J. Lopez, C. Alcaraz, and R. Roman, "Smart Control of Operational Threats in Control Substations", *Computers & Security*, vol. 38, pp. 14-27, 2013.
http://doi.org/https://doi.org/10.1016/j.cose.2013.03.013
NICS Lab. Publications: https://www.nics.uma.es/publications

Smart Control of Operational Threats in Control Substations

Javier Lopez[1], Cristina Alcaraz[1], and Rodrigo Roman[2]

[1]Computer Science Department, University of Malaga,

Campus de Teatinos s/n, 29071, Malaga, Spain

[2]Institute for Infocomm Research, 1 Fusionopolis Way,

#19-01 Connexis, South Tower, Singapore 138632

[1]{jlm,alcaraz}@lcc.uma.es, [2]rroman@i2r.a-star.edu.sg

October 27, 2015

Abstract

Any deliberate or unsuitable operational action in control tasks of critical infrastructures, such as energy generation, transmission and distribution systems that comprise sub-domains of a Smart Grid, could have a significant impact on the digital economy: *without energy, the digital economy cannot live*. In addition, the vast majority of these types of critical systems are configured in isolated locations where their control depends on the ability of a few, supposedly trustworthy, human operators. However, this assumption of reliabilty is not always true. Malicious human operators (criminal insiders) might take advantage of these situations to intentionally manipulate the critical nature of the underlying infrastructure. These criminal actions could be not attending to emergency events, inadequately responding to incidents or trying to alter the normal behaviour of the system with malicious actions. For this reason, in this paper we propose a smart response mechanism that controls human operators' operational threats at all times. Moreover, the design of this mechanism allows the system to be able to not only evaluate by itself, the situation of a particular scenario but also to take control when areas are totally unprotected and/or isolated. The response mechanism, which is based on Industrial Wireless Sensor Networks (IWSNs) for the constant monitoring of observed critical infrastructures, on reputation for controlling human operators' actions, and on the ISA100.11a standard for alarm management, has been implemented and simulated to evaluate its feasibility for critical contexts.

Keywords: Smart Grids, Energy Control Systems, Wireless Sensor Networks, Reputation, Digital Economy, Security

1 Introduction

One of the foundations of the digital economy is the digitalization of knowledge into information, which can travel anywhere in the shortest time possible [1]. This seemingly simple axiom has changed our lives in many aspects: the way we work, the way we socialize, the way we conduct business. However, these digital services are heavily dependent on Critical Infrastructures (CIs) [2]. CIs are complex and highly interconnected systems (e.g., finance, communications/telecommunications, Information Communication Technologies (ICT), energy, health, logistics, and water management systems) that are crucial for the well-being of the society. If some of these infrastructures stop working, the digital economy simply vanishes. Without telecommunication services, knowledge cannot be distributed. Without energy distribution systems, what is real cannot become virtual, and the virtual cannot be accessed. In fact, the economic losses caused by power outages in companies that rely heavily on information management have been well documented (cf. Lineweber et al. [3]).

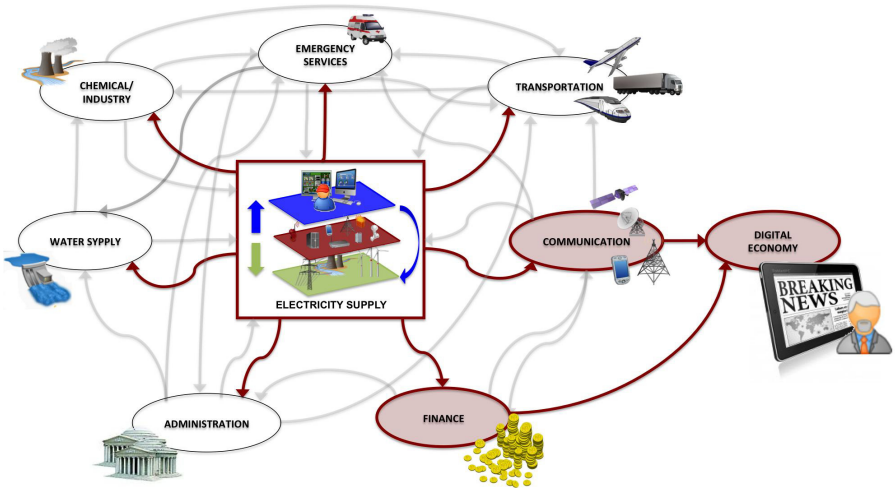

Figure 1: Interdependence Relationships and Impact on the Digital Economy

It is precisely because of their importance in keeping the digital economy alive, this paper focuses on energy systems. More specifically, on energy systems belonging to the 21^{st} century known as Smart Grids. According to the National Institute of Standards and Technology (NIST) conceptual model [4], a Smart Grid is a complex infrastructure composed of many systems and subsystems (e.g., energy generation, transmission and distribution systems) that interact with each other in a complex way. Such interactions can bring numerous challenges in maintaining the safety-critical property, which is concerned with

the ability of the system to operate under adverse, accidental and unplanned situations [5, 6]. Moreover, errors can result in a cascading effect with a high probability of a more catastrophic system breakdown [7, 8] due to the existing interdependency relationships between critical sectors and their CIs (e.g., communication systems, energy, transportation, administrations, etc.). This degree of connectivity between CIs, shown in Figure 1, makes these infrastructures an attractive target where adversaries could hamper the normal executation of critical services. In fact, various studies (cf. [9]) warn that these types of infrastructures are increasingly being threatened by both external and internal adversaries.

One of the protection strategies that could be used to mitigate a cascade effect would be to design and implement automated solutions that dynamically and efficiently detect and warn of emergency situations, allowing human operators in the field to control the situation in a timely manner (cf. NIST [4], Federal Energy Regulatory Commission (FERC) in [10]). However, the use of automated systems is not sufficient to ensure an efficient response and a successful resolution of a problem. It is also necessary to control the actions taken by human operators. Not only might they be malicious insiders wanting to carry out criminal actions against the system, but also they may not be the most suitable people to deal with an emergency situation (e.g., due to a lack of skills). For example, the cause of the north-east blackout of 2003 [11], which affected U.S. and Canada and caused losses of about USD 6bn, was a human operator's mistaken action that solved a failure registered in a telemetry device, but in doing so forgot to restart the monitoring system.

Given this, the work proposed in this paper focuses on energy control domains that supervise systems and substations of power generation, transmission and distribution. This control is performed by specialised systems known as Supervisory Control and Data Acquisition (SCADA) systems [5, 7], which are responsible for constantly monitoring operational activities and automation functions. This supervision enables authorized human operators to (either remotely or locally) access resources deployed in remote substations to: (i) transmit commands (operational instructions), (ii) disseminate alarms (warning messages based on priorities to warn of a situation) and measurements (readings of voltage denoted in this paper as v_i, such as $v_i \in [V_{min}, V_{max}]$ where V_{min} and V_{max} represent prescribed valid thresholds defined by energy systems/countries), and (iii) check for the existence of anomalous states. An anomalous state can be defined as something that is not standard or normal for the system, such as $v_i \notin [V_{min}, V_{max}]$.

Considering this scenario and its influence on other critical sectors, our solution uses an automated incident response mechanism based on Industrial Wireless Sensor Networks (IWSNs), reputation and the ISA100.11a standard [12]. Once an anomalous state has been detected, the system will intelligently dispatch critical incidents (represented through alarms) to those members of staff with more experience and a greater ability to solve them. It is worth highlighting that the work presented here continues and improves upon the research suggested in [13], not only by enhancing the model with a smart control applica-

ble for any type of application domain but also by using simulations to validate the mechanism.

