is a complex and distributed system composed of communication networks using a wide range of technologies for control in real-time. These technologies allow human operators to keep a global view of the real state of the critical infrastructure and its application context. However, this technological use involves a new challenge give that these control systems are more and more dependent on communication systems to supervise remote substations localized at different and distant geographical localizations. A failure in the satellite/microwave communication could result in a lack

of monitoring, meaning important consequences in energy distribution. Then, it is clear that different stakeholders are joining efforts to try to solve some security issues related to communication and technology systems.

So far, some security aspects have already been considered by the literature. Among them, identification and authorization, security policies, control access policies, communication network protection and information systems protection. All of these security areas make use of different security mechanisms (such as firewalls, Demilitarized Zones (DMZs), Intrusion Detection Systems (IDS), Virtual Private Networks (VPNs), etc.), cryptographic primitives, standards and recommendations (such as ANSI/ISA-99 [3]). However, there are other security mechanisms that are not yet properly used by the Industry, such as for example EWSs. These systems could add new security functionalities by offering control of anomalous events. Thus, it is possible to previously predict a failure or a threat, and react against it. Therefore, these mechanisms could aid to control significant anomalies which could trigger a possible cascading effect. Precisely, the purpose of this paper is to design an EWS based on a WSN and on forensic techniques to offer: (i) a constant control of anomalous events, (ii) a timely response and (iii) capacity for learning of future anomalous events. As a result, the system will be able to face new situations without requiring a manual procedure to update its knowledge.

The paper is organized as follows. Section 2 presents the SCADA architecture and an alternative technology for industrial control. Section 3 highlights our contribution (specifically in Section 3.2) and justifies its importance in industrial systems through a use case presented in Section 3.3. Finally, Section 4 concludes the paper and outlines the future work.

2 SCADA System and Control Technologies

Any activity and event executed in an electrical energy system must be properly controlled. To this end, these systems have to trust other specific systems to manage, control and supervise such activities, ensuring performance and reliability in energy distribution. These control systems are known as SCADA systems.

2.1 SCADA Network Architecture

A SCADA system is based on three types of sub-networks (see Figure 1): (i) the central network, (ii) remote substations composed of Remote Unit Terminals (RTUs) and (iii) the corporative network. The operations carried out in the central network are related to the control and management of the critical infrastructure. Such operations are managed through specific operator consoles or human-machine interfaces (HMIs), which allow operators to read specific physical parameters (e.g. electrical signals, temperature, etc.) or alarms received from RTUs, or even transmit certain commands to specific field devices located in remote substations. The operations carried out in the corporative network are directly related to the general supervision of the system whose accesses to databases and servers (installed in the central network) are rather restricted.

This network architecture is complex and heterogeneous (see Figure 1), where new and old technologies have to coexist in a same environment of control. To be more

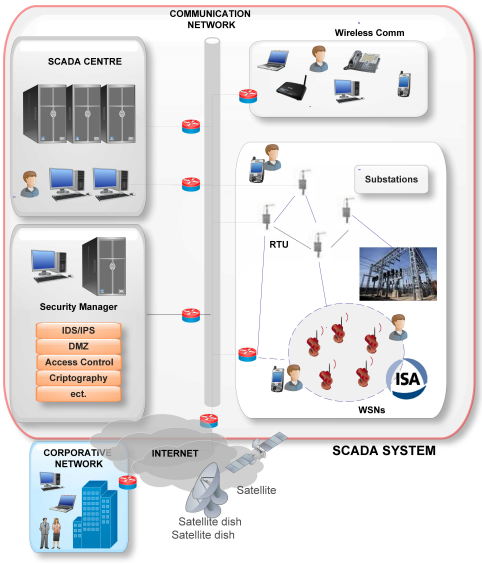

Fig. 1. A SCADA Network Architecture

precise, a SCADA system, belonging to the third generation or *Networked* generation, includes in its network design both serial and TCP/IP communication in order to break with the isolation concept of the previous generations (i.e. *Monolithic* and *Distributed*) [4]. Furthermore, TCP/IP connections make possible monitoring in real-time, peer-to-peer communication from anywhere at any time, multiple sessions, concurrency, maintenance, redundancy, security services and connectivity.