The paper is organized as follows. In Section 2, we introduce the proposed approach, describing the components that are in charge of managing all those parameters and variables required for the construction of the mechanism. Section 3 explains in detail how the approach behaves to solve critical situations, placing particular emphasis on how it is able to address five possible incident response scenarios. All of these scenarios are analysed and described in Section 3.1, and Section 4 concludes the paper and outlines future work.

2 A Smart Incident Response Mechanism for Energy Control Domains

We have designed a dynamic response mechanism based on a hierarchical sensor network and reputation so as to speed up suitable and reliable actions to address anomalies within a system.

2.1 Background and General Architecture

Before introducing the general architecture of the incident response mechanism proposed in this paper, a brief background of the importance of protecting these types of systems is outlined in the following lines. According to the NIST in [4], cybersecurity and situational awareness are two priority areas to be considered for protection from anywhere and at any time. Both areas require a set of security solutions to guarantee availability, integrity and confidentiality to a certain level of information and resources. In order to understand the importance of these areas, Table 1 illustrates some of the incidents and that have threats occurred over the last decade in control systems and in particular in energy systems [14].

Table 1: Threats and Incidents in Energy Control Systems, Retrieved from [14]

Year	Threat	Operandi Mode	Consequences
2000	***Maroochy Water System***	Intentional Cyber-attack∗	Environmental Impact
2003	***Davis-Besse Nuclear Power Plant***	SQL Slammer Worm	Operational Disruption
2003	***Electrical Blackout on August 14***	Man-Made Error∗	Transnational Impact
2010	***Stuxnet***	Worm	Alteration in the Operational System
2011	***Night Dragon***	Worm and Trojan	Disclosure of Critical Information
2011	***DUQU***	Virus	Disclosure of Critical Information
2012	***Flame***	*Worm*	Disclosure and Destruction of Critical Information

As can be noted in Table 1, threats (either attacks or incidents[1] can trigger

[1] An incident can originate with a technical error or an intentional action carried out by

an internal adverse effect that could collapse, disrupt or alter operational functionalities [5]. Given that the consequences can become catastrophic to national or transnational level with a serious social or economic impact [11]. Effective solutions of situational awareness are fundamental to help the underlying system know the real state of its resources and provide a rapid and efficient response irrespective of the location of the incident. To address all of these capacities, Figure 2 illustrates the architecture of our response mechanism based on an IWSN composed of sensor clusters and gateways.

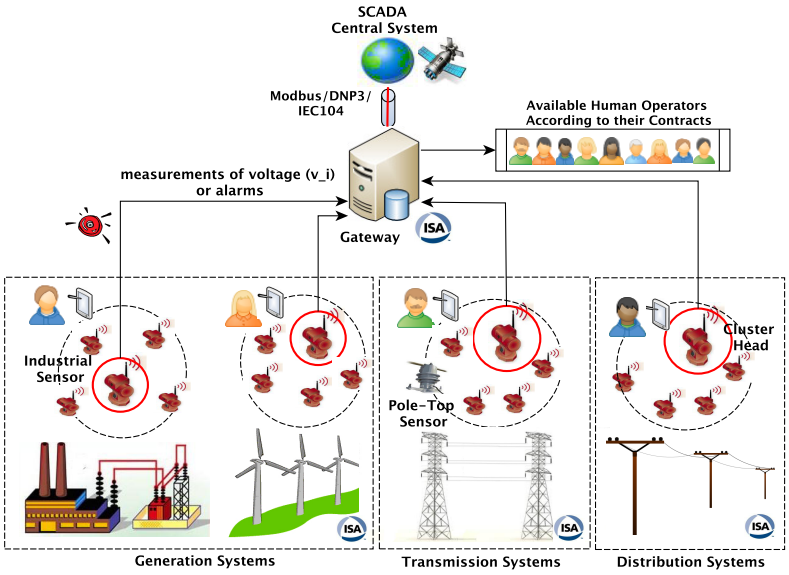

Figure 2: General Architecture of the Incident Response Mechanism

In particular, Illustration 2 depicts how sensor networks have to be deployed close to the CI under observation, such as electrical generators, transformers or pylons. These sensor networks [15] are based on autonomous, self-configurable and smart sensor nodes (s_j with identification ID_{s_j}) with the capability to carry out wireless diagnostic tasks with a low installation and maintenance cost. They are able to continuously monitor physical events such as levels of voltage, temperature or pressure, and to measure these values with great accuracy. Moreover, these sensors are also responsible for tracking, detecting and warning of anomalous behaviour, unexpected states and anomalies associated with the underlying infrastructure, in addition to warning of and reporting any

members of the organization. This is denoted in Table 1 with the symbol '$*$').

threatening situation. On the other hand, the gateway serves as a special interface between the sensor network and the control system. It is in charge of retransmitting measurements and alarms from sensor clusters to the SCADA Central system. This means that the gateway should be configured with the potential resources to interpret and translate different types of messages; i.e., SCADA messages (e.g., ModBus/TCP, DNP3 or IEC-104 commands) to a protocol that sensor nodes can understand (e.g., ISA100.11a messages), and vice versa. However, its activity does not end here. The gateway is also in charge of managing critical alarms received from the IWSN in order to provide a rapid response when anomalies arise within the system. Given the importance of this network architecture for our mechanism, the remainder of this section describes in detail its functionalities.

2.2 Cluster Head: Dissemination and Alerts

The sensor network architecture proposed in this paper is based on a hierarchical configuration composed of sensor node clusters. For each cluster, we select a trustworthy node, known as a Cluster Head (CH), with sufficient resources to address an essential part of the approach, and all the processes related to data filtering and aggregation (typical tasks of a CH). The reason why we have determined this type of network architecture is suitable for this is twofold. First, a hierarchical network is a good approach for managing existing resources within an IWSN such as the energy consumption or computational capabilities. Second, this configuration enables the system to efficiently detect and locate anomalies by knowing the sensor deployment and the grouping of nodes. Thus, if an incident happens at a given point of the CI, it is possible to attend to it rapidly.

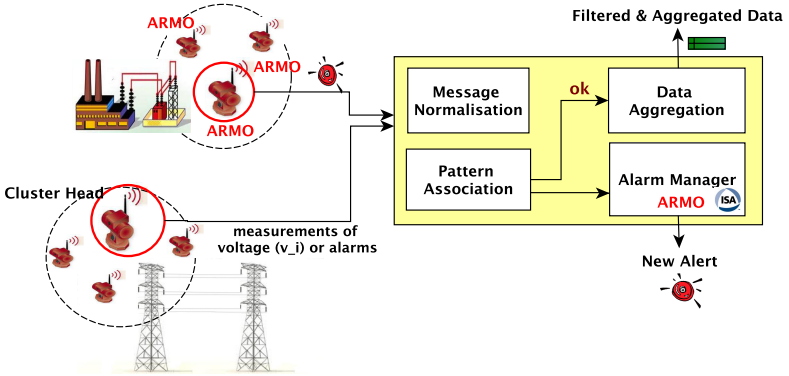

Figure 3: Architecture of the Cluster Head

Figure 3 illustrates the architecture of a CH together with the different types of functional components integrated inside the architecture, such as: *Message Normalisation, Behaviour Pattern Association, Data Aggregation* and *Alarm Manager*. The functionality of these components help CHs to be able to receive, check and validate any type of information produced by their sensors. Given that the scenario is related to an energy system, this information can range from measurements to alarms. It should be noted that the combination of a set of parameters related to a context (e.g., temperature, pressure) increases the knowledge level of the system to identify critical scenarios in a more accurate manner. This means that before the deployment of sensors, an analysis of the context and its parameters, as well as the combination of such parameters should be properly addressed. However, and given that all of these analyses basically depend on the context observed and its infrastructure (e.g., turbines, pylons, generators), the paper focuses on a single parameter; the level of voltage.