Likewise, all these technical advances are also used in remote substations, where RTUs are able to provide a hierarchical and an inter-RTU communication (i.e., interconnectivity among RTUs) under TCP/IP, as well as wired and wireless communication interfaces, Web services, management and forwarding to other remote points. Due to these advances, RTUs might work as data concentrators (to store large data streams) and/or as remote access controllers (to autonomously and remotely reconfigure/recover parts of the system). Lastly, migration to TCP/IP also meant the standardization and implementation of new SCADA protocols capable of understanding TCP/IP connections. Currently, there are several IP-based SCADA protocols, such as Modbus/TCP, DNP3, IEC-104 and ICCP/TASE2. The three first ones are used for automation, whereas ICCP is specific for inter-communication between telemetry control systems.

Special attention should be paid to wireless industrial sensor networks since this is nowadays one of the most demanded wireless control technologies by the Industry. In fact, they are considered as an optional control technology (see Section 2.2) for monitoring since it can offer the same functionalities as an RTU but to a low installation and maintenance cost. This new alternative and its communication constitute an essential part of the contribution of this paper (see Section 3.2).

2.2 WSN, an Alternative for the Control

A WSN is basically composed of resource-constrained devices, known as sensor nodes. They are autonomous devices capable of sensing information from their surroundings (such as high/low temperature or strong fluctuations in power lines), as well as being capable of processing data streams and communicating with other network nodes. Sensor nodes are also self-configurable, self-healing and smart devices. Precisely, self-configurability allows a sensor network to adapt its topology in order to react against failures, whereas self-healing provides capabilities for facing unexpected network events. Moreover, sensor nodes are able to collaborate among them in order to achieve a common goal (e.g. control of energy generators). Therefore, this technology can be useful in monitoring and surveillance applications, and in inaccessible applications for the human-being (e.g. electrical posts).

Regarding the network architecture, WSNs can be deployed and distributed following a flat, hierarchical or hybrid configuration. In a flat configuration, all the nodes can participate in both the decision-making processes and the internal protocols. In contrast, in a hierarchical configuration they are grouped into clusters where all the organizational decisions are addressed by a single entity known as *cluster head* [5]. This node is also in charge of aggregating data streams from different sensor sources for increasing the accuracy of the observed parameters.

As previously commented, this technology is currently considered as one of the most demanded wireless technologies by the control Industry, since it guarantees the same control services as a RTU but to a low installation and maintenance cost [6]. More explicitly, these control services are: on-demand query, detection/tracking capacity of anomalous situations, generation of alarms, and reporting of any life-threatening situation. In addition, there are some examples within the literature that show its useful features for critical systems, since they are also considered as a suitable tool for their protection [7]. Moreover, several wireless industrial communication standards have been recently defined for WSNs, such as ZigBee PRO [8], WirelessHART [9] and ISA100.11a [10]. As a special note, it is important to highlight that this paper is mainly focused on ISA100.11a, since it is an extended version of WirelessHART and it improves some of its services [6].

ISA100.11a allows both mesh and star topologies using: (i) sensor nodes, (ii) routers, (iii) gateways (one or several) to establish redundant connection with the SCADA centre, (iv) backbone routers to provide connectivity to other networks, and (v) two special managers: a system manager and a security manager. The system manager is in charge of allocating resources and providing communication, whereas the security manager affords key management services. Moreover, ISA100.11a is based on the IEEE 802.15.4-2006 standard, which specifies the physical (PHY) and Media Access Control layer (MAC) layers for Wireless Personal Area Networks (WPANs), providing it with security mechanisms based on AES-128 bits, Message Authentication Codes (MAC) and an Access Control List (ACL) to authenticate any received message. Furthermore, this standard guarantees an adaptive frequency hopping method and a blacklisting method, synchronization, redundant paths, diagnostic mechanisms, low duty cycle, frequent key update, firmware update in all the devices, compatibility with IPv6 and the 6LowPAN standard, as well as alarm and priority management. Specially, this priority management

depends on four subcategories (a device diagnostic, a communication diagnostic, a security alert and a process alarm) and on five priority levels (urgent, high, medium, low and journal). Information from sensors is accessed and managed by objects, such as for example DMAP (Device Management Application Process) and ARMO (Alert Reporting Management) objects. To be more precise, the ARMO class is included within the DMAP class where their objects are able to manage, configure, supervise and request parameters belonging to sensor nodes.

3 Early Warning Systems on the Critical System Protection

A SCADA centre is the main system in charge of managing any data stream received from remote substations. So far, its security basically depends on security policies, access control mechanisms, security applications and specialized mechanisms whose basis is supported by patterns and rules that are capable of identifying anomalous behaviours or events[1], like IDSs. However, all of these security mechanisms do not provide enough resources to predict anomalous events and to previously react against them, such as an EWS could offer us.

3.1 Preventing and Controlling a Cascading Effect

Some examples in real life have shown the importance of protecting these types of critical systems. For example, in 2003, numerous blackouts occurred in United States and Canada, and even in Europe because of various failures found in the information and communication technologies systems (ICTs) [11]. In 2009, a U.S. electrical grid was penetrated by Chinese and Russian intruders resulting in the disruption of the system [12]. In the same year, Brazil and Paraguay suffered a serious blackout during four days due to a failure in Itaipu Dam [13]. Furthermore, the U.S. Department of Energy's Idaho laboratory documented a cyber-attack performed on an energy generator that was shaken violently before going into total meltdown [14]. The idea consisted of showing that many of our critical infrastructures are subject almost to the same vulnerabilities. If this attack had been carried out on a real electrical energy plant, the results could have been devastating for society and economy, whose effect would correspond to a cascading effect. [2]. Due to this, some actions plans and European initiatives have already been proposed [15], as well as approaches based on EWSs [16] to prevent anomalous situations.

Basically, an EWS consists of integrated techniques with capability for providing an advanced monitoring. In other words, this system is able to offer, on the one hand, an analysis and intelligent interpretation of readings obtained from sensors distributed in remote substations. On the other hand, it has the decision-making capacity for avoiding or reducing the propagation of a possible effect originated by an anomalous event [17]. For example, if a threat/failure appears in a substation, it is not enough to detect it and

[1] It is important to know the difference between an event and a failure/threat. An anomalous event can be considered as an array of suspected actions. In contrast, a failure or a (either logical or physical attack) threat can be considered as an event sequence related to an anomalous behaviour pattern (or rule).

subsequently correct it. The success of an EWS depends on the ability to anticipate the events that could lead to major problems. This way of predicting events could help us face a situation that may disrupt the performance and business continuity of our system or systems because of the strong relationship of interdependence among them.

In any EWS there are four main components: (i) a *detection component*, based on information received from sensors capable of predicting a possible threat, (ii) a *reaction component*, (iii) an *information recollection component* to store evidences, and (v) an *alarm management component*. The reaction component includes a process of decision-making whose determination will depend on the type of threat, criticality of the affected environment, interaction with other involved elements, associated risk and relationship between damage and cost. All of these components have to be working during the three following phases [18]: (1) before a threat/failure (an EWS must anticipate and warn that a set of suspected actions have been registered), (2) during an attack/failure (an EWS must avoid that an effect starts to propagate itself, using for example any isolation technique of nodes, components, networks or connectivity among systems) and (3) after a successful attack/failure (an EWS must control the propagation of a threat towards other systems).

Our contribution goes a step further. The approach proposed in this paper is based not only on components previously mentioned but also on forensic techniques as a special support that aids to understand, at first level, the causes of an incidence and to learn from it. To this end, our forensic component has to include a set of processes capable of analyzing the evidences that took place before and during a fact, in addition to applying learning techniques to automatically update the knowledge of the system with new behaviour patterns. Lastly, it is important to highlight that although this approach has been exclusively focused on energy control systems, it can be equally applied in other critical systems (see Section 3.3).

3.2 Early Warning System based on Forensic Techniques

This section presents our approach of an EWS based on the ISA100.11a standard, which defines a set of parameters, services and connections among network components [10]. In our case, sensor nodes are grouped into clusters and deployed close to controlled critical infrastructure, i.e. close to electric energy generators (see Figure 2). This network follows a hierarchical structure to allow a more detailed control in different areas, facilitating a better localization of anomalies. For example, if a failure happens in a determined point of the infrastructure, it is possible to attend it by knowing a priori the affected area belonging to a specific cluster.