The Message Normalisation component is in charge of combining and representing different input data (measurements or alarms) in the same generic format in order to standardise network messages. This module is essential for ensuring its suitability in other contexts where the underlying communication may not necessarily be ISA100.11a. It may be based on WirelessHART™ [16], ZigBee PRO [17] or other future communication protocols. Nevertheless, we focus on ISA100.11a because it is an extended version of WirelessHART™ and improves some services related to security and communication reliability [18]. Indeed, industrial sensor networks should be able to face threatening situations and harsh environmental conditions (e.g., industrial noise, humidity, vibrations) that could hamper the transmission or change the network topology, resulting in isolated areas. These services are discussed below.

The result of such a normalisation is then analysed by the *Behaviour Pattern Association*, which uses an existing knowledge source based on anomalous behaviour patterns, such as $v_i \in$ or $\notin [V_{min}, V_{max}]$. Any value outside of these thresholds, i.e., $v_i \notin [V_{min}, V_{max}]$, should be notified to both the SCADA Centre and the nearest human operator in the field. Otherwise, if this value of reading (v_i) is inside the valid threshold, it must be filtered and aggregated by the Data Aggregation component.

As for the ISA100.11a standard, it offers mesh communication using: (i) sensor nodes (typically working at 26MHz, RAM 96KB, 128KB Flash Memory and 80KB ROM), (ii) routers, (iii) hand-held devices for maintenance purposes, (iv) gateways (one or several), (v) backbone routers, and (vi) two managers: a system manager, in charge of allocating resources and providing communication, and a security manager, in charge of offering security services that aim to avoid criminal actions from malicious outsiders. These security services can be: (i) non-secured (not recommended), (ii) secured with symmetric keys, and (iii) secured with asymmetric keys, certificates signed by a certificate authority, and Elliptic Curve Cryptography (ECC) schemes. These two security options have different agreement processes with building blocks of 128-bits keys, and distinct pre-configuration processes of data. Additionally, ISA100.11a is based on the IEEE 802.15.4 standard for Wireless Personal Area Networks (WPANs) [19],

which specifies its Physical (PHY) and Media Access Control (MAC) layers, 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. On the other hand, the standard also provides security at link and transport level using Message Integrity Codes, and unique symmetric keys of 128-bits for solving confidential issues.

Apart from this, ISA100.11a offers other interesting services for reliability in communication channels and coexistence with other systems. Among them, it is worth pointing out; network redundancy, link robustness, control of industrial noise or obstacle through frequency hopping and blacklisting methods, control of collisions in channels by defining a specific time division multiple access based on a fixed time-slot, network diagnosis, compatibility with the 6LowPAN standard [20] to connect with the Internet, routing discovery, use of low-duty cycle, and alarm management based on priorities [18, 21].

The alarm management is based on the DMAP (Device Management Application Process) class that includes a set of objects used for configuring, supervising and requesting parameters belonging to sensor nodes. In particular, DMAP includes the ARMO (Alert Reporting Management Object) class for managing, at first level, alerts and generating reports through the AlertReport service to ARO (Alert Receiving Object). ARO is a class configured in a single device in the network. In our case, it will be located and integrated inside the gateway. Given the importance of this last class for alarm management in the gateway, it will be discussed in the following section.

2.3 Gateway: Alert and Response

As previously mentioned, the gateway is the interface responsible for receiving information from cluster heads. This relationship and the architecture of a gateway is depicted in Figure 4, which shows how the ARO class receives alarms from clusters using one organised queue and sorted by priorities; and for each priority, ARO uses a buffer with a maximum size. The priority management of ISA100.11a depends on the five priority levels; *journal, low, medium, high* and *urgent*. Although the management of these levels could be very different given their levels of criticality, they can be treated by one or several AROs (contained within one gateway). In this way, a single ARO might collect all process alerts from across an entire network, or a set of AROs can be used, where each ARO only collects a single category of alerts. If each ARO collects only one type of alert, the collection of all alerts then requires five AROs. Nonetheless, and for simplicity, we only consider one ARO based on five queues (configured inside the gateway) and two main sets of ISA100.11a alarms. These sets are as follows:

1. ISA100.11a non-critical alarms with range $(1-3)$. They include alarms designated as journal (1), low (2), medium (3).

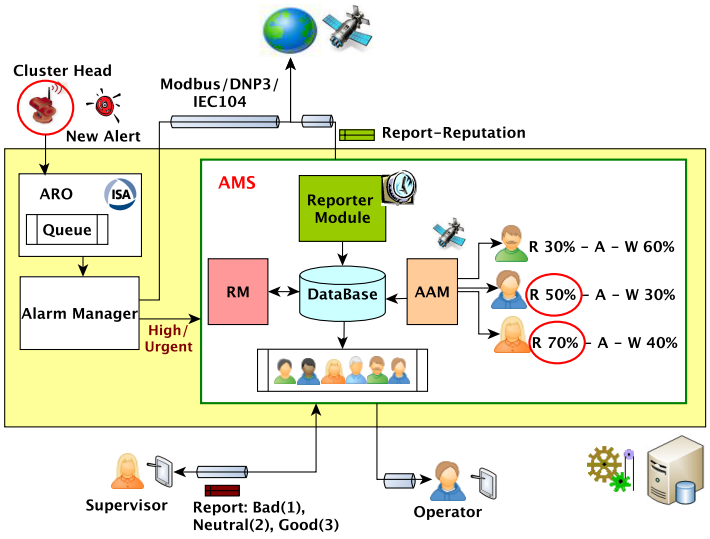

Figure 4: Architecture of the Gateway

2. ISA100.11a critical alarms with range $(4-5)$. They include alarms designated as high (4) and urgent (5), and represent those events that can potentially have an impact on the market, the social welfare and on the safety-critical between systems [5]. Due to the potential effects of these events in the digital economy, they need to be managed as soon as possible.

Both measurements (v_i) and alarms ($(1-3)$ and $(4-5)$) are sent to the SCADA Centre to be used for accountability purposes. Nevertheless, critical alarms ($(4-5)$) are also re-sent to the nearest and most suitable human operator in field to immediately deal with the situation. To this end, the gateway is based on three main components: *ARO*, *Alarm Manager* and *Alarm Management System* (AMS). The ARO component comprises all the features of the ARO class belonging to ISA100.11a, which have already been given above. The Alarm Manager component is in charge of managing the alarms received from the network according to their kinds of priorities ($(1-3)$ and $(4-5)$). The AMS is, to the contrary, the principal component responsible for locating the most suitable operator in the field with the experience and capability to properly respond to critical alarms in time.

In order to simplify our mechanism, we assume that the communications between sensors (i.e., ID_{s_1} - ID_{s_2} or ID_{s_i} - CH_j) and between CH_j and the gateway can be protected using either the security services offered by the ISA100.11a standard (cf. Section 2.2) or some existing lightweight key management scheme for WSNs, such as LEAP (Localized Encryption and Authentication Protocol). According to [22], the selection of these schemes will depend not only on the type of application domain, its natural conditions and its requirements for protection

of CIs, but also on the features and properties (e.g., computational cost, degree of communication, resilience, security, etc.) of each scheme. Although these security solutions can be enough to protect the communication channels and offer a minimum of protection, we cannot disregard the fact that security breaches and threats can arise at any moment [18]. It is also necessary to consider other additional lightweight security mechanisms, such as intrusion detection systems for WSNs, strategic models for location privacy, trust management, etc [23].

Regarding the rest of the communications, i.e., between the gateway and the operators' hand-held devices and between the gateway and the SCADA Centre, they should be protected using additional security services. Some of these security services could be, for example, all of those offered by the TCP/IP standard, which are also included within the RFC-6272 for the new version of the Internet Protocol IPv6 (titled as Internet Protocols for the Smart Grid) [24]. This RFC has been defined to allocate a considerable number of devices, where it is expected that the vast majority of them will be connected with the Smart Grid such as automated substations, meters or sensors. Note that this topic is quite important for the modernisation of the grid, if in addition we consider the current intentions of governments to invest in dynamic and automated substations. This is the case of the American Recovery and Reinvestment Act (ARPA) of 2009, which invested in one hundred automated substations with more than one thousand sensor nodes to detect changes and prevent local or regional power blackouts [25].

Continuing with the new version of IPv6 and its security services, it has inherited some services from the IPv4 which are configured throughout the TCP/IP stack. Some of them are, for example, the Extensible Authentication Protocol (EAP), Internet Key Exchange protocol version 2 (IKEv2), IPSec, Transport Layer Security (TLS) protocol using a varied cipher suite (e.g., ECC), Secure Shell protocol (SSH), or the use of Public Key Infrastructure (PKIX) or Kerberos for key management. Unfortunately, this new version IPv6 has also inherited some vulnerabilities of the IPv4, such as the tracking of addresses that could go against the security and privacy of the system [26]. For this reason, it is also important to consider other feasible solutions, such as the use of tunnelling mechanisms to provide secure virtual connectivity between networks (e.g., Virtual Private Networks (VPNs)), as well as the use of existing approaches for secure communication between peers such as the MT6D proposed by Groat et.al. in [26]. MTD6 consists of modifying the addresses of the network layer and transport layer to obscure routing addresses, using encryption and authentication services. Nor can we ignore the possibility of using current IP-based SCADA protocols with lightweight security solutions such as the DNP Secure Authentication (SA) protocol proposed by the DNP Users Group [27], in addition to considering existing guidelines, recommendations and standards.

Although all these security mechanisms can become effective solutions to ensure a minimum protection, their full integration can infer certain computational complexities that can hamper the normal execution of operational tasks. It is necessary to select those security mechanisms/services that guarantee a minimum of protection while considering a trade-off between performance and

security [5]. This means that before the commissioning phase, engineers should analyse the prerequisites of the context, its complexities and security problems to properly select which security services/mechanisms should be configured, as well as how and where.

2.4 AMS: Dynamically Dispatching Responsibilities

Figure 4 depicts the main modules of the Alarm Management System component: a *Reputation Manager* (RM), an *Adaptive Assignment Manager* (AAM), and a *Reporter* Module. The RM is integrated within the mechanism to manage values associated with the reputation. Although this module is useful for calculating, updating and storing the human operators' overall behaviour, it does not hold decision-making capabilities to estimate those prominent candidates for resolving a critical incident. This task is carried out by the AAM component. In contrast, the Reporter module is responsible for, periodically or on-demand, preparing and notifying the SCADA Central system of the current level of knowledge and experience in field.

For our approach, four chief and minimal parameters are needed to change the reputation value and they will be required to formally define the mathematical equations later. These parameters are as follows:

1. *Feedback* on the operator's attitude, which is denoted here as F_{sup}. Each human operator has to be assigned with an initial value of reputation. To clarify the importance of this value, three types of human operators are categorized:

   - A *trustworthy* entity: the level of reputation is kept with high values at all times.
   - An *untrained* entity: the level of reputation varies according to the needs of the system to upgrade its hardware or software resources.
   - A *criminal* entity: the level of reputation is significant, where malicious actions have put the security of the underlying system at risk.

   For the control of human actions, the system should assume that new integrations of human operators are trustworthy entities in order to ensure a rapid assistance in emergency situations. This means that their values of reputation should be higher than the average to give them an opportunity to act within the system, but lower than the most respected operators to allow important alarms to be managed by existing trusted human operators. However, this task requires a previous analysis of the application context, its level of criticality and its associated security risks to estimate those trustworthy ranges that should be associated with such a context [28]. Given that these analyses are dependent on the application domain and its organization, we assume that each human operator is a trustworthy and trained entity whose value of reputation is initialised with the maximum value (i.e., 100%). This initial reputation could change over

time according to their experience or knowledge gained to resolve incidents. The feedback on the resolution is obtained from a human operator with a higher reputation level, who takes on the role of supervisor and is also selected by the system.

When we require feedback of a given incident, the system must allocate two available human operators. One of them will manage the incident and the other, i.e., the supervisor, will send feedback to the system rating how satisfactory the action taken by the first human operator was. For the feedback, the system allows supervisors, through hand-held devices, to rate the handling of the incident and send it back to the gateway with one of the following values: *bad* (1), *neutral* (2) and *good* (3).

2. Level of *criticality* of the received alarm, symbolised as C_{al}. It is an input parameter for the management of reputation. As our approach only deals with critical incidents with a priority range $(4-5)$, this level of criticality can only have two values: high (4) or urgent (5) to identify criminal actions against the welfare of the system. In order to combine the supervisor's feedback with this other factor, we could multiply them and obtain a modified feedback; i.e.: $C_{al}\ (4-5) \times F_{sup}\ (1-3)$. However, we also consider essential the supervisor's reputation as a parameter for modifying the feedback; i.e.: $C_{al}\ (4-5) \times F_{sup}\ (1-3) \times Rep_{sup}\ (\%)$. This way, the higher the supervisor's reputation is, the more relevant the feedback will be.

3. Human operator's *workload*, denoted as $WL_{op/sup}$. This is another essential parameter that will change the value of reputation. This parameter is related to the overload of critical incidents that an operator might be dealing with at a certain time, and its value is key when measuring the efficacy of a response in a fair manner. Namely, if a human operator is overloaded with critical incidents and he/she cannot respond to a new incident, his/her punishment should be much less than for an operator who had a low workload.

4. *Time of response*, represented as T_{sup}. This is another parameter that determines whether a human operator carried out the task assigned at a specific time $[T_i, T_j]$, where $T_i \leq T_{sup} \leq T_j$. This parameter will be essential for updating the supervisor's reputation.

Once these parameters have been declared, and taking into account the nomenclature defined in Table 2, the next step is to formally define the mathematical equations that will change the reputation value.