Due to the functionality of each cluster head, it is possible to filter readings (e.g. temperature, voltage) and check alarms generated by sensors at a first level. The result must be retransmitted to a special node (i.e., a gateway), which includes all the logical of the approach (see the Figure 2). As already mentioned, ISA100.11a allows network configurations based on gateways with enough resources to interpret and translate SCADA commands (e.g. step up input voltage) to a protocol that the sensor nodes can understand, and vice versa. Moreover, the EWS design could be implemented in several gateways, one of them working as a primary node and the rest in standby. Note that this

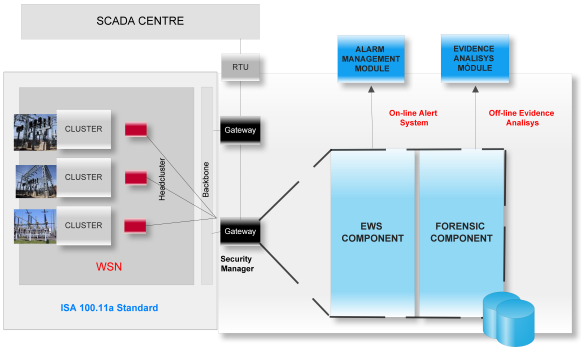

Fig. 2. An Early Warning System based on WSNs and Forensic Tecniques

aspect is out of the scope of this paper, but we believe that it should be considered for a future work.

Our EWS design is based on two main components: (i) an *EWS component* and (ii) a *forensic component*. Both collaborating with each other in order to share information. From an abstract point of view, the EWS component will be in charge of analyzing and managing event streams received from cluster heads in ***on-line*** mode [19]. In particular, this type of management involves analyzing, prioritizing and alerting the closest field operator through an alarm that facilitates a timely response.

Likewise, the EWS component has to activate the forensic component in order to inform the SCADA centre about the causes of a fact and its origin, specifying the evidences happened. However, its functionality does not finish here. The forensic component has to be able to learn from this fact, as well as generating a new pattern/rule if a specific event is not associated to a determined pattern. To this end, it will be necessary to analyze a set of factors (e.g. past evidences, sensitive parameters, context conditions, criticality of affected area, impact and risk, etc.) and/or use specialized techniques, some of which will be discussed below. The procedure finishes when the new pattern is stored for a future use. Due to the complexity of this last component, it has to work in ***off-line*** mode (i.e., it is only activated when an anomalous event is detected), avoiding that the overall performance of the system becomes degraded. Lastly, both modes allow the system to manage properly any type of event given that the EWS component and the Forensic component always deliver such events to the SCADA center.

EWS component Figure 3 shows how the system is able to receive any event flow and how the system is able to filter and normalize such information to be managed later by the rest of modules. The idea is to combine and represent different event inputs in a same generic format under a semantic abstraction. This abstraction facilitates obtaining a general description of the entities and elements involved with their respective ontological links. The final representation has to be analyzed and compared using a knowledge source based on anomalous behaviour patterns or rules.

However, how can we establish the difference between a normal behaviour or an anomalous behaviour in our critical environment [19, 20]? To answer this question, it

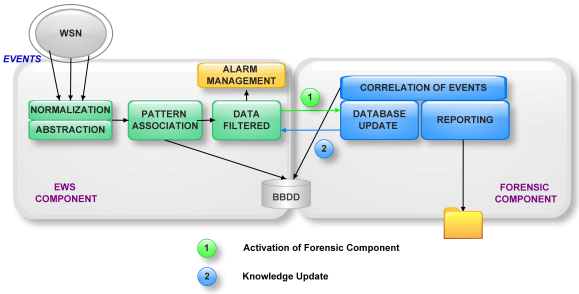

Fig. 3. Internal Structure of the EWS based on WSNs and Forensic Techniques

is necessary to identify a priori a set of anomalous events within this particular critical scenario, such as a circuit break, stresses, strong fluctuations, high voltage in a power line, structural changes in the environment, etc. However, these are not the only events to be taken into account within a control industry. Nowadays, it is important to consider those events related to ICTs since today's industry is more and more dependent on them for the control. Hence, an event can be also found at any level of the TCP/IP standard, i.e. from the physical level to the application level. For instance, an anomalous event may come as disturbances in IP packets (e.g. IEC-104 commands), changes in nodes synchronization processes, changes in network initialization processes or alterations in key negotiation processes. It would be also interesting to analyze the state of communication channel, the functionality of nodes (dead or alive nodes), addressing, I/O interfaces, routing and interconnection among nodes. Furthermore, some security weaknesses, vulnerabilities, threats and intruders corresponding to specific industrial standards, among them the ISA100.11a standard, have already been analyzed in [6].

Four situations may arise in our critical context: (i) *false positive*, if the analyzed event is innocuous, but it is classified as a threat (failure/intrusion); (ii) *true positive*, if the analyzed event is properly classified as a threat (failure/intrusion); *false negative*, if the analyzed event is a threat (failure/intrusion) but it is classified as normal/innocuous; and *true negative*, if the analyzed event is correctly classified as normal/innocuous. This fact means that our approach has to be configured with some existing anomaly-based detection technique (e.g. Bayesian networks, Markov models, fuzzy logic, etc. [21]) to ensure a low false negative rate. Note that a low false positive rate would also be ideal, but a low false positive rate in a CI is not really a problem, since any type of suspect threat/failure must be managed. The problem emerges when anomalous events really appear in the system and they are not properly detected.

The next step of this component would be to analyze what type of information to include in an alarm (such as the identification of the affected node, the localization of the affected area/line, the event, etc.) and locate the closest field operator in the area. To this end, the alarm manager must configure in its system an intelligent mechanism with a support to estimate the suitable field operator to efficiently respond to a determined incidence, such as the Automated Adaptive Response Manager based on reputation proposed in [22]. Finally, and equally, it is important to provide the forensic component with enough information to carry out its activities.

Forensic component This component, configured in parallel to the EWS component, is based on forensic techniques. A traditional forensic technique is composed of four essential phases [23]: (i) information recollection, (ii) relevant information extraction, (iii) information analysis and (iv) reporting. Note that the two first phases were already carried out by the EWS component through a filtered and an abstract representation of an event sequence received from sensors. On the contrary, the two last phases have to be contemplated by this component to correlate and trace such an event sequence, which will likely lead to an incidence.

A way of correlating and tracing events could be to include a unique ID to each system process, such as Goel et.al. described in [20]. Thus, it is possible to efficiently trace accesses registers, services and resources, as well as commands and alarms signalled. Another solution could be to represent the event sequence and their links through a Markov graph on a time line [24]. However, none of them establishes a relationship between an event/process and a responsible member in the system. For this reason, the operator's ID must be also required for the detection along with an identity database to efficiently carry out this new purpose. As a result, the system will be able to estimate the real causes of an incidence along with the responsible operator/s. Last but not least, in case where an event (or an event sequence) is not related to a pattern, the system will have to activate the *pattern generation* module to update our knowledge source (i.e., the pattern database) of our design (see Figure 3), using for example data-mining [25].

3.3 Use Case and Discussion

In order to understand with more detail the functionality of our approach, the discussion will mainly be focused on analyzing a Denial of Service (DoS) attack in a specific cluster head corresponding to an energy substation. It is clear that the intruder's goal is basically to isolate an essential part of the control. Nevertheless, our system can face this situation, since the gateway has to constantly receive information from the environment. If a cluster head stopped sending messages during a long time, then the gateway detects an anomalous behaviour in the network and it starts to check the node state and its availability (i.e., dead or alive node) using DMAP objects. If the node does not respond, then the EWS component determines that something happened in that network area.

Consequently, the EWS component also starts to analyze the application context using information of neighbour nodes (i.e. using DMAP objects to receive such information from them) and anomaly-based patterns. Obviously, in this situation, the first patterns to analyze should be those related to the availability (e.g. flooding, black hole attack, wormhole attack, etc.) to provide a quick response. When an intrusion is detected in the system, the alarm management module has to generate an ISA100.11a alert (using ARMO objects) with high priority in order to guarantee assistance in the isolated area. The information to transmit has to include, at least, the affected area localization, the compromised node and the type of event. Note that if such alarm is not attended in a determined time $t1$, a new alarm will have to be sent with an urgent priority to ensure response in a time $t2$, where $t1 > t2$. This time limitation makes the system react quickly, and thus to recover the control before a serious problem appears definitively in the non-controlled and unattended area.