As the supervisor's feedback is a determinant parameter for computing a new human operator's reputation value, two ways for calculating the reputation are given in our approach:

Table 2: Nomenclatures

Nomenclature	Definition
C_{al}	Criticality of alarm labelled with value $(4-5)$
$Rep_{op/sup}$	Reputation of the human operator and supervisor
F_{sup}	Supervisor's feedback
$WL_{op/sup}$	Workload of the human operator and supervisor
$Av_{op/sup}$	Availability of the operator and supervisor
$Tconf_{op}$	Human operator's time of confirmation to accept the management of an incident
$Tinc_{op}$	Incident resolution time by a human operator
$Resp_{sup}$	Supervisor's responsibility for attending to an incident
$Tinc_{sup}$	Incident resolution time by a supervisor
$Tcon_{op}$	Time of confirmation of the operator to address a situation
$Tres_{op}$	Time of response of the operator to address a situation
$Tsup_{sup}$	Time of response of the supervisor to address a situation
Δ_{T_i}	Time of sensing and sending readings (v_i) to cluster heads

$$New\ Rep_{op} = \begin{cases} Equation\ 1 : C_{al} \times Rep_{sup} \times F_{sup} \times WL_{op} & \text{if } F_{sup} = 2, 3; \\ \\ Equation\ 2 : \frac{C_{al} \times Rep_{sup} \times F_{sup}}{WL_{op}} & \text{if } F_{sup} = 1; \end{cases}$$

It is clear that Equation 1 and Equation 2 differ from each other in workload. Similarly, the RM can also increase or decrease the supervisor's reputation value according to the criticality of the alarm, the current supervisor's workload and the response time. Note that the time factor is a very relevant parameter for determining whether or not a particular supervisor carried out his/her activities in field. In fact, it could be considered as the "supervisor's supervisor". Given this, the supervisor's new value of reputation can be computed as follows:

$$New\ Rep_{sup} = \begin{cases} Equation\ 3 : C_{al} \times WL_{sup} & \text{if } T_{sup} \in [T_i, T_j]; \\ \\ Equation\ 4 : \frac{C_{al}}{WL_{sup}} & \text{if } T_{sup} \notin [T_i, T_j]; \end{cases}$$

Moreover, the AAM component is in charge of taking alarms as input and determining which human operator and supervisor are the most appropriate to take them up. This component is not intended to completely replace the response and alert management capabilities of human operators and supervisors. Rather, it complements their work by selecting the most skilled pair of human operators that may provide a rapid and effective response to an emergency situation. In addition to this, it offers all relevant information to supervisors, in such a way as to assist them in completing their tasks. In order to determine which operator and supervisor are the most suitable to take care of an incident, the AAM needs to operate some of the parameters mentioned above, such as the C_{al}, $Rep_{op/sup}$ and $WL_{op/sup}$. However, it is also important to contemplate the availability of both the operator and supervisor according to their contracts and working time. This availability is denoted as $Av_{op/sup}$.

It is important to point out that the reputation system will be more effective when there is some kind of incentive for maintaining a good reputation level. We believe that the system's organisation must operate within the concepts of reward or punishment to encourage a good operational performance. Human operators with a higher reputation could be rewarded with some benefits such as a pay rise, days-off or maybe even some kind of promotion. On the other hand, if they continuously fail in performing their tasks or they are not performing as well as the system requires, they could be given a worse position in the organisation or even be fired. Considering these two extremes, two scenarios could present themselves within the system: human operators could reach the minimum or the maximum reputation values; i.e., 0% or 100%. In the case of the former, the Reporter module should notify the relevant managers in the organisation, who own the SCADA system, of this fact in order to apprise them of the situation. In the case of the latter, the organisation should reward those staff with higher reputation so as to maintain that desirable threshold.

This way of automating the knowledge allows the system to keep a more accurate overview of its organisation and functionality of its individual parts, as well as the real state of the entire system [5]. This process does not only involve registering processes and functional activities, but also actions and decisions within the system. The Reporter module, which is in charge of reporting the latest activities executed, also performs this activity, summarising operators' attitudes and ability to attend to incidents through their reputation values. The following data sequence could be an example of relevant information to be sent to the SCADA Centre:
$Report$=$\{(ID_{op_i}, Rep_{op_i}, WL_{op_i}, \{action_1, ..., action_n\}, \{ID_{sup_i}, ..., ID_{sup_k}\}), ...\}$, where $action_i$ includes the action taken and time of response.

3 Incident Management and Scenarios

We have implemented this mechanism in Java, where we have simulated a critical scenario of small dimensions. This scenario, illustrated in Figure 5 is based on four virtual cluster heads (CH_1 with 3 sensors, CH_2 with 4, CH_3 with 3 and CH_4 with 4) where each sensor of a CH produces and sends evidence every time period, denoted as Δ_{T_i}. Given that a SCADA system has to be available 24/7, these clusters are controlled and supervised by two virtual operators with different work times ($Av_{op/sup}$), and all of them initialised with a reputation value ($Rep_{op/sup}$) of 100%.

Each cluster creates an event sequence on a time-line and each sequence is different from the others due to the restriction of randomness between clusters. For the generation of such event sequences, we assume the following criteria: each sensor node periodically produces events every $\Delta_{T_i} = One\ minute$, with values that can range from valid readings, labelled with priority 0, to alarms, labelled with priority $(1-5)$ (i.e., journal (1), low (2), medium (3), high (4),

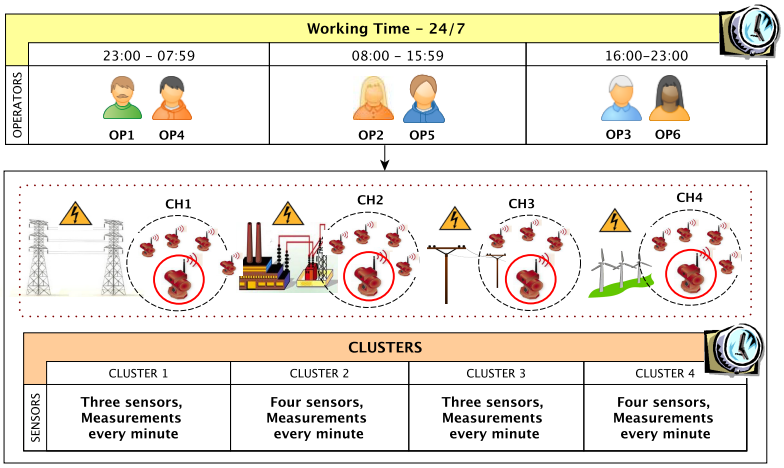

Figure 5: Constraints and Criteria for our Approach and its Implementation

and urgent (5)). This means that any alarm that exceeds the limits of normality (which are established by the organization and its security policies) should be treated correctly. In our case, we consider that the normality limit is (0-3) (non-critical alarms), and any event with label (4-5) must be sent to the most suitable and available operator with the ability to resolve the situation as soon as possible.

To control the randomness between readings and avoid abrupt changes in them, we have also taken into account both the frequency of a type of event and the time needed to generate a new type of event. Thus, if a particular event with a determined priority is produced frequently in a short time period, then the next event to create will be the one with a higher priority. This way, we can represent different states with different priorities, and this will enable us to carry out the analysis of actions taken later on.

To assign critical incidents, the AAM has to identify suitable staff. To speed up the search for prominent candidates, the AAM has to establish a processing order of $Rep_{op/sup}$, $Av_{op/sup}$, $WL_{op/sup}$. One possible processing sequence could be ($Av_{op/sup}$, $WL_{op/sup}$, $Rep_{op/sup}$), since availability ($Av_{op/sup}$) may reduce the group of human operators to be evaluated, making the process quicker, leaving aside those employees that are not actually at work. The next parameter should be the workload of the staff that are less busy ($WL_{op/sup}$), and select from them a couple of operators (the operator and supervisor) with higher reputations ($Rep_{op/sup}$). In other words, let $OP = \{op_1, op_2, ..., op_6\}$ be the set of operators, and for each $op_i \in OP$ we assume the following information; an ID_{op_i}, a working hours (e.g., eight hours per day with rotating shifts), a Rep_{op_i}, and an indicator of workload (measured in percentage). Then, the AAM computes the following lines:

$$OP_2 = FindOperatorsAccordingToTheirAvailability(OP);$$
$$OP_3 = FindOperatorsAccordingToTheirWL(OP2);$$
$$OP_4 = FindOperatorsAccordingToTheirReputation(OP3);$$

OP_2, OP_3 and OP_4 represent subsets of candidates belonging to OP, where the number of members in OP_4 should be higher than or equal to one in order to select, at least, one human operator in the field.