In parallel, the forensic component has to determine the main causes and the operator's ID, analyzing commands, active services, registers, unauthorized accesses, etc. Some of these attacks were recently analyzed in [6], where type of intruder (i.e., insider and/or outsider), original causes and countermeasures were identified. Taking advantage of this analysis, we can previously initialize the system with information from attacks and provide the SCADA centre with information to identify intruders and some countermeasures. For example, and according to this, if a black hole attack (not retransmit messages to the next hop) was launched, then we can ensure that a selective forwarding attack previously took place by a malicious insider with enough permission to access the energy substation. All of this information must be immediately sent to the SCADA centre. Lastly, it is worth mentioning that this component does not require updating the database, since the attack was properly detected by the EWS component. Otherwise, a learning technique/model should have been applied, such as for instance a Markov model or data-mining. Nonetheless, this is still an unexplored research area, since the context is highly-critical and it requires a constant performance and reliability of the learning.

Finally, the expected results from the approach in critical scenarios are as follows:

1. Supervision in areas to offer a timely response and control of a possible cascading effect.
2. Safety and Security: Safety in the control of cascading effect and its repercussion in our society and economy. This control is based on a detection mechanism under the use of a persistent and smart alarm manager. This manager is capable of reaching the most suitable field operator (which is equipped with mobile devices) to attend a determined incidence. With respect to security, the system is able to identify a responsible operator since an event is associated to an operator's ID, in addition to learning how to face future situations through forensic techniques.
3. Performance: The approach is included in a high-resource gateway (or several) to work in parallel with other elements of the system. It is important to highlight that part of this logic runs in off-line mode.
4. Adaptability. This approach can equally work in an ISA100.11a network, a ZigBee PRO network and a WirelessHART network, since all of them keep certain topological, structural and functional characteristics. Moreover, as this approach is based on a specific and recognized standard, it can also work in any type of application context (e.g. a transportation system, oil/water distribution systems...).
5. Auditing and maintenance. The system could improve its auditing and maintenance procedures given that the the system is able to keep the operator's ID and explain the causes of an incident.

4 Conclusions and Future Work

This paper presents a design of an Early Warning System used to control anomalous behaviours and events registered in electrical energy substations. The approach is based on Wireless Sensor Networks under the ISA100.11a standard and on forensic techniques. More specifically, WSNs allow supervising the controlled critical infrastructure whereas the forensic techniques ensure an updated knowledge. The idea is to anticipate

anomalous event sequences, react against them on time and dynamically learn from new anomalous situations. As a result, the proposed design tries to solve one of the security issues still unexplored in critical systems, i.e. the control of the cascading effect.

The approach is based on two main components whose main goals are: (i) to detect an anomaly, (ii) to efficiently manage an alarm, (iii) to identify the most suitable field operator to attend it, (iv) to analyze causes and responsible members, and (v) to automatically learn from this anomaly. This latter point helps the system not to require a manual process to update its own knowledge source. The functionality of this approach has been also discussed by using a specific scenario as a use case. Lastly, this paper has also opened new research areas to explore, such as intelligent alarm management systems, dynamic localization mechanisms, and design of both detection models and forensic techniques for highly-critical applications, which require a quick and reliable response.

For the future, we intend to implement the proposed design in order to show its feasibility in a real and critical context, in addition to researching how to directly include all the logic of this approach within sensor nodes. However, this will depend on the computational capabilities and resources offered by sensor nodes, which are still constrained. Likewise, a security analysis of the approach will have to be performed to evaluate its integrity against existing and future vulnerabilities, threats and failures.

Acknowledgments

This work has been partially supported by the projects: PROTECT-IC (TSI-020302-2009-10), ARES (CSD2007-00004) and SPRINT (TIN2009-09237), being the last one also co-funded by FEDER. The first author has been funded by the Spanish FPI Research Programme. The authors would like to thank M. Carmen Fernandez-Gago her constructive comments and valuable suggestions.