As for incident management, after selecting a human operator to manage an incident received from the AAM system, a supervisor is chosen for monitoring the way in which such an incident is going to be resolved by the first operator. This means that the human operator must confirm the acceptance of the assignment before a defined time passes ($Tcon_{op}$). At that moment the resolution of the incident starts and the supervisor is informed of the assignment carried out by the AAM system. When resolving a problem, a time counter $Tres_{op}$ is also activated. This counter will warn the supervisor when an incident remains unresolved for longer than it should. Moreover, this counter could also help calculate the efficiency of the human operator in the resolution of incidents. Finally, a third time counter must be used ($Tsup_{sup}$) to check that the maximum time spent by a supervisor on managing an incident, which was not resolved by a human operator, is reached or not. These three counters are shown in Figure 6 where the arrows represent the attendance scheme given above.

When a supervisor is in charge of managing an incident, the AAM system should offer her/him all the information generated in the assignation process. Thus, the supervisor can use this report to evaluate the reason why the operator did not successfully resolve the incident. Moreover, the supervisor must make a decision about how to proceed with the resolution of the incident before *Tsup* is overtaken; otherwise his/her reputation must be modified by the RM.

Considering the equations described in Section 2.4 and the nomenclature in Table 2, five main cases have been implemented for the simulation:

1. *Case 1*: $Tconf_{op} \leq Tcon_{op}$ and $Tinc_{op} \leq Tres_{op}$ (see Figure 6-1). The incident is successfully resolved by the assigned human operator before $Tres_{op}$ is reached, and the supervisor checks his/her resulting action. Then, the human operator's reputation must be increased using Equation 1.

2. *Case 2*: $Tconf_{op} \leq Tcon_{op}$ and $Tinc_{op} > Tres_{op} \Rightarrow Resp_{sup}$ and $Tinc_{sup} \leq Tsup_{sup}$ (see Figure 6-2). The incident is not successfully resolved by the operator and $Tres_{op}$ is reached. Then, the supervisor checks the human operator's actions taken to deal with the situation, such that $Tinc_{sup} \leq Tsup_{sup}$. Finally, the operator's reputation is decreased using Equation 2 and the supervisor's reputation is increased using Equation 3.

3. *Case 3*: $Tconf_{op} > Tcon_{op} \Rightarrow Resp_{sup}$ and $Tinc_{sup} \leq Tsup_{sup}$ (see Figure 6-3). The operator does not (or cannot) confirm the acceptance of the assignment given by the AAM system because the counter $Tcon_{op}$ is

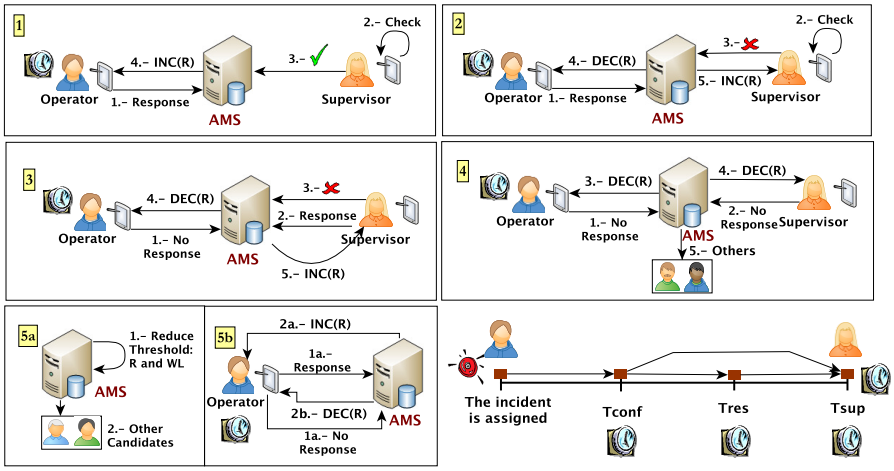

Figure 6: A Schema with Four Possible Scenarios and Maximum Times of Response

overtaken. This fact forces the supervisor to take charge of the incident. If it is resolved in time $Tinc_{sup} \leq Tsup_{sup}$, then the supervisor's reputation will be increased through Equation 3 and the human operator's reputation will be decreased using Equation 2.

4. *Case 4*: $Tconf_{op} > Tcon_{op} \Rightarrow Resp_{sup}$ and $Tinc_{sup} > Tsup_{sup}$ (see Figure 6-4). Neither the human operator nor the supervisor have acted in a proper and timely manner, since both the $Tcon_{op}$ and the $Tsup_{sup}$ have been attained. Therefore, the human operator's reputation and supervisor's reputation are decreased accordingly using, respectively, Equation 2 and Equation 4. In order to attend to the situation in advance, the AAM must find another pair of members of staff (a human operator and a supervisor) to immediately take up the incident.

5. *Case 5*: The AAM is unable to find a suitable pair of human operators. This situation may lead to two further cases.

   Case 5-a: The actual candidates do not have enough reputation ($Rep_{op/sup}$) and workload ($WL_{op/sup}$) to be selected for the assignment of an incident. To address this situation, it would be useful, for example, to reduce or adjust the established thresholds for reputation and workload, and thereby find a second list of possible candidates. Figure 6-5a illustrates this scenario where the AAM produces a new list of operators and re-executes the steps above.

   Case 5-b: A low availability of operators. Here, the AAM takes the role

of supervisor in order to monitor the operator's actions, increasing or decreasing the reputation according to the response time (see Figure 6-5b). For the increase, the AAM uses Equation 3 and for the decrease it uses Equation 4. In the case where there is a decrease of reputation, the AAM also has to reassign the incident until it is resolved due to the criticality of the situation. If after resolution the human operator presents a low reputation, the Reporter module must warn the SCADA Centre of the situation.

Note that the two assumptions taken for the fifth case will depend on the security policies and requirements of the organization. However we have taken these conditions as an initial approach in order to offer a reliable response when critical incidents arise. Likewise, it should also be noted that Case 5-b may be a feasible solution for those small application scenarios where the operational control is reduced to basically one individual in the field.

3.1 Results and Further Discussion

Taking into account the schemas illustrated in Figure 5 and Figure 6, and the classification of entities stated in Section 2.4, this section analyses the results obtained from the simulation performed throughout one complete working day (24 hours). This result is represented in both Figure 7 and Figure 8. Figure 7 illustrates the incidents attended to by the six human operators, supervisors and the AAM; whereas Figure 8 shows how operators (on the left) are able to deal with incidents together with their supervisors (on the right). In order to understand each operator's behaviour, a brief discussion for each of them is given in the following lines.

- Operator 1 - Supervisor 4 & AAM with 114 incidents assigned: Operator 1 has maintained a positive conduct at all times, while he/she is supervised by both Operator 4 and the AAM. This double supervision has been chosen because Operator 4 has been discarded as a supervisor due to his/her behaviour in the past. For this reason, the AAM again takes on his/her supervision. This role is represented in Figure 6 by a dashed line.
  - Result: Operator 1 is a *trustworthy* entity without any (a priori) criminal intention against the system.
- Operator 2 - Supervisor 5 with 41 incidents assigned: Operator 2 has not carried out the correct actions during his/her working day, and more specifically at the start. However, it is possible to see that he/she has progressively improved his/her precision in decision-making over time.
  - Result: Operator 2 is an *untrained* entity without any (a priori) criminal intention against the system.

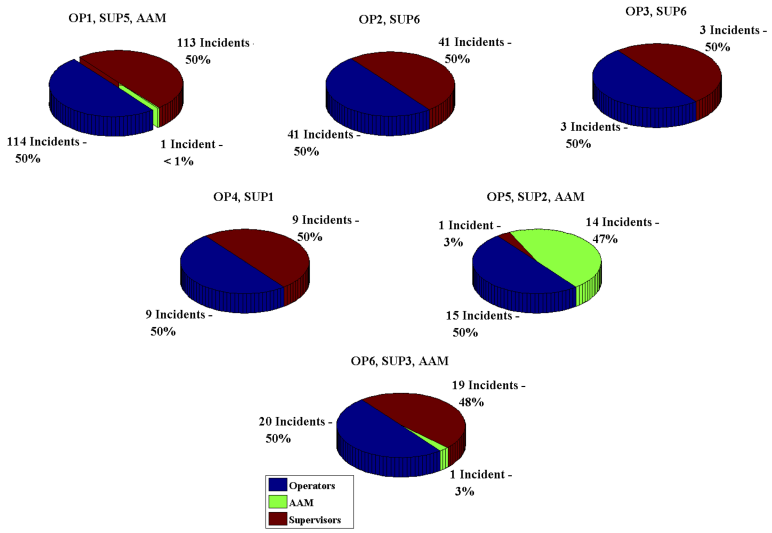

Figure 7: Percentage of Incidents

- Operator 3 - Supervisor 6 with 3 incidents assigned: Operator 3's behaviour becomes unacceptable by reaching the threshold of reputation. In this situation, the Reporter module has to alert the SCADA Centre of the situation as soon as possible.

  – Result: Operator 3 is 'possibly' a *criminal* entity against the system that needs to be controlled.

- Operator 4 - Supervisor 1 with 9 incidents assigned: as Operator 3, the Reporter module must warn the SCADA Centre of Operator 4's behaviour immediately.

  – Result: Operator 4 is 'possibly' a *criminal* entity against the system that needs to be controlled.

- Operator 5 - Supervisor 2 & AAM with 15 incidents assigned: according to Supervisor 2, Operator 5 has maintained an acceptable behaviour in terms of his/her working times. However, neither Operator 5 nor Supervisor 2 have not responded properly to the incidents at the end of the process. Therefore, the AAM has had to penalize both of them, and retake control of the situation.

  – Result: Operator 5 is a *trustworthy* entity that possibly needs training.

- Operator 6 - Supervisor 3 & AAM with 20 incidents assigned: as in the first case, the AAM has taken control of the situation, since Operator 3 has failed at a given moment of the past. In this situation, the Reporter module has to notify the SCADA Center immediately.

  - Result: Operator 6 is a *trustworthy* entity without any (a priori) criminal intention against the system.

The sharp drop of reputation at the initial phase of Operators 2, 3 and 4 is due to the fact that they have been unable to properly take up critical incidents when their workloads are relatively low. As expected, the system significantly punished this behaviour using Equation 2. The resulting reputation graph can lead a supervisor to study the background of these operators, and take disciplinary action if necessary. In contrast, the system applied a lesser sanction to those operators with high WL_{op}, since it is aware that this overload may be the cause of denying actions or failing in their decision-making. This is, for example, the case of Operator 5. Nevertheless, if this operator's inadequate behaviour continues, it will be reflected in the reputation graph.

As a result, a set of benefits could be obtained from this approach, which seems to be a prominent solution for an area still unexplored. First of all, the fact of selecting the most suitable human operator for performing a certain task on time ensures reliability and availability of the control service. Second, the storage of reputation values could reveal information about malicious intentions resulting from internal members, and even determine their actual knowledge and experience considering the level of man-made mistakes or unwillingness to resolve critical situations. This operational control also makes it clear that problems associated with the cascading effect can be avoided, mitigated or prevented before disruptions arise. The practical supervision of actions in real-time helps the system increase its capacity for situational awareness to control those improper (intentional/unintentional) actions that can trigger an adverse internal effect with a high probability of reaching other critical systems (cf. Section 1). Finally, the tracking of activities for situational awareness also improves the governance of the system, its risk management, auditing and maintenance.

4 Conclusions

As response is a priority topic to protect critical systems against malicious insiders (or even incompetent operators), we have presented, in this paper, a smart response mechanism based on Industrial Wireless Sensor Networks, on the ISA100.11a standard and on reputation. Through the combination of these three components, the mechanism is able to : (i) know natural conditions of the critical infrastructure at any time, (ii) detect and warn of all those situations classified as anomalous through behaviour patterns; and (iii) estimate and identify the pair of human operators with enough experience to properly attend to such situations.

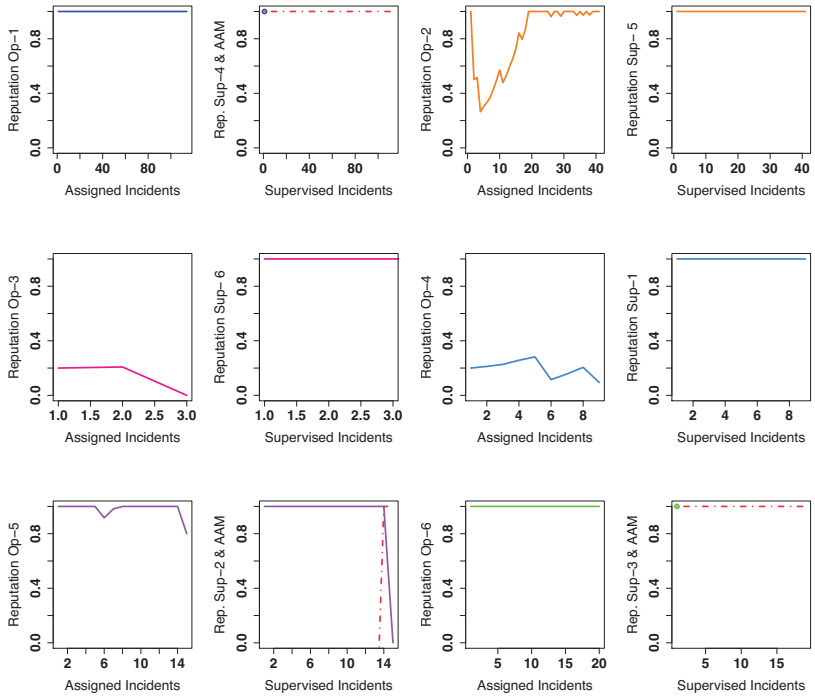

Figure 8: Operators and Supervisors' behaviour

By using this response mechanism, emergency situations that might have an impact on the digital economy (e.g., affecting the power grid of a particular area) can be properly detected and managed.