References

1. NIST, *Smart Grid Cyber Security Strategy and Requirements*, The Smart Grid Interoperability Panel-Cyber Security Working Group, Draft NISTIR 7628, U.S. Department of Commerce, 2010.
2. J. Peerenboom and R. Fisher, “Analyzing Cross-Sector Interdependencies”, IEEE Computer Society, HICSS, IEEE Computer Society, pp. 112–119, 2007.
3. ANSI/ISA-99.02.01-2009 standard, “Security for Industrial Automation and Control Systems Part 2: Establishing an Industrial Automation and Control Systems Security Program”, 2009.
4. R. Mcclanahan, “SCADA and IP, Is Network Convergence Really Here?”, IEEE Industry Applications, 2003.
5. J. Lopez, R. Roman and C. Alcaraz, “Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network”, Foundations of Security Analysis and Design V , LNCS 5705, pp. 289–338, Springer, 2009.
6. C. Alcaraz, J. Lopez, “A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems”, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. PP, Issue 99, pp. 1-10, 2010.

7. R. Roman, C. Alcaraz and J. Lopez, “The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection”, Information Security Technical Report, vol. 12, num 1, pp. 24-31, Elsevier Advanced Technology, 2007.
8. ZigBee Alliance, http://www.zigbee.org/,accessed on May, 2010.
9. WirelessHART, http://WirelessHART.hartcomm.org/,HART Communication Foundation, accessed on February, 2010.
10. ISA100.11a, “ISA-100.11a-2009. Wireless systems for Industrial Automation: Process Control and Related Applications”, ISA. The International Society of Automation. 2009.
11. Bialek J., “Critical Interrelations between ICT and Electricity System”, Electricity security in the cyber age: Managing the increasing dependence of the electricity infrastructure on ICT (NGInfra), Utrecht, The Netherlands, 2009.
12. Electricity Grid in U.S. Penetrated By Spies, The WallStreet Journal, http://online.wsj.com/article/SB123914805204099085.html, News registered on April 2009.
13. Power Failure Blacks Out Much of Brazil, Paraguay, The WallStreet Journal, http://en.wikipedia.org/wiki/Itaipu, News registered on November 2009.
14. D. Salmon, M. Zeller, A. Guzman, V. Mynam, M. Donolo, “Mitigating the Aurora Vulnerability With Existing Technology”, Schweitzer Engineering Laboratories, Inc., 2007.
15. Critical Infrastructure Warning Information Network, EPCIP, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, accessed on July, 2010.
16. M. Apel, J. Biskup, U. Flegel, M. Meier,“Towards Early Warning Systems - Challenges, Technologies and Architecture”, 4th International Workshowp on Critical Information Infrastructure Security (CRITIS 2009), Bonn, Germany, 2009.
17. K. Walter, E. Nash, “Coupling Wireless Sensor Networks and the Sensor Observation Service - Bridging the Interoperability Gap”, 12th Agile International Conference on Geographic Information Science, 2009.
18. S. Bastke, M. Deml, S. Schmidt,“Internet Early Warning Systems. Overview and Architecture”, December, 2009.
19. “Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State-of-the-Art Revie”, Office of Research and Development National Homeland Security Research centre. EPA, United States Environmental Protection Agency. August, 2005.
20. A. Goel, M. Shea, S. Ahuja, W. Feng, D. Mailer, J. Walpole, “Forensix: A Robust, High-Performance Reconstruction System”, 2009.
21. P. Garcia, J. Diaz, G. Macia, E. Vazquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges”, Computers & Security Journal, Elseiver, vol 28, num 1-2, pp. 18–28, 2009.
22. C. Alcaraz, I. Agudo, C. Fernandez-Gago, R. Roman, G. Fernandez and J. Lopez, “Adaptive Dispatching of Incidences based on Reputation for SCADA Systems”, Privacy & Security in Digital Business, LNCS 5695, pp. 86–94, 2009.
23. NIST, “Guide to Integrating Forensic Techniques into Incident Response”, National Institute of Standards and Technology. 2006.
24. Bon K. Syr, “Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS”. Elsevier. Information Fusion. February, 2009.
25. S. Zanero, S. Savaresi, “Unsupervised learning techniques for an intrusion detection system”, SAC ’04: Proceedings of the 2004 ACM symposium on Applied computing, pp. 412–419, 2004.