For evaluating human operators' behaviour, a set of parameters has been identified, among them to stress the criticality of the received alarm from a sensor network, which can range from non-critical to critical ISA100.11a alarms. In order to validate the mechanism, we have simulated a critical scenario so as to show its suitability for particular environments, such as (large or small) subdomains of Smart Grid systems. In fact, our main goal with this simulation has been to demonstrate and illustrate how actions taken can affect the system and how the mechanism is able to find a response. In addition, the act of keeping feedback associated with the reputation and the actions taken within the system will help managers and/or liable members know the operators' knowledge level at any given time, or even the possibility of suspicious actions. These registers will also help the system improve its entire governance. This includes training, risk management, auditing and maintenance.

As for future work, and taking advantage of the capabilities of ISA100.11a and sensor nodes to connect to the Internet through 6LowPAN, it would be desirable to extend the approach to offer operational response when a substation remains isolated or the gateway is out of service (either temporarily or not). In particular, we are currently trying to resolve some challenges identified in [29, 30] so as to find a way to ensure protection and a suitable trade-off between security and performance when sensors are being connected. This way, human operators can continue their operational activities by receiving direct information from sensors, keeping their situational awareness at all times. Moreover, we wish to extend the advantages of this approach to consider topics of prevention through lightweight forecasting models (e.g., statistical techniques for threat observation or error detection such as the control of frequency of occurrence) so as to anticipate problems before serious disruptions arise.

Acknowledgements

This work has been partially supported by the Spanish Ministry of Science and Innovation through the research project ARES (CSD2007-00004), by the Andalusian government through the research project PISCIS (P10-TIC-06334), and by the Spanish Ministry of Industry, Energy and Tourism through the research project SECRET (TSI-020100-2011-152), being this last one co-funded by FEDER. Additionally, in the particular case of the second author, the research leading to these results has received funding from the Marie Curie COFUND programme "U-Mobility" co-financed by Universidad de Malaga and the European Community Seventh Framework Programme under Grant Agreement No. 246550.

References

[1] D. Tapscott (1996), The digital economy: Promise and Peril in the Age of Networked Intelligence, vol. 1. New York: McGraw-Hill.

[2] H. Tanaka (2009), Quantitative Analysis of Information Security Interdependency between Industrial Sectors, 3rd International Symposium on Empirical Software Engineering and Measurement, USA.

[3] D. Lineweber, and S. McNulty (2001), The Cost of Power Disturbances to Industrial & Digital Economy Companies, EPRI?s Consortium for Electric Infrastructure for a Digital Society (CEIDS).

[4] NIST Special Publication 1108R2 (2012), NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, Office of the National Coordinator for Smart Grid Interoperability, February.

[5] C. Alcaraz, and J. Lopez (2012), Analysis of Requirements for Critical Control Systems, International Journal of Critical Infrastructure Protection, Elsevier, vol. 2, no. 3-4, pp. 137-145.

[6] P. Kotzanikolaou, M. Theoharidou, D. Gritzalis (2013), Accessing N-order Dependencies between Critical Infrastructures, International Journal of Critical Infrastructures, vol.9, no. 1/2, pp. 93-110.

[7] B. Reaves, and T. Morris (2012), An Open Virtual Testbed for Industrial Control System Security Research, International Journal of Information Security (IJIS), Springer Berlin/Heidelberg, 11, 4, pp. 215-229.

[8] J. Peerenboom and R. Fisher (2007), Analysing Cross-Sector Interdependencies, IEEE Computer Society, HICSS, IEEE Computer Society, pp. 112–119.

[9] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke (2012), SCADA Security in the Light of Cyber-Warfare, Computers & Security, 31, 4, pp. 418-436.

[10] Federal Energy Regulatory Commission (2009), Smart Grid Policy, 128 FERC 61,060, Docket No. PL09-4-000, 18 CFR Chapter I, July.

[11] S. Joo, J. Kim, and C. Liu (2009), Empirical Analysis of the Impact of 2003 Blackout on Security Values of U.S. Utilities and Electrical Equipment Manufacturing Firms, IEEE Transactions on Power Systems, 22, 3, pp. 1012 -1018.

[12] ISA (2009). ISA (2012), *ISA100.11.a-2009: Wireless Systems for Industrial Automation - Process Control and Related Applications*, `http://www.isa.org/`, Retrieved on February 2013.

[13] C. Alcaraz, I. Agudo, C. Fernandez-Gago, R. Roman, G. Fernandez and J. Lopez (2009), Adaptive Dispatching of Incidences based on Reputation for SCADA Systems, 6th International Conference on Trust, Privacy & Security in Digital Business, LNCS 5695, Springer, pp. 86-94.

[14] B. Miller, D. Rowe (2012), A Survey of SCADA and Critical Infrastructure Incidents, Conference on Information Technology Education, pp. 1-6.

[15] V. Gungor, B. Lu and G. Hancke (2010), Opportunities and Challenges of Wireless Sensor Networks in Smart Grid, IEEE Transactions on Industrial Electronics, 57, 10, pp. 3557-3564.

[16] HART Communication Foundation (2009), WirelessHART, `http://wirelesshart.hartcomm.org/`, Retrieved on February 2013.

[17] ZigBee Alliance (2008), ZigBee-08006r03: ZigBee-2007 Layer PICS and Stack Profiles (ZigBee-PRO), Rev. 3, `http://www.zigbee.org/`, Retrieved on February 2013.

[18] C. Alcaraz and J. Lopez (2010), A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 40, 4, pp. 419-428.

[19] IEEE 802.15.4-2006 (2006), IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks, `http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf`, Retrieved on February 2013.

[20] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler (2007), RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Network Working Group, Request for Comments: 4944, September.

[21] S. Petersen and S. Carlsen (2011), WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor, IEEE Network Industrial Electronics Magazine, 5, 4, pp. 23-34.

[22] C. Alcaraz, J. Lopez, R. Roman, and H. - H. Chen (2012), Selecting Key Management Schemes for WSN Applications, In Computers & Security, Elsevier, vol. 38, no. 8, pp. 956-966.

[23] J. Lopez, R. Roman and C. Alcaraz (2009), Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks, On Foundations of Security Analysis and Design 2009, FOSAD 2009, LNCS 5705, Springer, pp. 289-338.

[24] F. Baker and D. Meyer (2011), RFC 6272-Internet Protocols for the Smart Grid, Internet Engineering Task Force (IETF), June.

[25] The White House, Office of the Press Secretary (2009), President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid, October.

[26] S. Groat, M. Dunlop, W. Urbanksi, R. Marchany, and J. Tront (2012), Using an IPv6 Moving Target Defense to Protect the Smart Grid, 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1-7, Washington DC (USA), January.

[27] EPRI, DNP Security Development, Evaluation and Testing Project Opportunity, Electric Power Research Institute, `http://mydocs.epri.com/docs/public/000000000001016988.pdf`, Retrieved on February 2013.

[28] M. Theoharidou, P. Kotzanikolaou, D. Gritzalis (2009), Risk-Based Criticality Analysis, IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection III, Springer, 311, pp. 35-49, 2009.

[29] C. Alcaraz, R. Roman, P. Najera, and J. Lopez (2013), Security of Industrial Sensor Network-based Remote Substations in the context of the Internet of Things, In Ad Hoc Networks, Elsevier.

[30] W. Zhu, Y. Xiang, J. Zhou, R. Deng, and F. Bao (2011), Secure Localization with Attack Detection in Wireless Sensor Networks, International Journal of Information Security (IJIS), Springer Berlin, 10, pp. 155-171.